# Parallels Device Management for Configuration Manager

Administrator's Guide

v9.1

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
Switzerland
Tel: + 41 52 672 20 30
www.parallels.com

# Contents

CHAPTER 1

# Introduction

Parallels® Device Management for Configuration Manager extends Microsoft Configuration Manager with the ability to manage Mac computers and Apple mobile devices. For companies that already use Configuration Manager to manage Windows computers in their organization, Parallels Device Management enables IT administrators to use Configuration Manager as their only system to manage PCs, Mac computers and Apple mobile devices.

## In This Chapter



# Parallels Device Management Features Overview

Parallels Device Management adds the following Mac and Apple mobile device management features to Microsoft Configuration Manager:

| Feature | Description |
|---|---|
| Active Directory and network discovery of Mac computers | Discover Mac computers on a network and automatically enroll them in Configuration Manager. |
| Enroll and manage Mac computers via Apple DEP | Support for the Apple Device Enrollment Program (DEP) and unique integration with Configuration Manager enables the IT to seamlessly set up and provision new Mac computers for their employees. |
| Enroll and manage Mac computers over the Internet | Support for Configuration Manager native Internet-Based Client Management (IBCM) enables Mac users and the IT to enroll and manage Mac computers over the Internet. |
| Enroll and manage Apple mobile devices via MDM | Enroll Apple mobile devices in Configuration Manager via Parallels MDM Proxy. |
| Inventory of Mac and Apple mobile device hardware and installed applications | Hardware and software inventory is automatically collected and can be viewed in the Configuration Manager console. |
| Software metering | Monitor and collect software usage data from Mac computers. Determine actively used software titles, software that causes problems, evaluate your software license needs, etc. |

| | |
|---|---|
| Apple VPP support | Deploy licensed AppStore applications and automatically track the number of consumed licenses. |
| Mac and Apple mobile devices configuration management via Configuration Profiles | Configure Mac computers and enforce compliance using the Configuration Manager Compliance Settings functionality. |
| macOS software deployment | Enables you to use the Configuration Manager Software Distribution functionality to install software and updates on managed Mac computers. |
| Operating system deployment | Deploy macOS images to Mac computers using the Configuration Manager Task Sequence functionality. |
| Remote lock and wipe | Remotely lock and wipe a Mac computer or an Apple mobile device it it's lost or stolen. |
| macOS patch management | Automates patch and update management of Mac computers. |
| Parallels Application Portal | Allows Mac users to view and install macOS applications made available to them by the IT administrator. |
| FileVault 2 encryption management | Enforce FileVault 2 encryption on managed Mac computers. |
| Parallels Desktop configuration management | Configure Parallels Desktop and virtual machines installed on a Mac. |

Parallels Device Management fully integrates with the Configuration Manager console, so IT administrators can manage Mac computers, Apple mobile devices, and Windows computers using the same familiar graphical user interface.

# About This Guide

This guide contains information about how to use Parallels Device Management for Configuration Manager. For the information about how to deploy Parallels Device Management for Configuration Manager, see the **Parallels Device Management for Configuration Manager Deployment Guide** at https://www.parallels.com/products/mac-management/resources/.

CHAPTER 2

# License Activation

After you install Parallels Device Management, you need to activate it before you can enroll Mac computers and Apple mobile devices in Configuration Manager. Read this chapter to learn how to activate your Parallels Device Management installation.

## In This Chapter



# License activation overview

To enroll and manage Mac computers and Apple mobile devices in Configuration Manager, you need to purchase two separate subscriptions, one for Mac computers and one for Apple mobile devices. Each subscription type must be registered and activated separately, as described later in this chapter.

Before activating a Parallels Device Management installation, please make sure that:

- you have registered for a Parallels account (https://my.parallels.com);
- you have purchased a Parallels Device Management subscription (Desktop or Mobile, or both depending on your requirements) and registered your license key(s) in Parallels My Account.

For the complete information about Parallels Device Management licensing and Parallels My Account, please refer to the **Parallels Device Management for Configuration Manager Licensing Guide**, which can be downloaded from the Parallels website at https://www.parallels.com/products/mac-management/resources/

Once your license keys are registered in Parallels My Account, you can proceed with activating your Parallels Device Management installation. First, you need to choose whether you want to use the online or offline activation method. The method you choose depends on the following:

- If the server on which you have Parallels ConfigMgr Proxy installed has limited or no Internet access, you must use the offline activation method.
- If the server has Internet access, you can use the online activation method.

The subsequent sections describe each activation method in detail.

# Online activation

**Note:** During the online activation, Parallels ConfigMgr Proxy needs to communicate with the Parallels License Server at https://pmm.parallels.com. You need to make sure that the Parallels ConfigMgr Proxy server can access this resource. If this requirement cannot be met, you will have to use the offline activation method as described in the section that follows this one.

To activate a Parallels Device Management installation using the online activation method:

1. Open the Configuration Manager console.
2. Navigate to **Administration** / **Overview** / **Parallels Device Management** / **Licenses**.
3. In the **Licenses** list (the right pane), you will see two items, one for Mac computers and one for Apple mobile devices for each primary Configuration Manager site. To distinguish between the two, look at the **License Type** column, which should say either **Desktop** (Mac computers) or **Mobile** (Apple mobile device).
4. Right-click an item that corresponds to the license type that you want to activate and choose **Activate License**.
5. In the **Activate License** dialog, input your license key and select the **Activate online** option.
6. Click **Next**.
7. Parallels Device Management connects to the Parallels License Server and verifies the license key. If the key is valid, the license information is displayed on the screen. If the license key is invalid, or if the key belongs to a different subscription type (e.g. Mobile instead of Desktop, or vice versa), you will see an error message and will need to correct it.
8. Review the license information and click **Activate**.
9. On successful activation, the display value of the **License status** column in the **Licenses** list in the Configuration Manager console changes to **Activated**.

Your Parallels Device Management installation is now activated and the activation information is added to Parallels My Account.

# Offline activation

If the server on which you have Parallels Configuration Manager Proxy installed has limited or no Internet access, you must use the offline activation method described below.

**Important:** Before using offline activation, you must contact your Parallels sales representative or a sales engineer and request to enable this functionality in Parallels My Account. By default, this functionality is disabled.

To activate Parallels Device Management:

1. Open the Configuration Manager console.
2. Navigate to **Administration** / **Overview** / **Parallels Device Management** / **Licenses**.
3. In the **Licenses** list (the right pane), you will see two items, one for Mac computers and one for Apple mobile devices for each primary Configuration Manager site. To distinguish between the two, look at the **License Type** column, which should say either **Desktop** (Mac computers) or **Mobile** (Apple mobile device).
4. Right-click an item that corresponds to the license type that you want to activate and choose **Activate License**.
5. The **Activate License** dialog opens.
6. Input your license key and select the **Activate offline** option.
7. Click **Next**.
8. Click the **Download** button to save to offline activation request file. Specify a location and file name and click **Save**. Do not close the **Activate License** dialog.

You now need to obtain the license activation file from Parallels My Account. To do so:

1. Visit https://my.parallels.com and sign in using your email address and password.
2. On the **Dashboard** page, click on the "Active subscriptions" row inside the **Parallels Device Management** card.
3. On the **Parallels Device Management** page that opens, click the **More** drop-down menu (in the upper right) and choose **Offline Activation and Validation**.
4. On the **Uploading Offline Validation File** page, submit the offline activation request file you saved earlier (drag and drop the file or click **Select File** and browse for it).
5. Follow the instructions and download the license activation file to your computer.
6. Go back to the Configuration Manager console where you should have the **Activate License** dialog still open. In the dialog, click **Browse** and select the license activation file you've downloaded from Parallels My Account.
7. Click **Next**. Your license information will be displayed on the screen. Review the information and click **Activate**.
8. On successful activation, the display value of the **License status** column in the **Licenses** list in the Configuration Manager console changes to **Activated**.

Your Parallels Device Management installation is now activated and the activation information is added to Parallels My Account.

# View and update license information

After you activate a Parallels Device Management installation, you can view the license information in the Configuration Manager console.

To view the license information:

1. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **Licenses**.
2. Right-click a license (Desktop or Mobile, depending on your needs) in the **Licenses** list and choose **Properties**.
3. The **License Information** dialog opens where you can view the following information:
   - **License key**: The license key that was used to activate this installation.
   - **License type**: Desktop (Mac computers) or Mobile (Apple mobile devices).
   - **Issue date**: The license key issue date.
   - **End date**: The license key end date.
   - **Max number of managed devices**: The maximum number of Mac computers or Apple mobile devices (depending on the license type) that can be managed in this Parallels Device Management installation.
   - **Devices under management:** The current number of managed Mac computers or Apple mobile devices.
   - **Remaining**: The number of individual licenses (devices that can be managed) remaining.

The license usage information is reported back to the Parallels License Server automatically once a week. The information can then be viewed in Parallels My Account. This allows you to see the license usage info for all your Parallels Device Management installations (if you have more than one) in one place.

**Note:** If you activated Parallels Device Management using the offline activation method, you need to synchronize the local license information with Parallels My Account using the offline refresh method as described below.

### Refresh the license information

The **Refresh** button on the **License Information** dialog allows you to retrieve the current license information from the Parallels License Server to reflect possible changes to your subscription. Normally, this update is done automatically every 24 hours if the server on which the Parallels ConfigMgr Proxy is running has Internet access. By clicking the **Refresh** button, you can retrieve this information at any time. This functionality is useful, for example, when you upgrade your subscription to have more licenses and want the licenses to become available in your Parallels Device Management installation without waiting for the automatic refresh to happen.

If the server on which Parallels ConfigMgr Proxy is running has Internet access, simply click the **Refresh** button to update the license information. If the server has limited or no Internet access, read the following subsection.

### Using the offline refresh method

If the server hosting Parallels ConfigMgr Proxy has limited or no Internet access, you must use the offline refresh method by following these steps:

1. Click **Refresh**.
2. If this Parallels Device Management installation was activated using the offline method, you will first be asked to save the offline request file.
3. After you save the file, you'll be asked to specify the file containing the latest subscription information. You must obtain this file from Parallels My Account. Do not close this dialog (you will return to it later) and proceed to then next step.
4. Visit https://my.parallels.com and sign in using your email address and password.
5. On the **Dashboard** page, click on the "Active subscriptions" row inside the **Parallels Device Management** card.
6. On the **Parallels Device Management** page, click the **More** drop-down menu (in the upper right) and choose **Offline Activation and Validation**.
7. Submit the offline request file you saved earlier (drag and drop the file or click **Select File**).
8. Follow the instructions and download the subscription information file to your computer.
9. Go back to the Configuration Manager console and submit this file. Your local subscription information will be updated with the latest information from the file you've obtained from Parallels My Account.

# Exceeding the license limit

Each Parallels Configuration Manager Proxy installed in a Configuration Manager hierarchy constantly monitors the total number of managed Mac computers and Apple mobile devices. If at any time the number of devices exceeds the license limit, the following happens:

1. The information about the event is recorded to the Parallels ConfigMgr Proxy log file.
2. If an attempt is made to enroll a new device, an error message may (or may not) be shown on the device during the enrollment procedure.
3. All managed devices will continue to be enrolled in Configuration Manager and will retrieve their baselines normally.
4. The Problem Monitor icon will indicate an error (will change its color to yellow) and will display a corresponding error message. The notification message (a balloon) will pop up in the Problem Monitor once an hour.

5 Similar notification messages will be shown in the Configuration Manager console when you try to perform some of the administrative task, including:

- Creating/editing Configuration Profiles.
- Creating/editing Parallels Desktop and Virtual Machine configuration items.
- Creating/editing FileVault2 configuration items.
- Pushing policies.

### What you can do when the license limit is exceeded

If the license limit is exceeded, you can do the following:

- To stop receiving alerts in the Configuration Manager console or the Problem Monitor, remove the excess Mac computers or Apple mobile devices from Configuration Manager.
- If the Parallels Device Management installation was activated using a sublicense, you can add more licenses to it in Parallels My Account. To do this, you must have unused licenses in the subscription.
- If you used the master license key to activate Parallels Device Management (not a sublicense), then it means that you don't have any licenses left and need to upgrade your subscription (i.e. buy more licenses).

# Deactivating Parallels Device Management

If you need to use an active license key to activate a different Parallels Device Management installation, you must first deactivate the current installation and release the key. Depending on whether you activated Parallels Device Management using the online or offline activation method, the deactivation should be performed using the same method.

To deactivate a Parallels Device Management installation:

1 In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **Licenses**.

2 Right-click a license in the **Licenses** list (Desktop or Mobile, depending on which license you are releasing) and choose **Properties**.

3 The **License Information** dialog opens.

4 Click **Deactivate**. Depending on the original activation method, one of the following will happen:

- Online activation: Parallels Device Management connects to Parallels cloud and deactivates your Parallels Device Management installation. You license key is released and you can use it to activate a different installation. If this is your case, you may stop reading here and skip the rest of this section.

- Offline activation: Parallels Device Management is deactivated but the license key is not fully released. In order to complete the deactivation, you need to update the license key information in Parallels My Account. Follow the steps below to learn how to do it.

5 When using the offline deactivation method, you'll be asked to save the offline deactivation request file. Specify a location and file name and click **Save**.

6 You now need to submit the file to Parallels My Account. To do so, visit https://my.parallels.com and sign in using your email address and password.

7 On the **Dashboard** page, click on the "Active subscriptions" row inside the **Parallels Device Management** card.

8 On the **Parallels Device Management** page that opens, click the **More** drop-down menu (in the upper right) and choose **Offline Activation and Validation**.

9 Submit the offline deactivation request file you saved earlier (drag and drop the file or click **Select File**).

Parallels Device Management is now fully deactivated and the license key can be used to activate a different installation.

CHAPTER 3

# Enrolling Mac Computers in Configuration Manager

Before you can manage Mac computers in Configuration Manager, the computers must first be enrolled. There are several enrollment methods. Which method you choose depends on requirements specific to your organization. This chapter described each enrollment method in detail.

## In This Chapter



# User-initiated MDM enrollment

User-initiate MDM enrollment consists of the following basic steps:

1. The IT administrator provides instructions to users on how to initiate the enrollment; the instructions include a special enrollment URL.
2. A user opens the URL, enters credentials to establish eligibility, and initiates the enrollment.
3. A user then downloads and installs an MDM configuration profile by following the onscreen instructions and enrolls the Mac computer in MDM.

The rest of this section describes individual steps in detail.

### Obtaining the enrollment URL

To obtain the enrollment URL:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Mac Management** / **Mobile Device Management** / **MDM Proxy**.
2. Select an MDM Proxy for the desired Configuration Manager site.
3. Right-click the MDM Proxy and choose **Properties**.
4. In the dialog that opens, find the **Enrollment URL** property and copy its value.
5. Send the copied enrollment URL to Mac users using email or another form of communication.

### User-initiated enrollment

To initiate MDM enrollment, a Mac user should do the following:

1. Open the enrollment URL that they received from the administrator.
2. Enter their AD domain credentials when prompted. If the user is eligible for MDM enrollment, a screen opens explaining to the user which computer management tasks the IT administrator will be able to perform on an enrolled Mac. To initiate the enrollment, the user clicks **Enroll**.
3. The next screen informs the user that they need to download and install their organization's MDM profile. To download the profile, the user clicks **Continue**.
4. After the profile is downloaded, a screen opens with instructions on how to install the downloaded MDM profile. To install the profile, the users opens System Preferences in macOS and clicks the **Profiles** icon.
5. The user then clicks **Install** on the download MDM profile and clicks **Install** again to confirm the installation.
6. A dialog opens asking the user to enter administrative credentials on this Mac in order to install the MDM profile. The user enters credentials and clicks **Enroll**.
7. When the MDM enrollment is completed, the user will see a notice that the Mac computer is enrolled into management.

### Parallels Mac Client installation

Parallels Mac Client is automatically push-installed on a Mac right after the MDM enrollment is finished. If a Parallels Mac Client is already installed on this computer, the automatic installation will not be performed.

### User-initiated MDM Enrollment for DEP Macs

Please note that user-initiated MDM enrollment cannot be used and will fail on DEP-enabled Macs.

### MDM profile usage and expiration

- After an MDM profile is downloaded to a Mac computer, it will expire in one hour if not installed. An expired profile cannot be used for enrollment on this or any other computer.
- Once installed on particular Mac, an MDM profile cannot be used on any other computer.

# DEP enrollment

The Apple Device Enrollment Program (DEP) provides a fast, streamlined way to deploy your corporate-owned Mac computers purchased directly from Apple or through Apple Authorized Resellers. Parallels Device Management for Configuration Manager supports Apple DEP and provides you with the ability to automatically enroll new Mac computers in Configuration Manager during the initial DEP setup procedure.

To use the DEP functionality, you must be enrolled in Apple Deployment Programs. For more information, please see the Apple Business Manager Getting Started Guide: https://www.apple.com/business/docs/site/Apple_Business_Manager_Getting_Started_Guide.pdf.

## Enable DEP

To enable the DEP functionality in Configuration Manager, you need to install Parallels IBCM/MDM Proxy and enable the Parallels MDM functionality. If you haven't done so already, please install and configure Parallels IBCM/MDM Proxy as described in the **Parallels Device Management for Configuration Manager Deployment Guide**, the **Deploying IBCM/MDM Proxy** chapter.

## Create an enrollment profile for Mac computers

A device enrollment profile is a collection of settings that will be applied to a Mac computer when it is deployed using the Apple Device Enrollment Program. Every Mac must have an enrollment profile assigned to it before it can be deployed. Parallels Device Management includes the functionality to create device enrollment profiles right in the Configuration Manager console.

To create a device enrollment profile:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program** / **Enrollment Profiles**.
2. Right-click anywhere in the right pane and choose **New Enrollment Profile for Mac Computers**. The **New Enrollment Profile for Mac Computers** wizard opens.

Complete the wizard as described below.

### General Information

On the **General** wizard page, set the following options:

1. Specify the profile name, so it can be easily identified in the Configuration Manager console and on the Apple DEP website.
2. Specify the support phone number, email address, and department name if needed (these properties are optional).

3 **Supervise devices**. If this option is selected, the device supervision during the enrollment process will be allowed.

4 **Allow profile removal**. If this option is selected, a user will be able to remove the profile from a Mac computer. Note that this option can be cleared only if the **Supervise devices** option (above) is selected. This option is selected by default.

5 **This profile is mandatory**. If this option is selected, a user will be required to apply the profile on a Mac.

6 When done, click **Next** to continue.

### User Experience

On the **User Experience** page, select the steps to exclude from the Setup Assistant, which will run during the enrollment process. These are the standard DEP enrollment steps. When done, click **Next** to continue.

### Local Accounts

The **Local Accounts** page allows you to configure a local account type that will be created during enrollment. You have an option to create an administrator or standard local account, or you can skip account creation completely.

To create a local user account during enrollment, select one of the following options:

- **Administrator Account**: create an account in Setup Assistant with administrative privileges.
- **Standard Account**: create an account in Setup Assistant with permissions of a standard user. Requires the Local Administrator Account to be created (see below).

To skip the **Account** page in Setup Assistant, select **Skip Account Creation**. This option requires the Local Administrator Account to be created (see below).

The **Create Local Administrator Account** option will be enabled or disabled depending on the following:

- If you select **Administrator Account**, you can select or clear the **Create Local Administrator Account** option depending on your needs. When it is selected, you can specify the username and password in the fields provided. Allowed characters in the **Username** field are: /^[a-z][-_a-z0-9]*$/. The password must contain a minimum of 4 characters.
- If you select **Standard Account** or **Skip Account Creation**, the **Create Local Administrator Account** option is automatically selected and disabled.

Select the **Hide account from users** option to hide the account from the UI (Login Window, Users&Groups pane in the System Preferences, etc.). To show the account, clear the option.

If any of the values on this page are entered incorrectly, the **Next** button will be disabled and an exclamation mark icon will be shown next to a field that needs correction.

### MDM Profile

This page allows you to specify a macOS configuration profile and save it in the device enrollment profile as an MDM profile. After a Mac computer is deployed via DEP and enrolled in Configuration Manager, this profile is pushed to it and is used to configure macOS.

To specify a macOS configuration profile:

1. Click the **Upload Profile** button and select a profile (a file with the ".mobileconfig" extension).
2. When the profile is uploaded, the contents of the profile will be displayed in the read-only text field as raw XML. Note that if a profile contains the MDM payload, it will be replaced with the automatically generated MDM payload.
3. Click **Next.** The profile will be saved and pushed to the Apple DEP website. A progress bar is displayed while the profile is uploaded.
4. Click **Finish**.

If needed, you can create multiple enrollment profiles and then assign different profiles to different devices.

### Configuration Profile

The **Configuration Profile** page lets you include one or more configuration items in an enrollment profile containing configuration profiles. This is to enable the administrator to apply a policy to a device before it actually fully enrolled in Configuration Manager. This function, therefore, allows you to bypass the standard policy retrieval mechanism in Configuration Manager, which can take some time when dealing with newly enrolled devices.

To specify configuration profiles:

1. Click the "Add configuration item" icon (the yellow star).
2. A dialog opens displaying configuration items containing only device configuration profiles. User profiles cannot be used with this functionality and will not be included in this list.
3. Select a configuration item and click **OK**. The configuration item is added after the currently selected item or to the end of the configuration profiles list.

To remove a configuration item from the enrollment profile, select it and click the "Remove configuration item" icon (the "X").

Note that if a configuration item was removed from Configuration Manager, but is still assigned to an enrollment profile, it will be marked in red on the **Configuration Profiles** page. Such a configuration item must be removed from the enrollment profile or you will not be able to make any changes to the profile.

Here's how configuration profiles are deployed during DEP enrollment:

1. At the time of DEP enrollment, the latest version of the configuration item is used to deploy a configuration profile.
2. The profile is installed before the user is even able to log in to the device.
3. If the latest version somehow contains a user configuration profile (which cannot be used), then this profile will not be deployed. This will not affect the installation of other profiles.
4. If a profile could not be installed for any reason, this step will be skipped and the device configuration will proceed normally.

### Task Sequence

This page allows you to specify an existing task sequence to run immediately after the automated enrollment is completed. The purpose of this function is as follows. Normally, you deploy a task sequence to a device collection in Configuration Manager in order for it to run on destination Mac computers. On newly enrolled Mac computers, however, a task sequence will run after a long delay because it takes time for Configuration Manager to assign new devices to a device collection. To avoid this delay, you can specify a task sequence on this page and it will run on a Mac right after the Mac is enrolled, without waiting for Configuration Manager to complete the device collection assignment.

To specify a task sequence, click the **Browse** button and select a task sequence from the list. Note that only task sequences without OSD-related steps will be shown (no Apply OS, Capture OS or Partition Disk steps). The following is a complete list of supported steps:

- Install Package
- Install Application (VPP)
- Apply Configuration Profile (always installed via MDM as device profile)
- Execute Script
- Join Domain
- Set Hostname
- Kernel Extensions
- Set Variables

Note that steps Install Application (VPP), Apply Configuration Profile, and Kernel Extensions require IBCM to be configured.

The specified task sequence will run immediately after the automated enrollment completes. The Mac user will see the **Executing Task Sequence** screen. Note that the user can close this screen, but the task sequence will continue to run in the background until it is finished.

For more information, please also see **Task Sequences (p. 152) and Non-operating system deployments (p. 181).**

### Manage enrollment profiles

To view an existing device enrollment profile:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program / Enrollment Profiles**.
2. Right-click a profile and choose **Properties**. The **Enrollment Profile for Mac Computers** dialog opens.
3. In the dialog, go through the tab pages and view the profile properties.
4. On the **Configuration Profile** tab page, you can click the **Download Profile** button to download the previously uploaded profile.

Almost all settings in this dialog are read-only. The reason for this is Apple doesn't support editing of existing enrollment profiles. The only exception is the **Task Sequence** tab where you can select a different task sequence. Note that if the currently specified task sequence was removed or became incompatible (e.g. OSD step was added) then the exclamation icon would be shown.

To delete a profile, right-click it and choose **Delete**. If a profile has been used already to enroll Mac computers, a warning message will be displayed to prevent accidental removal of a valid and potentially useful profile.

## View Mac computers assigned to the primary site

To view Mac computers assigned to the primary site:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program / Devices**.
2. The right pane lists Mac computers assigned to the site. These are the Mac computers that you can deploy using the Device Enrollment Program.

Note that Mac computers are always assigned to the primary Configuration Manager site.

To view the properties of a Mac computer, right-click it and choose **Properties**. The **Device Properties** dialog opens displaying the properties described below.

- **Assigned SCCM site**: The name of the site to which this device is assigned.
- **Enrollment status**: Displays one of the following values:
  a. **Not assigned** — no enrollment profile is assigned to the device.
  b. **Assigned** — a profile is assigned but the device is not enrolled in Configuration Manager.
  c. **Enrolled** — a profile is assigned and the device is enrolled in Configuration Manager.
  d. **Disowned** — the device disowned and removed from Configuration Manager (not reversible).

- **OS:** The device's operating system. This option is valid in X-Server-Protocol-Version 2 and later.
- **Device family:** Apple product family (iPad, iPhone, iPod, or Mac). This option is valid in X-Server-Protocol-Version 2 and later.
- **Serial number:** The device's serial number.
- **Model:** Model name.
- **Description:** Device description.
- **Color:** The color of the device (string).
- **Asset tag:** The device's asset tag (string).
- **Device assigned by:** The email of the person who assigned this device.
- **Device assigned date:** A time stamp in ISO 8601 format indicating when the device was assigned to the site.
- **Profile status:** Profile installation status. Can be one of the following: **empty** (if this value is displayed, no other profile fields are shown), **assigned, pushed, removed**
- **Profile uuid:** The unique ID of the assigned profile.
- **Profile assign time:** A time stamp in ISO 8601 format indicating when a profile was assigned to the device.
- **Profile push time:** A time stamp in ISO 8601 format indicating when a profile was pushed to the device.

## Assign an enrollment profile to Mac computers

After completing the steps describes in previous sections, you need to assign an enrollment profile to Mac computers that you plan to deploy using the Device Enrollment Program. A profile can be assigned to devices either manually or automatically.

### Manually assigning a profile

To manually assign an enrollment profile to one or more devices:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program** / **Devices**.
2. Selects one or more Mac computers, then right-click on the selection and choose **Assign Enrollment Profile**. The **Device Enrollment Profile Assignment** dialog opens.
3. Select a profile and click **OK** to assign it to the selected Mac computers.
4. When a Mac is deployed using the Apple Device Enrollment Program, a profile that you assign here will be used to configure it.

### Automatic profile assignment

Automatic profile assignment can be used when you add new devices. After you create one or more enrollment profiles, you can enable automatic assignment for one of them. This way, when a new device is added, the enrollment profile is automatically assigned to it.

**Note:** When automatic assignment is enabled for an enrollment profile, it will work for newly added devices only. All existing devices with no profile assigned will remain as they are. To assign a profile to these devices, you need to use the manual assignment method described above.

To enable automatic profile assignment:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program** / **Enrollment Profiles**.
2. Right-click a profile and choose **Enable Automatic Assignment to New Devices**.

You can enable only one profile of a particular type for automatic assignment. If you have more than one profile and enable one of them, all other profiles of the same type will be automatically disabled.

The status of the automatic assignment setting is displayed in the **Automatic Assignment** column in the profile list. The column will read "Enabled" or it will be blank depending on the status.

To disable automatic profile assignment, right-click the corresponding profile and choose **Disable Automatic Assignment to New Devices**. Note that if there's no profile with automatic assignment enabled, all newly added devices will not be assigned a profile and you'll have to do it manually. If a profile has already been assigned to a device, it will remain assigned, regardless of the status of the automatic assignment setting.

### Editing enrollment profiles

When you do any editing to an existing enrollment profile, a new copy of the profile is created. Note that this is not the same as normal editing where the item being edited is simply updated. In this case, an entirely new copy of the profile with its own ProfileUUID and name is created. If a profile was assigned to one or more devices, the assignment will automatically change to use the new profile.

To modify an enrollment profile:

1. Right-click a profile in the list and choose **Properties**.
2. Make the required modifications and specify a new name for the profile. The new name is a requirement and, if not done, will produce an error. Note that for profiles created prior to Parallels Device Manager v9.0, this rule will also be enforced on next editing.
3. Click **OK** to save the changes.

A new profile will appear in the profile list and all devices that were previously assigned to the old profile will be re-assigned to this new profile (see more info below). The old profile will still be kept in the database but will be handled as follows:

- The profile is marked as "Obsolete".
- It is hidden if no devices were assigned to it prior to editing. Otherwise, the profile will still be visible in the list but will not be editable or assignable.
- If one or more devices could not be re-assigned to the new profile, you'll see a warning saying so. If this happens, you can find the affected devices using the old profile UUID (ProfileUUID) and try assigning the new profile to them manually.

## Deploy Mac computers

Your Mac computers are now ready to be deployed and enrolled in Configuration Manager. The procedure consists of the following steps:

1. When a user starts a Mac for the first time, the Mac connects to the Apple DEP website and obtains the enrollment profile that you assigned to it.
2. The Mac then connects to Parallels IBCM/MDM Proxy (which faces the Internet and is accessible through it) as instructed by the enrollment profile settings.
3. The Parallels IBCM/MDM Proxy registers the Mac in Configuration Manager.
4. If an MDM profile is specified in the enrollment profile, then this profile is pushed to the Mac.
5. Parallels Mac Client is then installed on the Mac. If the Mac is not connected to your organization's network (i.e. it cannot communicate with the Parallels ConfigMgr Proxy), it will not be enrolled in Configuration Manager at this time. However, as soon as the Mac is connected to the network, Parallels Mac Client will connect to Parallels ConfigMgr Proxy and will enroll the Mac in Configuration Manager.

Once a Mac is enrolled in Configuration Manager, you can manage it as any other managed device.

# Network discovery

Parallels Device Management allows you to discover your Mac computers and push install Parallels Mac Client on them. The following discovery methods are supported:

- Parallels Network Discovery
- Configuration Manager Active Directory System Discovery

Parallels Network Discovery can discover any Mac on your network. Active Directory System Discovery can discover domain joined Mac computers. You can use one of the methods or both depending on your situation. For example, if all your Mac computers are domain joined, you can use Configuration Manager AD System Discovery. If some (or all) of your Mac computers are non-domain joined, you can use Parallels Network Discovery to discover these Mac computers.

