BeyondTrust

Privilege Management
Mac Admininstration Guide 5.4.51.0

Powered By Defendpoint

TC:6/12/2019

Table of Contents

Privilege Management Introduction

Privilege Management 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 in 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 whitelisting, 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 will 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 / response codes, or password protection to add additional security layers, or simply improve prompts to reduce helpdesk enquiries.

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.

Install the Privilege Management Policy Editor

Using an administrator account, log into the Windows computer where you want to manage Privilege Management for Mac.

> ***Note:*** *Ensure you have the relevant Group Policy management tools installed on the desktop or server where you will install Privilege Management Policy Editor.*

To install Privilege Management Policy Editor, run the appropriate installation package:

- For 32-bit (x86) systems, run **PrivilegeManagementPolicyEditor_x86.exe**.
- For 64-bit (x64) systems, run **PrivilegeManagementPolicyEditor_x64.exe**.

Install Privilege Management Policy Editor:

1. The installation will detect if any prerequisites are needed. Click **Install** to install any missing prerequisites. This may take a few minutes.
2. Once the prerequisites have been installed, the **Welcome** dialog box appears. Click **Next** to continue.
3. After reading the license agreement, select **I accept the terms in the license agreement** and click **Next**.
4. Enter your name and the name of your organization, and click **Next** .
5. If you want to change the default installation directory, click **Change** and select a different installation directory. Click **Next**.
6. If you are only managing Windows machines with Privilege Management and want to evaluate it for use with McAfee ePolicy Orchestrator, check the **McAfee ePolicy Orchestrator Integration** box. Otherwise, leave it unchecked and click **Next**.
7. Click **Install** to start installing Privilege Management Policy Editor.
8. Once installed, click **Finish**. Privilege Management Policy Editor has now been successfully installed.

> ***Note:*** *To use the Event Import Wizard, you must install the Microsoft SQL Server 2008 R2 Native Client. For installation instructions and to download this component, visit https://www.microsoft.com/en-gb/download/details.aspx?id=16978.*

Install the Privilege Management for Mac Client

The Privilege Management for Mac client enables Privilege Management settings to be applied to Mac computers.

To install Privilege Management for Mac, download and run the client installer package (*.pkg).

Privilege Management for Mac may be installed manually, but for larger installations we recommend you use a suitable third party software deployment system.

> ***Note:*** *There is no license to add during the client installation, as this is deployed with the Privilege Management Workstyles, so the client may be installed silently.*

Uninstall Privilege Management for Mac

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

Uninstall Privilege Management

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 and the Privilege Management ePO Adapter locally on a Mac, 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 once you have uninstalled Privilege Management, run the following command:

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

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

Upgrade the Privilege Management Mac Client

This process applies to iC3. For ePO, you can manage the upgrade through ePO Server.

To upgrade Privilege Management for Mac:

1. Uninstall Privilege Management (or unload daemon).
2. Install the new version of Privilege Management for Mac.

3. Install the new version of the iC3 Mac adapter.

Your events for iC3 are migrated as part of this process.

Privilege Management Reporting Console

The Reporting Console is an MMC snap-in and may connect to the local computer or a remote computer. The Reporting Console enables you to view Privilege Management events and privilege monitoring logs for the relevant computer.

To run the Privilege Management Reporting Console:

1. Launch **mmc.exe**.
2. Select **Add/Remove Snap-in** from the **File** menu.
3. Select **Privilege Management Reporting** from the available snap-ins and click **Add**.

   Before the snap-in is added, you are prompted to select a computer to manage. The local computer is selected by default. To connect to a remote computer select the **Another computer** option button and enter the name of the remote computer or click the **Browse** button to browse for a computer. Privilege Management supports connection to a central event collector if you are using event forwarding to centralize events to a server.

   You may also select an alternative location for the privilege monitoring logs, if you have a scripted solution in place to centralize the privilege monitoring logs to a server. Enter the network location or click the **Browse** button to browse to the location.
4. Click **Finish**.
5. Click **OK**.

Note: *You can add multiple instances of the Privilege Management Reporting snap-in and connect them to different computers.*

Auditing Report

The Auditing Report lists all the Privilege Management events that have been logged at that computer.

Available event information includes, but is not limited to:

- Date
- Event ID
- Filename (Codebase for ActiveX controls)
- Command Line
- Event Description
- Username
- Computer Name
- Policy
- Application Group
- Reason
- Custom Token
- Hash (CLSID for ActiveX controls)

- Certificate
- PID
- Parent PID
- Trusted Application Name
- Trusted Application Version

By default, the report will show all Privilege Management events from the event log, but you can filter the report on date, event number, username, and computer name. Click **Update Report** to reload the report.

The application definitions that are contained within each event may be copied and then pasted into application groups in the Privilege Management Policy Editor. Select one or more events, and then select **Copy** from the context menu. You can now paste the applications into an application group.

Privilege Monitoring Report

Application View

The application view shows a list of all applications that have been monitored. Applications are identified by their file hash.

For each application the following information is available:

- Filename/Codebase
- Type
- Instances
- Description
- Certificate
- Hash (CLSID for ActiveX controls)
- Version (ActiveX controls only)

The instances column shows the number of times the application has been run. To view the individual instances for an application, double-click the entry in the list or select **Show Details** from the context menu. The **Process View** appears.

By default, the report shows all the monitored applications, but you may filter the report on date, username, and computer name. Click **Update Report** to reload the report.

Process View

The process view shows a list of the individual processes that have been monitored for an application.

For each process the following information is available:

- Date
- PID
- Command Line
- Filename

To view the activity for a process, double-click the entry in the list or select **Show Details** from the context menu. The **Activity View** appears.

Activity View

The activity view shows a list of all the privileged activity that has been carried out by a process. Privileged activity is any activity that would fail under a standard user account.

For each activity entry the following information is available:

- Date
- Operation
- Object
- Parameters

To go back to the process view, double-click the back up entry in the list or select **Back Up** from the context menu. The **Process View** appears.

Diagnose Connection Problems

The Privilege Management Reporting Console needs to connect to the registry and administrator file shares when connecting to a remote computer.

If the Reporting Console fails to connect or fails to retrieve data, the most common causes are:

1. The **Remote Registry** service needs to be started on the remote machine. On Windows 7, this service is not set to start automatically, so you should ensure it has been started.
2. The Windows Firewall may be blocking the incoming requests. Enabling the **File and Printer Sharing** exception in the Windows Firewall settings should resolve this problem.

Launch the Privilege Management Policy Editor

The Privilege Management Policy Editor is accessed as a snap-in to the Microsoft Management Console (**MMC.exe**).

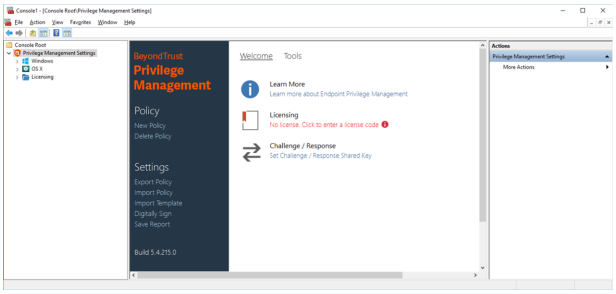
From your administrator account, run **MMC.exe**. Type **MMC** into the **Search Box** from the **Start Menu** and press the **Enter** key.

We will now add Privilege Management as a snap-in to the console.

1. Select **File** from the menu bar and select **Add/Remove Snap-in**.
2. Scroll down the list and select the **Privilege Management Settings** snap-in. Click **Add** and then click **OK**.
3. Optionally, select **File > Save as** and save a shortcut for the snap-in to the desktop as **Privilege Management**.
4. Select the **Privilege Management Settings** node in the left-hand pane and select the operating system node to display the main screen in the details pane.

