Privilege Management for Mac Rapid Deployment Tool 1.2

TC:11/8/2023

Table of Contents

Privilege Management for Mac Rapid Deployment Tool

The Rapid Deployment Tool is designed to assist organizations in easily on-boarding an estate of macOS endpoints without the need for their IT, or other responsible departments, to manually configure each endpoint directly.

Overview

Use the Rapid Deployment Tool to create packages that can be distributed to macOS computers. A package file contains configuration information for the following supported platforms:

- Privilege Management for Mac
- Privilege Management Console on-premises
- Privilege Management Cloud
- BeyondInsight platforms

We recommend using an MDM, such as Jamf or Intune, to deploy the PKG files to computers.

> *For more information on Intune deployments, please see our Knowledge Base article, How to Install Privilege Management for Mac and Connect to PM Cloud using Intune.*

Jamf Integration

You can connect to a Jamf instance to create a package record for the created settings package. A policy referencing that package can be pushed to endpoints.

You can also optionally automatically scope the newly created policy to an existing group in Jamf.

> *For more information, please see "Export a Package to Jamf" on page 10.*

Compatibility

- macOS version 10.15 or later
- BeyondInsight Adapter 5.6
- Privilege Management Console 2.4 SR2 or later

Create Packages

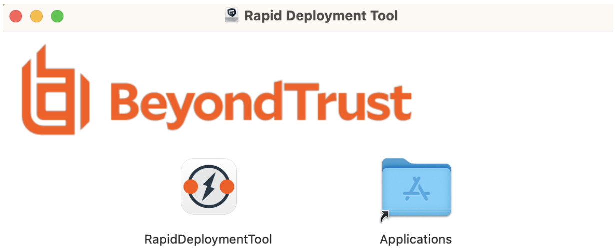
You can create the following installable packages:

- **Base Platform:** Deploys settings relevant only to Privilege Management for Mac.
- **Privilege Management Console:** Deploys configuration settings for the Privilege Management Console (on-premises or PM Cloud) management platform. You can also optionally include Base Platform settings in the same package.
- **BeyondInsight**: Deploys configuration settings for the BeyondInsight management platform. You can also optionally include Base Platform settings in the same package.

Start the Rapid Deployment Tool

The Rapid Deployment Tool is created and distributed in a DMG file.

1. Once the tool is mounted, a dialog box opens. Drag and drop the application into **/Applications/**. Alternatively, use an install rule using Privilege Management for Mac.



Create a Package with Privilege Management for Mac Base Settings

Create a package to deploy Privilege Management for Mac settings to your macOS computers.

The Base Platform includes settings that are different than Privilege Management for Mac policy settings.

> ***Tip:*** *At any time when configuring settings on a platform page, click the* ***Home*** *icon to return to the main Rapid Deployment Tool page. Be sure to save any settings changes.*

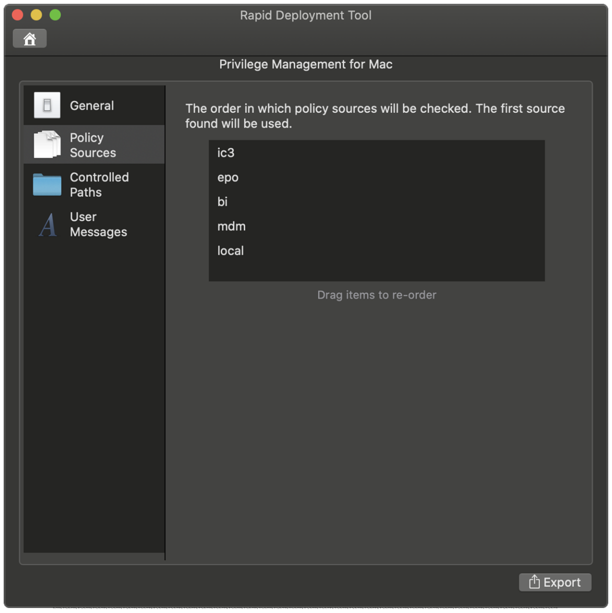
1. Start the Rapid Deployment Tool, and then select **Privilege Management Base Platform**.
2. On the **General** tab, configure the following:
   - **Prompt users to copy applications into the applications folder:** Also known as the *MountAssist* feature. Select to inspect any mounted DMG volumes the user downloads and opens for applications that are allowed by the policy. If any are found, the user is automatically prompted to choose whether they want to copy the application to the **/Applications** location.
   - **Anonymous Logging:** Prevents user/machine identity from being written to audit data. Organizations may need to select this option for legal or other security requirements compliance. This anonymous logging setting is independent of the anonymous logging options residing in the policy.
   - **Sudo Management Control:** When selected, Privilege Management for Mac ensures that sudo commands consult the endpoint policy. If no match is found in the policy, then the default sudoers behavior is applied.
   - **Show badge icons for all applications:** Privilege Management for Mac allows users to install and remove applications to the **/Applications** location by use of a context menu in Finder. When this option is selected, users will see a badge icon indicating this option is available to them.