# Enabling remote access on Mac computers

To push install Parallels Mac Client on a discovered Mac, Parallels ConfigMgr Proxy needs to log into it. In order to do this, the Mac must be configured to accept SSH connections.

**Note:** If a Mac computer is enrolled in Configuration Manager via Apple DEP, the SSH access doesn't have to be enabled on it, so the requirements described in this section can be ignored.

In addition to enabling SSH access on a Mac computer, an administrator account must be set up on it that Parallels ConfigMgr Proxy can use. This can be a domain account (for domain joined Mac computers) or a local account (for either domain joined or other Mac computers).

## Grant administrative privileges on a Mac to a domain user or group

If you want to use a domain account to push install Parallels Mac Client, you need to grant administrative privileges to it on a Mac. You can do this as follows:

1. Open **System Preferences** > **Users & Groups** and click **Login Options** at the bottom of the left pane.
2. In the right pane, click **Network Account Server: Edit...**

   Please note that if the button says "Join..." (not "Edit") then this Mac is not a member of a domain, so the following instructions will not work.
3. In the dialog that opens, click **Open Directory Utility**.
4. On the **Services** tab page of the **Directory Utility** dialog, select **Active Directory** and then click the pencil icon to edit the settings.
5. In the dialog that opens, click **Show Advanced Options** and then click the **Administrative** tab.
6. Select the **Allow administration by** option and add the desired domain user or group to the list. Remember the account as you will use it later to configure the client push installation.
7. Click **OK** to save the changes and then close all dialogs.

## Grant administrative privileges to a local Mac user

If you have Mac computers that are not members of a domain (or if you don't want to use a domain account for any reason), you need to create a local macOS user with administrative privileges. To add a user, open **System Preferences** > **Users and Groups**, click the plus-sign icon, select **Administrator** and specify the user information. Remember the user name and password as you will use it later to configure the client push installation.

## Enable SSH access on a Mac

To enable SSH access on a Mac:

1. Open **System Preferences** > **Sharing**.

2 Enable the **Remote login** service.

3 If you have granted permissions on this Mac to a domain account, add it to the list of users who are allowed remote access. If you'll be using a local user, add that user to the list.

After enabling SSH access on a Mac and granting a local or a domain user SSH access, you should verify that you can actually establish an SSH connection. The Mac should allow SSH connection with password authentication.

### Using multiple accounts

When creating local accounts or granting permissions to domain accounts on multiple Mac computers, you can set up the same account on all of them. This way you can configure Parallels ConfigMgr Proxy to use the same account name and password to log into every Mac. However, if you want to use multiple accounts, you can do that too. For example, you can use one account on a certain group of Mac computers and another on a different group. Parallels ConfigMgr Proxy will try every account that you configured, one by one, until a connection with a Mac can be established. Adding the account information to the push installation configuration is described later in this section.

## Configuring Parallels Mac Client push installation properties

Parallels Mac Client push installation properties must be configured, so that Parallels ConfigMgr Proxy can push install Parallels Mac Client on discovered Mac computers.

To configure push installation properties:

1 In the Configuration Manager console, navigate to **Administration** / **Site Configuration** / **Sites** and select your Configuration Manager site.

2 Click the **Mac Client Push Installation** toolbar item (or right-click on the site and choose **Parallels Mac Client Push Installation**). This opens the **Parallels Mac Client Push Installation Properties** dialog.

3 On the **General** tab page, select the **Enable automatic site-wide client push installation** option.

4 Specify one or more collections containing Mac computers to which you'll be push installing Parallels Mac Client. The **Install client to all Mac OS X Systems** option covers all Mac resources in every collection. The second option allows you to select one or more specific collections.

5 Select the **Accounts** tab and then click the New icon to specify an account that will be used to push install Parallels Mac Client on discovered Mac computers. This can be a domain account or a local Mac account. See **Enabling Remote Access on Mac Computers** (p. 28) for the information on how to configure the accounts.

6 Click **OK** to save the Parallels Mac Client push installation properties.

Once the push installation properties are configured, Parallels ConfigMgr Proxy will begin monitoring the system for discovered Mac computers. If you already have Mac resources in Configuration Manager that don't have Parallels Mac Client installed, Parallels ConfigMgr Proxy will identify these resources as Mac computers and will try to push install Parallels Mac Client on them. Newly discovered Mac computers will also be identified and the client will be push installed on them as well. The following sections describe how to configure and run Parallels Network Discovery and provide additional information about Configuration Manager Active Directory System Discovery.

# Using Parallels Network Discovery

Parallels Network Discovery can discover Mac computers on your network and automatically push install Parallels Mac Client on them. Both domain joined and non-domain joined Mac computers can be discovered in one run.

## Configuring Parallels Network Discovery

Before using Parallels Network Discovery to discover Mac computers and push install Parallels Mac Client on them, you need to configure it as described below:

1. In the Configuration Manager console, navigate to **Administration / Overview / Parallels Device Management / Discovery Methods**. The list in the right pane will be populated with one or more "Parallels Network Discovery" items according to the following conditions:
   - If you don't have secondary sites, the list will contain just one Parallels Network Discovery item.
   - If you have secondary sites, but Parallels Configuration Manager Proxy is installed only on the primary site, the list will contain just one item.
   - If you have secondary sites, and the Configuration Manager Proxy is installed on the primary and a secondary site, the list will contain one item for each site where the Proxy is installed.
2. Right-click the Parallels Network Discovery item for the desired site and then select **Properties**. The **Parallels Network Discovery properties** dialog opens.

### General

On the **General** tab page:

1. Select the **Enable network discovery** option.
2. Specify the TCP ports to scan (or use the default ports). Multiple ports can be separated by a comma, space, or semicolon.
3. Select the Nmap timing policy from the drop-down list. The default Nmap settings provide the optimal balance between the quality of the results and the time it takes to scan the network.

### Accounts

On the **Accounts** tab page, click the provided link to open the **Parallels Mac Client Push Installation Properties** dialog. If you haven't configured these properties yet, please refer to **Configuration Parallels Mac Client Push Installation Properties** (p. 29) for more information.

### Boundaries

On the **Boundaries** tab page, specify the Configuration Manager boundaries to search. You can use boundaries as a search option together with the options on the **Subnets** tab page. Searching boundaries should be the primary method. Boundaries and boundary groups must be configured in Configuration Manager for this to work.

Other elements on the **Boundaries** tab page are the following:

- **Boundary Groups** — Lists boundary groups. Highlight a group to view its member boundaries in the list below it. To include the entire group in a discovery search, select the checkbox in front of the group name.
- **Boundaries** — Lists boundaries that belong to the highlighted boundary group. Select the boundaries to include in a discovery search.
- **Filter** — Allows you to specify a filter for the **Boundaries to search** lists. You can type any part of the text that might appear in the boundary's name, type, or description.

### Subnets

On the **Subnets** tab page, you can specify the subnets to search:

1. Select **Search local subnets** if that's what you want to do. To search other subnets (in addition to or instead of local subnets), click the New icon and then enter the **Subnet** and **Mask** information. Make sure that the **Enable subnet search** checkbox is selected and then click **OK**.
2. On the **Schedule** tab page, click the New icon to set a schedule for running discovery. The **Custom Schedule** dialog opens.
3. Set the start date and time for a discovery run.
4. Set the discovery duration. This setting specifies the maximum length of time for a discovery run. If all resources are discovered before this time is up, the run will continue with minimal network traffic. If the run doesn't complete before this time, only the resources already discovered will be included in the result.
5. In the **Recurrence pattern** group box, select how this schedule will recur. The following choices are available:
   - **None**: The scheduled run is a one-time-only event.
   - **Weekly**: The scheduled run will occur weekly at the same start time.
   - **Monthly**: The scheduled run will occur monthly at the same start time.

- **Custom Interval**: The scheduled run will occur at a custom interval set by the administrator.

When done, close all dialogs to save the Parallels Network Discovery configuration settings.

### Running Parallels Network Discovery

When Parallels Network Discovery runs, it will perform the following actions:

1. When discovery finds a Mac, it will add it to Configuration Manager as a resource and will continue searching the network.
2. Parallels Configuration Manager Proxy will then connect to the Mac over SSH and will push the Parallels Mac Client installation package to it.
3. The installer will install Parallels Mac Client on the Mac and then enroll it in Configuration Manager.

In a situation when a discovered Mac has Parallels Mac Client already installed, the following scenarios will be considered:

- If the client is registered with a different Parallels Configuration Manager Proxy, but reports the same Configuration Manager site code as the current site, the client is re-registered with the current Configuration Manager Proxy and the Mac remains to be managed on the current site. This scenario may occur when you re-install the Configuration Manager Proxy on your Configuration Manager site (e.g. install in on a different computer).
- If the client is registered with a different Parallels Configuration Manager Proxy and reports a different site code, the client registration will remain the same and the Mac will be ignored by Network Discovery. This situation may occur when a Mac computer (e.g. a laptop) is managed by Parallels Device Management in one organization and is brought in to another organization that also uses Parallels Device Management to manage their Mac computers. The site code comparison allows you to prevent a situation when a Mac is added by mistake to a wrong Configuration Manager site.

The discovered Mac computers are placed into the **All Mac OS X Systems** collection. Please note that if you have secondary sites, Mac computers within their scope will be placed into the same **All Mac OS X Systems** collection on the primary site.

## Using Configuration Manager Active Directory System Discovery

Configuration Manager AD System Discovery can discover domain-joined Mac computers. You can configure and run the AD System Discovery using the standard Configuration Manager functionality. Once the Mac resources are discovered, Parallels Device Management will automatically identify them as Mac computers and push install Parallels Mac Client on them. Active Directory specific properties will persist after the Parallels Mac Client installation and will be kept up-to-date by the scheduled runs of AD System Discovery.

**Note:** Please note that for Parallels Device Management to push install Parallels Mac Client on Mac computers discovered by AD System Discovery, the push installation properties must be configured as described in the **Configuring Parallels Mac Client Push Installation Properties** section (p. 29).

# Manual installation of Parallels Mac Client

This section describes how to manually install Parallels Mac Client on a Mac computer and enroll it in Configuration Manager.

## Obtain Parallels Mac Client installer

First, a Mac user needs to download the Parallels Mac Client installer to their computer. The installer is placed on a local server when you install Parallels Device Management. You can obtain a URL to the installer location as follows:

1. Make sure that the Parallels Configuration Manager Proxy service is installed and running.
2. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **Mac Client Enrollment.**
3. In the **Mac Client Enrollment** list, right-click the **Mac Client installation package download URL** item and then click **Properties** in the context menu.
4. Copy the URL from the **Mac Client Installer URL** field and give it to the Mac user (e.g. email it). The URL will look similar to the following:

   `https://myhost.local:8761/files/pma_agent.dmg`
5. The Mac user enters the URL into a Web browser to download the `pma_agent.dmg` image.

**Note:** Parallels Device Management supports the Internet-Based Client Management functionality that allows you to enroll and manage Mac computers via the Internet. If you are using this functionality, then it means that some of your users don't have access to your local network. For these users, you can download the Parallels Mac Client installer to your computer first and then make it available to them using some other method. For more information about enrolling and managing computers via the Internet, see **Internet-Based Client Management** (p. 150).

## Install Parallels Mac Client

To install Parallels Mac Client on a Mac computer:

1. After you've downloaded the `pma_agent.dmg` file to a Mac computer, double-click it to open the image.
2. Double-click the **Parallels Mac Management for Microsoft SCCM.pkg** icon. This will start the installation assistant.
3. Follow the onscreen instructions. When asked, provide a user name and password. The user must have permissions to administer this Mac.
4. When the installation is complete, click **Close** to exit the installation assistant.

### Enroll the Mac computer in Configuration Manager

After you close the installation assistant, the Mac enrollment wizard automatically opens:

1. Read the information provided on the **Introduction** page. Here, you can specify whether you are enrolling the Mac from the local network or over the Internet (p. 150). If you are enrolling over the Internet, select the **Enroll over the Internet** option (at the bottom of the page). If enrolling locally, clear the option. If you select the option, you will need to provide the enrollment URL in the next step. What this means to you as an administrator is that you will need to give this URL to a user before they install Parallels Mac Client on their computer. The URL is a public URL of the Parallels IBCM/MDM Proxy.
2. Click **Continue**.
3. If you've selected the **Enroll over the Internet** option in the previous step, the next page will ask you to specify the Configuration Manager enrollment URL (i.e. the public Parallels IBCM/MDM Proxy URL, see step 1 above). The URL must be entered using the following format:

   `https://<ibcm-proxy-host-name>/ParallelsMacManagement.Enrollment`

   **Example:** https://pmm-test.parallels.net/ParallelsMacManagement.Enrollment

   Enter the URL and click **Continue**. The installer will try to establish a connection with the Parallels IBCM/MDM Proxy. If it cannot connect, it will display an error. If the connection is successful, you will see a page with the details of an SSL certificate provided by the Parallels IBCM/MDM Proxy. To continue, you need to accept the certificate.
4. On the **Authorization** page, enter the following information:
   - **Active Directory domain:** The name of the domain where the Parallels Configuration Manager Proxy is installed. Please note that if you are enrolling over the Internet, the field will not be prefilled because the Mac Client is not trusted at this point and so exposing internal domain names wouldn't be appropriate.
   - **User name:** Your domain user name in the following format: *username@domain-name*, where *domain-name* is the domain to which this user belongs.
   - **Password:** User password.
5. Click **Continue**.
6. If you receive an error, click **Try Again** to return to the **Authorization** page and re-enter the information. The registration may fail for the following reasons:
   - The specified domain name and/or domain credentials are incorrect.
   - The Mac IP address falls outside the boundary defined in Configuration Manager.
   - The Configuration Manager Proxy service is not running.

   If you close the wizard without completing the enrollment, it will run automatically at predefined intervals (5-10 minutes) and every time you restart the Mac. To stop this from happening, either resolve the problem and enroll the Mac or uninstall Parallels Mac Client.

7 If firewall is enabled in macOS, a message will be displayed asking you if `pma_agent.app` should be allowed to accept incoming connections. Click **Allow**. This will add `pma_agent.app` to the firewall exception list.

The results of a successful client registration should be as follows:

- The Mac is enrolled in Configuration Manager.
- The Mac inventory is collected and saved in Configuration Manager.
- The Mac is added to the **All Mac OS X Systems** collection in the Configuration Manager console.

Once installed, Parallels Mac Client will run on a Mac in the background and will start automatically every time the Mac is restarted.

# Push install Parallels Mac Client from Configuration Manager console

You can push install or update Parallels Mac Client on Mac computers that are already enrolled in Configuration Manager or have been added to it as unmanaged resources. You can use this option to remotely repair Parallels Mac Client on a Mac if it's not functioning properly or to enroll Mac computers that show up in the Configuration Manager console as unmanaged resources.

To push install Parallels Mac Client:

1 In the Configuration Manager console, navigate to the collection containing your Mac resources.

2 Select the desired Mac computers, then right-click on the selection and choose **Install Parallels Mac Client**.

3 The **Push Install Parallels Mac Client** wizard opens.

4 On the first page, specify a user account to connect to Mac computers using one of the following options:

   - **Use accounts from Parallels Mac Client Push Installation properties**. Use this option if you have already configured one or more accounts as described in **Configuring Parallels Mac Client push installation properties** (p. 29).
   - **Use this account**. Specify an account name and password. This can be a domain account or a local Mac account. See **Enabling remote access on Mac computers** (p. 28) for the information on how to configure an account.

5 Click **Next**.

6 On the second page of the wizard, specify what to do if Parallels Mac Client is already installed on a Mac. The following options are available:

- **Install Parallels Mac Client if it is already installed**. If you select this option, Parallels Mac Client will be re-installed on a Mac over the existing installation. If you clear this option, Parallels Mac Client will not be re-installed unless the push installation process finds a re-installation necessary due to a problem of some sort.
- **Uninstall the existing Parallels Mac Client before installation**. This option becomes enabled only if you select the option above. If selected, Parallels Mac Client will first be uninstalled from a Mac and then a fresh installation will be performed. Note that during the uninstallation, the existing Parallels Mac Client state (policies received, software installation states, etc.) will be lost. If this option is cleared, the Parallels Mac Client state will be preserved.

7 Click **Next**.

8 A dialog opens displaying the progress (number of processed Mac computers). To see more information, click **Details**. To hide the dialog and continue the operation, click **Hide**. To cancel the operation, click **Cancel**.

# Installing Parallels Mac Client using a script

A special script is supplied with Parallels Device Management that you can use to perform an unattended Parallels Mac Client installation.

To obtain and use the script, follow these steps:

1 On the computer running Parallels Configuration Manager Proxy, navigate to the C:\Program Files (x86)\Parallels\Parallels Device Management for Configuration Manager\files directory.

2 Locate the `InstallAgentUnattended.sh` file and copy it to a Mac. Copy the file to a Mac. Alternately, you can use Apple Remote Desktop to run the script on a Mac remotely.

3 Please note that you must use `sudo` to run the script because enrolling a Mac in Configuration Manager requires superuser privileges.

When you run the script, provide the following parameters (in the order listed):

- `agent_download_url` — the URL of the Parallels Mac Client installer. The URL can be obtained in the Configuration Manager console as described in **Manual installation of Parallels Mac Client** (p. 33).
- `user_name` — specifies the name of a domain user account that will be used to register Parallels Mac Client with the Configuration Manager Proxy. Please note that that the name must contain the domain logon name (e.g. *UserName*). It must not contain a domain name separated by a slash or an at (@) sign.
- `user_password` — the domain user password.
- `domain_name` — your company's domain name.

Example:

```
$ sudo ./InstallAgentUnattended.sh https://myhost.local:8761/files/pma_agent.dmg
myname mypass mydomain
```

If you receive the "Permission denied" error when executing the script, run the following command to set the file permissions and then execute the script again:

```
$ chmod 755 InstallAgentUnattended.sh
```

If you wish, you can hard code the URL, user/password, and the domain parameter values in the script, so you (or the Mac user) won't have to enter them in the command line. To hard code the parameter values, open the script in an editor and change the values of the input parameters from `$1`, `$2`, `$3`, `$4` to the desired values. The parameter names in the script are self-explanatory. Once the script is ready, give it to your Mac users, so they can execute it on their Mac computers, or use Apple Remote Desktop to execute it on Mac computers remotely.

When the script runs on a Mac, it displays the information in the console about the processes that its running. When the script completes executing, it returns a numeric code. To see the return code, run the following command after the scrip finished executing:

```
$ echo $?
```

The "0" code returned by the above command indicates that Parallels Mac Client has been installed and registered properly. Any other code indicates a failure (you can also read the last messages in the console to get an idea of what went wrong).

# Configuring the macOS firewall

The firewall must be configured on a Mac to allow Parallels Mac Client communicate over network. When you manually install Parallels Mac Client, you will be asked if `pma_agent.app` should be allowed to accept incoming connections. You answer "Allow" or "Deny". The same message is displayed when the push installation is performed by network discovery. If you answer "Deny", you'll have to add `pma_agent.app` to the firewall exception list later as described below.

To add `pma_agent.app` to the firewall exception list:

1. From the Apple menu, select **System Preferences**. The **System Preferences** dialog opens.
2. Select **Security & Privacy** and then click the **Firewall** tab.
3. If the firewall is running, the green light indicator will be "on" and its label will read "Firewall: On".
4. Click **Advanced**.
5. Click the **+** icon. The Mac directory tree dialog opens.
6. In the directory tree, navigate to the `/Library/Parallels` folder and select the `pma_agent.app` file.
7. Click **Add** and then click **OK**.
8. Close the **System Preferences** window.

# Verifying Parallels Mac Client deployment

To verify that the Parallels Device Management deployment was successful, open the Configuration Manager console and navigate to **Assets and Collections** / **Devices** / **All Mac OS X Systems**. You should see some Mac computers in the list. If you ran Parallels Network Discovery to discover Mac computers, some of those Mac computers may not have Parallels Mac Client installed on them.

To see if a Mac has Parallels Mac Client installed and running, look at the **Client** and **Client Activity** properties, which should say "Yes" and "Active" respectively. If the **Client** property says "No", it means that the Mac cannot be managed in Configuration Manager because Parallels Mac Client is not installed on it. If the **Client Activity** property says "Inactive", the Mac may be turned off, disconnected from the network, or it may have some other issues that prevent the Configuration Manager to communicate with it.

# Viewing Parallels Mac Client properties

When Parallels Mac Client is installed on a Mac computer, the Mac user can view Parallels Mac Client properties and perform some tasks.

To open the Parallels Mac Client properties window:

1. On a Mac computer, open **System Preferences**.
2. Click the **Parallels Device Management** icon (or click **View** > **Parallels Device Management for Configuration Manager**).
3. The **Parallels Device Management for Configuration Manager** window opens:
4. The **General** box contains the following information:
   - **Certificate expiration date**. The date and time when the Parallels Mac Client certificate expires.
   - **Certificate subject name**. A globally unique name identifying the Parallels Mac Client for which the certificate was issued.
   - **Connected to ConfigMgr Proxy**. The last date and time the Parallels Mac Client established a connection with the Parallels Configuration Manager Proxy.
   - **Policies received**. The last time the Parallels Mac Client downloaded its policy.
   - **ConfigMgr Proxy Internet URL**. Displayed if a Mac computer is managed via the Internet (i.e. connects to Configuration Manager via the Parallels IBCM/MDM Proxy).
   - **ConfigMgr Proxy URL**. The URL of the computer where the Parallels Configuration Manager Proxy is running. This is the Parallels Configuration Manager Proxy with which this Parallels Mac Client is registered.
   - **Site code**. The code of the Configuration Manager site to which this Mac is assigned.

- **Unique identifier**. A globally unique ID assigned to this Parallels Mac Client instance.
- **Version**. The Parallels Mac Client version number.

5 The "gear" drop-down menu in the lower left corner allows the user to perform some actions. We will talk about these actions in detail later in this guide. The actions are:

- **Connect**. Connects to the Parallels Configuration Manager Proxy and downloads the latest policy from Configuration Manager. For details, see **Initiating policy retrieval from a Mac computer** (p. 196).
- **Report Inventory**. Sends an inventory update to Configuration Manager. For details, see **User-initiated inventory update**.
- **Send Problem Report**. Sends a problem report to the IT administrator. For details, see **Sending problem reports from Parallels Mac Client** (p. 193).

# Uninstalling Parallels Mac Client

To uninstall Parallels Mac Client from a Mac, execute the following command in Terminal:

```
$ sudo /bin/bash -c
/Library/Parallels/pma_agent.app/Contents/MacOS/pma_agent_uninstaller.app/Contents/Reso
urces/UninstallAgentScript.sh
```

You can also run the Parallels Mac Client uninstaller in interactive mode as follows:

1 Open Finder and choose **Go** > **Go to Folder**.

2 Type `/Library` and click **Go**.

3 Locate and open the **Parallels** folder.

4 In the **Parallels** folder, right-click the `pma_agent.app` file and click **Show Package Contents** in the context menu.

5 Open the `Contents/MacOS` folder.

6 Double-click the `pma_agent_uninstaller.app` file to start the uninstaller.

7 Follow the onscreen instructions to uninstall Parallels Mac Client.

After Parallels Mac Client is uninstalled, the Mac will remain in the Configuration Manager database but its management will not be possible. You can reinstall the client on the Mac later to restore management functions.

CHAPTER 4

# Enrolling Apple Mobile Devices in Configuration Manager

This chapter describes how to enroll Apple mobile devices in Configuration Manager.

## In This Chapter



# Prerequisites

Compared to Mac computers, Apple mobile devices don't need Parallels Mac Client in order to be managed in Configuration Manager. The enrollment and management is done entirely via MDM.

# User-initiated enrollment

A user-initiated enrollment of an Apple mobile device is performed by the device user using a URL received from the IT administrator. To obtain the URL, the administrator needs to do the following:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Mobile Device Management** / **MDM Proxy**.
2. Select an MDM Proxy Link for the desired Configuration Manager site and open its **Properties** dialog.
3. Copy the value of the **Enrollment URL** property. This is the URL that needs to be sent to users in order to enroll their Apple mobile devices in Configuration Manager. Note that the URL contains the site code of the primary Configuration Manager site to which the devices will be enrolled.
4. Make the enrollment URL available to mobile device users (e.g. email it).

When a device user receives the enrollment URL, they need to do the following:

1. Open the URL in a web browser on their Apple mobile device.
2. The authentication page opens, which allows you to determine whether the user is eligible for enrollment. The authentication is performed in the corporate AD domain.
3. The user enters his/her domain username and password and clicks **Log in**.
4. On successful authentication, the next page opens where the user needs to specify the device ownership to limit the scope of the allowed MDM management tasks. The following options are presented to the user:
   - **Personally Owned**
   - **Institutionally Owned**

   When the user selects the appropriate option, the page is updated with the list of MDM management tasks that the IT administrator will and will not be able to perform on the device. For the complete list, please see **MDM management scope** (p. 45).
5. Click **Enroll**.
6. The next page informs the user that to continue, they need to download and install the MDM profile for their organization. Click **Continue**.
7. A dialog opens asking a permission to download the profile to the device. Click **Allow** to continue.
8. When the profile is downloaded to the device, the confirmation message is displayed. Click **Close** to close the message box.

At this point, another page opens containing instructions on how to install the downloaded MDM profile in order to complete the enrollment. The instructions and the exact steps that need to be performed are described below:

1. On the Apple mobile device, open the Settings app.
2. Navigate to **General** > **Profiles** and select the **Parallels MDM configuration** profile.
3. Tap **Install** in the top right corner. If the profile is not signed, then the warning page is displayed. The user will still be able to install the profile by tapping **Install** again, but to avoid this situation (when a user may suspect that it's a malicious profile) a profile signing should be configured before inviting users to enroll in MDM.

If the profile installation fails (e.g. a connection with the server could not be established), a corresponding message is displayed. If this happens, the user should try again and repeat the profile installation steps.

# DEP enrollment

The Apple Device Enrollment Program (DEP) provides a fast, streamlined way to deploy iPhone and iPad devices purchased directly from Apple or through Apple Authorized Resellers. Parallels Device Management for Configuration Manager supports Apple DEP and provides you with the ability to automatically enroll new mobile devices in Configuration Manager during the initial DEP setup procedure.

To use the DEP functionality, you must be enrolled in Apple Deployment Programs. For more information, please see the Apple Business Manager Getting Started Guide: https://www.apple.com/business/docs/site/Apple_Business_Manager_Getting_Started_Guide.pdf.

## Enable DEP

To enable the DEP functionality in Configuration Manager, you need to install Parallels IBCM/MDM Proxy and enable the Parallels MDM functionality. If you haven't done so already, please install and configure Parallels IBCM/MDM Proxy as described in the **Parallels Device Management for Configuration Manager Deployment Guide**, the **Deploying IBCM/MDM Proxy** chapter.

## Create an enrollment profile for Apple mobile devices

A device enrollment profile is a collection of settings that will be applied to a device when it is deployed using the Apple Device Enrollment Program. Every device must have an enrollment profile assigned to it before it can be deployed. Parallels Device Management includes the functionality to create device enrollment profiles right in the Configuration Manager console.

To create a device enrollment profile:

1. In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program** / **Enrollment Profiles**.
2. Right-click anywhere in the right pane and choose **New Enrollment Profile for Mobile Devices**. The **New Enrollment Profile for Mobile Devices** wizard opens.

Complete the wizard as described below.

### General Information

On the **General** page, specify the following:

- **Profile name**: Profile name. This is a required field.
- **Support phone number**: The organization's support phone number. This field is optional.
- **Support email address**: The organization's support email address. This field is optional.
- **Department**: Department name. This field is optional.

- **Allow profile removal**: If this option is selected, a user will be able to remove the profile from the device. This option is selected by default.
- **Allow pairing**: This option allows you to restrict a device from connecting to a Mac or PC to sync content, view books with the Books app, or transfer photos and videos from the camera. If pairing is disabled at activation, it can't be enabled later. If pairing is enabled, it may be restricted or enabled remotely via MDM with a configuration profile. This option is selected by default.

### User Experience

On the **User Experience** page, select the steps to exclude from the Setup Assistant, which will run during the enrollment process. These are the standard Setup Assistant steps. The **All steps** option (located in the upper right-hand corner) allows you to select or clear all other options.

### MDM Profile

This page allows you to specify a mobile device configuration profile and save it in the device enrollment profile as an MDM profile. After a device is deployed via Apple DEP and enrolled in Configuration Manager, this profile is pushed to it and is used to configure the device.

To specify a configuration profile:

1. Click the **Upload Profile** button and select a profile (a file with the ".mobileconfig" extension).
2. When the profile is uploaded, the contents of the profile will be displayed in the read-only text field as raw XML. Note that if a profile contains the MDM payload, it will be replaced with the automatically generated MDM payload.
3. Click **Next.** The profile will be saved and pushed to the Apple DEP website. A progress bar is displayed while the profile is uploaded.
4. Click **Finish**.

If needed, you can create multiple enrollment profiles and then assign different profiles to different devices according to your needs.

### Configuration Profiles

The **Configuration Profiles** page allows you to include one or more configuration items in an enrollment profile. Configuration profiles from these configuration items will be pushed to a device during the DEP enrollment without any delay.

To specify a configuration item:

1. Click the "Add configuration item" icon (the yellow star).
2. A dialog opens displaying configuration items containing only device configuration profiles. User profiles cannot be used with this functionality and will not be included in this list.

3 Select a configuration item and click **OK**. The configuration item is added after the currently selected item or to the end of the configuration profiles list.

To remove a configuration item from the enrollment profile, select it and click the "Remove configuration item" icon (the "X").

Note that if a configuration item was removed from Configuration Manager, but is still assigned to an enrollment profile, it will be marked in red on the **Configuration Profiles** page. Such a configuration item must be removed from the enrollment profile or you will not be able to make any changes to the profile.

Here's how configuration profiles are deployed during DEP enrollment:

1 At the time of DEP enrollment, the latest version of the configuration item is used to deploy a configuration profile.

2 The profile is installed before the user is even able to log in to the device.

3 If the latest version somehow contains a user configuration profile (which cannot be used), then this profile will not be deployed. This will not affect the installation of other profiles.

4 If a profile could not be installed for any reason, this step will be skipped and the device configuration will proceed normally.

### Manage enrollment profiles

To view an existing mobile device enrollment profile:

1 In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program / Enrollment Profiles**.

2 Right-click a mobile device profile and choose **Properties**. The **Enrollment Profile for Mobile Devices** dialog opens.