Navigate the Privilege Management Policy Editor

The left-hand pane containing the **Privilege Management Settings** item is referred to as the *tree pane*. The folders beneath **Privilege Management Settings** in the tree pane are referred to as *nodes*. The middle pane, which displays content relevant to the selected node, is referred to as the *details pane*.



If you expand the **Privilege Management Settings** node, you will see three nodes:

- **Windows**: Create Privilege Management for Windows endpoints.
- **OS X**: Create Privilege Management for macOS endpoints.
- **Licensing**: Manage Privilege Management licenses.

If you expand the **Windows** node, you will see five nodes:

- **Workstyles**: Assign privileges to applications.
- **Application Groups**: Define logical groupings of applications.
- **Content Groups**: Define specific file content.
- **Messages**: Define end user messages.
- **Custom Tokens**: Define custom access tokens.

If you expand the **OS X** node you will see three nodes:

- **Workstyles**: Assign privileges to applications.
- **Application Groups**: Define logical groupings of applications.
- **Messages**: Define end user messages.

Once a Workstyle has been created and selected in the tree pane, the Workstyle tabs will be displayed in the details pane.

Automatic Save

By default, the Privilege Management Settings editor will automatically save any changes back to the appropriate GPO or local XML file if you are using the standalone console.

Automatic saving can be disabled, by deselecting the **Auto Commit Settings** menu option on the **Privilege Management Settings** node, but is not recommended unless you have performance issues. If you deselect the **Auto Commit Settings** option, then you must select the **Commit Settings** menu option to manually save any changes back to the GPO. The **Auto Commit Settings** option is persisted to your user profile, so it will be set for all future editing of Privilege Management Settings.

Policies and Templates

A Privilege Management policy is made up of one or more items from the following groups. Each of these groups can be a node in **Privilege Management Settings**:

- **Workstyles**: A Workstyle is part of a policy. It's 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 behavior.
- **Messages**: Messages are used by Workstyles to provide information to the end user when Privilege Management has applied certain behavior you have defined and needs to notify the end-user.

Users

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

Policies

Privilege Management policies are applied to one or more endpoints. The **Policy Summary** screen summaries for the number of Workstyles, application groups, target URL groups, target content groups, messages, tokens, and licenses in the policy. As this is a blank policy, all summaries will be zero.

Each item summary includes an **Edit** <Item> button, which allows you to jump to that section of the policy.

Privilege Management incorporates an autosave, autosave recovery, and concurrent edit awareness feature to reduce the risk or impact of data loss and prevent multiple users from overwriting individual polices.

A Privilege Management template is a configuration that is merged with your existing policy. A template also consists of any number of Workstyles, Application Groups, Content Groups, Messages, and Custom Tokens.

Edit Group Policy

To edit policy, we recommend you use the Group Policy Management snap-in. Once you have installed the Privilege Management Policy Editor, the Privilege Management settings are available in the Group Policy Management snap-in. The Group Policy Management snap-in can be accessed from the Microsoft Management Console or Group Policy Management editor.

Note: *If you want to create local policy to administer your endpoints, you can use the Privilege Management snap-in in the Microsoft Management Console or the Local Group Policy Editor. This will create a local policy only.*

Privilege Management Settings

You can right-click on the **Privilege Management Settings** node to access the following commands.

You can click **Tools** in the right-hand panel to access:

- "Privilege Management Activity Viewer" on page 18
- "Privilege Management Response Code Generator" on page 19

By default, **Auto Commit Settings** is selected. This means any changes made here are saved and applied using group policy. Alternatively, you can clear **Auto Commit Settings** and select **Commit Settings** when you specifically want those settings to apply.

The following options are also available:

- "Create" on page 15
- "Delete" on page 15
- "Export" on page 16
- "Import" on page 16
- "Import Template" on page 16
- "Digitally Sign" on page 16
- "Save Report" on page 16
- "Set Challenge/Response Shared Key" on page 16
- "Show Hidden Groups" on page 16
- "View" on page 17

Create

Creates a new Privilege Management policy. This will delete any existing policy for all operating systems. If you have an existing policy, you are prompted to remove all existing settings when you click **Create**. Click **Yes** to delete your existing policy and create a new one or **No** to keep your existing policy.

Delete

Deletes your existing Privilege Management policy. You are prompted to remove all existing settings when you click **Delete**. Click **Yes** to delete your existing policy or **No** to keep your existing policy.

Delete Items and Conflict Resolution

Some items within **Privilege Management Settings** are referenced in other areas, such as application groups, messages, and custom tokens. These items can be deleted at any time, and if they are not referenced elsewhere, they delete without any further action required.

When an item is deleted, Privilege Management Policy Editor will check for any conflicts which may need to be resolved. If the item you attempt to delete is already in use elsewhere in your settings, then a conflict will be reported and must be resolved.

You can review each detected conflict and observe the automatic resolution which will take place if you proceed. If more than one conflict is reported, use the **Next conflict** and **Previous conflict** links to move between conflicts.

If you want to proceed, click **Resolve All** to remove the item from the areas of your **Privilege Management Settings** where it is currently in use.

Export

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

To export a policy, click **Export** and give the file a name. Click **Save**.

Import

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

To import a policy, click **Import**, navigate to the policy XML you want to import, and click **Open**.

Import Template

Allows you to import template policies.

For more information, please see "Templates" on page 19.

Digitally Sign

You can digitally sign the Privilege Management settings. Privilege Management can either enforce or audit the loading of signed settings.

For more information, please see **Sign Privilege Management for Windows Settings** in the Privilege Management for Windows Group Policy Administration Guide.

Save Report

You can obtain a report of your Windows policy which can be saved locally, if required.

Set Challenge/Response Shared Key

This allows you to set the Challenge/Response Shared Key for the policy. This is encrypted once you have set it. This key is then required by the Challenge/Response generator to generate response codes. The only way to change the Challenge/Response Shared Key is by setting a new one.

Show Hidden Groups

You can show or hide application groups in Privilege Management.

To show groups that have been hidden by default, right-click on the **Privilege Management Settings** node and select **Show Hidden Groups**. You can hide the groups again by clearing **Show Hidden Groups**.

View

This allows you to view the **Workstyles Editor** (default) or the **HTML Report** for your Windows policy.

For more information, please see "HTML Report" on page 17.

You can review each detected conflict and observe the automatic resolution which will take place if you proceed. If more than one conflict is reported, use the **Next conflict** and **Previous conflict** links to move between conflicts.

If you want to proceed, click **Resolve All** to remove the item from the areas of your **Privilege Management Settings** where it is currently in use.

License

Privilege Management for Mac requires a valid license code to be entered in the Privilege Management Policy Editor. 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 managed endpoints, even if it doesn't have any Workstyles. This ensures all endpoints receive a valid Privilege Management license if they have Privilege Management for Mac installed. If you are unsure, then we recommend you add a valid license when you create the Privilege Management policy.

Insert a License

1. Click **No License. Click to enter a license code** to enter a license if one doesn't already exist, or **Valid License** if you want to enter an additional license code.
2. Paste your Privilege Management license code and click **Add**. The license details are shown.

HTML Report

The Privilege Management settings may be viewed as an HTML report for your Windows policy only. This report follows the same style as the Group Policy Management Console (GPMC) reports.

To show the HTML view:

1. Select the **Privilege Management Settings** node.
2. Right-click and select **View > HTML Report**.

Privilege Management uses the same style as the GPMC for its HTML reports. You can expand and collapse the various sections of the HTML report to show or hide more detailed information.