- **Allow biometric authentication in place of password authentication:** Select to permit users to authenticate using TouchID authentication rather than a password.
- **Do not allow standard users to modify or remove Privilege Management for Mac**: Select to prevent Standard Users from tampering with the Privilege Management for Mac client, all platform adapters, policies, and settings files.
- **Enable policy rule caching**: Privilege Management for Mac caching detects and stores user actions that have been repeated recently. This improves performance during user actions which require many execution events within a short period of time (for example, compiling software).

3. On the **Policy Sources** tab, move the policy source you are using to the top of the list.

   Privilege Management for Mac can receive policy from multiple sources. The ordered list is the priority order for loading configurations. The first policy provider found is chosen as the active policy source. No other policy sources will be used.

   For example, in the image iC3 is a higher priority than ePO. If an endpoint has policies from both providers (not recommended) then only the iC3 policy applies to the endpoint.

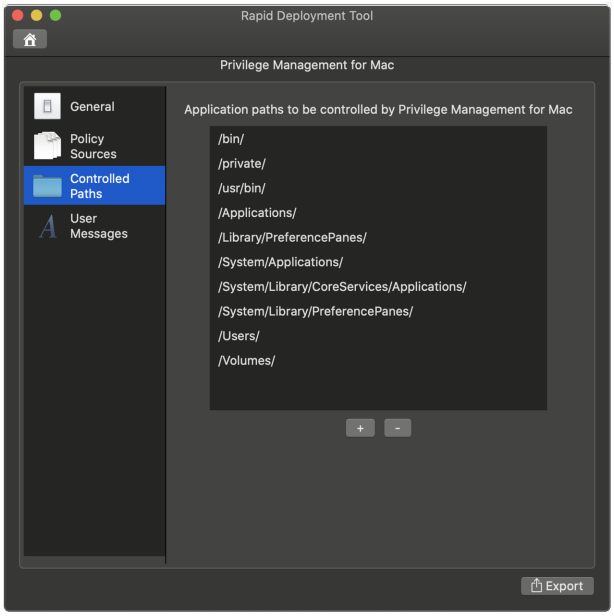


The order in which policy sources will be checked. The first source found will be used.

ic3
epo
bi
mdm
local

Drag items to re-order

4. On the **Controlled Paths** tab, add or remove application paths to be controlled by Privilege Management for Mac. The locations listed are subject to Application Control rule processing. If an application is launched from a location which is not in this list, then it will not be subject to Application Control.



Application paths to be controlled by Privilege Management for Mac

/bin/
/private/
/usr/bin/
/Applications/
/Library/PreferencePanes/
/System/Applications/
/System/Library/CoreServices/Applications/
/System/Library/PreferencePanes/
/Users/
/Volumes/

5. On the **User Messages** tab, customize the messages presented to the user by the MountAssist feature. You can use the following placeholders for the message format: **[APP_NAME]** and **[MOUNT_NAME]**.