3 In the dialog, go through the tab pages and view, or modify if necessary, the profile properties.

To delete a profile, right-click it and choose **Delete**. If a profile has been already assigned to one or more mobile devices, a warning dialog will be shown. If you continue and delete the profile, it will be unassigned from the devices.

## Assign an enrollment profile to Apple mobile devices

After completing the steps describes in previous sections, you need to assign an enrollment profile to mobile devices that you plan to deploy using the Apple Device Enrollment Program.

To assign an enrollment profile to one or more mobile devices:

1 In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program** / **Devices**.

2 To distinguish between Mac computers and Apple mobile devices, use the **Device Family** column to sort the list.

3 Selects one or more mobile devices, then right-click on the selection and choose **Assign Enrollment Profile**. The **Device Enrollment Profile Assignment** dialog opens.

4 Select a profile and click **OK** to assign it to the selected mobile devices.

When a mobile device is deployed using the Apple Device Enrollment Program, a profile that you assign here will be used to configure it.

## Deploy Apple mobile devices

Your Apple mobile devices are now ready to be deployed and enrolled in Configuration Manager. The procedure consists of the following steps:

1 When a user starts a device for the first time, the device connects to the Apple DEP website and obtains the enrollment profile that you assigned to it.

2 The device then connects to Parallels IBCM/MDM Proxy (which faces the Internet and is accessible through it) as instructed by the enrollment profile settings.

3 The Parallels IBCM/MDM Proxy registers the device in Configuration Manager.

4 The MDM profile specified in the enrollment profile is pushed to the device.

Once a mobile device is enrolled in Configuration Manager, you can manage it as any other managed device.

# Mobile device resources in Configuration Manager

A mobile device resource (SMS_R_System.ClientType = 3) is created in Configuration Manager automatically during the user-initiated device enrollment. The following resource properties are recorded and stored in Configuration Manager:

| Information type | Device property |
|---|---|
| Device owner | Company / Personal |
| Serial number | Device information > SerialNumber |
| Activation Lock State | Device information > IsActivationLockEnabled |
| Is Supervised | Device information > IsSupervised |

To see mobile device resources, in the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Device Collections** / **All Mobile Devices**. Double-click the collection to see its contents. To see the properties of a resource, right-click it and choose **Properties**.

# MDM management scope

During the enrollment process, an Apple mobile device user needs to select the device ownership type from **Personally owned** or **Institutionally owned** (see the preceding sections for details). Depending on the selection, the scope of the MDM management tasks that the administrator will be able to perform will be limited as described below.

### Institutionally owned

The administrator will be able to perform the following tasks:

- Lock the device
- Apply institutional settings (will be added in a future version)
- Install and remove institutional data (will be added in a future version)
- Install and remove institutional apps (will be added in a future version)
- Remove the passcode (will be added in a future version)
- Wipe all data and settings from the device
- Add/remove configuration profiles
- Add/remove provisioning profiles (will be added in a future version)

The administrator **will not be able to perform** the following tasks:

- Remove anything they did not install
- Track the location of the device

### Personally owned

The administrator will be able to perform the following tasks:

- Lock the device
- Apply institutional settings (will be added in a future version)
- Install and remove institutional data (will be added in a future version)
- Install and remove institutional apps (will be added in a future version)
- Add/remove configuration profiles
- Add/remove provisioning profiles (will be added in a future version)

The administrator **will not be able to perform** the following tasks:

- Access the user personal information
- Wipe all data and settings from the device
- Remove anything they did not install
- Track the location of the device

# Mobile device license management

To enroll and manage Apple mobile devices in Configuration Manager, you need an active license of type **Mobile** in the primary Configuration Manager site. For details about activating a license, see **License Activation** (p. 11).

When an Apple mobile device is enrolled in Configuration Manager, a single individual license is consumed from the license volume. If a device is no longer used in your organization, you can de-enroll it and return the license that it's using back to the license volume, so it can be used by another device. See **De-enroll an Apple mobile device** (p. 47).

# De-enroll an Apple mobile device

To de-enroll an Apple mobile device from Configuration Manager, follow the instructions below:

1. In the Configuration Manager console, open the **All Mobile Devices** collection.
2. Right-click a mobile device and choose **De-enroll**.
3. A dialog opens explaining the de-enrollment procedure. Specifically, when you de-enroll a mobile device, all institutional data, configuration profiles, and institutional settings will be removed from the device. It will still be possible to re-enroll the device later, if needed.
4. Click the **De-enroll** button to complete the de-enrollment procedure.

Please note that when you de-enroll a device, it will no longer be managed in Configuration Manager. The corresponding Configuration Manager resource, however, will remain in the Configuration Manager database.

# Managing Apple mobile devices

Once an Apple mobile device is enrolled in Configuration Manager, you can begin managing it. Parallels Device Management supports the following management tasks for Apple mobile devices:

- **Compliance Settings** (p. 62) allow you manage configuration and compliance of Apple mobile devices in your organization.
- **Hardware and Software Inventory (p. 50)** lets you collect inventory information about Apple mobile devices.
- **Remote Lock and Wipe** (p. 145) allows you to lock and wipe a managed mobile device if it's lost or stolen.
- **De-enroll an Apple mobile device** (p. 47) so it's no longer managed in Configuration Manager.

CHAPTER 5

# Device Collections in Parallels Device Management

Configuration Manager collections help IT administrators to manage resources by combining them into logical groups based on a certain criteria. Different collections are used for Mac computers and Apple mobile devices, as described below.

## In This Chapter



# Mac Computer collections

Parallels Device Management adds the **All Mac OS X Systems** collection to organize Mac computers and the **Unknown Mac OS X Systems** collection that's used for macOS deployment.

To see the **All Mac OS X Systems** collection, open the Configuration Manager console and navigate to **Assets and Compliance / Overview / Device Collections / All Mac OS X Systems**. The collection can contain both managed and unmanaged Mac computers. A Mac is added to a collection as an unmanaged resource if Parallels Mac Client is not installed on it or if it's not registered with the Configuration Manager Proxy. You can still view the properties of an unmanaged Mac and connect to it using SSH or VNC if needed.

To identify managed and unmanaged Mac resources in the **All Mac OS X Systems** collection:

1. Right-click a resource and select **Properties** from the context menu.
2. In the **Properties** dialog, select the **General** tab.
3. In the **Discovery data** list, look up the "Client Version" property:
   - The client version of a managed resource will contain the Parallels Mac Client version number followed by "-PMA". For example: "5.1.6.804674-PMA".
   - The client version of an unmanaged resource will be "Unknown-PMA".

The **All Mac OS X Systems** collection uses the following criteria in the `WHERE` clause of its SQL statement:

```
ClientVersion LIKE '%-PMA'
```

Therefore, the Mac resources that have the client version ending with "PMA" are displayed in the **All Mac OS X Systems** collection. You can create your own collections for Mac resources using a different criteria if needed.

Note that when a Mac computer is enrolled in Configuration Manager, its serial number is automatically recorded and can be viewed in the device **Properties** dialog (described above). As an example, this information can be used to quickly create device collections based on serial numbers.

**Unknown Mac OS X Systems** is a special collection to which you deploy task sequences as part of macOS deployment. The collection is not supposed to contain any devices. For more information, see **Task Sequences** (p. 152).

# Apple Mobile Device collection

Apple mobile devices are placed into the standard **All Mobile Devices** collection. To see the collection in the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Device Collections** / **All Mobile Devices**. Double-click the collection to see its contents.

A mobile device resource is added to the collection automatically when the device in enrolled in Configuration Manager. To see the properties of resource, right-click it and choose **Properties**. For additional info, see **Mobile device resources in Configuration Manager** (p. 45).

CHAPTER 6

# Hardware and Software Inventory

## In This Chapter



# Overview

Hardware and software inventory information is collected from enrolled Mac computers and Apple mobile devices on a schedule and is saved in the Configuration Manager database. The inventory information is filtered in such a way that it doesn't contain any personal data. For Mac computers, you can also perform a manual (unscheduled) inventory update from the Configuration Manager console or from a Mac computer itself.

# View the inventory

To view the collected hardware and software inventory for a resource:

1. Open the collection containing managed resources (e.g. **All Mac OS X Systems** or **All Mobile Devices**).
2. Right-click a resource and select **Start** > **Resource Explorer** in the context menu.
3. The **Resource Explorer** snap-in opens where you can browse the inventory categories (classes) and view the relevant hardware and software information.

# Request an inventory update from the Configuration Manager console (Mac computers only)

To request an unscheduled inventory update for Mac computers from the Configuration Manager console:

1. In the Configuration Manager console, open the device collection containing your Mac computers.
2. Select one or more Mac computers (or the entire collection), then right-click on a selection and choose **Request Inventory Update**.
3. A dialog opens displaying the progress (number of processed Mac computers). To see more information, click **Details**. To hide the dialog and continue the operation, click **Hide**. To cancel the operation, click **Cancel**.
4. Once the operation is completed, you can view hardware and software inventory as described above.

# Send an inventory update from a Mac computer

You can also send an inventory update to Configuration Manager directly from a Mac computer. To do so:

1. Log in to the Mac computer.
2. Open **System Preferences** and click the **Parallels Device Management** icon.
3. In the **Parallels Device Management for Configuration Manager** dialog, click the "gear" icon in the lower left corner and choose **Report Inventory** in the drop-down menu. The inventory update is sent to Configuration Manager silently with no additional user interaction required.

You can also send an inventory update to Configuration Manager from a Mac computer using the `pmmctl` utility located in `/Library/Parallels/pma_agent.app/Contents/MacOS`. The utility has a single argument `report-hv-inventory`:

```
$ pmmctl report-hv-inventory
```

You can execute the command in Terminal or create a script that will execute it. The command may return an error in plist format if an error occurs.

# Extending hardware inventory for Mac Computers

By default, Parallels Mac Client installed on a Mac computer collects a predefined set of hardware inventory information about managed devices, which it reports to Configuration Manager. You can extend this set by using custom inventory data files, which you create yourself using the specifications described later in this section. By doing so, you can collect any hardware information (custom or standard) that is not collected by Parallels Mac Client by default.

For example, let's say each device in an organization has an asset number as part of a catalog which is maintained by hand. Parallels Mac Client is not aware of this number, but using a custom inventory data file and a matching hardware inventory class, you can include this information in hardware inventory and then see it in the Configuration Manager console. You can also use custom inventory data files to collect the information that belongs to standard Configuration Manager hardware inventory classes, but which is not collected by Parallels Mac Client by default.

### Custom inventory class

Before you create a custom inventory data file, you need to choose a hardware inventory class that will be used to report the information to Configuration Manager. A hardware inventory class should have properties that satisfy the reported data structure. At the same time, the custom data file must have attributes that match the class properties that you'll use to report the desired information (see the **Custom data file format** subsection below).

Which hardware inventory class you choose depends on your needs. You can select an existing class, add a new class from the hierarchy's top level server, or you can create a completely new class if you wish.

You can view existing hardware inventory classes as follows:

1. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Client Settings**.
2. Right-click **Default Client Settings** in the right pane and click **Properties**.
3. Select **Hardware Inventory** in the left pane.
4. In the right pane, click **Set Classes**. The Hardware Inventory Classes dialog opens where you can view existing classes.

To add a class from the hierarchy's top level server:

1. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Client Settings**.
2. Right-click **Default Client Settings** in the right pane and click **Properties**.
3. Select **Hardware Inventory** in the left pane.

4 In the right pane, click **Set Classes**.

5 Click **Add** and then click **Connect**.

6 Specify the name of the computer from which to retrieve WMI classes and the WMI namespace to use. If you want to retrieve all classes below the namespace that you specified, click **Recursive**. If you are connecting to a remote computer, specify login credentials for an account that has permission to access WMI on that computer.

7 Click **Connect**.

8 In the **Add Hardware Inventory Class** dialog, select a desired class and click **OK**.

If you decide to create a new class, you need to describe it in a .mof file using the Managed Object Format (MOF) language. For the information on how to create MOF files, please refer to the Microsoft documentation. Once you have a .mof file, you need to import it into Configuration Manager as follows:

1 In the Configuration Manager console, navigate to **Administration** / **Overview** / **Client Settings**.

2 Right-click **Default Client Settings** in the right pane and click **Properties**.

3 Select **Hardware Inventory** in the left pane.

4 In the right pane, click **Set Classes**.

5 Click **Import** and select the .mof file containing the class definition.

6 Click **OK**.

### Custom data file format

A custom inventory data file is an information property list file (plist) serialized to XML format. A single file contains inventory data for a single hardware inventory class. The file name must be the same as the class name that will be used to report the information to Configuration Manager. For example, if the class name is WarrantyInfo, then file name must be WarrantyInfo.plist.

The structure of a custom inventory data plist file is as follows:

1 At the top level there is an array containing one or more dictionaries, one for each instance of the reporting class.

2 Each dictionary contains one or more key/value records which represent the class instance properties (the key names must be the same as the matching class property names).

3 The values of the records must be one of the primitive plist data types, which includes:

- string
- integer
- real
- true/false
- date

**4** Here's an example of a custom hardware inventory plist file:

```
<plist>
    <array>
        <dict>
            <key>Attribute A</key>
            <date>2018-11-29T09:34:17Z</date>

            <key>Attribute B</key>
            <string>Active</string>
        </dict>
        <dict>
            <key>Attribute A</key>
            <date>2018-11-29T09:34:17Z</date>

            <key>Attribute B</key>
            <string>Active</string>

            <key>Attribute C</key>
            <string>QWE123456</string>
        </dict>
    </array>
</plist>
```

### Custom data file location

Custom inventory plist files must be placed into the following directory by default:

`/Library/Application Support/Parallels/PMA_Agent/inventory`

You can also place these files into a different directory, but you need to specify a search path to it by creating the `CustomInventoryFolders` key in the PMA Agent preferences file, which is located in `/Library/Preferences/com.parallels.pma_agent.plist`. The example below shows how to specify a path:

```
<key>CustomInventoryFolders</key>
<string>/Users/User1/SearchFolder1;/Users/User2/SearchFolder2</string>
```

To obtain the complete list of directories where the search for custom inventory files is performed, use the following command:

```
pmmctl get-config --inventory-file-folders
```

### Creating and deploying plist files

You can create custom inventory plist files in advance or you can use a script or an executable program to create them on the fly. Consider the following options:

- Create a file manually and then deploy it to Mac computers once or using a schedule.
- Create a script that generates a plist file based on some criteria and then deploy it to Mac computers using a Configuration Item.
- Create an executable program that generates a plist file and then deploy it to Mac computers. During deployment, specify that the program should run automatically (ones or periodically).

### Reporting custom inventory

In order for the information from a custom inventory plist file to be collected by Configuration Manager's hardware inventory, you need to enable it as follows:

1. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Client Settings**.
2. Right-click **Default Client Settings** in the right pane and click **Properties**.
3. Select **Hardware Inventory** in the left pane.
4. In the right pane, set the value of the **Collect MIF files** option to either **Collect IDMIF files** or **Collect IDMIF and NOIDMIF files**.

Parallels Mac Client running on a Mac computer performs the custom hardware inventory reporting on the same schedule as the standard hardware inventory. When it's time to report, Parallels Mac Client processes all of the custom plist files that it finds. When executing this task, Mac Client does the following:

- Ignores the files larger than the value specified in the **Maximum custom MIF file size (KB)** option in the Hardware Inventory default settings.
- Reads a plist file and reports any issues with its structure to the log file. You can review the log file in case of any errors.
- Uses the file name to identify the hardware inventory class name to report.
- Does not make any changes to the file, and does not delete it after processing.

### PLIST and MOF file examples

The following is a sample .mof file describing a hardware inventory class:

```
[ SMS_Report (TRUE),
  SMS_Group_Name ("TPM Status"),
  SMS_Class_ID ("MICROSOFT|TPM_STATUS|1.0"),
  Namespace ("\\\\.\\\\root\\\\cimv2\\\\sms") ]
class SMS_TPM : SMS_Class_Template
{
    [ SMS_Report (TRUE), key ]
        Boolean     IsReady;
    [ SMS_Report (TRUE) ]
        uint32         Information;
    [ SMS_Report (TRUE) ]
        Boolean     IsApplicable;
};
```

The following is a matching .plist file containing the information that is reported to Configuration Manager using the class above:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"https://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
    <dict>
```

```
        <key>IsApplicable</key>
        <false/>
        <key>IsReady</key>
        <false/>
    </dict>
</array>
</plist>
```

# Reporting UAMDM Status

User Approved MDM (UAMDM) is a macOS concept that requires a Mac user interaction in order to enroll a device in MDM. When a user is asked to approve MDM, they can do it immediately or they can postpone it, which may result in MDM enrollment delays. As an administrator, you have the ability to determine the UAMDM status of a particular Mac through custom inventory reporting and take appropriate actions if necessary.

UAMDM status is reported using the extended hardware inventory functionality, which is described in the **Extending hardware inventory** section (p. 52). Once you understand how the extended inventory works, you can use it to set up UAMDM status reporting using the following basic steps:

1. Choose an inventory class (or create a custom class) for UAMDM status reporting. For example, you can create a custom class and name it "UAMDM Status" (we'll use this name later in this section as an example).
2. Create a script that will detect the UAMDM status of a Mac computer and will create an inventory plist file containing the status (see the end of this section for the command line used to determine the status).
3. Run the script on a Mac computer using root privileges (in a production environment you can do it manually or you can use Task Sequences, depending on your situation).
4. Once the UAMDM status information is saved in a plist file, it will be included in the next hardware inventory report.
5. To view the UAMDM status in the Configuration Manager console, open your Mac collection, right-click a Mac of interest and select **Start** > **Resource Explorer**. Find the "UAMDM Status" class (we use our class example here) in the list of hardware inventory classes and see the status.

For the information on how to create custom inventory classes and inventory plist files, please see the **Extending hardware inventory** section (p. 52).

To determine the UAMDM status of a Mac computer, use the `profiles` command line tool (execute it with root privileges) as follows:

```
profiles status -type enrollment
```

The output may contain different information depending on the actual MDM enrollment status and enrollment method. If the Mac was enrolled in MDM with user approval, then the output will contain the "User Approved" string, as in the following example:

```
Enrolled via DEP: No
MDM enrollment: Yes (User Approved)
```

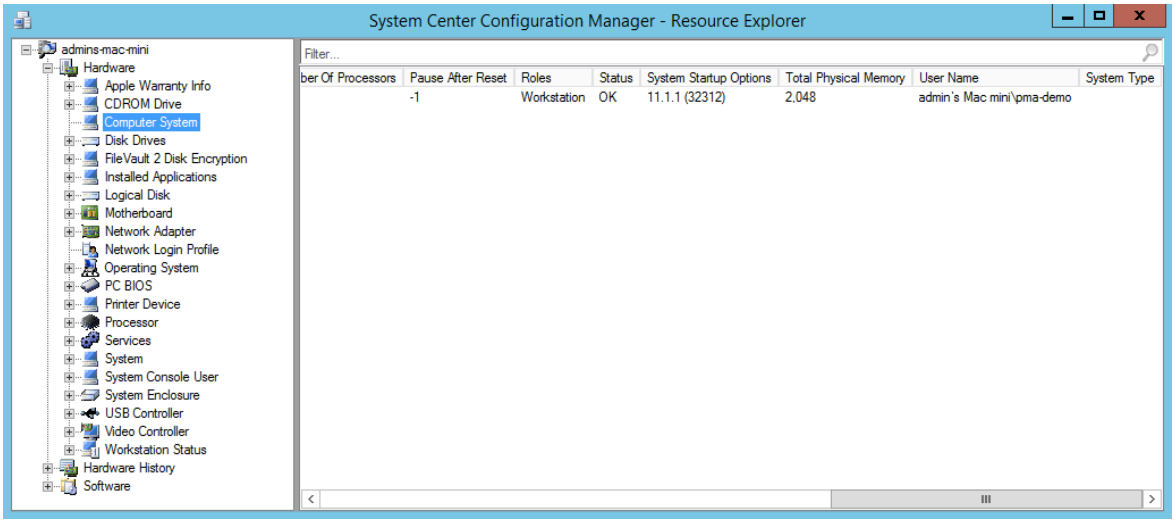
In your script (the one that creates the custom inventory plist file), you can, for example, search for the "User Approved" string and populate the file based on the results (e.g. set the value of a key to 1 or 0). This key and its value will then be included in the hardware inventory report, which you can view in the Configuration Manager console.

# Reporting Mac user logon information

Mac user logon details are reported by Parallels Mac Client to Configuration Manager and are saved in hardware inventory. The logon information is reported using the standard nodes in the hardware inventory tree, which are described below.

### Computer System

This node reports general computer information along with names of currently logged on users. The **User Name** column contains the user name in the `qualifier\account` format, where qualifier is the computer's NetBIOS name or a domain name. If there's no currently logged on user, the column will contain `SYSTEM` as a value.

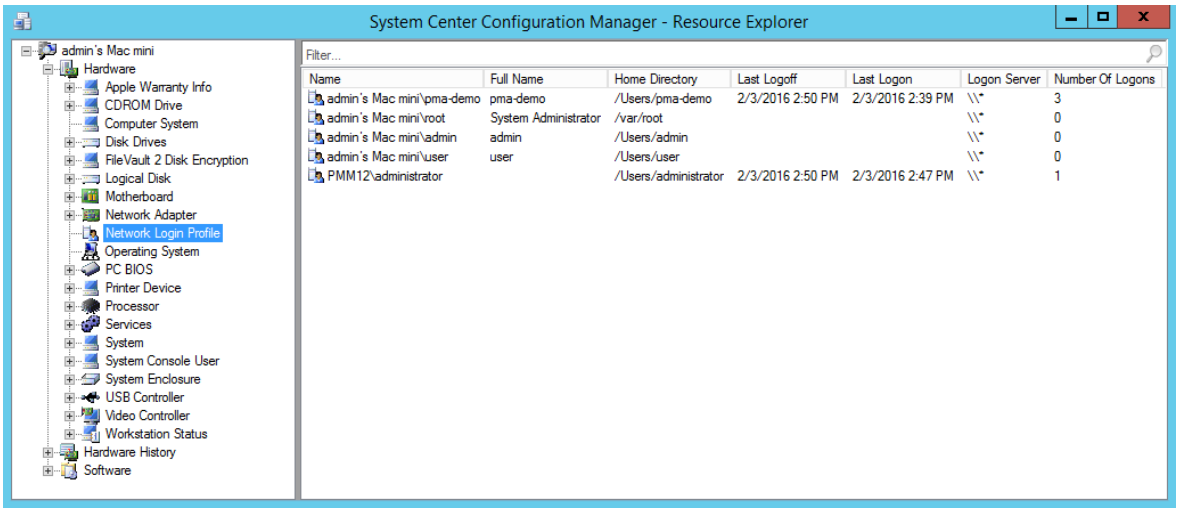



### Network login profile

This node reports all existing local user accounts (even if they haven't logged on recently) and all domain users who have logged on in the last 90 days. Each row in the list represents the network login profile of a specific user:

- The **Name** column contains the name of the account on a domain or the computer.
- The **Full Name** column contains the full name of the user belonging to the network login profile.
- The **Home Directory** column contains the path to the home directory of the user.

- The **Last Logoff** and **Last Logon** columns indicate date and time the user last logged off the system and logged on to system respectively.
- The **Number of Logons** column indicates the number of successful times the user tried to log on to this account.

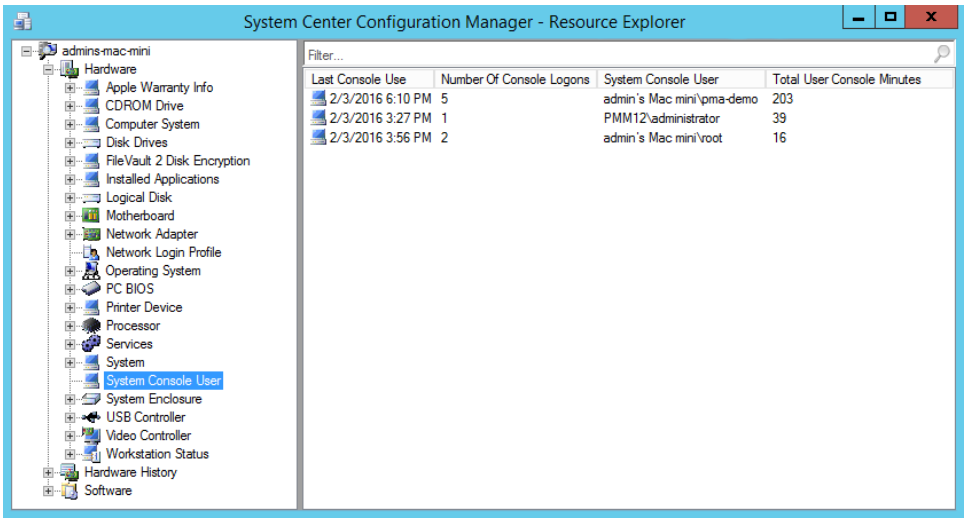



## System console user

This node allows you to easily see the top console user, which is the user who spends the most time logged on to the console. The information reported here is gathered from the macOS user accounting database by using logon and logoff events. When matching logon and logoff events are found, the information is used to calculate the amount of time the user was logged on. The resulting information is aggregated by user and ordered by total console usage. The information is calculated and displayed for the last 90 days.

- The **Last Console Use** column contains the last date and time when the user logged off from the console.
- The **Number Of Console Logins** column contains the total number of logons recorded in the user accounting database for the specific user.
- The **System Console User** column contains the user name for the user logged on to the console.

- The **Total User Console Minutes** column contains the total number of console logon minutes recorded in the database for the user.



CHAPTER 7

# Software Metering

## In This Chapter



# Overview

Software metering is used to monitor and collect software usage data from managed Mac computers. Software metering data, combined with software inventory data, can help you to determine the following:

- Which software titles are actively used by Mac users.
- Which software titles cause problems.
- Whether users run unauthorized software.
- How many licenses of particular software your organization actually need.

Software metering data for an individual Mac computer is collected by Parallels Mac Client running on it. To enable this functionality, you need to configure software metering rules in the Configuration Manager console. Parallels Mac Client running on a Mac evaluates these rules and begins collecting metering data. It then reports the collected data to Configuration Manager on a periodic basis. You can view the software metering data using the Configuration Manager reporting functionality.

# Configuring a software metering rule

To configure a software metering rule:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Software Metering**.
2. Right-click **Software Metering** and choose **Create Software Metering Rule** in the context menu (or click the **Create Software Metering Rule** button on the ribbon).
3. The **Create Software Metering Rule Wizard** opens.
4. On the **General** page of the wizard, specify the following:

- In the **Name** field, enter a rule name.
- In the **File name** field, specify an executable file name to identify the software that you want to monitor. Click the **Browse** button to browse for a file.
- The **Original file name** field can be used to specify the original file name (from the file header) if the name of the executable has changed. When you specify the original file name, the **File name** field is optional.
- In the **Language** drop-down list, select **-Any-**. This is a requirement, so you have to select this option.
- Specify the rest of the options as needed or keep the default values.

5 Click **Next** and complete the wizard.

The new software metering rule appears in the **Software Metering** list in the console. To create more rules, repeat the steps above.

# Viewing software metering data

You can view software metering data that was reported to Configuration Manager by Parallels Mac Clients using the Configuration Manager reporting functionality. To do so:

1 In the Configuration Manager console, navigate to **Monitoring** / **Overview** / **Reporting** / **Reports**.

2 Filter the available reports using the 'Category equals software metering' filter.

3 Double-click a report of interest to see the report data.

CHAPTER 8

# Compliance Settings

## In This Chapter



# Overview

Compliance settings is a set of tools that allow you to assess compliance of Mac computers and Apple mobile devices in your organization with regard to whether the operating system on a device is configured properly, volumes on Mac computers are encrypted, Parallels Desktop (if used in your organization) and virtual machines are configured on a Mac computer according to your requirements. Compliance is evaluated by creating a configuration baseline that contains configuration items that you want to evaluate and then distributing the baseline to managed devices.

**Note:** The only configuration item that is supported on Apple mobile devices is Configuration Profile. The rest of the configuration items described in this section apply to Mac computers only.

The subsequent sections contain information about how to create configuration items, set up a configuration baseline, and then deploy the baseline to a Mac or Apple mobile device collection.

# Creating a macOS/iOS configuration profile

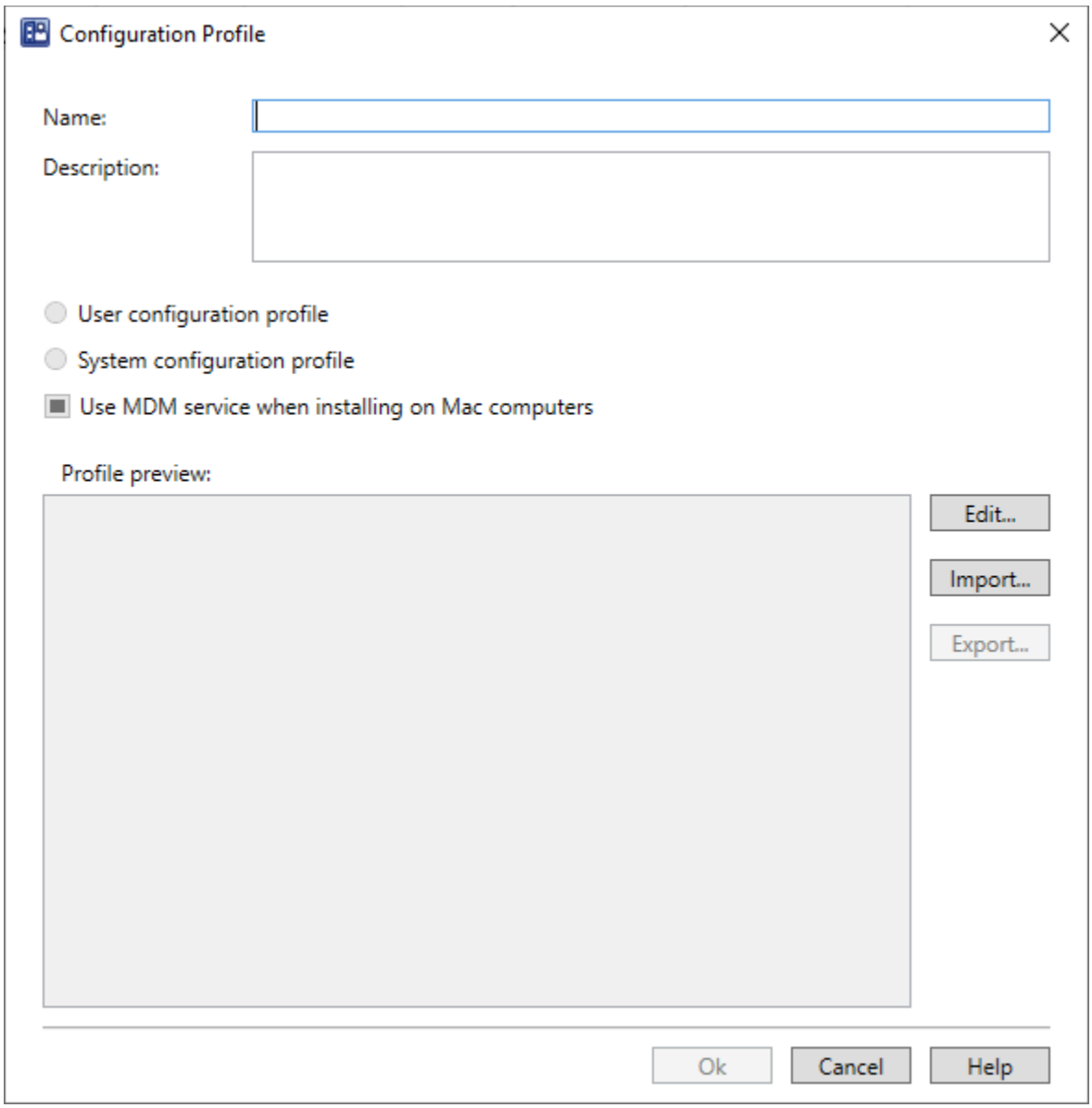
**Note:** When you install Parallels Device Management, you have an option to install iMazing Profile Editor from DigiDNA (the editor is installed together with ConfigMgr Console Extension component). If you skipped the installation, an older macOS profile editor will be used. We recommend that you install iMazing Profile Editor for its advanced capabilities of creating configuration profiles for macOS and iOS.

To create a configuration profile:

1 In the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Compliance Settings** / **Configuration Items**.

2 Right-click **Configuration Items** and choose **Create Parallels Configuration Item** > **macOS/iOS Configuration Profile**.

3 The **Configuration Profile** dialog opens.

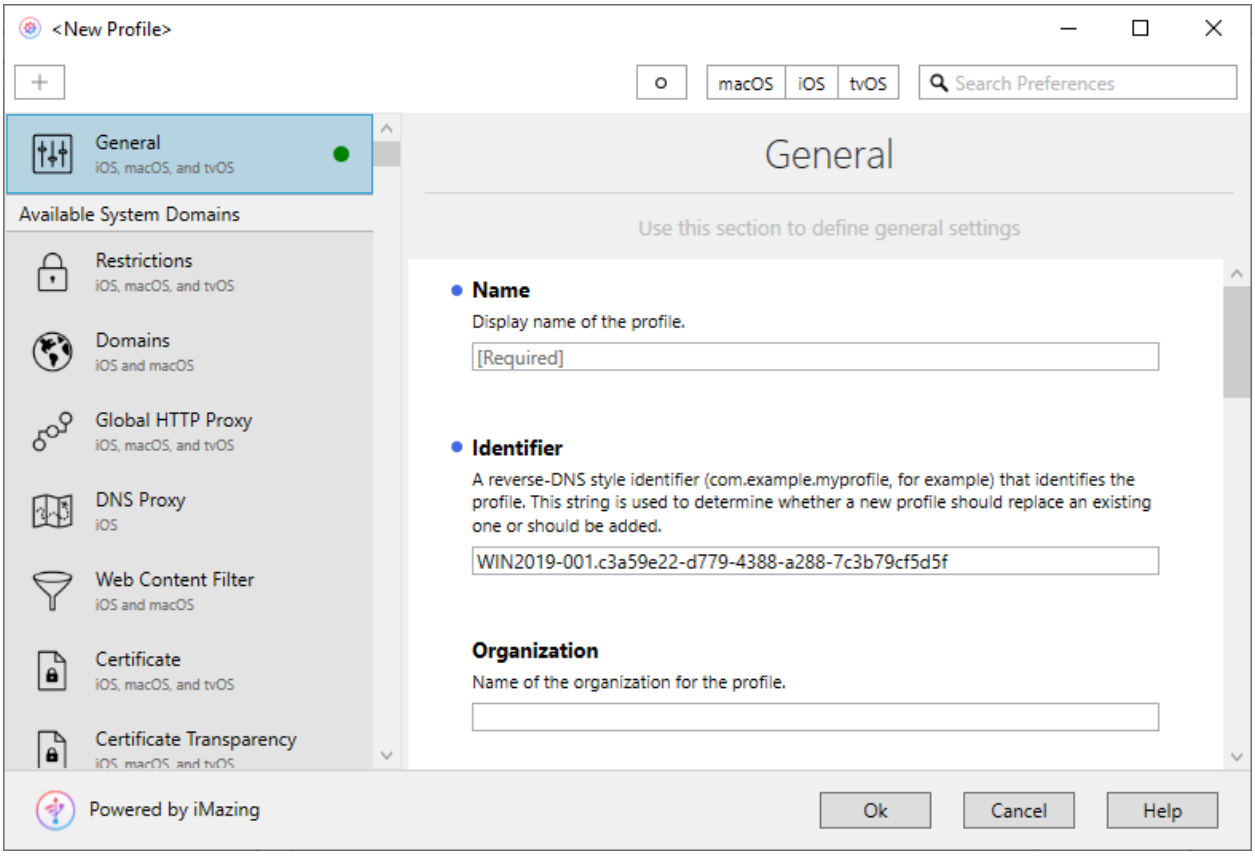



4 Type a profile name and an optional description. Note that other options (User/System configuration profile and Use MDM service) cannot be selected at this time. You need to create or import a configuration profile first, as described below.

5 To create a configuration profile using an integrated profile editor, click **Edit**. If you have a profile as a ".mobileconfig" file, click **Import** to import it. To create a ".mobileconfig" file, you can use iMazing Profile Editor that comes with Parallels Device Management. You can also import a profile if you created one previously using another third-party profile editor.

6 When you click **Edit**, the iMazing Profile Editor window will open if it's installed on your computer. If the editor is not installed, you will be asked if you want to install it. If you skip the installation, the older profile editor will open. Note that the older editor has limited capabilities and allows you to create only macOS configuration profiles. To create iOS configuration profiles, you still need to use another editor, such as iMazing Profile Editor. The rest of this section describes how to use iMazing Profile Editor. For the description of the older profile editor, see **Using the older profile editor** (p. 66).

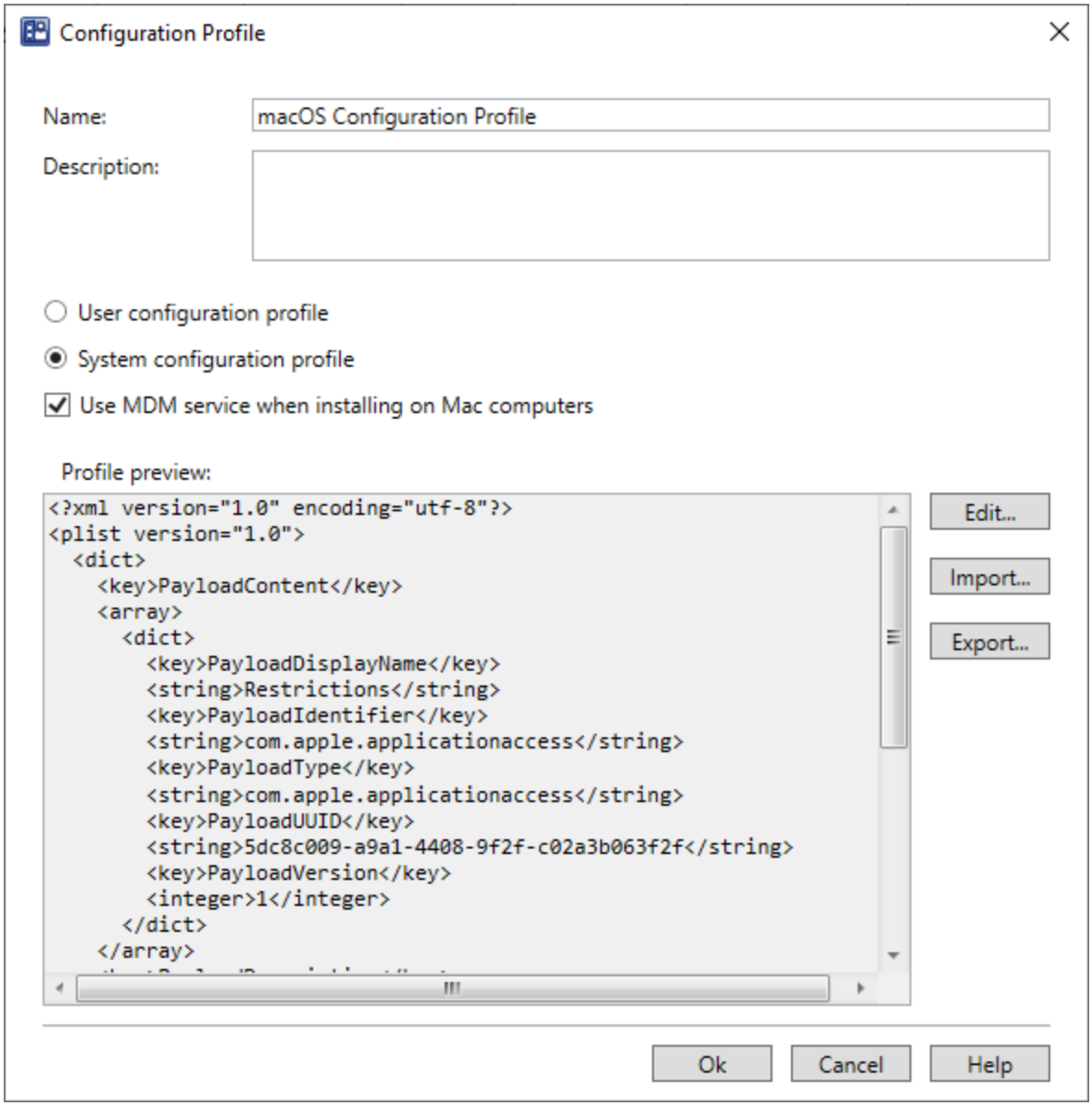
7 iMazing Profiler Editor lists available payloads in the left pane. The right pane allows you to configure the selected payload. You can filter the payload list using items on the toolbar. The **[o]** item displays only payloads and individual settings that have been already configured. Other items display payloads and settings specific to a corresponding platform. To display all available payloads and settings, clear all items.




8 To configure a payload, select it in the left pane. If the payload has not been configured yet, click the **Add configuration payload** button in the right pane (or click the plus-sign icon in the upper left-hand corner). Specify the payload settings in the right pane.

9 To save the payload data, click **OK**.

**10** Back in the **Configuration Profile** dialog, the saved payload XML data is displayed in the **Profile preview** text box. If you need to save the data as a ".mobileconfig" file, click **Export**.




**11** You can now specify the User/System profile (payload scope) and Use MDM service options as follows:

- **User configuration profile** or **System configuration profile**: These settings specify whether the profile will be installed system-wide or only for the installing user. Note that this choice is also specified in the **General** section of a configuration profile (the **Payload Scope** setting). If you change it here, the setting you select will override the setting in the **General** section of the configuration profile.

> **Note:** The System Policy Control payload (com.apple.systempolicy.control) must only exist in a device profile. If the payload is present in a user profile, an error will be generated during installation and the profile will fail to install.

- **Use MDM service when installing on Mac computers**: Select this option to install the configuration profile via MDM. See **Installing a configuration profile via MDM** below for additional information.

12 When done, click **OK** to save the configuration profile.

13 The profile will appear in the **Configuration Items** list in the Configuration Manager console. To edit an existing profile, right-click it and choose **Edit Parallels Configuration** Item.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying configuration baseline** (p. 95) for more information.

### Installing a configuration profile via MDM

As per Apple requirements, MDM must be used to install configuration profiles in the following cases:

- Kernel Extension Policy and Privacy Preferences Policy Control payloads can only be delivered to Mac computers via user-approved MDM.
- When deploying a configuration profile on Mac computers running macOS Big Sur.

You can also use MDM to install any configuration profile of your choice.

To install a configuration profile via MDM, you need Parallels IBCM/MDM Proxy installed and your Mac computers must be enrolled in MDM. For details, please see the **Parallels Device Management for Configuration Manager Deployment Guide**, the **Deploying IBCM/MDM Proxy** chapter.

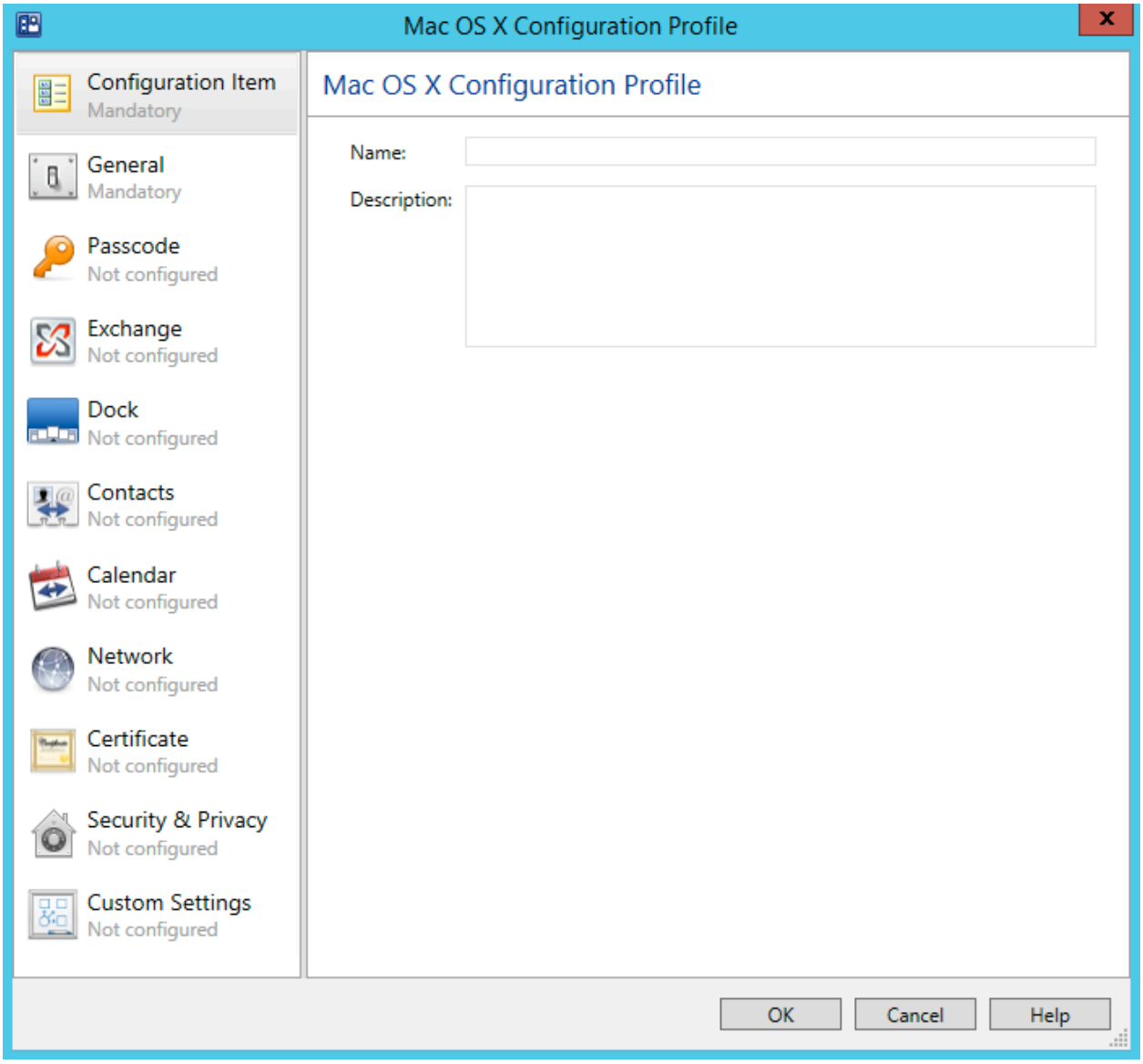
Consider the following possible scenarios:

- If you are using Apple DEP to enroll your computers in Configuration Manager, you should already have them enrolled in MDM, so no additional configuration steps are necessary.
- If you are not using Apple DEP (or if some of your Mac computers were not enrolled through it), you need to install and configure Parallels IBCM/MDM Proxy and then enroll Mac computers in MDM. You will also need to make sure that MDM is approved by each individual Mac user because this is an Apple requirement for computers enrolled in MDM outside of DEP.

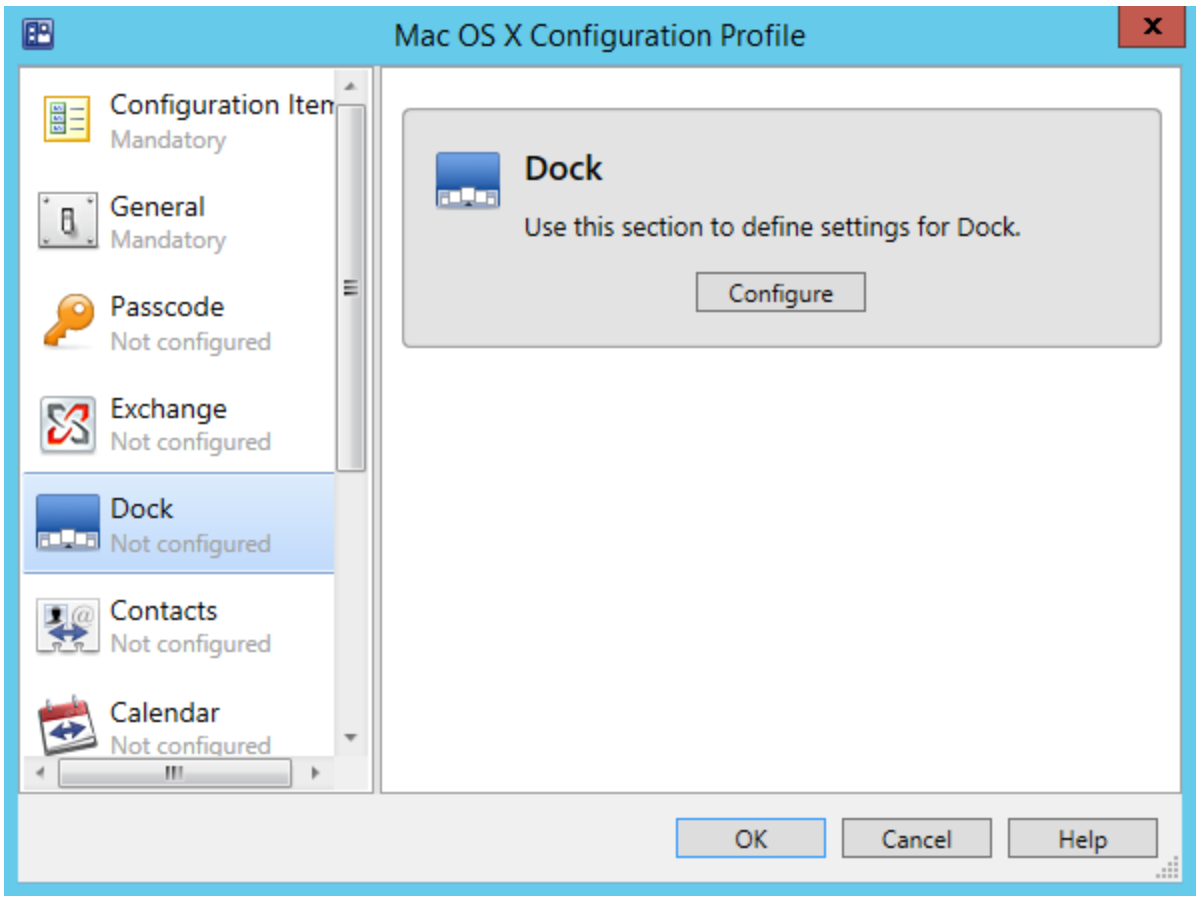
## Using the older profile editor

The previous section described how to create a configuration profile using iMazing Profile Editor. If you chose not to install it for any reason, the older profile editor will be used. Please note that the older profile editor allows you to create a configuration profile for macOS only. To create a profile for iOS, you need to use an external editor, which is why Parallels recommends to install iMazing Profile Editor capable of creating profiles for macOS and iOS.

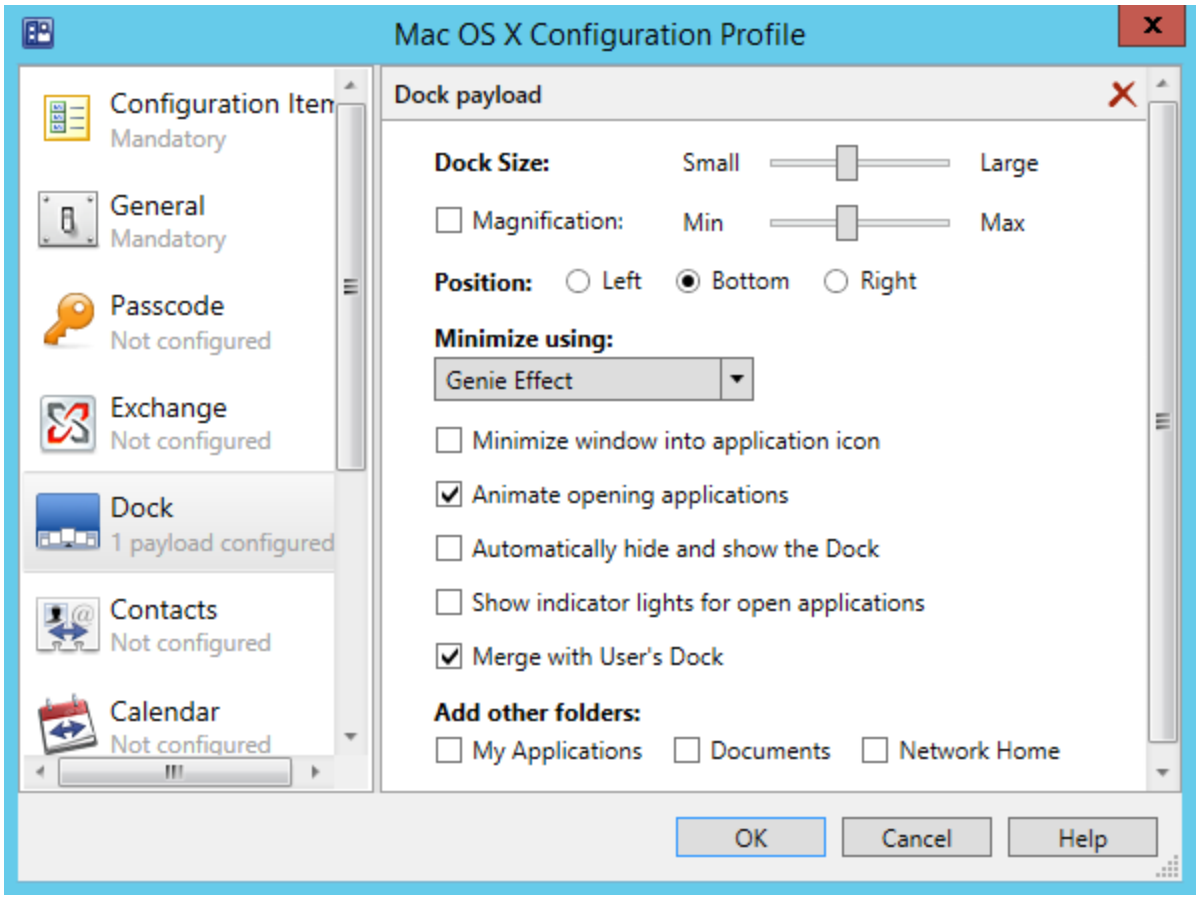
The beginning steps of creating a configuration profile are exactly the same as described in the previous section. The difference is, the older profile editor opens when you click **Edit** in the **Configuration Profile** dialog.



The left pane of the profile editor contains the list of payloads. The right pane contains settings for a selected payload. When you select a payload for the first time, the right pane will only contain a short description and the **Configure** button.



Clicking the **Configure** button will show the configurable properties for the selected payload.




Specify the desired payload properties and continue to another payload. Click **OK** at any time to save the changes and close the dialog.

If you don't specify any values for a payload, it will be excluded from the configuration profile and will not be evaluated on Mac computers. If you configured a payload but would like to remove it from the profile, click the **X** icon in the payload header area.

### Allowing users to specify macOS profile settings

**Note:** This option does not support macOS 11 Big Sur.

When setting up a macOS profile for multiple users, it may not be possible to specify all of the settings in advance. For example, when configuring the **Exchange** payload, the user account, email address, and password must be specified individually for each user. In a case like this, you may allow Mac users to provide the required settings interactively when the profile is applied on a Mac.

Some of the editable fields on payload screens are marked in light gray as *required*, *set on device*, and *optional*. Required fields must have a value or you will not be able to save the profile. "Set on device" fields can be mandatory or optional, and are usually set on a Mac by the Mac user (e.g. user names and passwords).

The logic that determines whether the profile is applied on a Mac interactively or silently is as follows:

- To use the interactive mode, enter the `%user_interaction_required%` tag into a field instead of a value. If a payload contains this tag in at least one field, a Mac user will be prompted to manually enter all of the missing settings. The interactive mode will be used even if none of the missing settings are actually required on the macOS side. You can enter the `%user_interaction_required%` tag into any field that you want a user to set manually, including the required, set-on-device, and optional fields.
- If a payload does not contain the `%user_interaction_required%` tag, an attempt will be made to apply the profile on a Mac silently. If the profile cannot be applied silently (one or more settings that are required on the macOS side are missing), the interactive mode will be used and the user will have to specify them manually.

In interactive mode, a standard System Preferences dialog will be opened in macOS for each corresponding payload where the user will have to specify the required settings. The dialog has the **Install** and **Cancel** buttons. To apply the settings, the user clicks the **Install** button. If the specified values don't pass validation, the user will have to enter them again. On success, a report will be sent to Configuration Manager. If the user clicks the **Cancel** button, the profile installation is aborted and a report is sent to the administrator.

Please note that when you create a macOS configuration profile using an external editor, you should have an option to set the **Profile Distribution Type** to **Automatic Push** or **Manual Download**. When you use the profile editor in the Configuration Manager console (described in this section), the distribution type is always **Manual Download**. The requirements for specifying certain settings are not as strict with the **Manual Download** distribution type.

### Payloads overview

The first item in the payload list is **Configuration Item**. It's not really a payload and is used to specify a configuration item name and optional description. This is the name that will appear in the **Configuration Items** list in the Configuration Manager console after you save the profile.

The **General** payload (second in the list) is used to specify general information for the configuration profile.

The rest of the payloads are used to specify the corresponding macOS system preferences. The following list provides a general description of each payload. For the complete information about creating a macOS configuration profile, please refer to Apple documentation.

| Payload | Description |
|---|---|
| Passcode | Used to specify passcode policies. |
| Exchange | Exchange account configuration. |
| Dock | Dock item settings. Dock appearance settings. |
| Contacts | Contacts LDAP configuration (CardDAV). |
| Calendar | Calendar server account configuration (CalDAV). |
| Network | Network Interface (Ethernet or Wi-Fi). |
| Certificate | X.509 certificates. |
| Security & Privacy | Usage and diagnostic information opt-out. |
| Custom Settings | Used to configure settings of macOS applications which are stored in preference files (.plist) in a standard location on a Mac. For details about using this payload, please read the **Using the Custom Settings payload** section (p. 71). |

### Saving the configuration profile

When you are finished entering the configuration profile information, click the **OK** button. This will create a configuration item that will appear in the **Configuration Items** list in the Configuration Manager console. Press **F5** to refresh the list.

To edit the profile, right-click it and select **Edit Parallels Configuration Item** from the context menu.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying configuration baseline** (p. 95) for more information.

## Using the Custom Settings payload

The **Custom Settings** payload is a part of the Compliance Settings functionality. It is a special payload used to specify preferences for macOS applications which are stored in application preference files (.plist) in a standard location in macOS.

Preferences for a particular application are normally configured in macOS by clicking the application name in the menu bar and then choosing **Preferences** (e.g. **Finder** > **Preferences**). This opens a dialog where you can specify various settings for the application. By using the **Custom Settings** payload, you can specify these settings in a macOS configuration profile for one or more macOS applications and then apply this profile to managed Mac computers.

To create a **Custom Settings** payload:

1. First, create a macOS configuration profile as described in **Using the older profile editor (p. 66).**
2. In the **Mac OS X Configuration Profile** dialog, select the **Custom Settings** payload in the left pane.

3 In the right pane, click the **Configure** button. This will show the controls that you can use to specify the desired application preferences. Note that you can create as many sets of preferences as you desire, where each set defines preferences for a single application. To add a set, click the plus sign icon in the upper right. Each time you press the icon, another set of controls is added to the right pane at the bottom.

To specify application preferences:

1 First, you need to enter a value in the **Preference domain** field. Each macOS application has a preference domain as part of the macOS Preference System. For example, the preference domain of the Finder application is com.apple.finder; Safari web browser has the preference domain defined as com.apple.Safari, etc. Application preferences that you specify will be applied to the preference domain specified in this field.

2 Use the **Property List Values** section to specify application preferences (properties). Each property is a key-value pair. You need to specify a key name, data type, and a value. Properties are organized in a macOS application preference file in a tree. When adding properties, make sure to use **Add** or **Add child** buttons, so that a property is correctly positioned in the tree. Please also make note of the following:

- Once you select a key type in the **Type** column, you cannot change it to a different type. If you've selected a wrong type, you need to remove the property (click the **Remove** button) and enter it again.
- When you specify a key type as **Data** (the <data> XML element in a .plst file), the **Upload** button appears in the **Value** column. Click the button and then specify a file containing the data. Please note that the file size must not exceed the 1 MB limit in order to be used in the **Custom Settings** payload. If the file is too big, you will receive an error and will not be able to upload the file.

Once you've entered the desired data, click **OK** to save the configuration profile.

# Enforcing FileVault 2 encryption

FileVault 2 is an encryption method that can be used with volumes on Mac computers to keep their data secure.

Before creating a FileVault 2 configuration item, you need to decide whether you want to use an *institutional* or a *personal* recovery key. The following explains what these keys are.

When preparing to encrypt the disk, the Mac user is asked to specify a password that will be used to unlock an encrypted disk. If the user forgets the password, he/she will not be able to log into the computer. The *recovery key* is a "safety net" that can be used to unlock the disk if the user forgets the password.

When creating a FileVault 2 configuration item, choose the key type:

- **Institutional**. An institutional recovery key is created in advance by the system administrator and then used for all Mac computers being encrypted. The key is stored in a keychain file, which the system administrator should keep in a safe place. If a Mac user forgets his or her personal password for unlocking the disk, this recovery key can be used to unlock it.
- **Personal**. A personal recovery key is created automatically for each individual Mac during the encryption procedure and is saved in the database on the primary Configuration Manager site. If a Mac user forgets the password for unlocking the disk, the personal recovery key for the disk can be retrieved from the database and can be used to unlock the disk.

Based on the type of the recovery key that you would like to use, read one of the following topics to learn how to create a FileVault 2 configuration item:

- **FileVault 2 encryption with institutional recovery key** (p. 73)
- FileVault 2 encryption with personal recovery key (p. 81)

# FileVault 2 encryption with institutional recovery key

This section describes how to create a FileVault 2 configuration item using an institutional recovery key.

## Creating FileVaultMaster keychain

To use an institutional recovery key on multiple Mac computers, you need to create a FileVaultMaster keychain file. The file will contain a recovery key (private key) needed to recover a disk encrypted with FileVault 2 and a public certificate.

To create a FileVaultMaster keychain, run the following command in Terminal:

```
$ security create-filevaultmaster-keychain /path/to/FileVaultMaster.keychain
```

You can omit the target path and filename if you want to create the `FileVaultMaster.keychain` file in the default `/Users/user-name/Library/Keychains` directory.

When prompted, choose and enter a password for the new keychain, This will become your master password. After the keychain is created, make one or more backup copies of the `FileVaultMaster.keychain` file and store them in a safe location, such as an external drive or an encrypted volume.

You now need to export the X.509 asymmetric public certificate from the FileVaultMaster keychain to a DER encoded certificate file.

To export the certificate:

1. Run the Keychain Access application (Applications/Utilities).
2. In the **Keychain Access** window, select "FileVaultMaster" keychain in the **Keychains** panel.

3 In the right pane, right-click the "FileVault Recovery Key" certificate and then click **Export** in the context menu.

4 Choose the name and location for the new file. Make sure that the **File Format** field has "Certificate (.cer)" option selected.

5 Click **Save** to export the certificate.

6 Copy the exported `.cer` file to a location where it can be accessed from the computer running the Configuration Manager console. You will later add this file to a configuration item to be distributed to Mac computers.

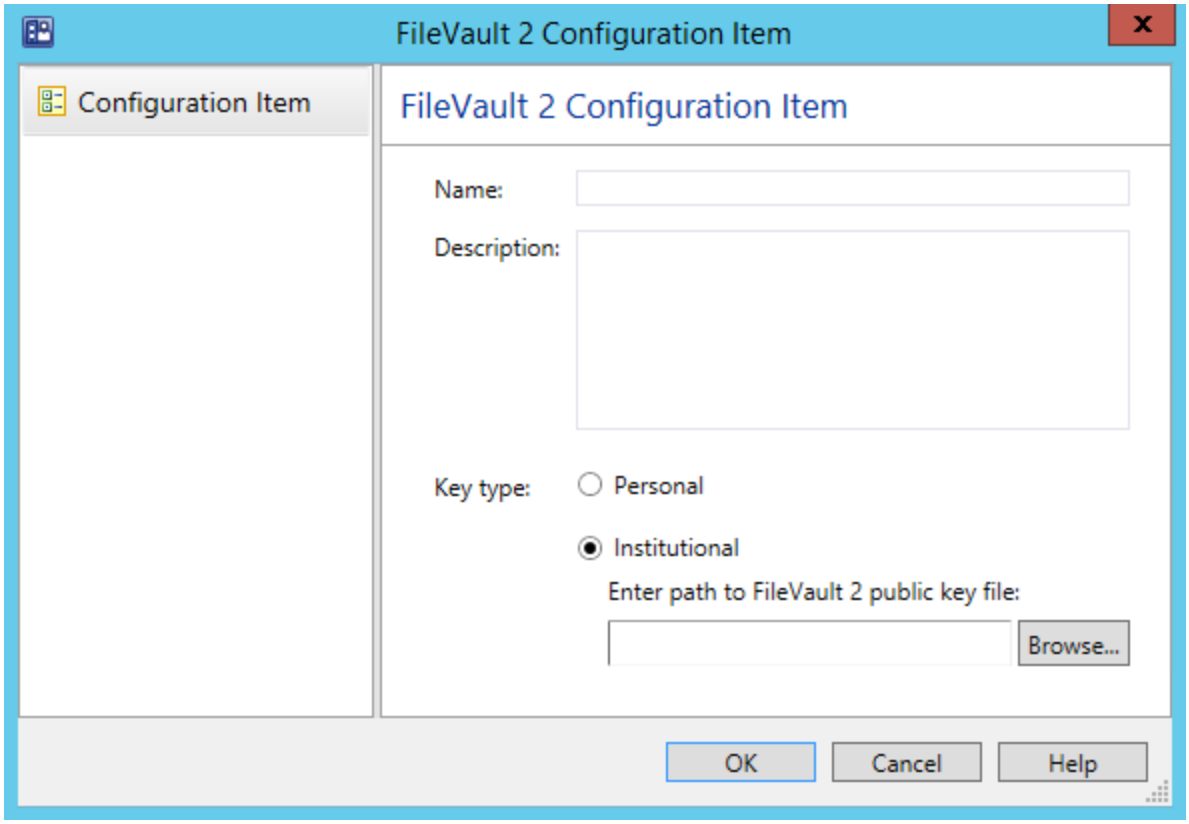
## Creating a FileVault 2 configuration item

To create a FileVault 2 configuration item using an institutional recovery key:

**Note:** If you want to use a personal recovery key, jump to **FileVault 2 Encryption with personal recovery key** (p. 81).

1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.

2 Right-click **Configuration Items** and then point to **Create Parallels Configuration Item** and click **FileVault 2 Configuration Item**.




3 Enter a configuration item name and description.

4 Select **Institutional** as key type. Please note that once a volume on a Mac has been encrypted, you will not be able to modify the following:
   - You cannot switch between personal and institutional recovery key.
   - You cannot change the existing FileVault 2 public key by providing another key file.
5 Click **OK** to create the configuration item.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a device collection. See **Deploying configuration baseline** (p. 95) for more information.

## Viewing and monitoring FileVault 2 encryption status

When the disk encryption operation is initiated on a Mac, the Parallels Mac Client begins reporting the encryption status to the Parallels Configuration Manager Proxy. The current encryption status is saved in the Mac's hardware inventory record in Configuration Manager and can be viewed in the Configuration Manager console. If at some later point the Mac user (or a third-party program) encrypts, decrypts, or re-encrypts the disk, the Parallels Mac Client running on a Mac will detect it and the encryption status will be immediately updated.

You can view the FileVault 2 encryption status for a particular Mac or you can run a report and view the information for all Mac computers as a single list.

### Viewing the FileVault 2 status for a specific Mac

1 In the Configuration Manager console, open the collection containing Mac computers (e.g. **All Mac OS X Systems**).
2 Right-click a Mac and select **Start > Resource Explorer** from the context menu. The **ResourceExplorer** window opens.
3 In the resource tree, navigate to **Hardware** / **FileVault 2 Disk Encryption**. The encryption information for the Mac is displayed in the right pane.

A single row of information represents a corresponding Mac volume and contains the following columns:

- **Key Type** — the type of the recovery key that was assigned or created during encryption. The possible values are:
  - **Unknown** — the disk is not encrypted or the disk is encrypted by the Mac user or a third-party (see the **Status** column).
  - **Personal** — personal recovery key.
  - **Institutional** — institutional recovery key.
- **Status** — the current encryption status. The possible values are described in the table below.
- **Volume** — the volume name.

### Viewing the FileVault 2 disk encryption report

In the Configuration Manager console, navigate to **Monitoring** / **Reporting** / **Reports**. Locate the **FileVault 2 Disk Encryption** report and double-click it. The **FileVault 2 Disk Encryption** dialog opens displaying the report.

Each row in the report represents a corresponding Mac volume and contains the following columns:

- **Netbios Name** — the Mac netbios name.
- **Volume** — the volume name.
- **Status** — the FileVault 2 encryption status (see the table above).
- **Key Type** — the recovery key type (Unknown, Personal, or Institutional).
- **Time** — the date and time the record was last updated.

The following table lists all possible FileVault 2 encryption states and transitions:

| State/Transition | Description |
|---|---|
| FileVault 2 is Off | FileVault 2 is not enabled on the Mac. |
| Encryption initiated, waiting for reboot | FileVault 2 encryption is in progress. The Mac is about to be rebooted to complete the encryption. |
| Encryption in progress | Encryption is in progress. |
| Encrypted | The Mac has been encrypted with FileVault 2. |
| Decrypting | Decryption is in progress. |
| Decrypting finished, waiting for reboot | Decryption finished. The Mac is about to be rebooted to complete the decryption. |
| Decrypted | The Mac has been decrypted. |
| Encrypting in progress by a 3rd party | An encryption operation has been initiated on the Mac by the user or a third-party program. |
| Encrypted by a 3rd party | The Mac has been encrypted by the user or a third-party program. |
| Decrypting (after 3rd party encrypting) | A decryption operation is in progress. The original encryption was performed by the Mac user or a third-party program. The decryption has also been initiated by the user or a third-party program. |
| Decrypting finished (after 3rd party encrypting), waiting for reboot | The Mac has been decrypted. The original encryption was performed by the Mac user or a third-party program. The decryption was also performed by the user or a third-party program. The Mac is about to be rebooted. |

After Mac computers have been encrypted, the best way for the IT administrator to monitor the Mac encryption status is to configure a baseline containing a FileVault 2 configuration item to run as often as necessary (e.g. daily). If an unauthorized change is made to the FileVault 2 encryption, the baseline run will report an error to Configuration Manager. The IT administrator will be able to see it and check the hardware inventory record for a particular Mac.

**Note:** You should be aware of one scenario when the FileVault 2 encryption status may not be reported accurately in the Mac hardware inventory. This will happen when (a) a Mac is removed from the Configuration Manager site, (b) the Parallels Mac Client is uninstalled from it, and (c) the Mac is then assigned to the site again. If the Mac was encrypted with FileVault 2 prior to removing it from the site, the encryption status will be reported as **Encrypted by a 3rd party**. To make the status to report accurately, you'll need to decrypt the disk and then encrypt it again.

## Encrypting a Mac computer with FileVault 2

After you deploy a configuration baseline to a device collection, Mac computers in the collection will be evaluated for compliance. If FileVault 2 is already enabled on a Mac, no action will be performed on it. If FileVault 2 is not enabled, the Mac user will see a dialog where they will need to take actions. Depending on the macOS version, the dialog behaves differently. See below for details.

### macOS Catalina and macOS Big Sur

The user will see a dialog saying that their computer must be encrypted to comply with the organization security policy. The dialog is displayed to the current user. If there are no users at the console at the moment, the dialog is displayed to the first user who logs in. The user can be a local or a mobile account user.

To encrypt the computer, the user must log out. If the user cannot log out at the moment, they can click the **Postpone** button and choose a time interval when the reminder should be displayed.

When the user clicks **Log out**, the logout process is initiated. The user is asked to enter their password to add them to the FileVault list (so they can unlock the computer later). Once the user enters the password, the computer is encrypted. Note that on APFS volumes, all users who have Secure Token in their account will be added to the FileVault list.

The user can now log back in and continue working on the computer.

### macOS Mojave and earlier (pre-Catalina)

The user will see a dialog saying that the Mac is about to be encrypted. The dialog has two buttons: **Encrypt** and **Postpone**:

- If the user clicks **Encrypt**, another dialog opens where the user must select one or more macOS user accounts that will be allowed to unlock the disk after it is encrypted.

  **Note:** The dialog displays all user accounts that exist on this Mac, but the user needs to select only those accounts that should be allowed to unlock the disk. If more accounts are added to the Mac later, they will not have this privilege. To grant the privilege to the new account(s), the disk encryption must be removed and then the encryption procedure must be performed from the beginning.

To select an account, the user needs to click the **Enable** button next to the account name and then enter a password that will be used to unlock the encrypted disk. The user can enable multiple macOS user accounts if needed, but at least one account must be enabled to continue. When the necessary accounts are enabled, the user clicks **Encrypt** to enable FileVault 2. To perform the actual encryption, the user must restart the Mac.

- If the user postpones the encryption on the first dialog, the dialog will open again in 5 minutes. The user has the ability to keep postponing the encryption procedure indefinitely. The time period after which the dialog is displayed is doubled each time the user clicks **Postpone**, but will never exceed one hour.

## Recovering encrypted disk using a password

If a FileVault 2 encrypted disk becomes unbootable, you will need to unlock it. The following steps describe how to unlock an encrypted disk using a password of a macOS account that's authorized to unlock the encryption.

To unlock an encrypted disk:

1. Boot your Mac from the Recovery HD partition by holding down **Command –R**.
2. Use the following command to list the available Core Storage volumes:
   ```
   $ diskutil cs list
   ```
3. Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.
4. Use the following command to unlock the disk. Be sure to insert the UUID from the previous step:
   ```
   $ diskutil corestorage unlockVolume UUID -stdinpassphrase
   ```
5. When asked, enter the password of an account that's authorized to unlock the disk.
6. If successful, the drive will unlock and mount. You'll be able to back up the data using Disk Utility, or by using a command line tool such as ditto.
7. Once the disk is unlocked, you can decrypt it by executing the following command:
   ```
   $ diskutil corestorage revert UUID -stdinpassphrase
   ```
   Once the volume is decrypted, you'll have full access to the hard disk.

## Recovering encrypted disk using institutional key

Normally, you unlock an encrypted disk using a password of an authorized macOS account. Alternately, you can unlock an encrypted disk using a recovery key. For instance, this could be the only option if the user forgets the password.

To unlock an encrypted disk using an institutional recovery key, you need the original FileVaultMaster.keychain file that contains the recovery key. You must also know the master password that you've set when you created the file.

### Finding the correct FileVaultMaster.keychain file

If you have more than one FileVaultMaster.keychain file and you forgot which one is which, you can compare the SHA1 fingerprint of the certificate in the file to the fingerprint of the original certificate that Parallels Device Management has saved in its database. If you know exactly which file contains the correct recovery key, skip this and the following sub-sections and read the **Unlock the Disk Using the Institutional Recovery Key** sub-section that follows them.

To retrieve the SHA1 fingerprint of the original certificate that used during encryption:

1. In the Configuration Manager console, navigate to the device collection containing the Mac (e.g. **All Mac OS X Systems**).
2. Locate the Mac in the list. If you can't find the Mac, read If **You Can't Find the Mac in Any of the Collections** below.
3. Right-click the Mac and then click **Properties**.
4. In the **Properties** dialog, click the **FileVault 2** tab to view the FileVault 2 encryption information for the Mac. The properties are:
   - **Hardware ID**. Contains the Mac hardware ID.
   - **Serial Number**. Contains the Mac serial number.
   - **Personal Key.** Contains the personal recovery key (will be blank if an institutional key was used).
   - **Institutional key**. Contains the SHA1 fingerprint of the institutional key certificate (will be blank if a personal key was used).
   - **LVGUUID**. The UUID of the logical volume group.
   - **LVUUID**. The UUID of the logical volume.
   - **PVUUID**. The UUID of the physical volume.
5. Compare the value of the **Institutional key** property to the fingerprint of the certificate in a FileVaultMaster.keychain file. The file that has the matching fingerprint contains the correct institutional recovery key.

### If you can't find the Mac in any of the collections

If the Mac is no longer assigned to the Configuration Manager site (i.e. you can't find it in any of the device collections), you can still retrieve its FileVault 2 encryption info from the Parallels Device Management database. The FileVault 2 encryption records are never deleted even for Mac computers that are no longer assigned to the site.

To retrieve the FileVault 2 encryption info for an unassigned Mac:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Parallels Device Management / Extended Device Information**.

2 Right-click the **Extended Device Information** item in the right pane and choose **Properties** in the context menu.

3 In the dialog that opens, enter the Mac's serial number or hardware ID and then click **Search**.

4 If the Mac was previously encrypted through Parallels Device Management, a dialog will open containing the FileVault 2 encryption properties for this Mac.

5 Use the value of the **Institutional key** property to compare it to the SHA1 fingerprint of the certificate in a FileVaultMaster.keychain file.

### Unlock the disk using the institutional recovery key

Assuming that you have the correct FileVaultMaster.keychain file, do the following to unlock the encrypted disk:

1 Boot your Mac from the Recovery HD partition by holding down **Command –R**.

2 Connect an external drive containing the original `FileVaultMaster.keychain` file.

3 Run Terminal (Application/Utilities). If the keychain is stored in an encrypted disk image, use the following command to mount it:

```
$ hdiutil attach /path/to/diskImage
```

4 Use the following command to unlock the `FileVaultMaster.keychain` file:

```
$ security unlock-keychain /path/to/FileVaultMaster.keychain
```

5 Enter the Master Password to unlock the keychain. If the password is accepted, the command prompt will return.

6 Use the following command to list the available Core Storage volumes:

```
$ diskutil cs list
```

7 Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.

8 Use the following command to unlock the encrypted disk. Be sure to insert the UUID from the previous step and the correct path to the keychain file:

```
$ diskutil cs unlockVolume UUID -recoveryKeychain /path/to/FileVaultMaster.keychain
```

9 When the command completes, the volume will be unlocked and mounted. You'll be able to back up data using Disk Utility, or by using a command line tool such as ditto.

If the command fails, it is possible that the disk was re-encrypted by the Mac user or a third-party program. You can compare the UUIDs of the volumes displayed by the `diskutil cs list` command to the **LVGUUID, LVUUID,** and **PVUUID** values on the **FileVault 2** tab of the Mac **Properties** dialog (see the **Retrieve Personal Recovery Key** subsection above). The values should match. If they don't, it means that the disk was re-encrypted, in which case the recovery key stored in the keychain file will not work.

10 Once the disk is unlocked, you can decrypt it by running the following command:

```
$ diskutil cs revert UUID -recoveryKeychain /path/to/FileVaultMaster.keychain
```

# FileVault 2 encryption with personal recovery key

This section describes how to create a FileVault 2 configuration item using a personal recovery key.

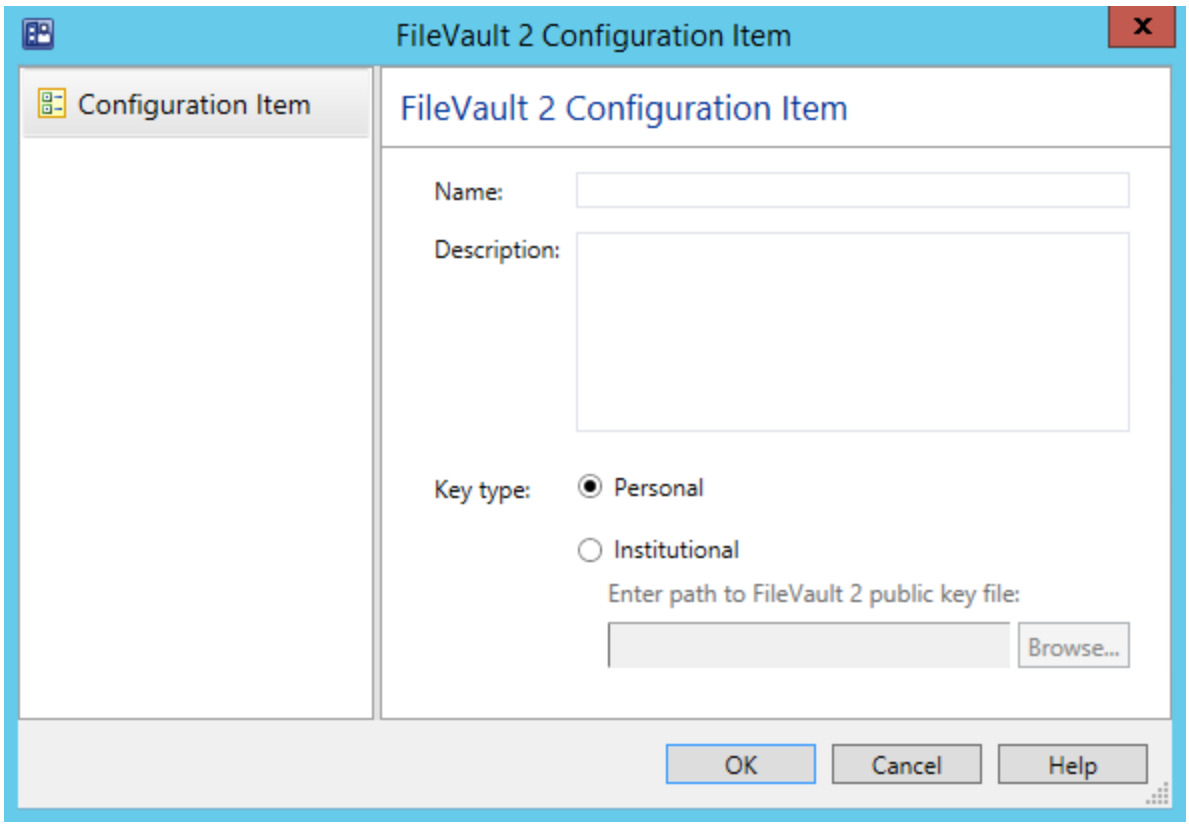
## Creating a FileVault 2 configuration item

To create a FileVault 2 configuration item using a personal recovery key:

**Note:** If you want to use an institutional recovery key, jump to **FileVault 2 encryption with institutional recovery key** (p. 73).

1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.

2 Right-click **Configuration Items** and then point to **Create Parallels Configuration Item** and click **FileVault 2 Configuration Item**.




3 Enter the desired configuration item name and description.

4 Select **Personal** as key type. A personal recovery key will be created automatically for each Mac during the encryption operation. Each individual key will be stored in the database on the primary Configuration Manager site and can be retrieved and viewed in the Configuration Manager console.

Please note that you cannot switch between personal and institutional keys once the volume on a Mac has been encrypted.

5 Click **OK** to create the configuration item.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a device collection. See **Deploying configuration baseline** (p. 95) for more information.

## Viewing and monitoring FileVault 2 encryption status

When the disk encryption operation is initiated on a Mac, the Parallels Mac Client begins reporting the encryption status to the Parallels Configuration Manager Proxy. The current encryption status is saved in the Mac's hardware inventory record in Configuration Manager and can be viewed in the Configuration Manager console. If at some later point the Mac user (or a third-party program) encrypts, decrypts, or re-encrypts the disk, the Parallels Mac Client running on a Mac will detect it and the encryption status will be immediately updated.

You can view the FileVault 2 encryption status for a particular Mac or you can run a report and view the information for all Mac computers as a single list.

### Viewing the FileVault 2 status for a specific Mac

1 In the Configuration Manager console, open the collection containing Mac computers (e.g. **All Mac OS X Systems**).

2 Right-click a Mac and select **Start > Resource Explorer** from the context menu. The **ResourceExplorer** window opens.

3 In the resource tree, navigate to **Hardware** / **FileVault 2 Disk Encryption**. The encryption information for the Mac is displayed in the right pane.

A single row of information represents a corresponding Mac volume and contains the following columns:

- **Key Type** — the type of the recovery key that was assigned or created during encryption. The possible values are:
  - **Unknown** — the disk is not encrypted or the disk is encrypted by the Mac user or a third-party (see the **Status** column).
  - **Personal** — personal recovery key.
  - **Institutional** — institutional recovery key.
- **Status** — the current encryption status. The possible values are described in the table below.
- **Volume** — the volume name.

### Viewing the FileVault 2 disk encryption report

In the Configuration Manager console, navigate to **Monitoring** / **Reporting** / **Reports**. Locate the **FileVault 2 Disk Encryption** report and double-click it. The **FileVault 2 Disk Encryption** dialog opens displaying the report.

Each row in the report represents a corresponding Mac volume and contains the following columns:

- **Netbios Name** — the Mac netbios name.
- **Volume** — the volume name.
- **Status** — the FileVault 2 encryption status (see the table above).
- **Key Type** — the recovery key type (Unknown, Personal, or Institutional).
- **Time** — the date and time the record was last updated.

The following table lists all possible FileVault 2 encryption states and transitions:

| State/Transition | Description |
|---|---|
| FileVault 2 is Off | FileVault 2 is not enabled on the Mac. |
| Encryption initiated, waiting for reboot | FileVault 2 encryption is in progress. The Mac is about to be rebooted to complete the encryption. |
| Encryption in progress | Encryption is in progress. |
| Encrypted | The Mac has been encrypted with FileVault 2. |
| Decrypting | Decryption is in progress. |
| Decrypting finished, waiting for reboot | Decryption finished. The Mac is about to be rebooted to complete the decryption. |
| Decrypted | The Mac has been decrypted. |
| Encrypting in progress by a 3rd party | An encryption operation has been initiated on the Mac by the user or a third-party program. |
| Encrypted by a 3rd party | The Mac has been encrypted by the user or a third-party program. |
| Decrypting (after 3rd party encrypting) | A decryption operation is in progress. The original encryption was performed by the Mac user or a third-party program. The decryption has also been initiated by the user or a third-party program. |
| Decrypting finished (after 3rd party encrypting), waiting for reboot | The Mac has been decrypted. The original encryption was performed by the Mac user or a third-party program. The decryption was also performed by the user or a third-party program. The Mac is about to be rebooted. |

After Mac computers have been encrypted, the best way for the IT administrator to monitor the Mac encryption status is to configure a baseline containing a FileVault 2 configuration item to run as often as necessary (e.g. daily). If an unauthorized change is made to the FileVault 2 encryption, the baseline run will report an error to Configuration Manager. The IT administrator will be able to see it and check the hardware inventory record for a particular Mac.

**Note:** You should be aware of one scenario when the FileVault 2 encryption status may not be reported accurately in the Mac hardware inventory. This will happen when (a) a Mac is removed from the Configuration Manager site, (b) the Parallels Mac Client is uninstalled from it, and (c) the Mac is then assigned to the site again. If the Mac was encrypted with FileVault 2 prior to removing it from the site, the encryption status will be reported as **Encrypted by a 3rd party**. To make the status to report accurately, you'll need to decrypt the disk and then encrypt it again.

## Encrypting a Mac computer with FileVault 2

After you deploy a configuration baseline to a device collection, Mac computers in the collection will be evaluated for compliance. If FileVault 2 is already enabled on a Mac, no action will be performed on it. If FileVault 2 is not enabled, the Mac user will see a dialog where they will need to take actions. Depending on the macOS version, the dialog behaves differently. See below for details.

### macOS Catalina and macOS Big Sur

The user will see a dialog saying that their computer must be encrypted to comply with the organization security policy. The dialog is displayed to the current user. If there are no users at the console at the moment, the dialog is displayed to the first user who logs in. The user can be a local or a mobile account user.

To encrypt the computer, the user must log out. If the user cannot log out at the moment, they can click the **Postpone** button and choose a time interval when the reminder should be displayed.

When the user clicks **Log out**, the logout process is initiated. The user is asked to enter their password to add them to the FileVault list (so they can unlock the computer later). Once the user enters the password, the computer is encrypted. Note that on APFS volumes, all users who have Secure Token in their account will be added to the FileVault list.

The user can now log back in and continue working on the computer.

### macOS Mojave and earlier (pre-Catalina)

The user will see a dialog saying that the Mac is about to be encrypted. The dialog has two buttons: **Encrypt** and **Postpone**:

- If the user clicks **Encrypt**, another dialog opens where the user must select one or more macOS user accounts that will be allowed to unlock the disk after it is encrypted.

  **Note:** The dialog displays all user accounts that exist on this Mac, but the user needs to select only those accounts that should be allowed to unlock the disk. If more accounts are added to the Mac later, they will not have this privilege. To grant the privilege to the new account(s), the disk encryption must be removed and then the encryption procedure must be performed from the beginning.

To select an account, the user needs to click the **Enable** button next to the account name and then enter a password that will be used to unlock the encrypted disk. The user can enable multiple macOS user accounts if needed, but at least one account must be enabled to continue. When the necessary accounts are enabled, the user clicks **Encrypt** to enable FileVault 2. To perform the actual encryption, the user must restart the Mac.

- If the user postpones the encryption on the first dialog, the dialog will open again in 5 minutes. The user has the ability to keep postponing the encryption procedure indefinitely. The time period after which the dialog is displayed is doubled each time the user clicks **Postpone**, but will never exceed one hour.

## Recovering encrypted disk using a password

If a FileVault 2 encrypted disk becomes unbootable, you will need to unlock it. The following steps describe how to unlock an encrypted disk using a password of a macOS account that's authorized to unlock the encryption.

To unlock an encrypted disk:

1. Boot your Mac from the Recovery HD partition by holding down **Command –R**.
2. Use the following command to list the available Core Storage volumes:
   ```
   $ diskutil cs list
   ```
3. Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.
4. Use the following command to unlock the disk. Be sure to insert the UUID from the previous step:
   ```
   $ diskutil corestorage unlockVolume UUID -stdinpassphrase
   ```
5. When asked, enter the password of an account that's authorized to unlock the disk.
6. If successful, the drive will unlock and mount. You'll be able to back up the data using Disk Utility, or by using a command line tool such as ditto.
7. Once the disk is unlocked, you can decrypt it by executing the following command:
   ```
   $ diskutil corestorage revert UUID -stdinpassphrase
   ```
   Once the volume is decrypted, you'll have full access to the hard disk.

## Recovering encrypted disk using personal key

Normally, you unlock an encrypted disk using a password of an authorized macOS account. Alternately, you can unlock an encrypted disk using a personal recovery key. For instance, this could be the only option if the user forgets the password.

### Retrieve personal recovery key

First, you need to retrieve the personal recovery key that was created when a Mac was encrypted with FileVault 2.

The key is stored in the Parallels Device Management database and can be obtained as follows:

1. In the Configuration Manager console, navigate to the device collection containing the Mac (e.g. **All Mac OS X Systems**).
2. Locate the Mac in the list. If you can't find the Mac, read **If you Can't Find the Mac in Any of the Collections** below.
3. Right-click the Mac and then click **Properties**.
4. In the **Properties** dialog, click the **FileVault 2** tab to view the FileVault 2 encryption information for the Mac. The properties are:
   - **Hardware ID**. Contains the Mac hardware ID.
   - **Serial Number**. Contains the Mac serial number.
   - **Personal Key.** Contains the personal recovery key (will be blank if an institutional key was used).
   - **Institutional key**. Contains the SHA1 fingerprint of the institutional key certificate (will be blank if a personal key was used).
   - **LVGUUID**. The UUID of the logical volume group.
   - **LVUUID**. The UUID of the logical volume.
   - **PVUUID**. The UUID of the physical volume.
5. Copy the value of the **Personal key** property. If the property doesn't have a value but the **Institutional key** property underneath it does, then this Mac was encrypted with an institutional recovery key. If that's the case, please read **Recovering encrypted disk using institutional key** (p. 78).

### If you can't find the Mac in any of the collections

If the Mac is no longer assigned to the Configuration Manager site (i.e. you can't find it in any of the device collections), you can still retrieve the personal recovery key for from the Parallels Device Management database. The FileVault 2 encryption records are never deleted from it even for Mac computers that are no longer assigned to the site.

To retrieve the personal key for an unassigned Mac:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Parallels Device Management**.
2. Right-click **FileVault 2 Encryption Information** and then click **Properties**.
3. In the **FileVault 2 Encryption Information** dialog, enter the Mac's serial number of hardware ID. Click **Search**.
4. If the Mac was previously encrypted, a dialog will open containing the FileVault 2 encryption properties for this Mac.
5. Copy the value of the **Personal key** property.

### Unlock the disk using the personal recovery key

Once you have the personal recovery key, you can use it to unlock the encrypted disk:

1. Boot your Mac from the Recovery HD partition by holding down **Command –R**.
2. Use the following command to list the available Core Storage volumes:
   ```
   $ diskutil cs list
   ```
3. Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.
4. Use the following command to unlock the encrypted disk. Be sure to insert the UUID from the previous step:
   ```
   $ diskutil cs unlockVolume UUID -passphrase recoverykey
   ```
5. When the command completes, the volume will be unlocked and mounted. You'll be able to back up data using Disk Utility, or by using a command line tool such as ditto.

   If the command fails, it is possible that the disk was re-encrypted by the Mac user or a third-party program. You can compare the UUIDs of the volumes displayed by the `diskutil cs list` command to the **LVGUUID, LVUUID,** and **PVUUID** values on the **FileVault 2** tab of the Mac **Properties** dialog (see the **Retrieve Personal Recovery Key** subsection above). The values should match. If they don't, it means that the disk was re-encrypted, in which case the recovery key stored in the Parallels Device Management database will not work.
6. Once the disk is unlocked, you can decrypt it by running the following command:
   ```
   $ diskutil cs decryptVolume UUID -passphrase recoverykey
   ```

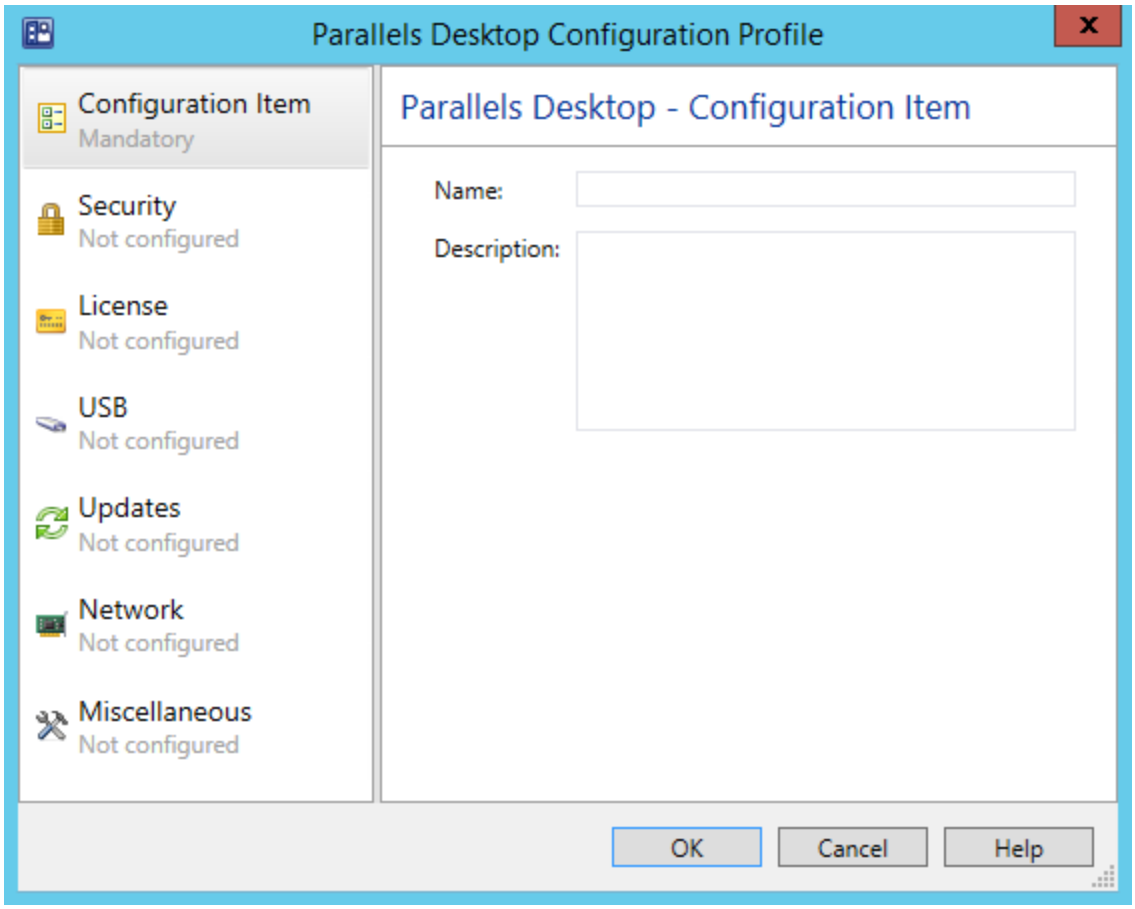
# Enforcing Parallels Desktop preferences

If your Mac computers have Parallels Desktop installed on them, you can monitor and enforce its preferences by creating a Parallels Desktop configuration item and specifying the required values.

To create a Parallels Desktop configuration item:

1. In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.

2 Right-click **Configuration Items**, point to **Create Parallels Configuration Item** and click **Parallels Desktop Configuration**. The **Parallels Desktop Configuration Profile** dialog opens.




3 Enter a name and and optional description for this configuration item.

4 The **Security** page allows you to specify password requirements for using Parallels Desktop features and whether or not the Mac users will be allowed to change Parallels Desktop preferences. To enable password requirements, click the ON/OFF switch to toggle it to "ON" and then select the desired options. Do the same for the **Edit Parallels Desktop settings** option.

- The **License** page allows you to specify the Parallels Desktop license key and customize the Request Support settings. The license key that you specify will be applied to Parallels Desktop on Mac computers (e.g. when you want to update it). The **Request support settings** allow you to specify the action for the **Help** > **Request Support** menu item in the Parallels Desktop graphical user interface.
- The **USB** behavior page allows you to specify what to do when a USB device is connected to a Mac.
- The **Updates** page allows you to specify Parallels Desktop update options.
- The **Network** page specifies the Parallels Desktop network settings.

- The **Miscellaneous** page allows you to specify the default virtual machine folder and the participation in Parallels Customer Experience program.

When finished, click **OK** to save the configuration item and close the dialog. To view the new item in the **Configuration Items** list, press **F5** to refresh it. To modify the configuration item, right-click it and choose **Edit Parallels Configuration Item**.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying configuration baseline** (p. 95) for more information.

# Enforcing Parallels Desktop VM settings

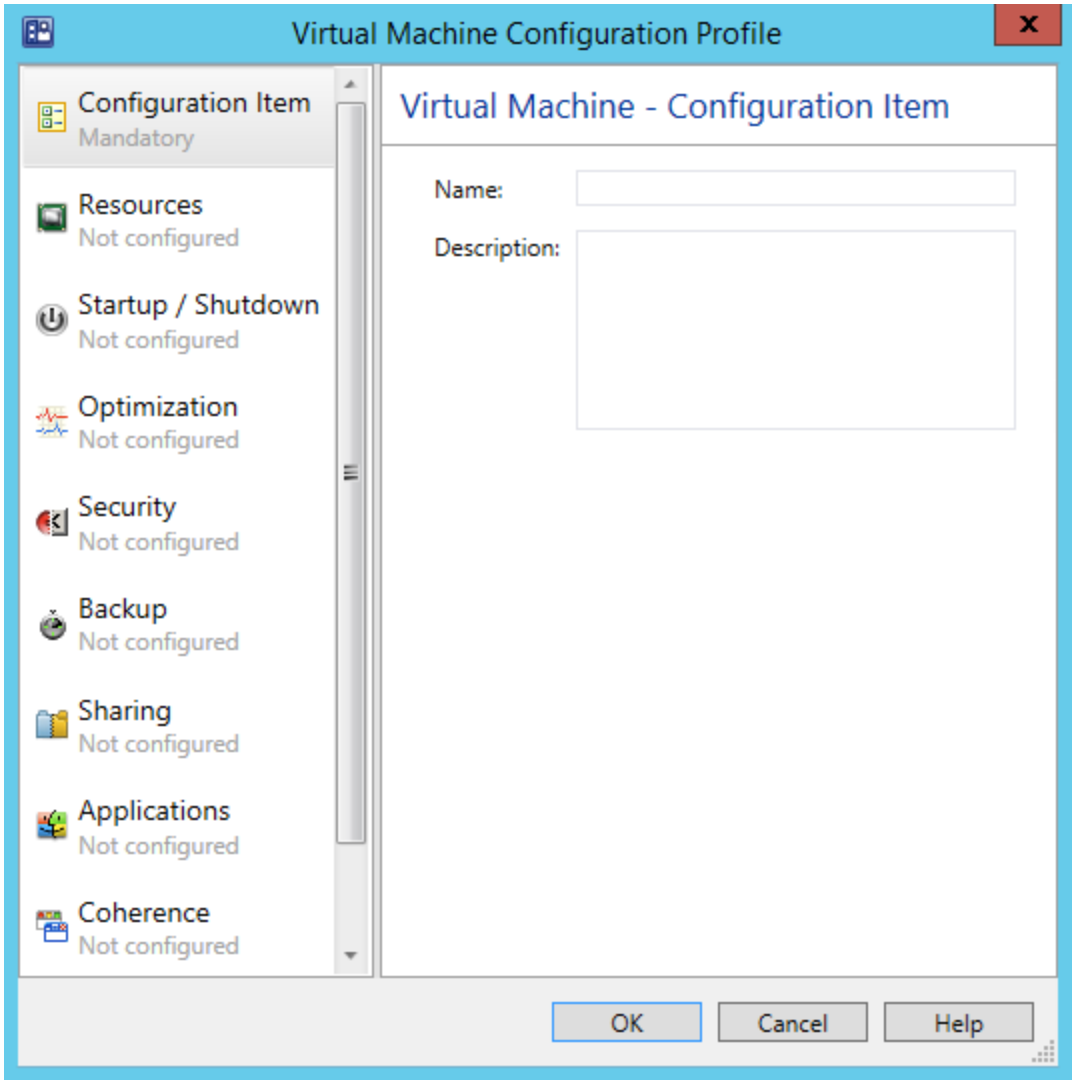
A Parallels Desktop virtual machine has numerous configuration options that can be customized according to your organization requirements. To monitor Mac computers for virtual machine configuration compliance you need to create a virtual machine configuration item specifying the desired configuration parameters.

**Note:** The settings that you specify in a virtual machine configuration item will be applied to all existing virtual machines on a Mac.

To create a virtual machine configuration item:

1. In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.
2. Right-click **Configuration Items**, point to **Create Parallels Configuration Item** and click **Parallels Virtual Machine Configuration**.

3 The **Virtual Machine Configuration Profile** dialog opens.




4 Enter a name and optional description for the configuration item.

5 To specify the virtual machine configuration options to monitor, select an item in the left pane and specify individual configuration settings in the right pane.

6 To include an option in the configuration profile and to specify its value click the ON/OFF switch to toggle it to "ON". To exclude an option, toggle the switch to "OFF". The excluded options will not be evaluated on managed Mac computers.

7 When finished, click the **OK** button to close the dialog.

To view the new configuration item in the **Configuration Items** list, press **F5**. To modify the configuration item, right-click it and choose **Edit Parallels Configuration Item**.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying configuration baseline** (p. 95) for more information.

# Using discovery and remediation scripts

In addition to configuration profiles described in the previous sections, you can assess compliance and enforce rules using scripts written in any language supported by macOS.

To use scripts, you need to create a standard Configuration Item in the Configuration Manager console. When creating a configuration item, you have an option to specify a *discovery script* and a *remediation script*. The discovery script is used to obtain the value of a setting on a Mac to be assessed for compliance. The remediation script is used to remediate a non-compliant value if needed (creating a remediation script is optional).

When a discovery script returns a value, it is assessed for compliance using the *compliance rules* defined for it. If the value is non-compliance and a remediation script exists, the value is passed to the script so that the necessary modifications can be done on the Mac. If a remediation script doesn't exist, the assessment stops and a noncompliance is reported to Configuration Manager. Each discovery script can assess a single value, but multiple scripts with their own compliance rules can be added to a given configuration item.

This section describes how to:

- Create a configuration item using the **Create Configuration Item Wizard** (p. 91)
- Create a discovery script (p. 93)
- Create a remediation script (p. 93)
- Specify the script interpreter to be used (p. 94)
- Define Compliance Rules (p. 95)

## Creating a configuration item

To use scripts to assess compliance, you need to create a standard Configuration Item.

To create a configuration item:

1. In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.
2. Right-click **Configuration Items** and then click **Create Configuration Item** in the context menu.
3. The **Create Configuration Item Wizard** opens.

Follow the wizard to create a configuration item as described below.

### General

Specify the general properties of the configuration item:

1. Specify the configuration item **Name** and an optional **Description**.
2. Select **Mac OS X** in the **Specify the type of configuration item that you want to create** list box.
3. Click **Next**.

### Supported Platforms

Select macOS versions to which this configuration item should be applicable. Please note that this selection will be ignored in the future releases of Parallels Device Management. If at that time you'll need to exclude a particular macOS version, you can create multiple Mac collections based on the macOS version criteria and then selectively deploy the configuration item to them.

### Settings

The **Settings** page is used to create a set of *settings* representing the conditions to assess for compliance on Mac computers. In our case, each *setting* will evaluate a particular value on a Mac.

To create a new setting:

1. Click **New** to open the **Create Setting** dialog.
2. In the **Create Setting** dialog, specify the setting **Name** and an optional **Description**.
3. In the **Setting type** list box, select **Script**.
4. In the **Data type** list box, select the data type of the value that this setting will evaluate on a Mac. The discovery script that you'll specify later should return a value of the same data type in the string format.
5. In the **Discovery script** section, click **Add Script**. The **Edit Discovery Script** dialog opens where you can specify the discovery script. See **Creating a discovery script** (p. 93) for the complete information.
6. If you would like to create a remediation script, click **Add Script** in the **Remediation script** section. The **Create Remediation Script** dialog opens where you can specify the remediation script. See **Creating a remediation script** (p. 93) for the complete information.
7. Once you've specified the discovery and remediation scripts, you need to define compliance rules specifying the conditions that make the value returned by the discovery script compliant on Mac computers. To define compliance rules, make sure that you are back in the **Create Setting** dialog and click the **Compliance Rules** tab. To create a new rule, click **New** to open the **Create Rule** dialog. Use the dialog to define the rule. See **Defining compliance rules** (p. 95) for the complete information. You can create more than one rule for a given configuration item setting.
8. When you are finished specifying scripts and compliance rules, click **OK** in the **Create Setting** dialog and then click **Next** on the **Settings** page of the wizard.

### Compliance Rules

The **Compliance Rules** page lists the compliance rules that you've created earlier. You can review and modify them if necessary. You can also create new rules here if needed. Click **Next** when ready.

### Summary, Progress, and Completion

Review the configuration item summary and click **Next** when ready. Wait for the configuration item to be created. Review the info on the **Completion** page and click **Close** to exit the wizard.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying configuration baseline** (p. 95) for more information.

## Creating a discovery script

A discovery script is specified using the **Edit Discovery Script** dialog, which is opened from the **Create Setting** dialog, which in turn is opened from the **Create Configuration Item Wizard** (p. 91).

The script can be written in any scripting language supported by macOS, such as Bash, Python, Apple Script, etc. See **Specifying a script interpreter** (p. 94) for additional information.

You can type (or copy and paste) the script into the **Script** edit box. If you have the script saved in a file, click the **Open** button to browse for it.

A discovery script is used to find and return a value to be assessed for compliance on a Mac. The value can be of any data type supported by Configuration Manager, but must be returned by the discovery script as a string. Write the script to obtain the value of a desired setting on a Mac and return it as a string via standard output. The returned value is evaluated using the compliance rules defined for this configuration item setting. If the value is non-compliance and a remediation script exists (p. 93), the value is passed to the remediation script for evaluation. If the remediation script doesn't exist, the assessment stops and noncompliance is reported to Configuration Manager.

Please note that a discovery script will run in macOS with root privileges. Please also note that you cannot access macOS GUI components from a discovery script. For example, you cannot open a dialog to be displayed to the Mac user.

## Creating a remediation script

A remediation script is created using the **Create Remediation Script** dialog, which is opened from the **Create Setting** dialog, which in turn is opened from the **Create Configuration Item Wizard** (p. 91).

The script can be written in any scripting language supported by macOS, such as Bash, Python, Apple Script, etc. See **Specifying a script interpreter** (p. 94) for additional information.

You can type (or copy and paste) the script into the **Script** edit box. If you have the script saved in a file, click the **Open** button to browse for it.

A remediation script is used to remediate non-compliance setting values found on a Mac. The non-compliance value is passed to the script as an input parameter after obtaining it with the discovery script and assessing it using the compliance rules. A remediation script should return 0 (zero) as a string via standard output.

When the remediation script returns, the discovery script is executed again to obtain the updated value. The value is then evaluated using the compliance rules. If the value complies, the assessment finishes with success. If the value is still non-compliance, a noncompliance is reported to Configuration Manager.

Please note that a remediation script will run in macOS with root privileges. Please also note that you cannot access macOS GUI components from a remediation script. For example, you cannot open a dialog to be displayed to the Mac user.

## Specifying a script interpreter

When creating a discovery or a remediation script, use the syntax described below to specify the interpreter that should be used to run it.

The first line of the script should begin with shebang and have the following format:

**#!** *interpreter* [*interpreter-args*] *<args-list-terminator>* [**#***comment*]

where:

- *interpreter* is the absolute path to the interpreter executable (e.g. `/bin/bash`).
- *interpreter-args* is the list of the interpreter arguments.
- *args-list-terminator* is the terminating character of the argument list. The terminator is needed for passing the result of the discovery script to the remediation script.

  Python example:

  ```
  #! /usr/bin/python -
  ```

  Bash example:

  ```
  #! /bin/bash --
  ```

- *comment* is a comment that you might want to add to the script.

## Creating compliance rules

A compliance rule defines compliance conditions for the value returned by the discovery script. The conditions are defined using the **Create Rule** dialog, which is opened from the **Create Setting** dialog, which in turn is opened from the **Create Configuration Item Wizard** (p. 91).

To create a rule, do the following in the **Create Rule** dialog:

1. Specify the rule **Name** and an optional **Description**.
2. Set the **Rule type** to **Value**.
3. Use **The setting must comply with the following rule** section to specify the rule.
4. If you specified a remediation script for this configuration item setting, you may select the **Run the specified remediation script when this setting is non-compliance** option. If this option is selected and the value is non-compliance, the remediation script will be executed and the value will be passed to it as a parameter.
5. The **Report noncompliance if this setting instance is not found** option affects the compliance or non-compliance reporting. When the script execution doesn't fail, but doesn't return any data either, the rule is not evaluated. Instead, the compliance status is determined by the state of this option as follows:
   - If the option is selected, compliance is reported.
   - If the option is cleared, non-compliance is reported.
6. Click **OK** to create the rule and close the dialog.

You can create more than one rule for a given configuration item setting. If there's more than one rule, they will be connected using the logical AND operator. Therefore, for a value to be compliant, all rules must evaluate as TRUE.

# Deploying configuration baseline

Once you've created one or more configuration items, you need to add them to a configuration baseline. Configuration baseline is a container that combines configuration items into a logical unit so they can be evaluated for compliance by Mac computers or Apple mobile devices as a group. You can add configuration items to an existing baseline or you can create a new one.

To create a configuration baseline:

1. In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.
2. Right-click **Configuration Baselines** and then click **Create Configuration Baseline** in the context menu. The **Create Configuration Baseline** dialog opens.
3. Enter the desired configuration baseline name and description.

4 Click the **Add** button and then select the configuration items that you want to add to the baseline. Click **OK** and click **OK** again.

The new configuration baseline will appear in the **Configuration Baselines** list. You can click **Refresh** on the toolbar to refresh the list.

Once a configuration baseline is created, you need to deploy it to a Mac collection.

To deploy a configuration baseline:

1 In the Configuration Manager console, right-click the baseline that you've created and click **Deploy** in the context menu.

2 In the **Deploy Configuration Baselines** dialog, click the **Browse** button.

3 In the **Select Collection** dialog, select **Device Collections** in the drop-down list box and then select the **All Mac OS X Systems** collection or **All Mobile Devices** (whichever applies) in the list. Click **OK**.

4 Back in the **Deploy Configuration Baselines** dialog, specify the desired schedule for the baseline and click **OK**.

A configuration baseline will run as scheduled for as long as it exists.

**Note:** If a baseline contains a configuration profile (as a configuration item), the profile will be evaluated on a device only once. All subsequent baseline runs will skip the evaluation of a configuration profile if it has already been evaluated and applied.

To stop the deployment of a baseline, remove the deployment from the device collection. To delete a baseline, right-click it and then click **Delete**.

# Receiving compliance settings reports

After a configuration baseline is deployed on Mac computers or Apple mobile devices, you can view the baseline compliance status report, which includes the following:

- A report for each configuration item applied on a Mac computer or Apple mobile device. Note that on Apple mobile devices, only the Configuration Profile item is supported and will be reported with an actual status. All other items (if any are included by mistake) will be reported as a failure.
- A summary report for the baseline after all configuration items are applied.

As soon as a report is generated, the Parallels Mac Client sends it to the Configuration Manager. When the Mac evaluation for compliance completes, the IT administrator can view the reports in the Configuration Manager console. If the Parallels Mac Client or a mobile device cannot establish a connection with the Configuration Manager, the reports are saved locally on the device and the transfer is resumed as soon as the connection becomes available.

To view the evaluation reports in the Configuration Manager console, you need a reporting point set up on your Configuration Manager site. If you don't have a reporting point, set it up in the Configuration Manager console using the standard Configuration Manager functionality.

To view the Compliance Settings reports:

1. In the Configuration Manager console, navigate to **Site Database** / **Computer Management** / **Reporting** / **Reports**.
2. In the report list, find the "Compliance for a computer by configuration item" report or the "Compliance for a computer by configuration baseline" report, right-click it and then click **Run** in the context menu.
3. Specify the report criteria using the provided options (computer name, configuration item name).
4. Click **Display** to view the report.

A compliance report contains the basic information about the Mac computer or mobile device and the configuration item (or configuration baseline) together with the following items describing the results of the compliance evaluation:

- **Compliance State** — describes whether the device complies with the corporate policies defined in the configuration item(s). The possible values are Compliant and Non-compliant.
- **Last Evaluation Date and Time (UTC)** — contains the last evaluation date and time.

CHAPTER 9

# Deploying Software via Package Deployment

## In This Chapter



# Overview

The software deployment feature automates the distribution of software to managed Mac computers. This Parallels Device Management feature uses the standard Configuration Manager Package deployment functionality.

Please note that Parallels Device Management supports Configuration Manager Package and Application deployment models. This section describes how to distribute software via Configuration Manager Package deployment. For Application deployment, please see **Deploying Software via Application Deployment.** (p. 103)

Parallels Device Management also supports software deployment via task sequences. For details, see **Non-operating system deployments** (p. 181).

# Creating a software package

A software package is a container for an application, file, or information that need to be applied to client Mac computers. A package also includes a program that contains instructions for how the contents of the package is to be applied on a Mac.

You create a package and a program using the standard **Create Package and Program Wizard** in the Configuration Manager console. Once the package is created, you can set additional package and program properties that are not available in the wizard. These properties can be used to better manage the package installation on a Mac computer.

To create a software package:

1 In the Configuration Manager console, navigate to **Software Library / Overview / Application Management / Packages**.

2 Click **Create Package**. The **Create Package and Program Wizard** opens.

Complete the **Create Package and Program Wizard** as described below.

### Package

On the **Package** page, specify the general package information:

1 Specify the package name and an optional description, manufacturer, language, and version information.

2 Select the **This package contains source files** option and then click **Browse** to select the folder containing the software installation image.

3 Click **Next**.

### Program Type

On the **Program Type** page, select the **Standard program** option and click **Next**.

### Standard Program

On the **Standard Program** page:

1 Specify the program name.

2 Specify the command line for the program using the following rules:

- A command line that doesn't start with the colon (:) is treated as a standard macOS shell command and is executed as-is. For example, to run the macOS installer(8) to install a .pkg package, the command line will look like this:

  ```
  installer -pkg "InstallMe.pkg" -target /
  ```

- To copy a directory from the distribution package to the Mac hard drive, use the following syntax:

  ```
  :<source_path>:<destination_path>:
  ```

  where <source_path> is the name and path of a directory inside the package, and <destination_path> is the name and path of a directory on a Mac. To reference directories inside an image file, the source path may contain the image file name (the file with the ".dmg" or ".iso" extension). For example, command line

  ```
  :firefox-8.0.1.dmg/Firefox.app:/Applications:
  ```

  will mount the firefox-8.0.1.dmg image to a temporary mount point and then copy the Firefox.app folder from that mount point to the /Applications folder on the Mac. The following example will do the same with the .iso image file

  ```
  :MySoft-image.iso/MyApp.app:/Applications:
  ```

- To run an installer command (macOS package installer tool), use the following syntax:

  ```
  :<package_path>::
  ```

  where <package_path> is the name and path of the package. When the client encounters this command, it will invoke installer(8) passing the package name to it as a parameter. For example, command line

  ```
  :MySoft/MySoft-1.0.dmg/packages/mysoft_v1.pkg::
  ```

  will mount the MySoft-1.0.dmg image to a temporary mount point, make it current directory, and execute the following command:

  ```
  $ /usr/sbin/installer -pkg "packages/mysoft_v1.pkg" -target /
  ```

  The following example will similarly mount an .iso image file:

  ```
  :MySoft/MySoft-1.0.iso/packages/mysoft_v1.pkg::
  ```

3 Specify whether you want to allow Mac users to interact with the program installation.

- To enable user interaction, in the **Run mode** drop-down list, select **Run with user's rights** or select the combination of the **Run with administrative rights** and **Allow users to view and interact with the program installation** options.
- To disable user interaction, set the **Run mode** option to **Run with administrative rights** and clear the **Allow users to view and interact with the program installation** option.

If you allow user interaction, a dialog will be displayed in macOS during program installation giving the user a choice to continue or to postpone installing the program. The message in the dialog will say whether an additional action, such as computer restart or user log-off, will be required (or may be required) after the program installation finishes. Based on this info, the user can decide whether to continue or to postpone the program installation. Please note that if a program installation is postponed, no other program can be installed before this one is installed first.

4 Click **Next**.

### Requirements

On the **Requirements** page, specify the following optional properties:

- **Estimated disk space**. Specifies the required disk space required to install the software on a target Mac. If a Mac doesn't have enough disk space, the software will not be installed on it and the Parallels Mac Client will report an error to the Configuration Manager.
- **Maximum allowed run time (minutes)**. Limits the maximum run time of the installation process. If the specified value is exceeded, the installation process is terminated and the failure is reported to the Configuration Manager.

Click **Next** and complete the wizard

Once the package is created, you can set additional package and program options that are not available in the wizard. The following subsections describe these options.

### Specifying actions to perform after the package installation finishes

You can configure the package program to restart a Mac or log off the user after the package installation finishes. Use these options when the software that you are distributing to Mac computers requires such actions to complete the installation.

To configure the program:

1. In the Configuration Manager console, select the package that you created and click the **Programs** tab at the bottom of the **Packages** workspace.
2. Select the program and click **Properties** on the toolbar. The program **Properties** dialog opens.
3. On the **General** tab, in the **After running** list, select the action that should be performed after the package installation finishes:
   - **No action required.** This is the default option. If selected, no additional action will be performed on a Mac after the package installation finishes.
   - **Configuration Manager restarts computer**. When this option is selected, a dialog box will be displayed in macOS notifying the user that the Mac must be restarted. The user can postpone restarting if needed. If the action is postponed, the user will be reminded to restart the Mac later. If there are other packages waiting to be installed on the Mac, they will be installed only after the Mac is restarted.
   - **Program controls restart**. Same as **No action required**.
   - **Configuration Manager logs user off**. A dialog box will be displayed notifying the user that they have to log off to complete the installation. The user can postpone it if needed. If the action is postponed, the user will be reminded to log off later. The Parallels Mac Client will report success to the Configuration Manager even if the user postpones logging off the Mac as long as the installation completes without errors. The Parallels Mac Client will send the detailed installation results to the Configuration Manager as soon as the user logs off and then logs on again. If there are other packages waiting to be installed on the Mac, the installation will begin only after the user logs off and then logs on again.

## Sending the package to a distribution point

To distribute a package to Mac computers, a copy of the package data must be sent to a distribution point from which the clients can download it.

To send a copy of the package to a distribution point, right-click the package and click **Distribute Content** in the context menu. Use the **Distribute Content Wizard** to specify a distribution point to which you want to send the package.

## Deploying the software

After you've sent the package to a distribution point, you can deploy the software.

To deploy the software:

1. In the Configuration Manager console, right-click the package and then click **Deploy** in the context menu. The **Deploy Software Wizard** opens.
2. On the **General** page, click the **Browse** button (next to the **Collection** field) and select the collection containing the desired Mac resources (e.g. **All Mac OS X Systems**). Click **OK** and then click **Next.**
3. On the **Content** page, verify the distribution point info and click **Next**.
4. On the **Deployment Settings** page, make sure that the **Purpose** option is set to **Required**. If it's set to **Available**, the package will be ignored by the Parallels Mac Client on a Mac computer.
5. On the **Scheduling** page, do not select any of the available **Schedule** check-boxes. Instead, click **New** to specify the assignment schedule.
6. In the **Assignment Schedule** dialog, specify one or more schedules and click **OK**.
7. Back on the **Scheduling** page, use the **Rerun behavior** drop-down list to select a desired behavior. This is important if you want to run the installation multiple times according to a schedule.
8. Use the default values on the rest of the wizard pages and complete the wizard.

The software will be advertised to Mac computers in the specified collection and will be installed according to the specified assignment schedule(s) and rerun behavior.

# Viewing the package status

While software distribution is in progress, the Parallels Mac Client running on a target Mac computer will report to the Configuration Manager the following events:

- **Download started** — the event is reported when the client on a Mac begins downloading the software.
- **Download finished** — the event is reported when the package download is complete.
- **Download failed** — the event is reported if the package download fails.

To view the status of a package:

1. In the Configuration Manager console, navigate to **Monitoring / Overview / System Status / Deployments**.
2. In the right pane, right-click the package and then click **View Status** in the context menu.
3. Use the **Deployment Status** view to examine the deployment status.

CHAPTER 10

# Deploying Software via Application Deployment

## In This Chapter



# Overview

Applications are similar to Configuration Manager packages but contain more information to support smart deployment. Parallels Device Management natively supports the Application Management feature of Configuration Manager and allows you to deploy applications on Mac computers.

Please also note that in addition to Packages and Applications, Parallels Device Management supports software deployment via task sequences. For details, see **Non-operating system deployments** (p. 181).

The steps to create and deploy a Mac application are:

1. Choose the installation type (silent or interactive) (p. 104)
2. Prepare a Mac application for Configuration Manager (p. 105)
3. Create a Configuration Manager application (p. 105)
4. Configure the deployment type (p. 107)
5. Deploy the application (p. 108)

The following sub-sections describe how the application is installed on a Mac and how to use the Parallels Application Portal.

- Installing the application on a Mac (p. 110)
- Using Parallels Application Portal (p. 111)

# Choose the installation type

When preparing a Mac application for deployment, you can configure it to be installed on a Mac silently (transparently to a Mac user) or you can allow the user to interact with the installation process.

### Silent installation

If you configure the application to install silently, it will be delivered to a Mac and installed without giving the user any control over the installation process. The only operation that the user will be asked to confirm is restarting the Mac if it is required by a particular application. The options that must be set in order to perform a silent installation are highlighted in the corresponding topics describing the application deployment steps.

### Interactive installation

An interactive installation informs the Mac user that the application is available for installation and, depending on the deployment configuration, gives the user full or limited control over the installation process.

When preparing an application for interactive installation, you can specify the following options:

- An application can be either required to be installed or the user can be given a choice whether to install it or not.
- The application installer can be displayed on the screen allowing the user to control the installation process, or the installer can run in the background thus performing an unattended installation. In both scenarios the user can choose whether to run the installer as soon as the application is available or to postpone it to a later time.

The options that must be set in order to perform an interactive installation are highlighted in the corresponding topics describing the application deployment steps.

### Parallels Application Portal

When an application is configured to be deployed interactively as described above, it will be added to the Parallels Application Portal on a Mac, which is a macOS application that allows a Mac user to view and install applications made available to them by their system administrator. Parallels Application Portal is described in detail in the **Using Parallels Application Portal** section (p. 111).

# Prepare a Mac application for Configuration Manager

Before you can deploy a native macOS software package (.app, .dmg etc.) in Configuration Manager, you must use the **CMAppUtil** tool to convert it to the **.cmmac** format that Configuration Manager understands. The **CMAppUtil** tool is provided by Microsoft and is included in the Mac client msi package. Use the instruction below to download the tool and use it to do the conversion.

To download the Mac client msi package:

1. Download the **ConfigmgrMacClient.msi** file from the Microsoft Download Center using the following URL: https://www.microsoft.com/en-us/download/details.aspx?id=100850
2. Run the downloaded file on your Windows computer to extract the **macclient.dmg** file.
3. Copy the **macclient.dmg** file to a Mac computer.
4. Double-click the file to see its contents. Extract the Tools folder from the file by dragging and dropping it to a folder on your Mac.

**CMAppUtil** supports the .dmg, .pkg, .mpkg, .app file formats.

To convert a macOS application package to the **.cmmac** format:

1. Copy the macOS package to the folder where you extracted to **Tools** folder.
2. Navigate to the **Tools** folder and enter the following command-line:

   **./CMAppUtil** *<properties>*

   For example, to convert an Apple disk image file named **MySoftware.dmg** stored in the user's home folder to the **.cmmac** format:

   **./CMApputil –c /Users/** *<User Name>* **/MySoftware.dmg -o /Users/** *<User Name>*

   The command above creates a **.cmmac** installation file compatible with Configuration Manager. The **-c** option specifies the source file being converted. The **-o** option specifies the output path. For the complete list of options, please consult the Microsoft **CMAppUtil** documentation.

When you have the **.cmmac** file, copy it to a network share where it can be accessed from the Configuration Manager console.

# Create a Configuration Manager application

To create a Configuration Manager application using the **Create Application Wizard**:

1. In the Configuration Manager Console, navigate to **Software Library** / **Application Management**.

2. Right-click **Applications** and click **Create Application**. This will open the **Create Application Wizard**.
3. On the **General** page, select **Mac OS X** in the **Type** drop-down list.
4. Click **Browse,** enter the network location of the `.cmmac` file that you've prepared earlier, select the file and click **Open**.
5. Click **Next**. Review the information on the **Import Information** page and click **Next**.
6. On the **General Information** page, specify the application name, and optionally publisher, and version. Click **Next**.
7. Review the application settings on the **Summary** page and click **Next**.
8. Wait until the application is created and then click **Close** to close the wizard.

The new application will appear in the **Applications** list in the Configuration Manager console**.**

### Specify application properties for Parallels Application Portal

The application properties described here determine how the application will be displayed in the Parallels Application Portal on a Mac. If you would like to configure the application to be installed silently (you will choose the installation type later), you may skip this sub-section.

To set up the application properties for the Parallels Application Portal:

1. Right-click the application that you've created in the previous step and click **Properties** in the context menu. This will open the application properties dialog.
2. Click the **Application Catalog** tab and set the following properties:
   - **Selected language** — select the language from the drop-down list. Click **Add/Remove** to add additional languages if needed.
   - **Localized application name —** specify the localized application name.
   - **User categories — c**lick **Edit** to specify user categories that the users of Parallels Application Portal can use to filter and sort the available applications. The **Edit** button opens the **User Categories** dialog. Select an existing category or click **Create** to create a new category.
   - **Icon —** click **Browse** to select an icon for this application.
   - **Display this as a featured app and highlight it in the company portal —** if you select this option, the application will be listed in the **Featured Applications** list in Parallels Application Portal.
3. Click **OK** to close the **Properties** dialog.

# Configure the deployment type

The deployment type for the application is created automatically when you create the Configuration Manager application. This section describes some of the deployment type properties that you may want to modify.

To modify the properties of the deployment type:

1 Select the **Deployment Types** tab at the bottom of the **Applications** workspace.

2 Right-click the deployment type and click **Properties** in the context menu.

3 The <*application_name*> **- Mac OS X Properties** dialog opens.

Use the instructions below to modify the deployment type properties as needed.

## Specify the installation command line

To specify the command that you want to use to install, and optionally uninstall, the application on a Mac, click the **Programs** tab. The **Installation program** field is used to specify the command line. The field is populated automatically and should already contain the installation command for the application. You can modify the command line as needed.

If you've configured the application for the Parallels Application Portal, you can optionally specify an uninstallation command for it. This will enable the **Remove** button in the Application Portal and will provide a convenient method for removing an application from a Mac. To add the uninstallation command line, use the following syntax:

**:**<*Installation command*>**:**<*Uninstallation command*>**:**

The <*Installation command*> and <*Uninstallation command*> parts should contain the installation and uninstallation commands respectively.

As an example, the following command line contains the installation and uninstallation commands for Firefox (please note the colon characters, which are required):

:/usr/bin/ditto "Firefox.app" "/Applications/Firefox.app":rm -rf "/Applications/Firefox.app":

When you add the uninstallation command to the command line, the **Remove** button in the Parallels Application Portal becomes available once the application is installed on a Mac. If you don't include an uninstallation command, the **Remove** button will be disabled for the given application.

## Specify the mandatory Mac restart option

To force a mandatory Mac restart after the application is installed on it, click the **User Experience** tab. In the **Action** drop-down list, select the action from the following options:

- **No action** — The Mac will be restarted only if the application installer requires it.
- **Configuration Manager client will force a mandatory device restart** — The Mac will be restarted regardless of whether the application installer requires it or not.

### Specify a detection method

The **Detection Method** tab page allows you to specify how Configuration Manager determines whether this deployment type is already present on a Mac. This information is automatically imported when you convert the macOS installation image to a **.cmmac** file.You can modify the imported information, if needed, by editing the existing clause or creating a new one.

To modify or create a clause:

1. On the **Detection Method** tab page, select the existing clause and click **Edit Clause** (or click **Add Clause**).
2. Select the **Setting Type**. The available options are **Application Bundle** and Package **ID:**
   - For **Application Bundle**, specify **Application bundle ID**, **Data Type** (**String** or **Version**), **Operator,** and **Value**.
   - For **Package ID**, specify **Package ID**, **Operator**, and **Value**.
3. Click **OK** to save the changes and close the dialog.

### Specify system requirements

The **Requirements** tab page allows you to specify system requirements that must be met to allow the application to be installed. The only requirement that can be currently specified is the macOS version.

To specify the macOS version requirement:

1. On the **Requirements** tab page, click the **Add** button.
2. In the **Category** drop-down list, select **Device**.
3. In the **Condition** list, select **Operating system**.
4. In the macOS tree, select one or more macOS versions. If you check **Select all**, all existing and all future macOS versions will satisfy the requirement.
5. Click **OK** to save the changes and close the dialog.

## Deploy the application

After you've created the Configuration Manager application and configured the deployment type, you need to deploy the application to a Mac collection.

To deploy the application:

1. Right-click the application and click **Deploy** in the context menu. This will open the **Deploy Software Wizard**.
2. On the **General** page, click **Browse** to select the target Mac collection.
3. In the **Select Collection** dialog, select **Device Collection** in the drop-down list, and then select the target collection (e.g. **All Mac OS X Systems**). Click **OK**.
4. Click **Next**.
5. On the **Content** page, click **Add** to add a distribution point that will host this content. Select a distribution point and click **OK**.
6. Click **Next**.
7. On the **Deployment Settings** page, in the **Action** drop-down list, select **Install**.
8. In the **Purpose** list, select **Available** or **Required:**
   - If you select **Available**, the application will appear in the Parallels Application Portal on a Mac as available for installation, but the user will not be required to install it.
