BeyondTrust

Privilege Management for Mac Rapid Deployment Tool 1.0

TC:6/30/2020

Table of Contents

Introduction

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

Deploy PKG files

The tool creates distributable packages which deploys configurations for Privilege Management for Mac. Optionally, packages can be created for Privilege Management Console and BeyondInsight platforms.

We recommend using an MDM, such as Jamf, to deploy the PKG files to endpoints.

Certificates

The packages are not digitally signed. If you distribute PKG files to end-users to run directly, then they should be aware the packages must be signed using their Apple development program certificate. If the package is run by an end-user directly without being signed, they may be prevented from doing so by the OS.

Create Packages With the Rapid Deployment Tool

Using the Rapid Deployment Tool, you can create the following deployment packages:

- **Base Platform**: Produces an installable package which deploys settings relevant only to Privilege Management for Mac.
- **Privilege Management Console**: Produces an installable package that deploys configuration settings for the Privilege Management for Mac management platform. You can also optionally include Base Platform settings in the same package.
- **BeyondInsight**: Produces an installable package that deploys configuration settings for the BeyondInsight management platform. You can also optionally include Base Platform settings in the same package.

Compatibility

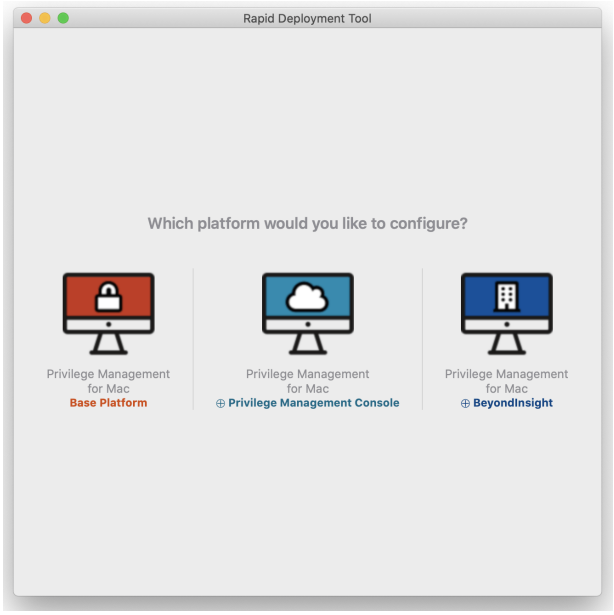
Minimum macOS version required is 10.15 Catalina

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 through Privilege Management for Mac.

2. When the Rapid Deployment Tool initially runs, select the platform to configure.



Create a Package with Privilege Management for Mac Base Settings

On selecting the Base Platform option you will be presented with a screen that contains configurable endpoint behaviors that are not normally part of the Privilege Management for Mac policy settings.

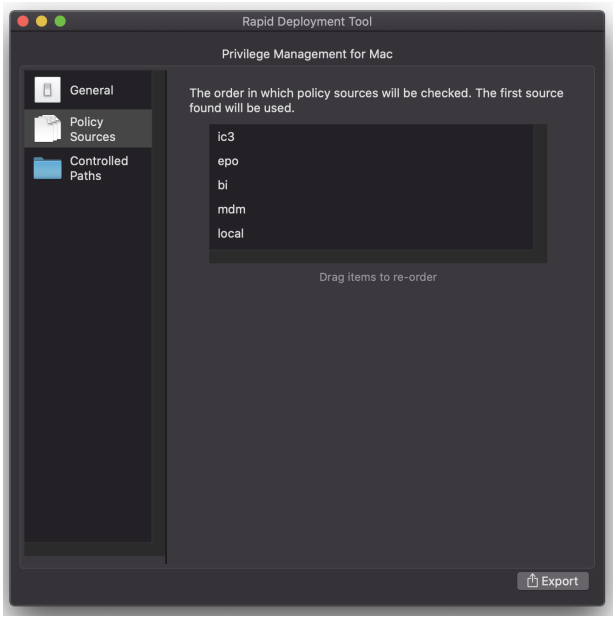
1. Start the Rapid Deployment Tool, and then select **Privilege Management Base Platform**.
2. On the **General** tab, configure the following:
   - **Prompt users to copy applications into the applications folder**: Also known as the MountAssist feature. Select to inspect any mounted DMG volumes the 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.

     Click **Set Messages** to customize the message presented to the user by the MountAssist feature. A dialog box is displayed where you can create the messages shown to the user in certain scenarios.

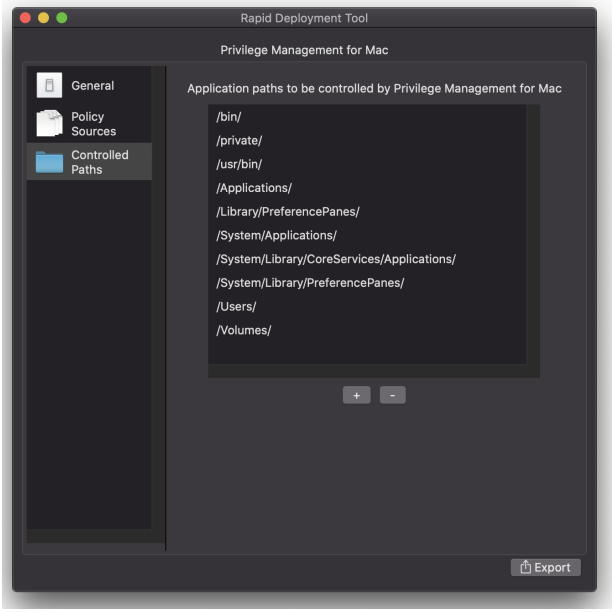
   - **Anonymous Logging**: Stops user/machine identity being written to audit data. Organizations may need to select this option for legal or other security requirements compliance. This anonymous logging setting is independent of the anonymous logging options residing in the policy.
   - **Sudo Management 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.
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.