6. After you select options, click **Export**. Select to save the settings to a file or export to Jamf.
7. Select a folder for the output file. The name of the file generated is always the same. If you select a folder that already contains a file of the same name, you cannot continue.

> *For more information, please see the following:*
>
> - *On user messages for DMGs, please see Manage Disk Mounted Images in the Privilege Management for Mac Guide at https://www.beyondtrust.com/docs/privilege-management/documents/windows-mac/pm-mac-admin.pdf*
> - *On Jamf integration, see "Export a Package to Jamf" on page 10*

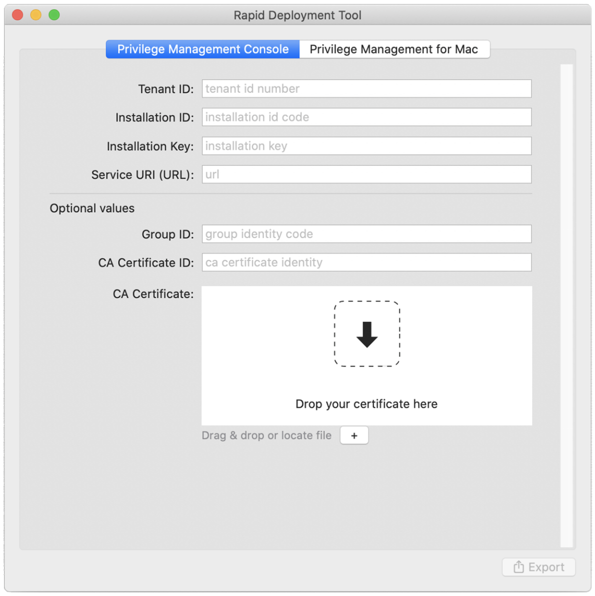
Create a Package for Privilege Management Console

Create a PMC package that provides the configuration settings for macOS computers to communicate to the PMC instance. A package can be created for PMC on-prem or PM Cloud platforms.

Optionally, configure the Privilege Management for Mac settings at the same time as the platform. Settings for both can then be included in the same package.

> ***Tip:** At any time when configuring settings on a platform page, click the **Home** icon to return to the main Rapid Deployment Tool page. Be sure to save any settings changes.*

1. Start the Rapid Deployment Tool, and then select the **Privilege Management Console** platform.



2. Configure the following settings for the PMC platform:
    - **Tenant ID:** GUID found on the PMC portal (environment to connect to).
    - **Installation ID:** GUID found on the PMC portal (environment to connect to).
    - **Installation Key:** GUID found on the PMC portal (environment to connect to) .
    - **Service URI**: The URL for your PMC instance. Usually in the format of *https://pmcqa.epm.beyondtrustcloud.com*. The URL is provided by the PMC system administrator.

- **Group ID:** Optional. GUID. If defined, the endpoint will be automatically assigned to that specific group.
- **CA Certificate ID:** Optional. The SHA-1 of a root Certificate Authority (CA) certificate or not specified when using a globally signed certificate.
- **CA Certificate:** Optional. If the webserver certificate is not signed by a globally trusted CA, the CA certificate must be distributed to the endpoints so that the system accepts the SSL negotiation. We do not recommend using self-signed certificates. At a minimum, use a privately managed CA.

3. Select the settings to export: management platform, the base platform, or both.
4. Click **Export**, and then select **Package** or **Jamf**.
5. Save the file.