To return to the **Workstyle Editor** view:

1. Select the **Privilege Management Settings** node.
2. Right-click and select **View > Workstyles Editor**.

You may also save the HTML report to a file (the HTML view does not have to be displayed to save the HTML report).

To save an HTML Report:

1. Select the **Privilege Management Settings** node.
2. Right-click and click **Save Report**.

3. Enter a filename for the report and click **Save**.

Note: *When displaying Resultant Set of Policy (RSoP) results, the Privilege Management Settings Policy Editor will default to HTML view, but a read-only Workstyles Editor view may also be displayed.*

Privilege Management Activity Viewer

The Privilege Management Activity Viewer is an advanced diagnostics tool designed to help identify improvements in Privilege Management Workstyles. It allows IT administrators to remotely connect to any Privilege Management for Mac instance on the network and view all recent activity on the desktop.

To access the Privilege Management Activity Viewer, select **Tools** from the right-hand panel of the **Privilege Management Settings** start page.

The Activity Viewer collects a complete audit of every application that was run on the desktop, and provides a detailed summary of how Privilege Management for Mac interacted with those applications, what actions it applied, and the rules it used to determine that action.

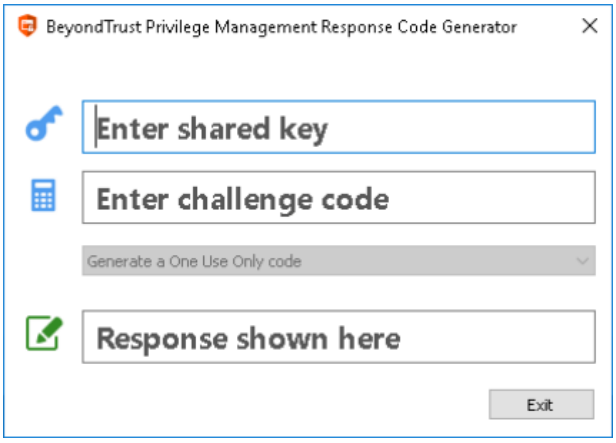
The activity is displayed in a rich, detailed, yet simple to use interface that provides every snippet of information required to better understand the Workstyles deployed to endpoints, how they affect the applications being run, and rapidly identify unexpected outcomes.

Privilege Management Response Code Generator

The Response Code Generator allows you to generate a response code using the **PGChallengeResponseUI** utility.

To generate a Response Code from **Privilege Management Settings**:

1. Click the **Tools** link from the right-hand panel of **Privilege Management Settings**.
2. Click **Launch Response Code Generator**.
3. Enter your shared key and the challenge code. The response code is shown in the third text field.



Templates

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

The following template is macOS specific:

- "macOS QuickStart" on page 19

macOS QuickStart

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 you thoroughly test this configuration to ensure it complies with the requirements of your organization.

This template policy contains the following elements:

Workstyles

- General Rules
- 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 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 authorizing for specific users.

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

macOS 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 what level of flexibility they need.

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

- Block any applications that are in the **Block Applications** group.
- Allow BeyondTrust 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 white-listed 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 have confirmed the application should be elevated.
- Allow applications 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 white-listed business applications and operating system functions to run.
- Allow users to run signed applications with admin rights once they have confirmed the application should be elevated.
- Prompt users to provide a reason before they can run unknown applications with admin rights.
- Allow applications 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 with support authorization.
- Allow known approved business applications and operating system functions to run.

macOS 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 whitelisted 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 whitelisted 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 whitelisted for all users

macOS 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.

As a minimum you need to:

- Configure the users or groups that can authorize requests that trigger messages.
- Customize the messaging with you company logo and wording
- Assign users and groups to the high, medium, and low flexibility workstyles.
- Populate the **Block Applications** application group with any applications you want to block for all users.
- Set your shared key so you can generate a Privilege Management Response code.

Privilege Management Policies for macOS

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

- **Workstyles**: A workstyle is part of a policy. It's used to assign application rules for users. You can create workstyles using the WorkStyle Wizard or import them.
- **Application Groups**: Application Groups are used by Workstyles to group applications together to apply certain Privilege Management behavior.
- **Messages**: Messages are used by Workstyles to provide information to the end user when Privilege Management has applied certain behavior you have defined and needs to notify the end-user.

For more information, please see the following sections:

- "Workstyles" on page 24
- "Application Groups" on page 31
- "Messages" on page 46

Note: *.mpkg (multiple package) format or launching multiple .pkg files at once is not supported and will be blocked by Privilege Management.*

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

Workstyles

Privilege Management workstyles are used to assign Application Groups 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 sections:

- "Application Groups" on page 31
- "Create Workstyles" on page 25

Workstyle Wizard

The workstyle wizard guides you through the process of creating a Privilege Management workstyle. The options you select determine the function of the workstyle.

1. Navigate to the **OS X** > **Workstyles** node.
2. Right-click the **Workstyles** node, and then click **Create Workstyle** on the top-right. The Workstyle Wizard is displayed.
3. You can optionally enter a license code at this stage or you can enter it later once the workstyle has been created.
4. 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 selected a blank workstyle, the next screen is **Finish** as there is nothing to configure.
5. **Filtering** (Controlling workstyle only). This determines who will receive this workstyle. You can choose from Standard users only or everyone. If you apply it to everyone, it will apply to Administrators. You can modify the filters and apply more detailed filtering once the workstyle has been created.
6. **Capabilities** (Controlling workstyle only). Allows you to choose Privilege Management, Application Control, or both. If you don't select either capabilities, the next screen is **Finish**. This workstyle would only contain filtering information.
7. **Privilege Management** (Controlling workstyle with the Privilege Management capability). Allows you to choose how you manage Authorization prompts including sudo control and Installer privileges.

***Note:** If you select **Present users with a challenge code** from the drop-down, 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.*

8. **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 whitelist or blacklist approach. We recommend you use a whitelist approach.
        - **As a whitelist**: How you want to handle non-whitelisted applications.
        - **As a blacklist**: How you want to handle blacklisted applications.
9. **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 select the check box on this screen to activate this workstyle immediately or you can leave the check box cleared to continue configuring the workstyle before you apply it to your endpoints.

For more information, please see "Challenge / Response Authorization" on page 52.

Depending on the type of workstyle you created and any capabilities that have been included, Privilege Management will auto-generate certain Application Groups (containing rules) and Messages. Filters are applied and subsequently configured as part of the workstyle.

For more information, please see the following sections:

- "Application Groups" on page 31
- "Messages" on page 46

Create Workstyles

The workstyle wizard guides you through the process of creating a Privilege Management workstyle. The options you select determine the function of the workstyle.

1. Navigate to the **OS X** > **Workstyles** node.
2. Right-click the **Workstyles** node, and then click **Create Workstyle** on the top-right. The Workstyle Wizard is displayed.
3. You can optionally enter a license code at this stage or you can enter it later once the workstyle has been created.
4. 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 selected a blank workstyle, the next screen is **Finish** as there is nothing to configure.
5. **Filtering** (Controlling workstyle only). This determines who will receive this workstyle. You can choose from Standard users only or everyone. If you apply it to everyone, it will apply to Administrators. You can modify the filters and apply more detailed filtering once the workstyle has been created.
6. **Capabilities** (Controlling workstyle only). Allows you to choose Privilege Management, Application Control, or both. If you don't select either capabilities, the next screen is **Finish**. This workstyle would only contain filtering information.
7. **Privilege Management** (Controlling workstyle with the Privilege Management capability). Allows you to choose how you manage Authorization prompts including sudo control and Installer privileges.

***Note:** If you select **Present users with a challenge code** from the drop-down, 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.*

8. **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 whitelist or blacklist approach. We recommend you use a whitelist approach.
        - **As a whitelist**: How you want to handle non-whitelisted applications.
        - **As a blacklist**: How you want to handle blacklisted applications.
9. **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 select the check box on this screen to activate this workstyle immediately or you can leave the check box cleared to continue configuring the workstyle before you apply it to your endpoints.