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.



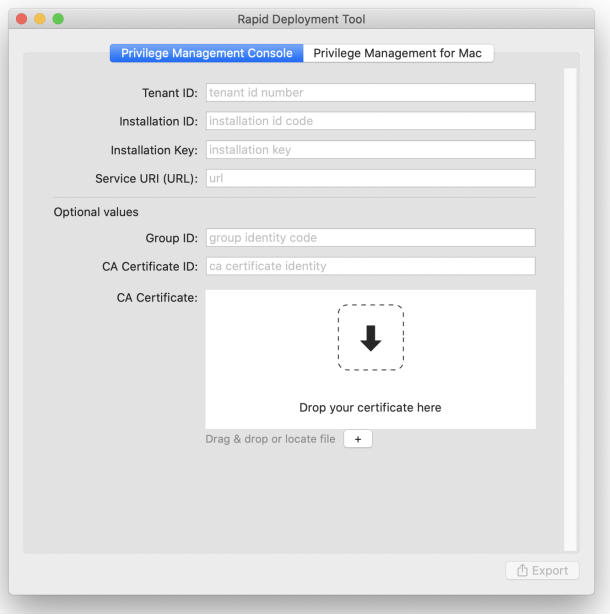
5. After you select your options, click **Export**.
6. Select a folder for the output file. The name of the file generated is always the same. If you select a folder that already contains a file of the same name you cannot continue.

Create a Package for Privilege Management Console

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

   When creating a Privilege Management Console package, there are two tabs on the Rapid Deployment Tool dialog box:

   - **Privilege Management for Mac**: Displays the macOS base settings described earlier.
   - **Privilege Management Console**: Displays configuration options for communicating with the Privilege Management Console instance.



2. Configure the following settings for the Privilege Management Console platform:
   - **Tenant ID**: GUID found on the PMC portal (environment to connect to) in **Administration > Diagnostics > Tenant ID**
   - **Installation ID**: GUID found on the PMC portal (environment to connect to) in **Administration > Agent Installation Keys > Installation ID**

- **Installation Key**: GUID found on the PMC portal (environment to connect to) in **Administration > Agent Installation Keys > Installation Key**
- **Service URI** (URL): Usually in the format : https://pmcqa.epm.beyondtrustcloud.com. The URL is provided by the PMC system administrator.
- **Group ID**: Optional. GUID, taken from **PMC portal > Groups**; 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, it is required that the CA certificate be distributed to the endpoints so that the system will accept the SSL negotiation. We do not recommend using self-signed certificates. As a minimum, use a privately managed CA.

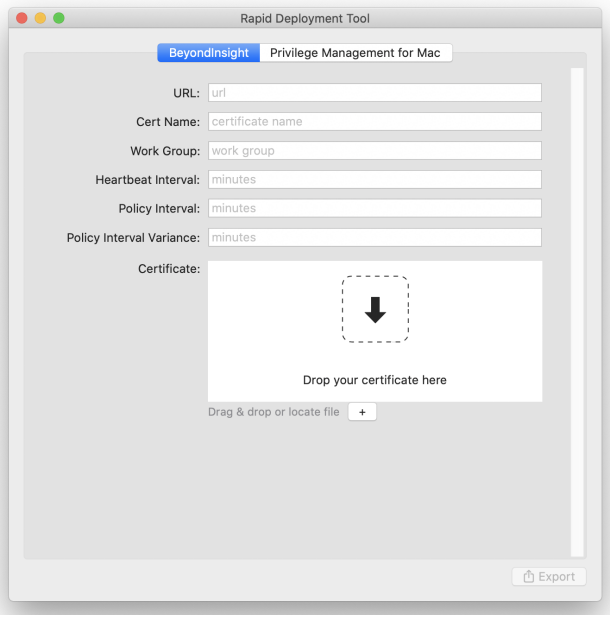
3. Select the settings to export: management platform, the base platform, or both.
4. Click **Export**.
5. Select a folder for the output file. The name of the file generated is always the same. If you select a folder that already contains a file of the same name you cannot continue.

Create a Package for BeyondInsight

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

   When creating a BeyondInsight package, there are two tabs on the Rapid Deployment Tool dialog box:

   - **Privilege Management for Mac**: Displays the macOS base settings described earlier.
   - **BeyondInsight**: Displays configuration options for communicating with the BeyondInsight instance.



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 certficate 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.
- **Certificate**: Drop the client certificate file exported from BeyondInsight. Alternatively, you can click the **+** button to locate the file using a file selection dialog box.

3. Select the settings to export: management platform, the base platform, or both.
4. Click **Export**.
5. 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.