For more information, please see:

- *About Jamf integration, see "Export a Package to Jamf" on page 10.*
- *For PM Cloud, see Install the Windows Adapter and Install the Mac Adapter in the Privilege Management Cloud Administration Guide at https://www.beyondtrust.com/docs/privilege-management/console/pm-cloud/index.htm.*
- *For PMC on-prem configuration for macOS, see Privilege Management Console QuickStart at https://www.beyondtrust.com/docs/privilege-management/console/pmc-windows/admin/quickstart.htm.*
- *For PMC on-prem configuration for Windows, Privilege Management Console QuickStart at https://www.beyondtrust.com/docs/privilege-management/console/pmc-windows/admin/quickstart.htm.*

Create a Package for BeyondInsight

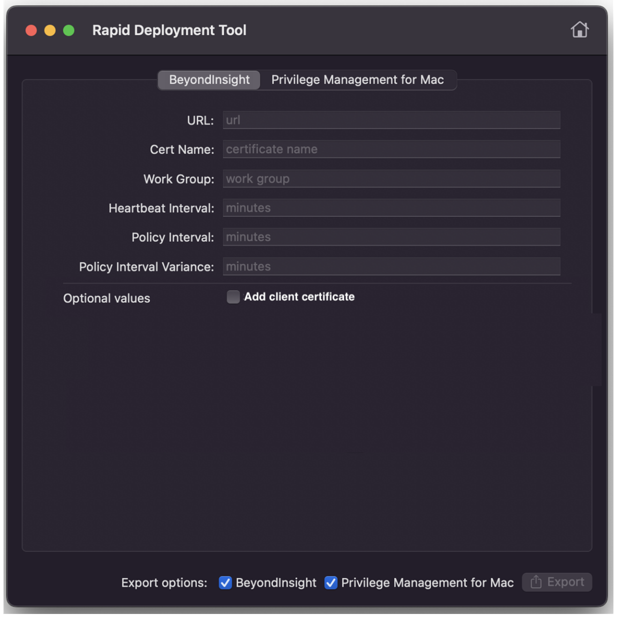
Create a BeyondInsight package that provides the configuration settings for macoS computers to communicate to the BeyondInsight instance.

Optionally, configure the Privilege Management for Mac settings at the same time as the platform. Settings for both can then be included in the same package.

***Tip:** At any time when configuring settings on a platform page, click the **Home** icon to return to the main Rapid Deployment Tool page. Be sure to save any settings changes.*

1. Start the Rapid Deployment Tool, and then select the **BeyondInsight** platform.

2. Configure the following settings for the BeyondInsight platform:
    - **URL:** The URL to the BeyondInsight server that is used for Central Policy management.
    - **Cert Name:** The name of the BeyondInsight client certificate used to communicate with BeyondInsight. The certificate file name is **eEyeEMSClient**.
    - **Workgroup:** The name of the Workgroup that is sent to BeyondInsight to assist when grouping assets.
    - **Heartbeat Interval:** The frequency interval, in minutes, to send a heartbeat to BeyondInsight. The heartbeat check ensures the endpoint can communicate to BeyondInsight.
    - **Policy Interval:** The frequency interval, in minutes, to poll for new policies.
    - **Policy Interval Variance:** The upper limit of random number of minutes to add on to the policy interval to prevent overloading the server.
    - **Add client certificate:** The name of the BeyondInsight client certificate used to communicate with BeyondInsight. The certificate file name is **eEyeEMSClient**. You can use a partial certificate name that enable connections to an endpoint. Use wildcards to set a partial certificate name, for example, *Hostname.EyeEmsClient*, can be matched with **.EyeEmsClient* or **.?yeEmsClient*.


Rapid Deployment Tool
BeyondInsight
Privilege Management for Mac
URL: url
Cert Name: certificate name
Work Group: work group
Heartbeat Interval: minutes
Policy Interval: minutes
Policy Interval Variance: minutes
Optional values
□ Add client certificate
Export options: ☑ BeyondInsight ☑ Privilege Management for Mac
Export

3. Select the settings to export: management platform, the base platform, or both.
4. Click **Export**, and then select **Package** or **Jamf**.
5. Save the file.

For more information about Jamf integration, see "Export a Package to Jamf" on page 10.

Digitally Sign a Package

Packages are not digitally signed.

If you distribute PKG files to end users to run directly, then they must be aware that packages must be signed using their Apple development program certificate. Otherwise, the OS might prevent an end user from running an unsigned package.

Create a Settings File

When creating a package, save the settings to a file so you can reuse the settings when creating a package with the same or similar configuration.