For more information, please see "Challenge / Response Authorization" on page 52.

Depending on the type of workstyle you created and any capabilities that have been included, Privilege Management will auto-generate certain Application Groups (containing rules) and Messages. Filters are applied and subsequently configured as part of the workstyle.

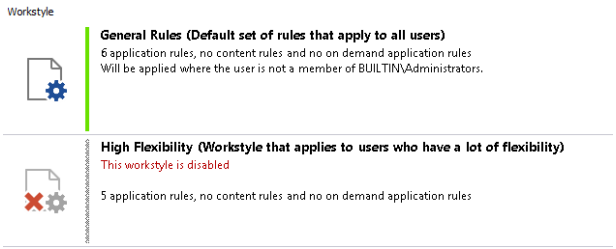
For more information, please see the following sections:
- "Application Groups" on page 31
- "Messages" on page 46

Disable or Enable Workstyles

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

To enable or disable a workstyle:

1. Navigate to the policy and select the **Workstyles** node. You can see which policies are disabled and enabled in the list.
2. Right-click on the workstyle and click **Disable Workstyle** to disable it or **Enable Workstyle** to enable it.



In the above example, the **General Rules** workstyle is enabled and the **High Flexibility** workstyle is disabled.

Workstyle Precedence

If you have multiple Workstyles, they are evaluated in the order 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 you order your Workstyles correctly because an application could match more than one Workstyle.

To change the precedence of a Workstyle:

1. Select the **Workstyles** node in the left-hand pane.
2. Right-click and choose from the options:
   - **Move Top**
   - **Move Up**
   - **Move Down**
   - **Move Bottom**

Workstyle Summary

You can view a summary of the Workstyles, Application Groups, and Messages in your policy for Mac by clicking the **OS X** node in the policy editor.

Some of these tabs may not be displayed if they have not been configured in your policy.

Overview

The **Overview** tab allows you to quickly access the following features of your policy:

- **General**: Allows you to edit the description of your workstyle and enable or disable it.
- **Totals**: Allows you to configure the following types of rule:
  - "Overview" on page 27
- **Filters**: Allows you to configure the following Filters:
  - "Account Filters" on page 28

Application Rules

Application rules are applied to Application Groups. Application rules can be used to enforce whitelisting, monitoring, and assigning privileges to groups of applications. They are a set of rules that apply to the applications listed in the application group.

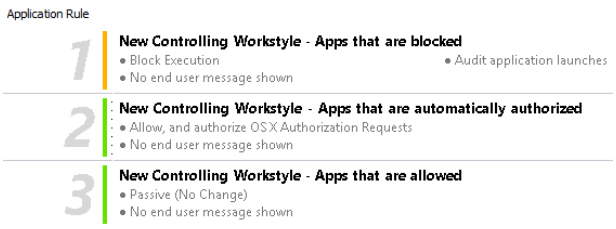
You need an **Application Group** before you can create an **Application Rule**.

For more information, please see the following sections:

- "Application Groups" on page 31
- "Create Application Groups" on page 31

Application Rules are color coded in the interface:

- **Green**: The default action is **Passive** (No Change) or **Allow**.
- **Orange**: The default action is Block.



Insert 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. For more information, please see "Application Groups" on page 31.
Default Action	Select from **Passive (No Change)**, **Allow Execution**, or **Block Execution**. This is what will happen if the application in the targeted application group is launched by the end-user.
Default 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.

Application Rule Precedence

If you add more than one application rule to a Workstyle, then entries that are higher in the list will have a higher precedence. Once an application matches an application rule, no further rules or Workstyles will be processed. If an application could match more than one Workstyle or rule, then it is important you order both your Workstyles and rules correctly. You can move application rules up and down to change the precedence.

Filters

The **Filters** tab of a Workstyle can be used to further refine when a Workstyle will be applied. By default, a Workstyle will apply to all users and computers who receive it. However, you can add one or more filters that will restrict the application of the Workstyle:

Account Filters

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

***Note:** When a new 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**, UID/GID, or both.

1. Expand the appropriate Workstyle in the left-hand pane and click **Filters**.
2. Select **Add a new local OS X account** or **Add a new domain account** if you want to use Windows AD to create your filters. If you choose this option, you need to create a mapping between your Windows SID macOS UID/GUID. 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.

For more information, please see https://blogs.technet.microsoft.com/activedirectoryua/2016/02/09/identity-management-for-unix-idmu-is-deprecated-in-windows-server/.

3. Click **OK** to finish configuring your 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

A computer filter can be used to target specific computers. You can specify a computer using either its host name, or by an IP address.

To restrict the Workstyle to specific computers by IP address:

1. Select the **Filters** tab, and click **Add a new filter**.
2. Click **Add a Computer Filter** > **Add a new IP rule**. The **Add IP rule** dialog box appears.
3. Enter the IP address manually, in the format **123.123.123.123**.
4. Click **Add**.

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

To restrict the Workstyle to specific computers by hostname:

1. Select the **Filters** tab, and click **Add a Filter**.
2. Click **Add a Computer Filter** > **Add a new hostname rule**. The **Add hostname rule** dialog box appears.
3. Enter a hostname, or alternatively browse for a computer. You can use the ***** and **?** wildcard characters in hostnames.
4. Click **Add**.

Note: *By default, a computer filter will apply if any of the computers or IP Addresses in the list match the computer or client. If you have specified multiple entries, and want to apply the Workstyle only if all entries in the computer filter match, then check the option* ***All items below should match****.*

If a computer filter is added, but no host names or IP addresses are specified, a warning will be displayed advising *No rules added*, and the computer filter will be ignored.

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. Navigate to the **OS X** > **Application Groups** node.
2. Right-click the **Application Groups** node, and then click **New Application Groups** on the top-right. The Workstyle Wizard is displayed.
3. Enter a name and a description (if required) for the new application group. Click **OK** to save your new application group.

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. Navigate to the **OS X** > **Application Groups** node.
2. Right-click the **Application Groups** and click **Properties** to view the properties. Make any changes you require and click **OK** to save the new properties.

Delete an Application Group

Application groups are usually mapped to one or more application rule in a workstyle. If you attempt to delete an application rule that is mapped to an application group, you are notified of this before you continue. If you continue to delete the application group, the associated application rule in the workstyle is also deleted.

To delete an application group:

1. Navigate to the **OS X** > **Application Groups** node.
2. Right-click on the **Application Group** you want to delete and click **Delete**.
3. 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 referencing that application group, then you are prompted to check the reference before you continue. If you click **OK**, then both the application group and the application rule referencing 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 containing the same applications as an existing application group. You can edit a duplicated application group independently of the application group it was duplicated from.

To duplicate an application group:

1. Navigate to the **OS X** > **Application Groups** node.
2. Right-click on the **Application Group** you want to duplicate and click **Copy**.

3. Select the **Application Groups** node, right-click, and select **Paste**. This will make a new copy of the application group and all the application rules it contained.

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

Rule Precedence

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

To change the precedence of a rule within a Workstyle:

1. Expand the relevant Workstyle and then select the rule type tab: **Application**, **On-Demand**, or **Content**.
2. Right click on the rule and use the following options to change the rule precedence:
    - **Move Top**
    - **Move Up**
    - **Move Down**
    - **Move Bottom**

Application Definitions

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

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 definition you configure before it will trigger a match. The rules are combined with a logical AND.

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

Application Requests Authorization

The application requires authorization, so you need to approve that request. This applies to anything in macOS that has a padlock on the dialog box or where the system requires authorization to change something. The URIs are unique to the application. The Auth Request URIs are generic and any Auth Request URIs can be requested by any application.

When an application triggers an authorization request, the application will use a unique Auth Request URI. This URI will be different to the URI of the application itself. This matching criteria allows you to target any authorization request by matching the Auth Request URI, allowing you to target that specific Auth Request URI and apply your own controls.

This matching criteria 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 criteria 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.

This matching criteria includes the following matching options:

- Auth Request URI (for example, **system.preferences.datetime**)
- 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 criteria can be used with the following application types:

- Binaries
- Bundles
- Packages
- System Preferences

Command Line Arguments

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

The Command Line Arguments matching criteria will match specifically the arguments passed to the binary or sudo command. The following example shows a command for listing 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 criteria in a Binary definition.
- **-la /Applications** are the arguments being passed to **ls**, and is targeted by using the Command Line Arguments matching criteria in a Binary definition.

Note: *Privilege Management 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 and sudo command, as well as 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 criteria 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 criteria 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 criteria can be used with the following application types:

- Binaries
- 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 62.*

File or Folder Name Matches

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

This matching criteria 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 recommended 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:

- 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 unsigned applications are not run. Instead, we recommend you run applications from the **/Applications/** folder.

Note: *Targeting bundles with an **Exact Match** path applies only to the main binary in the **Contents/MacOS** directory as specified in the bundle's plist.*

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

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

File Hash (SHA-1 Fingerprint)

This definition ensures 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 application binary or bundle. Changing the contents of an application results in an entirely different hash. Every application, and every version of the same application, has a unique hash. Privilege Management uses hashes to compare the application being executed against a hash stored in the configuration.

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

This matching criteria includes the following matching options:

- File Hash

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

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

Note: *Although File Hash is the more reliable matching criteria for matching a specific application, you must ensure 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 Version Matches

If the application you entered has a File Version property, then it is automatically extracted. You can choose to **Check Min Version**, **Check Max Version**, and edit the version number fields. Alphanumeric characters are supported in the version of applications.

For application types with defined versions, you can optionally use the File Version matching criteria 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 it's 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 criteria includes the following matching options:

- File Min Version
- File Max Version

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

- Bundles
- System Preferences

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 and child hierarchy for the application, looking for any matching parent process. 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 on macOS, the parent process will be **launchd**. However, sometimes applications like binaries and bundles are executed by other applications. For example, binaries like **curl** can be executed from **Bash**, and will be created as a child of the Terminal process. However, curl can also be used by applications.

The Parent Process matching criteria allows you to the target applications based on their parent process, so 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 you can identify multiple parents without having to create multiple definitions. This also means the parent process can be defined as any type of application (binary, bundle, system preference, or package) using any of the relevant matching criteria for each application.

This matching criteria includes the following matching options:

- Parent Process Group (dropdown menu of all application groups existing in the configuration)

This definition can be used with the following application types:

- Binaries
- Bundles

- Sudo Commands

Publisher Matches

This option can be used to check for the existence of a valid publisher. If you have browsed for an application, then the certificate subject name will automatically be retrieved, if the application has been 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, giving a guarantee the application is genuine and from a specific vendor. The certificate also ensures 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.

To check if an application has been digitally signed and what the certificate Authorities are, use the following command example to check the certificate of the **iTunes.app** application bundle:

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

If the application has a certificate, there will be 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 this example, you can see Apple uses the certificate Authority **Software Signing** to digitally sign **iTunes.app**.

With the Publisher matching criteria, you can target applications based on the publisher information contained in its certificate. This matching criteria 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 criteria 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 at the point it is downloaded, so 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. URI's follow a specific structure, typically referencing the vendor and application. For example, the URI for Apple iTunes is **com.apple.iTunes**.

The URI matching criteria 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 criteria 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:

- 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 following application types:

- Bundles

Install Action Matches

This definition can be used to allow installation of bundles to the **/Applications** directory. This matching criteria can be used in combination with other criteria to allow or deny installation of the matched bundle.

You can choose from the following options to allow installation to the **/Applications** directory:

- Yes
- No

This definition can be used with the following application type:

- Bundles

Delete Action Matches

This definition can be used to allow deletion of bundles from the **/Applications** directory. This matching criteria can be used in combination with other criteria to allow or deny deletion of the matched bundle.

You can choose from the following options to allow deletion from the **/Applications** directory:

- Yes
- No

This definition can be used with the following application type:

- Bundles

Management of Disk Mounted Images

Privilege Management examines each Disk Mounted Image (DMG) when Privilege Management for Mac is running with a valid license. If there are 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 a Privilege Management **Allow** rule, the copying of the bundle defaults to normal macOS functionality where admin credentials are required 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**.

Previously to trigger copy functionality, the bundle from the DMG had to be in an Application Group with a Privilege Management **Allow** rule. As of version 5.4, the same condition applies however, the bundle must also have **Install Action match** set to **Yes** in the Application matching criteria, within the **Application Groups** settings to right-click and **Install with Defendpoint**. Existing policies must be altered to reflect the changes in functionality.

For more information, please see "Management of System Applications" on page 41.

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 should be set to **false** to turn off the Privilege Management management of DMG files (it is set to **true** by default):

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

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

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

Format of Messages

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

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.

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 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**: Message that appears in the macOS notification center when the copying process fails.

If the message keys above have not been set, Privilege Management 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 the examples below:

Symbol	Escaped Form
“	&quot”
&	&amp”
‘	&apos”