The file extension for a settings file is **.rdt**. The default file name is the same as the platform. For example, the Privilege Management for Mac platform file name is **pmfm.rdt**.

Note: *For the PMC or BeyondInsight platforms, certificates and certificate passwords are not saved in the settings file. When using a saved settings file later, you must enter certificate information again before exporting the package.*

To create a settings file:

1. On the Rapid Deployment Tool home page, select the platform.
2. After entering settings for the package, select **File > Save as**.
3. Enter a file name, and then click **Save**.

Export a Package to Jamf

Using the Rapid Deployment Tool, you can establish a connection to Jamf, create a Jamf policy, and push the package to endpoints.

The Rapid Deployment Tool is currently only compatible with Samba (SMB) file share distribution points.

Connect to a Jamf Instance

When the Rapid Deployment Tool connects to a Jamf instance, the currently configured file share distribution points are retrieved. Ensure file share distribution points are already configured in Jamf before proceeding.

1. After you enter platform settings, click **Export**, and then select **Jamf**.
2. Enter the URL and user credentials for Jamf.
3. Select **Remember my URL and username** to retain the instance connection details. The connection details are remembered when the Rapid Deployment Tool restarts.

Create a Jamf Policy

After you successfully connect to a Jamf instance, create a Jamf policy. The policy and package are exported to the instance at the same time.

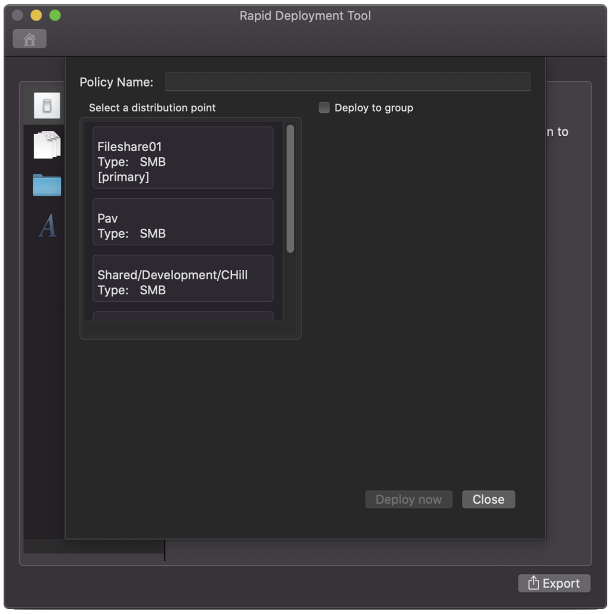
You can deploy the policy you create here to additional groups in the future using the Jamf web interface.

Policy names must adhere to the following rules:

- Must be plain text using standard characters.
- Cannot use emojis or characters more than 1 byte in size.
- Cannot duplicate policy names already in Jamf. Entering a duplicate name results in an error.

For more information, please see UTF-8 decoder capability and stress test at https://www.w3.org/2001/06/utf-8-wrong/UTF-8-test.html.

1. Enter a policy name.



Fileshare01
Type: SMB
[primary]

Pav
Type: SMB

Shared/Development/CHill
Type: SMB

2. Enter the fileshare distribution point (FDP).
3. Optionally, click **Deploy to Group** to display a list of groups in Jamf. The group must already exist in your Jamf environment. Select a group, and then select **Deploy Now** to push the policy and .pkg to the endpoints in the group.
4. If you do not want to select a group in Jamf, click **Deploy Now**.
5. You might be required to enter credentials (core macOS prompt) to connect to the FDP so the tool can copy the .pkg to the SMB share. Enter credentials for the FDP. A progress bar indicates the progress of the deployment to the FDP and the upload of the policy to Jamf.

> ***Note:*** *Jamf assumes a setup of a primary FDP and then mirrors. The policy uploaded to Jamf will reference the .pkg location as being on the primary FDP. If the set up is incorrect, then the .pkg will not deploy.*