Symbol	Escaped Form
<	&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>
```

Management of System Applications

Privilege Management examines each application and, if there is an application bundle where the application is associated with a Privilege Management **Allow** rule and **Install Action match** of **Yes**, the user can right-click the application and select **Install with Defendpoint**. This will install the bundle in the **/Applications** folder on the endpoint.

Similarly, if there is an application bundle where the application is associated with a Privilege Management **Allow** rule and **Delete Action match** of **Yes**, the user can right-click the application and select **Uninstall with Defendpoint**. This will uninstall the bundle in the **/Applications** folder on the endpoint.

For more information, please see "Install Action Matches" on page 39 and "Delete Action Matches" on page 39.

If the applications do not have a Privilege Management **Allow** rule with an **Install Action match** or **Delete Action match** of **Yes**, the management of the bundle defaults to normal macOS functionality where admin credentials are required to manage the bundle in the **/Applications** folder. Standard macOS functionality is used if anything other than an **Allow** rule with an **Install Action match** or **Delete Action match** of **Yes** is associated with the application bundle, such as **Block** or **Passive**.

Note: *You cannot use File Hash matching criteria to install or uninstall unsigned bundles.*

> ***Note:*** *Per system functionality, applications that are running or protected by System Integrity Protection (SIP) cannot be uninstalled.*

Manage the Defendpoint Finder Extension

To use **Install with Defendpoint** and **Uninstall with Defendpoint** menu functionality to manage the System Applications folder, the **Defendpoint Finder Extension** must be enabled under **System Preferences** > **Extensions** > **Finder Extensions**.

Insert a Binary

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

1. Select the application group you want to add the binary control to.
2. Right-click and select **Insert Application** > **Binary** .
3. Enter a **File** or **Folder Name**, or click **Template** to choose a template.
4. Enter a description or accept the default and click **Next** . You can leave the **Description** blank to match on all binaries.
5. You must configure the matching criteria for the binary. You can configure:
    - "File or Folder Name Matches" on page 34
    - "File Hash (SHA-1 Fingerprint)" on page 35
    - "Application Requests Authorization" on page 32
    - "Command Line Arguments" on page 33
    - "Publisher Matches" on page 37
    - "Parent Process Matches" on page 36
6. Click **Finish**. The binary is added to the application group.

Insert a Bundle

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

1. Select the application group you want to add the bundle control to.
2. Right-click and select **Insert Application** > **Bundle** .
3. Enter a **File** or **Folder Name**, or click **Template** to choose a template.
4. Enter a description or accept the default and click **Next** . You can leave the **Description** blank to match on all bundles.
5. You must configure the matching criteria for the bundle. You can configure:
    - "File or Folder Name Matches" on page 34
    - "File Hash (SHA-1 Fingerprint)" on page 35
    - "Source" on page 38
    - "File Version Matches" on page 36
    - "URI" on page 38
    - "Application Requests Authorization" on page 32

- "Publisher Matches" on page 37
- "Parent Process Matches" on page 36

6. Click **Finish**. The bundle is added to the application group.

Insert a Package

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

1. Select the application group you want to add the package to.
2. Right-click and select **Insert Application** > **Package**.
3. Enter a **File** or **Folder Name**, or click **Template** to choose a template.
4. Enter a description or accept the default and click **Next**. You can leave the **Description** blank to match on all packages.
5. You must configure the matching criteria for the package. You can configure:
   - "File or Folder Name Matches" on page 34
   - "File Hash (SHA-1 Fingerprint)" on page 35
   - "Application Requests Authorization" on page 32
   - "Publisher Matches" on page 37
6. Click **Finish**. The package is added to the application group.

Insert a Sudo Command

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

1. Select the application group you want to add the sudo command to.
2. Right-click and select **Insert Application** > **Sudo Command**.
3. Enter a **File** or **Folder Name**, or click **Template** to choose a template.
4. Enter a description or accept the default and click **Next**. You can leave the **Description** blank to match on all sudo commands.
5. You can leave the **Description** blank to match on all sudo commands.
6. You must configure the matching criteria for the sudo command. You can configure:
   - "File or Folder Name Matches" on page 34
   - "File Hash (SHA-1 Fingerprint)" on page 35
   - "Command Line Arguments" on page 33
   - "Publisher Matches" on page 37
   - "Parent Process Matches" on page 36
7. Click **Finish**. The Sudo command is added to the application group.

Sudo Switches

Privilege Management supports running sudo commands with the following switches:

- **-b**, **--background**
- **-e**, **--edit**

This switch requires configuration in Privilege Management for it to be supported. For more information, please see "Edit -e Switch" on page 44.

- **-i**, **--login**
- **-S**, **--stdin**
- **-s**, **--shell**
- **-V**, **--version**

When a sudo command is run, Privilege Management ignores any switches that have been used and will match the rest of the command against the application definition. If Privilege Management 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 are ignored.

If Privilege Management 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.

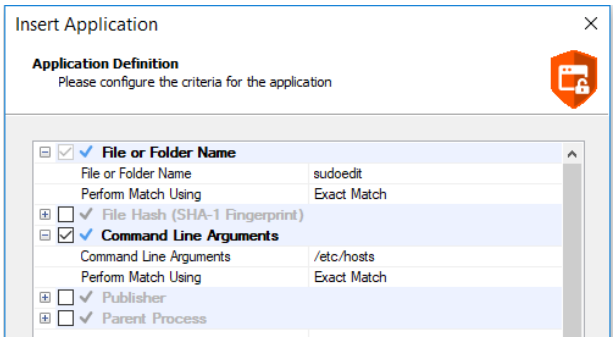
***Note:** The **-l --list** switch, which lists the commands the user is allowed to run, does not take into account the commands that are restricted by Privilege Management.*

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 must 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 files you want to control using this rule.

For example, the application definition shown in the following screenshot supports the sudo command **sudo -e /etc/hosts**.



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

Insert a System Preference Pane

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

1. Select the application group you want to add the system preference pane to.
2. Right-click and select **Insert Application** > **System Preference Pane**.
3. Enter an **Auth Request URI** or click **Template** to choose a template.
4. Enter a description or accept the default and click **Next**. You can leave the **Description** blank to match on all bundles.
5. You must configure the matching criteria for the system preference pane. You can configure:
   - "File or Folder Name Matches" on page 34
   - "File Hash (SHA-1 Fingerprint)" on page 35
   - "Source" on page 38
   - "File Version Matches" on page 36
   - "Application Requests Authorization" on page 32
   - "Publisher Matches" on page 37
6. Click **Finish**. The **System Preference Pane** is added to the application group.

Insert Applications from Templates

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

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

> For more information, please see "Use the Add Apps to Template Menu" on page 45.

Use the Add Apps to Template Menu

1. Select the application group you want to add the application to.
2. Right-click and select **Insert Application** > **Application Template**. Choose one or more applications to add to the application group. You can select multiple rows using standard Windows functionality.
3. Click **Insert** to add the applications.

Messages

You can define any number of end user messages. Messages are displayed when a user's action triggers a rule (application, on-demand, or content rule). Rules can be triggered by an application launch, block, or when content is modified.

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

Messages give the user information about the application or content, the action taken, and can be used to request information from the user. Messages also allow authorization and authentication controls to be enforced before access to an application is granted.

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

Once defined, a message may be assigned to an individual rule in the **Workstyles Rules** tab by editing the rule. Depending on the type of Workstyle you've created, Privilege Management may auto-generate certain messages for you to use.

Create Messages

To create a message:

1. Select the **Messages** node in the relevant Workstyle. The right-hand pane displays the **All Messages** page.
2. Right-click and click **New Message**.
3. Select a message template from the first dropdown. You can choose from:
    - Allow Message (Audit)
    - Allow Message (enter Reason)
    - Allow Message (with Authentication)
    - Allow Message (with Challenge)
    - Auth Request Replacement Message
    - Block Message
    - Request Message (enter Reason)
4. You can change the other options if required to customize it to your business.
5. If you select the check box **Show the details of the application being executed** the **Program Name**, **Program Publisher**, and **Program Path** names and variables are hidden from the preview and the message displayed on the endpoint.
6. Click **OK** to finish creating your message.

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

Message Name and Description

You can change the name and description of a message by right-clicking on the message and selecting **Rename** or **Properties** respectively.

Message Design

You can configure the following aspects of a message:

As you change the message options, the preview message updates to show you your changes in real-time. Program and content information is shown with placeholders.

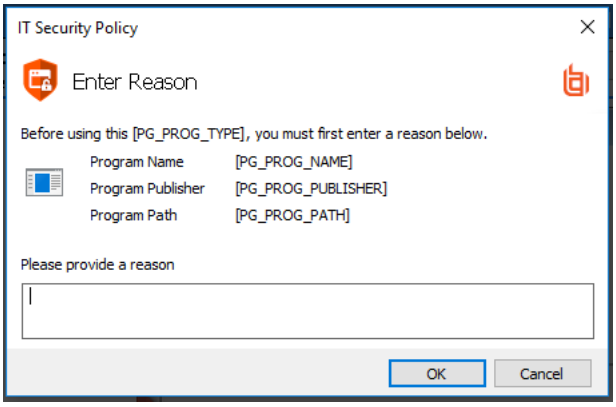
Once you have configured the message options, you can configure the **Message Text**, which includes the ability to configure different languages.

For more information, please see "Message Text" on page 50.

The options here are preselected based on the type of message you created but you can override those options if required.

Message Header Settings

The message header is 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
- Privilege Management Header
- Warning Header
- Question Header
- Error Header

Show Title Text

This check box is selected by default. You can clear 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

This section allows you to 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

This option is available if you selected **Solid** for the Background Type. Select **Custom** and choose the color you want for the background.

Color 2

This option is available if you selected **Gradient** for the Background Type. Select **Custom** and choose the second color you want for the background. Color 1 is the first colour for Gradient backgrounds.

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

You can use the **Authorization Type** dropdown to choose from **None**, **User must authorize**, or **Designated user must authorize**. An additional **Username and Password** field is added to the message for **User must authorize** or **Designated user must authorize**. You can use **User must authorize** to force the user to reenter their credentials and confirm they want to run the application.

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

The **Authentication Method** dropdown will show **Password only** if you selected **User must authorize** or **Designated user must authorize**. This cannot be changed as it's the only method of authentication supported for macOS.

If you selected **Designated user must authorize**, you must click **Edit Users** to designate which users can authorize the message.

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**.

For more information, please see "User Authorization" on page 48.

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 select the **Enabled** check box for **Challenge / Response Authorization** to add a challenge code to the message. This check box is already selected 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 must enter a shared key. You can click **Edit Key** to change the shared key for this message.

For more information, please see "Challenge / Response Authorization" on page 52.

Image Manager

The Image Manager associated with message creation allows you to **Add**, **Modify**, **Export**, and **Delete** images referenced in message headers.

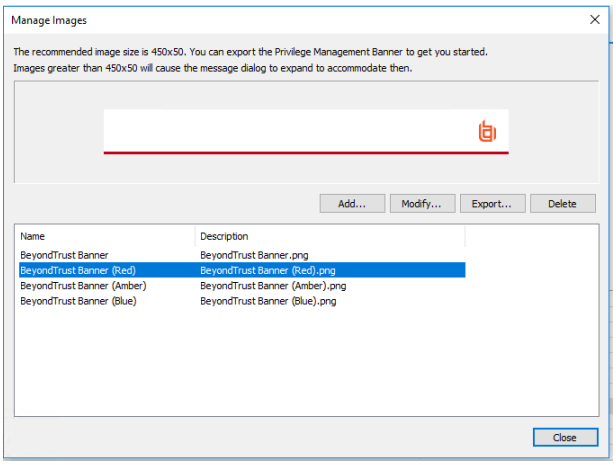
All images are stored inside the workstyles as compressed and encoded images.

We strongly recommend you delete any unused images to minimize the size of the policies, as Privilege Management 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 will be 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.*

Message Text

- "General" on page 51
- "Publisher" on page 51
- "User Reason" on page 51
- "User Authentication" on page 51
- "Challenge / Response Authorization" on page 51
- "Buttons" on page 51

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 displayed next to the Publisher if the publisher verification fails.

Privilege Management verifies the publisher by checking there is a publisher and also checking the certificate associated with that publisher is signed. Privilege Management does not check to see if the certificate has been revoked due to the length of the lookup process that would rely on network connectivity. Instead, Privilege Management 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. The **Yes** button is disabled until a reason is entered.

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.

Challenge / Response Authorization

- **Header text** controls the text that introduces the challenge / response authorization.
- **Hint text** controls the text in the response code field for challenge / response messages.
- **Information Tip Text** controls the text above the challenge and response code fields.

Buttons

- **OK Button** controls the text displayed on the button that appears on the bottom right.
- **Cancel Button** controls the text displayed on the button that appears next to the **Yes** button.

Depending on the message options, the message box will have either one or two buttons:

- 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 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 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 challenge / response needs a shared key. This key is defined when you set up the first challenge / response message in your policy, although you can change it later if required. If you create a workstyle containing a challenge / response message or you create a new challenge / response message and you are not prompted to create a shared key, then there is already a shared key for the policy. You cannot view this shared key, however you can change it here if required.

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

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

Challenge and response codes are presented as an 8 digit number, to minimize the possibility of incorrect entry. When a user is presented with a challenge code, the message may be canceled without invalidating the code. A new challenge code will be generated every time the user runs the application.

For more information on configuring challenge / response authorization enabled end user messages, please see "Message Design" on page 46.

Shared Key

The first time you create a Privilege Management 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 Settings.

To change the shared key:

1. Right-click **Privilege Management Settings** and select **Set Challenge / Response Shared Key**.
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 your shared key is at least 15 characters and includes a combination of alphanumeric, symbolic, upper, and lowercase characters. As a best practice, the shared key should be changed periodically.*

Generate a Response Code

There are 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 the MMC.

Note: *In order to generate a response code, you must have set a Challenge / Response Shared Key. You are prompted to do this when you create any policy that has a Challenge / Response message assigned to it. Alternatively, you can set the Challenge / Response Shared Key from the home page of the Privilege Management Settings node by clicking* ***Set Challenge / Response Shared Key****.*

You can generate a response code from the Privilege Management Policy Editor. This launches a tool called **PGChallengeResponseUI.exe**. This tool is part of your installation and can be used independently of the Privilege Management Policy Editor. The tool is installed to the path **<Installation Dir>\Avecto\Privilege Guard Privilege Management Policy Editors**.

To generate a response code in the Privilege Management Policy Editor:

1. Click the **Privilege Management Settings** node, and then **Tools** on the right-hand side.
2. Click **Response Code Generator**.
3. Enter the shared key you have defined and the challenge code from the end-user.
4. The response code is generated once both the **Shared Key** and the 8 character challenge code have been entered.

The response value can then be sent to the end user to enter into their challenge dialog.

Mac Deployment

Privilege Management settings can be exported from the MMC as a standalone XML configuration file, which can be distributed to macOS endpoints using your own deployment strategy.

To export the Privilege Management Settings to an XML file:

1. Select the **Privilege Management Settings** node.
2. Right-click and select **Export**.
3. Select an appropriate destination for the exported XML file, ensuring the file is named **defendpoint.xml**.

Add Privilege Management Settings to a Mac Client Computer

Privilege Management 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 this file is 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
```

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

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 Policy Structure and Precedence

Structure

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

- **ic3.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 the **dppolicyserver** are dependent on the settings under the **config.order** in the **defendpoint.plist**.

> ***Note:*** *If all policies are deleted, the* ***local.xml*** *policy is regenerated. The regenerated* ***local.xml*** *policy will not contain any license or rules.*

Precedence

The policy precedence is determined in the **defenpoint.plist** which is stored in **/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>ic3</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 if it can't find a policy of that name, it will progress to the next in the list.

If a policy is found with the correct name it will load it, irrespective of if it has a license.

Audit and Reports

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

BeyondTrust also provides 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 activity throughout the desktop and server estate. Each dashboard provides detailed and summarized information regarding **Application**, **User**, **Host**, and **Workstyle** usage.

For more information, please contact BeyondTrust.

For more information on how to configure Reporting in ePO, please see the *ePO Installation Guide*.

Events

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

The following events are logged by Privilege Management for Mac:

Event ID	Description
100	Process has started with admin rights added to token.
106	Process has started with no change to the access token (passive mode).
116	Process execution was blocked.
120	Process execution was canceled by the user
130	An application bundle that can be installed into the **/Applications** folder by a user that is not a member of the Administrator group.
131	An application bundle that can be deleted from the **/Applications** folder by a user that is not a member of the Administrator group.

Appendices

Troubleshoot

Check Privilege Management is Installed and Functioning

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

- **Privilege Management**: The graphical interface of Privilege Management on the toolbar for messages and end user interaction
- **defendpointd:** The Privilege Management daemon that manages interaction with Privilege Management
- **dppolicyserverd:** Manages policy and communicates with **defendpointd**
- **Custodian:** Manages authentication as required by Privilege Management

Note: *The Privilege Management service requires MSXML6 in order to load the Privilege Management settings, but the service will still run even if MSXML6 is not present.*

Windows 7 and Windows Server 2008 R2 already include MSXML6.

Check Settings are Deployed

Assuming Privilege Management for Mac is installed and functioning, the next step is to verify you have deployed settings to the computer or user.

Check 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 the computer or user receives at least one policy containing 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 Privilege Management is functioning and licensed, most other problems are caused by configuration problems or Workstyle precedence problems.

Once an application matches an application group entry in the **application rules**, then processing will not continue for that application. Therefore, it is vital you order your entries correctly:

- If you create multiple Workstyles, Workstyles higher in the list have a higher precedence.
- If you have multiple rules in the application rules section of a Workstyle, entries higher in the list have a higher precedence.

Application rules are applied to applications launched either directly by the user or by a running process.

If you have multiple policies applying to a user, computer, or both, then you should ensure policy precedence rules are not causing the problem. If multiple policies are applied to a computer or user, then Privilege Management for Mac will apply the policies based on alphanumeric order with the precedence list in **defendpoint.plist**.

Mac Specific

Multiple Mac Policies

For Mac estates being managed by ePO, multiple policies being applied simultaneously 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 the **epo001.xml**. Each policy is processed in an alpha-numeric/C locale order. This continues until the process hits a rule or the **dppolicyserverd** reads all of the policies without finding a match.

If multiple policies are loaded, only one of them requires a Privilege Management license. We recommend you do not 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 replaced GUIDs when loading them into memory if it was a duplicate.

Mac Application Templates

Privilege Management 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

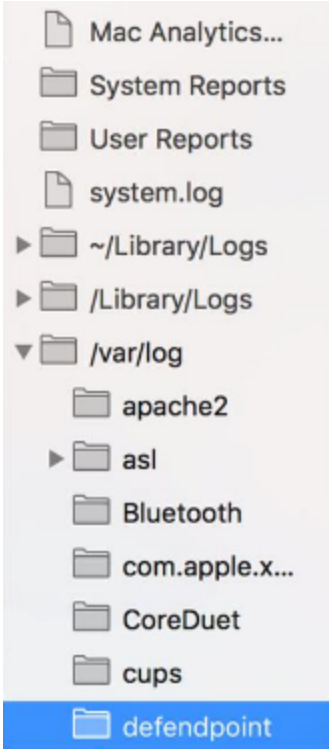
Each category then has a list of applications for that category. Picking an application will cause the application to be prepopulated with the appropriate information.

Mac Audit Logs

How to log events to a file:

1. When Privilege Management 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 recreates it dynamically. If the folder structure is deleted, Privilege Management 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 located at **/etc/newsyslog.conf**.

> ***Note:*** *This part of the set up must be done by a user who can write to this location or by using a mobile device management (MDM) solution.*

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 must populate the **logfilename**, **mode**, **count**, **size** and/or **when**, and **flags attributes** in the **newsyslog.conf** file.
    - **logfilename**: Path and filename
    - **mode**: File mode. For example, 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. For example, 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:

```
/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 the **Terminal** to see the state of the logging, when the next roll over is, and whether there are any syntax issues.

Mac Log Options

Privilege Management includes some advanced settings configured by editing a configuration file on disk. In order to edit the configuration file, you will need root privileges on the file **/Library/Application Support/Avecto/Defendpoint/defendpoint.plist**.

We recommend you edit the configuration file using a command line editor, such as vi:

```
sudo vi /Library/Application Support/Avecto/Defendpoint/defendpoint.plist
```

Unified Logging

Unified Logging is available in macOS 10.12 and later and supersedes Apple System Logger (ASL). Prior to macOS 10.12, log messages were written to specific disk locations. Unified Logging means the log messages are stored in memory or in a data store and can viewed in the Console application and the **log** command line tool.

For more information about Unified Logging, please see https://developer.apple.com/documentation/os/logging.

To view the debug logs of a process on the endpoint:

1. Open the **Console** app. By default, debug and info messages are not displayed. You can select an event in the main window to view the logs for it.
2. Click **Now** in the top left of the tool bar to see new messages in real time.
3. Select **Actions** > **Include Info Messages** and **Actions** > **Include Debug Messages** to add these to the log.
4. Using the search bar on the top-right, you can enter the name of a process that you want to filter on. For example, **defendpointd** for Privilege Management or **iC3Adapter** for iC3 Adapter log messages.

5. You can further manipulate the filter from the search bar or by right-clicking on the process and selecting an additional filter option.

Obtain Debug Logs from the Endpoint

Unified logging does not store info or debug strings on the hard disk. They are only displayed whilst the **Console** application is open. You must use the log config command to create plist files for each Privilege Management daemon and change the logging file. These plists are created in the **/Library/Preferences/Logging** directory.

To obtain debug logs from the endpoint using the **CaptureConfig** utility, please contact BeyondTrust Technical Support.

1. To create plists and change the logging level for the Privilege Management daemons, run the following commands in the terminal:

```
sudo log config --subsystem com.avecto.defendpointd --mode persist:debug
sudo log config --subsystem com.avecto.custodian --mode persist:debug
sudo log config --subsystem com.avecto.dppolicyserverd --mode persist:debug
sudo log config --subsystem com.avecto.Defendpoint --mode persist:debug
```

2. Once these commands have been run, you have two options:
   - Obtain a centralized log you can send to BeyondTrust Technical Support. This is the recommended approach.

IMPORTANT!

You would ideally collect the logs into a central log file using the following command, however this logs every process on the endpoint, not just the Privilege Management processes.

```
sudo log collect —-last <num><m/h/d>
```

***Note:** You must replace the **<num>** value with an integer and then append **m** for months, **h** for hours, or **m** for minutes depending on how long it took to replicate the issue. This will produce a .logarchive file in the current user's directory.*

   - Alternatively, you can create a log for each Privilege Management daemon by using the following commands. This process outputs .log files in the user's home directory that can be edited or moved as required. As this information is split across multiple log files, it is not the recommended approach, however it can be used when the first approach is not viable.

```
log show --predicate 'subsystem == "com.avecto.custodian"' --style json --debug --last 1h >
~/Documents/Custodian.logarchive
log show --predicate 'subsystem == "com.avecto.defendpointd"' --style json --debug --last 1h >
~/Documents/defendpointd.logarchive
log show --predicate 'subsystem == "com.avecto.dppolicyserverd"' --style json --debug --last 1h >
~/Documents/dppolicyserverd.logarchive
log show --predicate 'subsystem == "com.avecto.Defendpoint"' --style json --debug --last 1h >
~/Documents/Defendpoint.logarchive
```

Note: *We strongly recommend you delete the .plists after use and disable debug level of logging persistence, especially on an SSD.*

Anonymous Logging

By default, Privilege Management will include user and computer specific information in all audit events. You can set your application rules to not log this information for events associated with your rules by setting the **Raise an Event** option to **On (Anonymous)** on each rule.

You can also set whether user or computer information is kept anonymous for audit events that are not associated with a rule, such as events raised for having an invalid license.

To enable anonymous auditing for events not associated with a rule, edit the following section in the **defendpoint.plist** configuration file:

```
<key>AnonymousLogging</key>
<string>true</string>
```

To disable anonymous auditing for events not associated with a rule, edit the following section in the **defendpoint.plist** configuration file:

```
<key>AnonymousLogging</key>
<string>false</string>
```

Add Privilege Management Settings to a Mac Client Computer

Privilege Management 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 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
```

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

Note: *If all policies are deleted, the **local.xml** policy is regenerated. The regenerated **local.xml** policy will not contain any license or rules.*

Mac Command Arguments Not Supported

The following arguments are not supported by Privilege Management when you're using 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

Option (single dash)	Option (double dash)	Description
-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
-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

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

Third Party Licensing Information

We use the following third party software:

- Qt
- Sudo
- SwiftyJSON
- Rootfool

Sudo Copyright Notice

Sudo is distributed under the following license:

Copyright (c) 1994-1996, 1998-2019

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 - http://www.sentinelone.com

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

kernelControl.m