   - If you select **Required**, the user will be required to install the application. If you want the application to be installed silently, you must select this option and also select the **Hide in Software Center and all notifications** option described in step 12 below.
9. Click **Next**.
10. On the **Scheduling** page, specify the schedule at which this application should be available to Mac users.

    If you've selected the application **Purpose** as **Required** on the previous page (step 8 above), you need to specify the **Installation deadline** for the application. The following deadline options are available:
    - **As soon as possible** — Mac users will be required to install the application as soon as it is available. If a user fails to install the application right away, he/she will be reminded again in 24 hours. If the application is still not installed after that, it will be installed automatically.
    - **Schedule at** — Mac users will be required to install the application before the date and time specified here. If a user fails to install the application, it will be installed automatically.
11. Click **Next**.
12. On the **User Experience** page, select a notification type in the **User notification** drop-down list. Depending on the option selected, the following will happen when the application is ready to be installed on a Mac:
    - **Display in Software Center and show all notifications** — The user will be asked to install the application and will have an option to start or postpone the installation. If the application is configured as **Available** (i.e. not required, see step 8 above) the user will have a choice not to install it. The application will be added to the Parallels Application Portal where the user will be able to install it later. The installer graphical user interface will be displayed to the user providing full control over the installation process. When the installation is finished, the user will be asked to reboot the Mac if necessary.

- **Display in Software Center and only show notifications for computer restarts** — The application will be added to the Parallels Application Portal where the user will be able to install it later. No dialogs of any kind will be shown to the user.
- **Hide in Software Center and all notifications** — The user will not be informed that the application is available for installation. The installation will be performed completely silently and transparently to the user. The application will not be added to the Parallels Application Portal. If the installation requires Mac restart, the user will be asked to restart it and will be given an option to postpone restarting.

**13** Complete the wizard using the default values and close it when done.

Read on to learn how the application can be installed on a Mac after it's been deployed.

# Installing the application on a Mac

When the application becomes available for installation on a Mac, the following will happen depending on the installation type deployment configuration options.

### Installation is optional

If the application is not required (the **Deploy Software Wizard** > **Deployment Settings** > **Purpose** is specified as **Available)**, a dialog will be displayed to the user describing the application and providing the following choices:

- **Show in Application Portal** — Clicking this button will open the Parallels Application Portal where the user can view the application and install it if desired.
- **Install now** — Clicking this button will download the application and will run the application installer. The installer GUI will be displayed or hidden depending on the setting specified on the **User Experience** page of the **Deploy Software Wizard**.
- **Close** — Clicking this button will close the dialog. The user will be able to install the application later from the Application Portal.

### Installation is required

If the application is required (the **Deploy Software Wizard** > **Deployment Settings** > **Purpose** is specified as **Required)** and an interactive installation type was specified, a dialog will be displayed to the user with the following options:

**Postpone** — This button allows the user to postpone the installation. The **Remind me in** drop-down list allows the user to select the postponement period.

Depending on the installation deadline setting (set in the **Deploy Software Wizard** > **Scheduling** page**)**, the following rules apply:

- If the policy was downloaded prior to the installation deadline, the deadline will stay in effect.

- If the policy was downloaded after the deadline has passed, the effective deadline will be set to the time of the policy download plus 24 hours.

**Install now** — Clicking this button will close the dialog and will run the application installer.

### Installation is silent

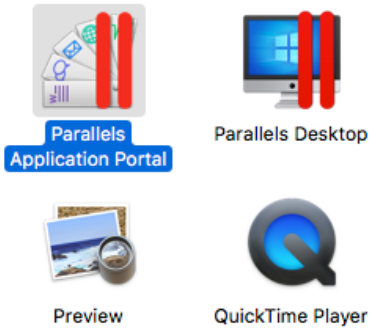
If the installation type was specified as silent (the **Deploy Software Wizard** > **User Experience page** > **Hide in Software Center and all notifications** option was selected), no message asking the user to install the application will be displayed, and the installation will be performed silently as soon as the policy is delivered to a Mac.

In all three scenarios above, after the application is installed, the user will be asked to reboot the Mac if the installer requires it or if the **Action** on the **User Experience** page of the **Mac OS X Properties** dialog is set to force a mandatory restart.

# Using Parallels Application Portal

Parallels Application Portal is a macOS application included in the Parallels Device Management for Configuration Manager package. The application is installed on a Mac when Parallels Mac Client is installed on it.

To start Parallels Application Portal on a Mac, navigate to **Finder** > **Applications** and double-click **Parallels Application Portal**.




Parallels Application Portal allows the Mac user to:

- View and install applications made available to them by their system administrator.
- View and remove installed applications.
- Filter the applications by category and publisher.

For an application to be listed properly in the Parallels Application Portal, it must be configured and deployed as described in **Deploying Software via Application Deployment** (p. 103).

When Parallels Application Portal starts, it should contain the list of installed and available applications. If a Mac is not assigned to a Configuration Manager site, the application list will be empty.

The **Parallels Application Portal** window has the following elements:

- **All Applications** tab — Lists all application, including installed applications and applications that are available for installation. If at least one application was configured as "featured", the list will be split into two parts: **Featured Applications** and **Other Applications**. An application can be configured as "featured" on the **Application Catalog** tab page of the *<application_name>* **Properties** dialog (p. 105). If Configuration Manager has multiple versions of the same application that supersede each other, only the top application will be displayed unless the system administrator has specified the supersedence relationship on the **Supersedence** tab page of the *<application_name>* **Properties** dialog in the Configuration Manager console.
- **Installed Applications** tab — Lists applications that are installed on this Mac.
- **Categories** list — Contains software categories that the user can select to filter the application lists.
- **Publishers** list — Contains the names of software vendors that the user can select to filter the application lists.

- **Install** button — Displayed for applications that are available for installation. Clicking this button will download an application to the Mac and install it.
- **Remove** button — Displayed for an application already installed on a Mac. Allows the user to remove the application from the Mac. Please note that this button will only be available for applications that were configured in Configuration Manager as "Available" (i.e. optional, as opposed to required) and for which the uninstallation command line was specified. For more info about the installation/uninstallation command line, see **Configuring the deployment type** > **Specify the installation command line** (p. 107).

# Uninstalling applications

To uninstall an application that was installed earlier, use the same Configuration Manager Application Deployment functionality.

To uninstall an application:

1. If the application you want to uninstall already exists as a Configuration Manager application, proceed to step 2 below. If not, create an application in Configuration Manager the same way as described earlier in this section (p. 105).
2. Configure the deployment type (p. 107) and specify the uninstallation command for the application in the **Programs** > **Installation program** field.
3. Deploy the application using the **Deploy Software Wizard (p. 108).** While doing so, specify the following:
   - Select **Uninstall** in the **Deployment Settings** > **Action** drop-down list.
   - For a silent uninstallation, select **Required** in the **Purpose** field. Note that at the time of this writing, **Required** is the only supported option.
   - Specify **Scheduling** and **User experience** settings as per your requirements.

When the policy is applied to a Mac computer, the application will be uninstalled at the time specified in the **Deploy Software Wizard** > **Scheduling** > **Installation deadline** setting.

### Removing an application that is already deployed

If the application that you want uninstalled from specific devices still has an active deployment with an action of **Install**, you can do one of the following:

- Remove the **Install** deployment from the entire device collection.
- Exclude desired devices from the device collection that has the **Install** deployment.

When one of the above is done, you'll be able to deploy the application with an action of **Uninstall**.

### Uninstallation of applications which were not installed via Parallels Device Management

Using the functionality described above, you can also uninstall applications that were not installed via Parallels Device Management. If a user installed an application on their own, and if it's the same application that you are deploying for uninstallation, it will be uninstalled.

### Visibility of the deployment with an action of Uninstall in Parallels Application Portal

A deployment with an action of **Uninstall** is visible in the Parallels Application Portal only if both of the following requirements are met:

- The deployment is active and does not conflict with the deployment with an action of **Install**.
- The deployed application is installed on a target Mac computer.

### Priorities of Install and Uninstall deployments which exist simultaneously

If an application is deployed twice to a device, once with an action of **Install** and once with an action of **Uninstall**, the application deployment with an action of **Install** will take priority. Note that this rule is only true if both deployments have a purpose of **Required**. If one of the deployments is configured as **Available**, the **Required** deployment takes priority. The following table lists all possible deployment combinations and the outcome:

| Deployments for an application that exist simultaneously | Deployment that takes priority |
|---|---|
| Install (Available) + Install (Required) | Equal (both are carried out) |
| Install (Required) + Uninstall (Required) | Install (Required) |
| Install (Available) + Uninstall (Required) | Uninstall (Required) |

CHAPTER 11

# Deploying Apple VPP Apps

Parallels Device Management for Configuration Manager v8.0 and newer includes support for Apple Volume Purchase Program (VPP). Using this functionality you can deploy licensed AppStore applications on Mac computers and Apple mobile devices and automatically track the number of consumed licenses.

## In This Chapter



# Prerequisites

To deploy Apple VPP apps in Configuration Manager, the following prerequisites must be met:

- Parallels IBCM/MDM Proxy must be installed and configured for MDM. Also, the Apple VPP support must be configured in Parallels Device Management. For details, please see **Parallels Device Management for Configuration Manager Deployment Guide**, the **Deploying IBCM/MDM Proxy** chapter.
- If deploying VPP apps on Mac computers, the computers must be enrolled in MDM. See **Enrolling Mac Computers in Configuration Manager** (p. 18).

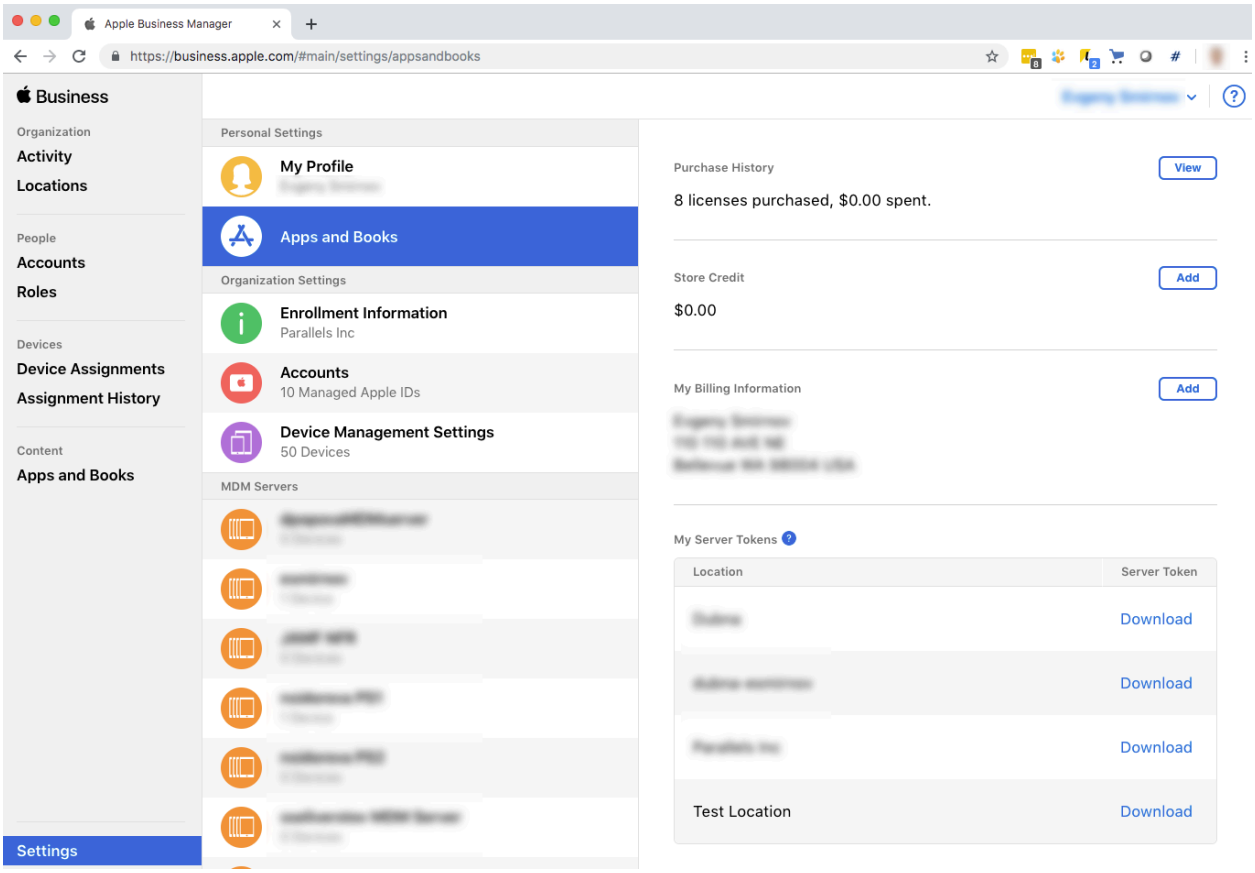
# Configuring Apple VPP support

If you plan to deploy Apple VPP apps via Configuration Manager, you need to add one or more VPP tokens to Parallels Device Management.

To add a VPP token:

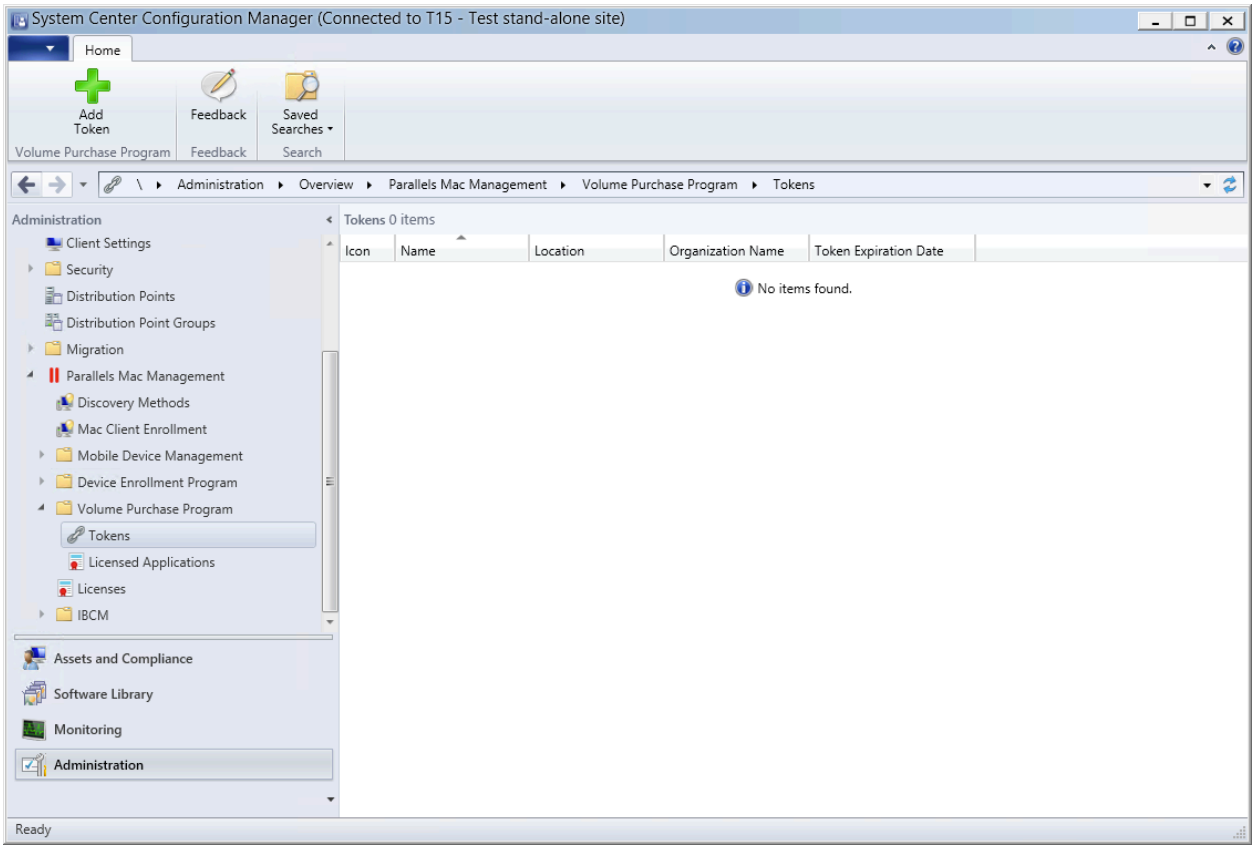
1 In a web browser, enter the Apple Business Manager URL: `business.apple.com`

2 Once logged in, chose a location (or create a new one). The screenshot below shows a sample Apple Business Manager home page that has the **Test Location**, which we'll use as an example:

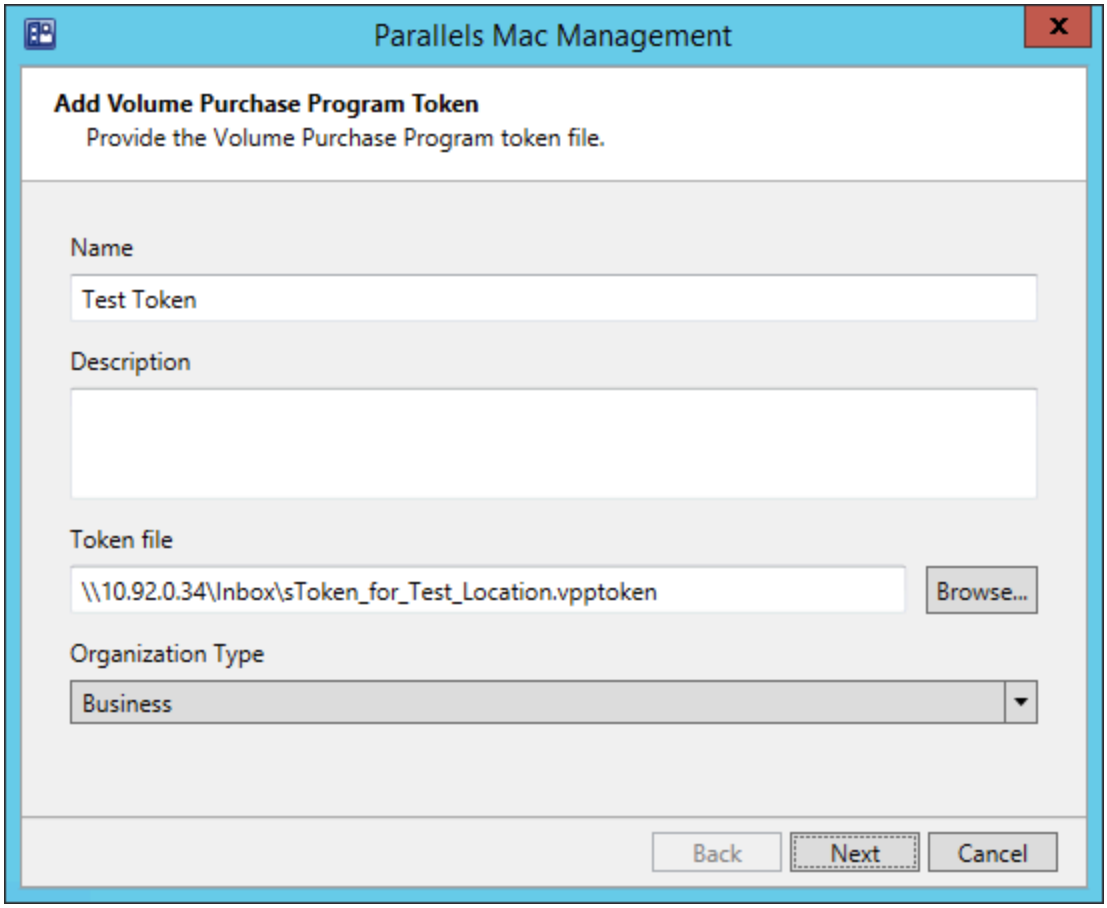



3 Click the **Download** link next to the location name to download the VPP token and save it locally.

**4** Open the Configuration Manager console and navigate to **Administration** / **Parallels Device Management** / **Volume Purchase Program** / **Tokens**:



5 Click **Add Token** on the toolbar. The **Add Volume Purchase Program Token** wizard opens.

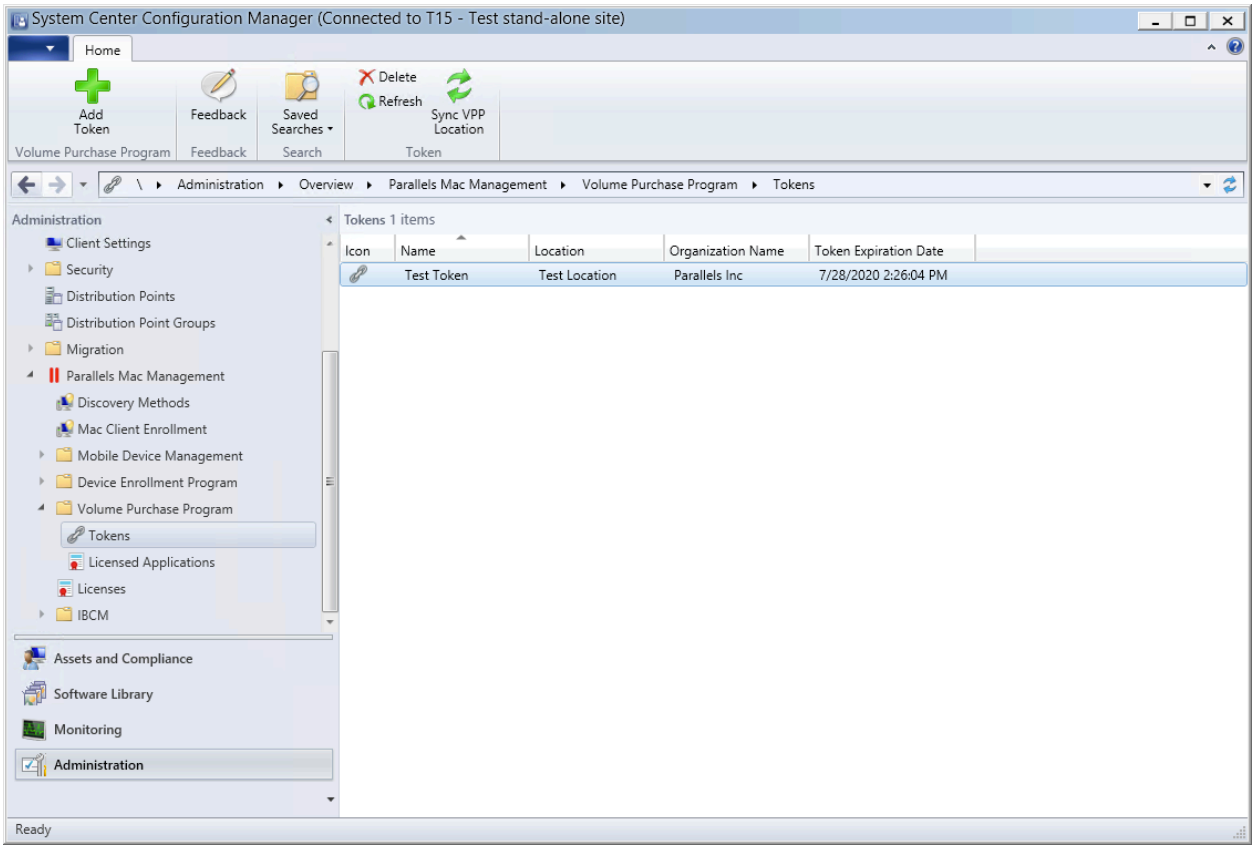



6 On the first page of the wizard specify a name for the token and an optional description.

7 Click the **Browse** button and select the token file that you've downloaded earlier from Apple Business Manager.

8 Click **Next**. You will see a page with a progress bar of the token import process. Wait until it's completed and click **Finish**.

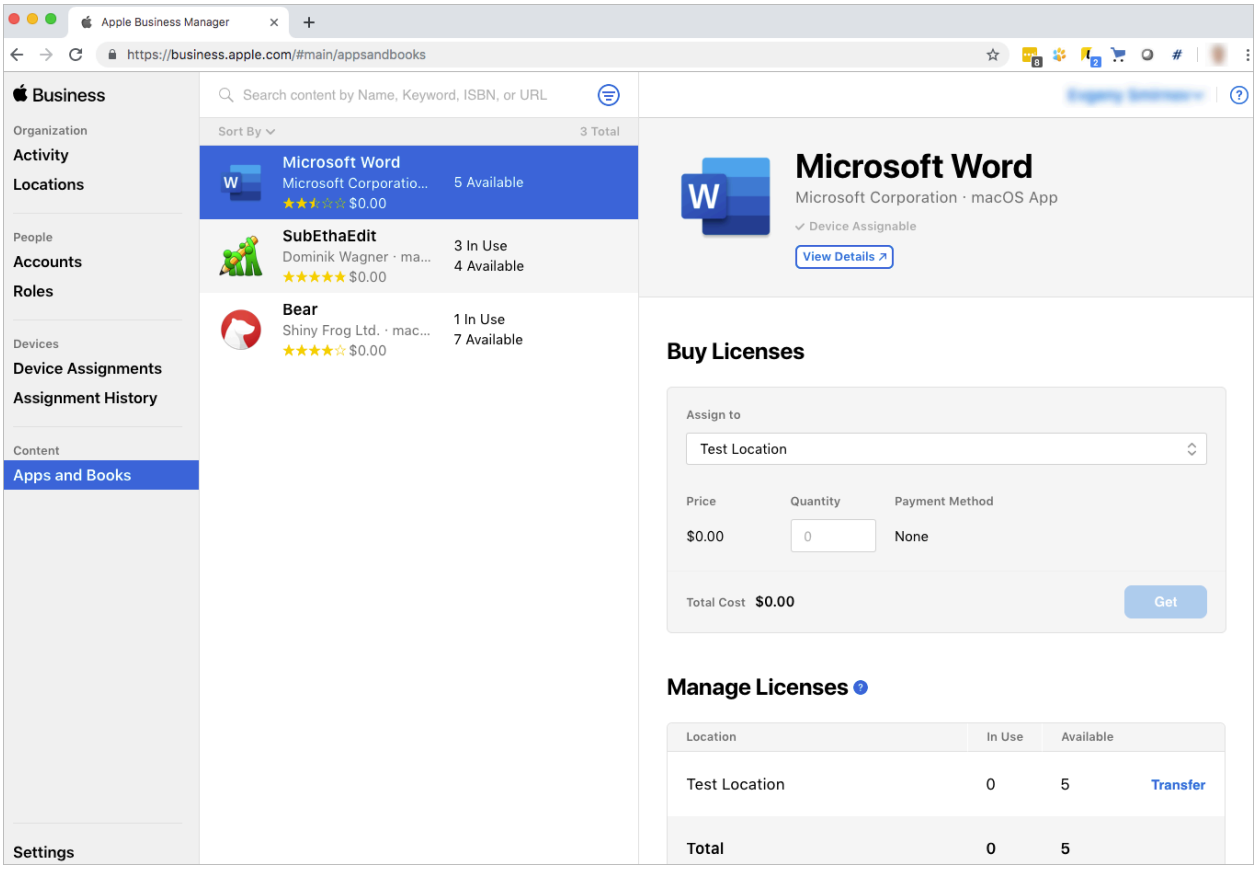
**9** The newly added token should now appear in the Configuration Manager console:




# Adding an application to Apple Business Manager

Before deploying Apple VPP apps, you need one or more of them in the Apple Business Manager location that you are using. If you don't have any applications, you need to purchase one or more to continue. If you have applications in other locations, you can transfer some licenses from them to this location.

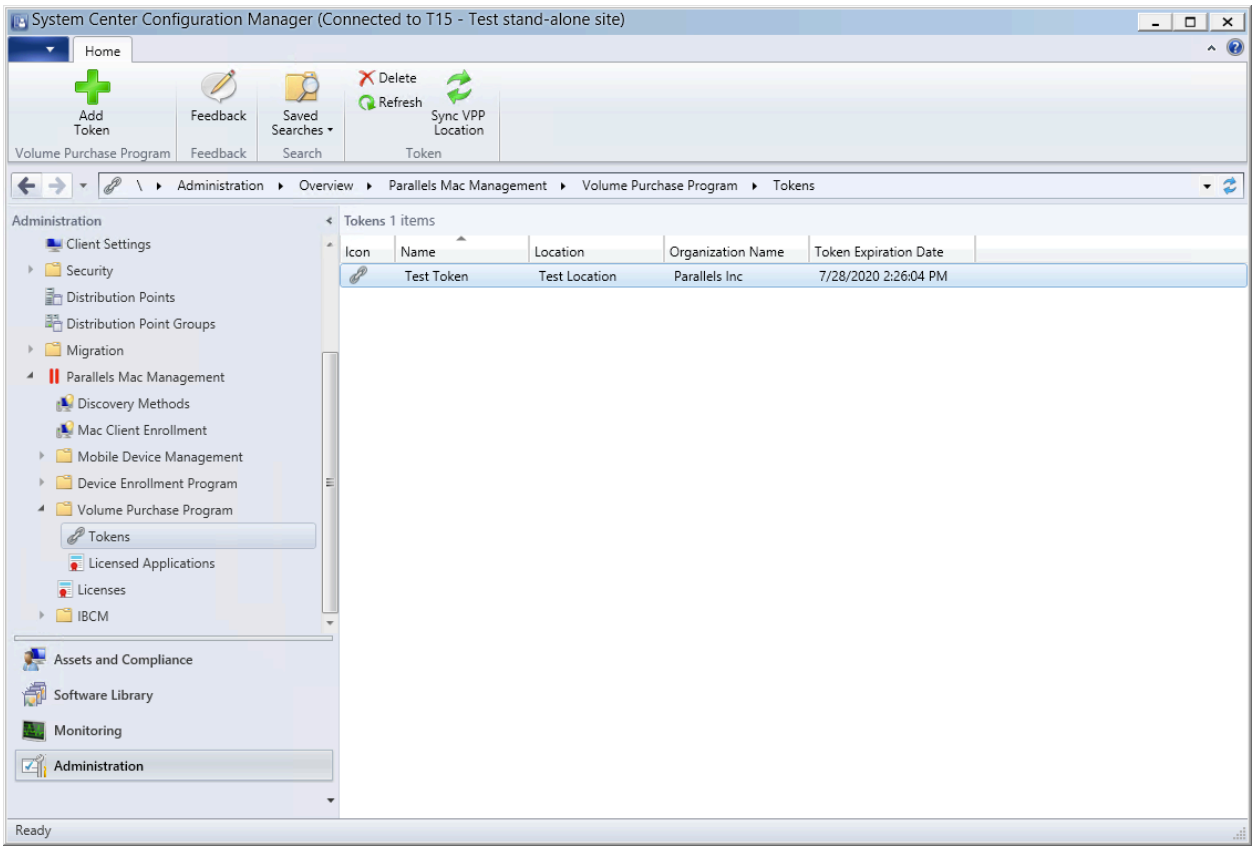
The following screenshot illustrates an application (Microsoft Word) as a VPP application in Apple Business Manager:



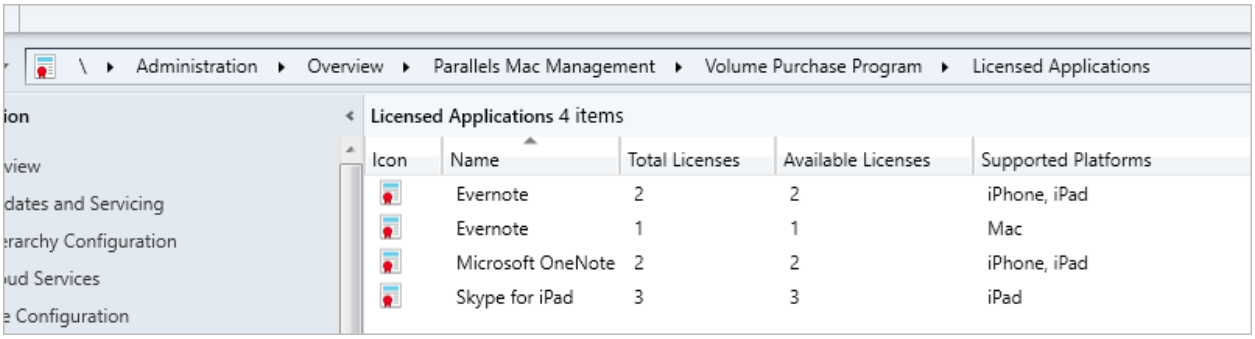

Please note that if you added an application to your location *after* adding the token to the Configuration Manager, the VPP information needs to be synchronized. Configuration Manager performs this synchronization periodically, so it will not happen immediately. If you don't want to wait, you can manually synchronize the VPP information as follows:

1 Navigate to **Administration** / **Parallels Device Management** / **Volume Purchase Program** / **Tokens**.

**2** Select the token for your location and click **Sync VPP Location** on the toolbar:




You should now see your VPP application(s) in the Configuration Manager console in **Administration** / **Parallels Device Management** / **Volume Purchase Program** / **Licensed Applications**:



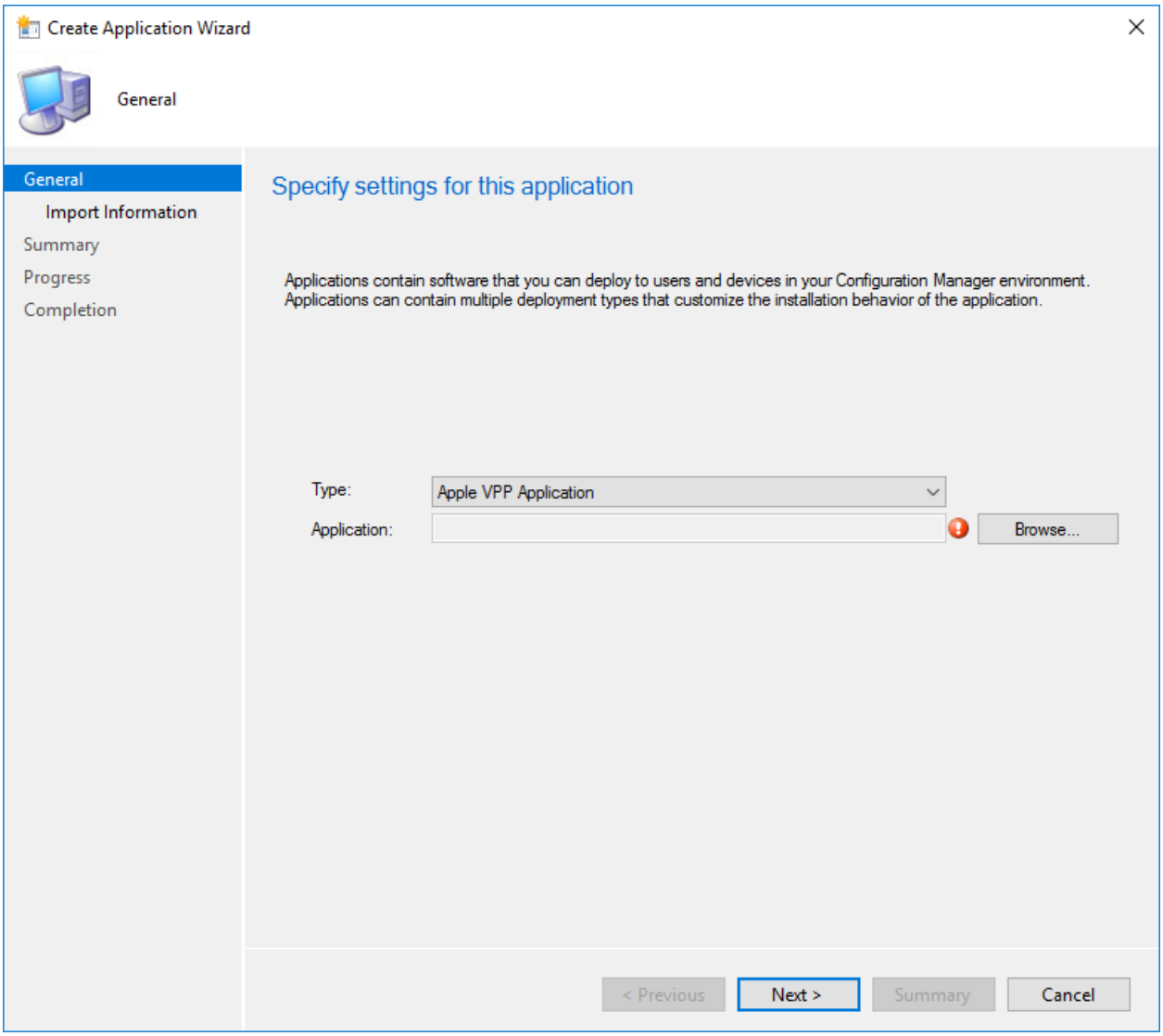

# Creating an application

Before you can install a VPP application on managed devices, you need to add the application to the software library in Configuration Manager. This is done via the **Create Application Wizard**.

To create an application in Configuration Manager:

1 In the Configuration Manager console, navigate to **Software Library** / **Overview** / **Application Manager** / **Applications**:

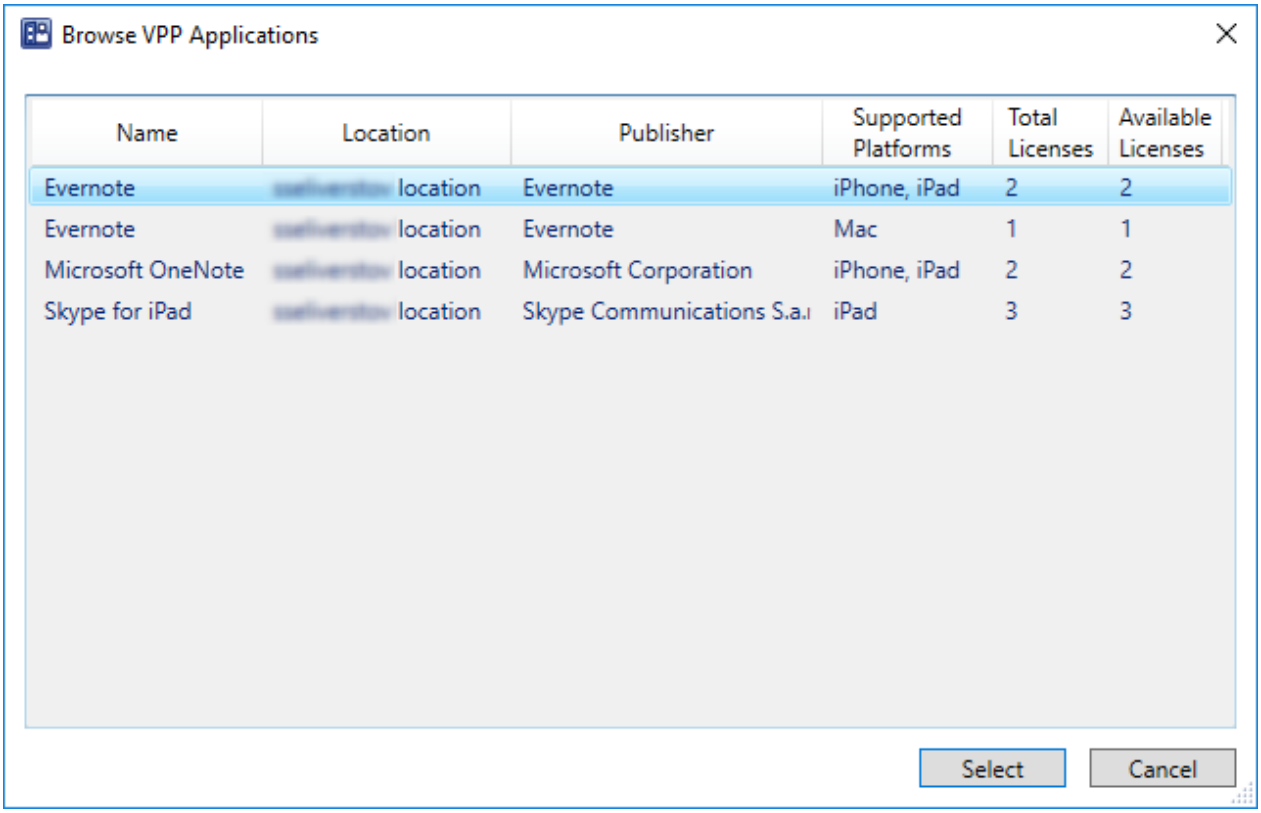
2 Click **Create Application** on the toolbar. The **Create Application Wizard** opens:




3 On the **General** page, in the **Type** drop-down list, select **Apple VPP Application** (see the screenshot above). Select this application type for both, macOS and iOS/iPadOS apps. See the note below for the information about the application type that was used in the past.

> **Note:** The older **Apple VPP Application for macOS** type that was used prior to Parallels Device Management v9.0 is not supported on Apple mobile devices and will be deprecated in future versions of Parallels Device Management. When creating applications for macOS or iOS/iPadOS with Parallels Mac Management v9.0 and newer, always use the **Apple VPP Application** type. Existing applications with the older type can still be deployed on Mac computers for the time being. All new applications (and specifically apps for mobile devices) must be of type **Apple VPP Application**.

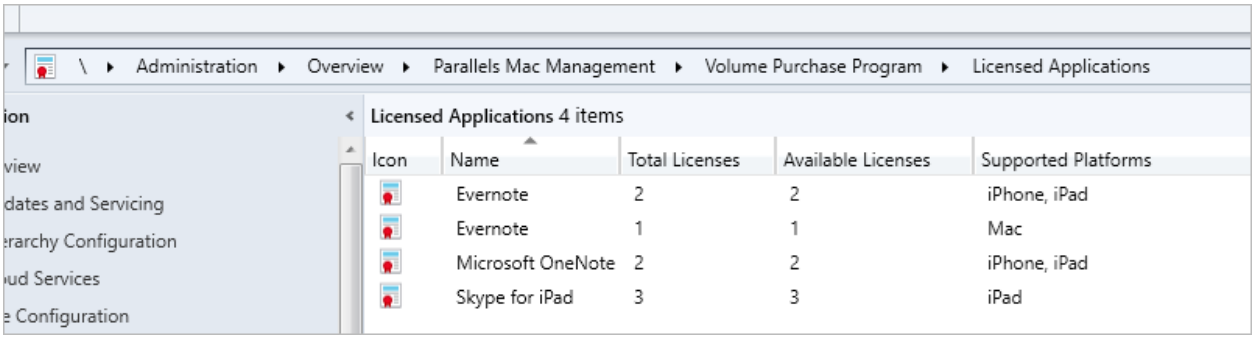
4 Click the **Browse** button. This opens the **Browse VPP Applications** dialog containing the list of VPP applications for which you have licenses. The value in the **Supported Platforms** column indicates whether it's a Mac app or a mobile device app. Depending on the target platform, choose an application accordingly.



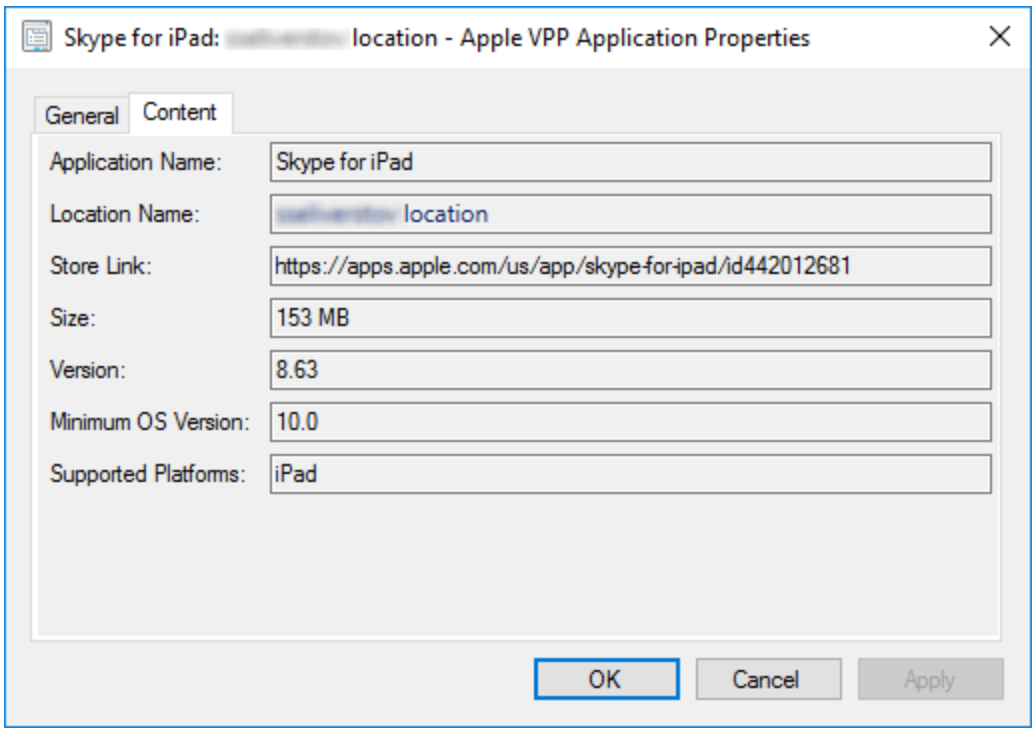

5 After selecting an application, click the **Select** button. The application information is obtained from VPP data and will be used in the subsequent wizard pages. For the simplest scenario you can keep the imported information and simply click **Next** on every subsequent page.

6 On the **Completion** page (the last page of the wizard) verify that the application was created successfully and click **Close** to exit the wizard:

When the wizard is closed, the application that you've just created will be displayed in the Configuration Manager console:



To see the deployment type properties, click the **Deployment Types** tab (at the bottom of the **Applications** pane). Right-click on a deployment name, and click **Properties**. This will open the following dialog with some additional application information:




# Deploying the application

After creating an application in Configuration Manager, you need to deploy it. This is done using the regular Configuration Manager deployment process, which is described in **Deploying Software via Application Deployment** (p. 103).

The deploy the application:

1. In the Configuration Manager console, right-click the application and click **Deploy**. The **Deploy Software Wizard** opens
2. On the **General** page, specify a target device collection if needed and click **Next**.
3. On the **Deployment Settings** page, select **Install** in the **Action** field. The **Purpose** field selection depends on the target device type:
   - Mac computers: select **Available** or **Required** according to your needs.
   - Apple mobile devices: select **Required**. Note that you must select **Required** for mobile devices.

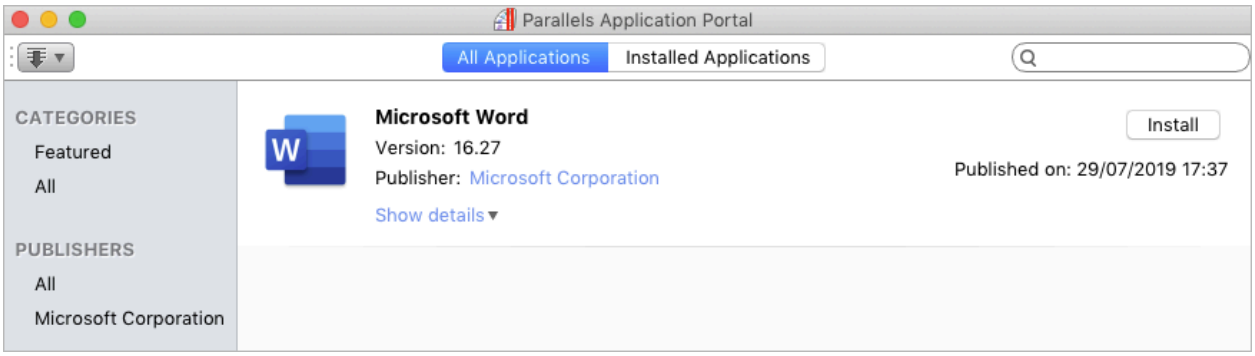
4 For the simplest scenario, you can keep default settings on all subsequent pages of the wizard (or you can modify some of them if needed). Please note that **User notifications** setting on the **User Experience** page are not applicable to applications deployed on Apple mobile devices and will be ignored.

5 Complete the wizard and close it.

# Installing the VPP application

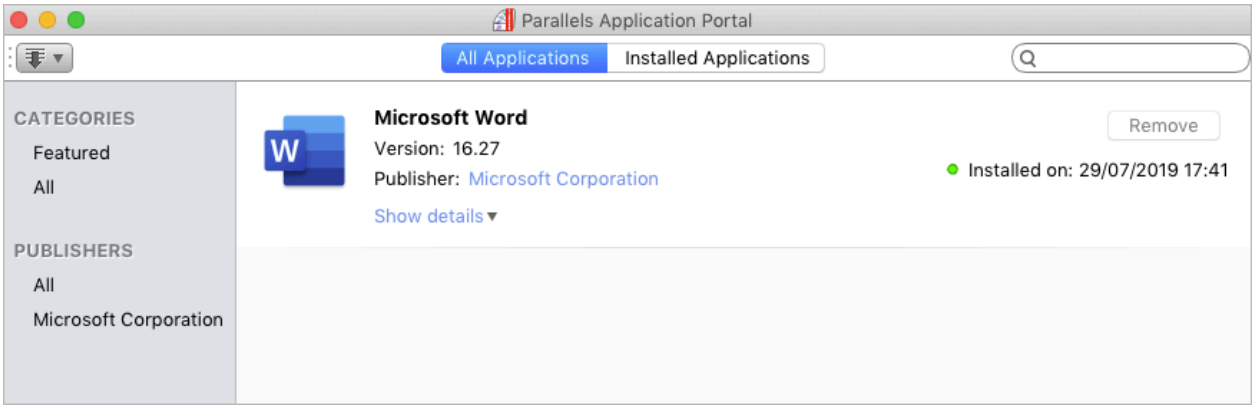
After the VPP application is deployed in Configuration Manager, it becomes available for installation on managed devices.

If you deployed an application for Mac computers as **Available**, it will appear on a Mac in Parallels Application Portal according to a schedule (see the screenshot below). If an application is deployed as **Required**, the installation will be silent.



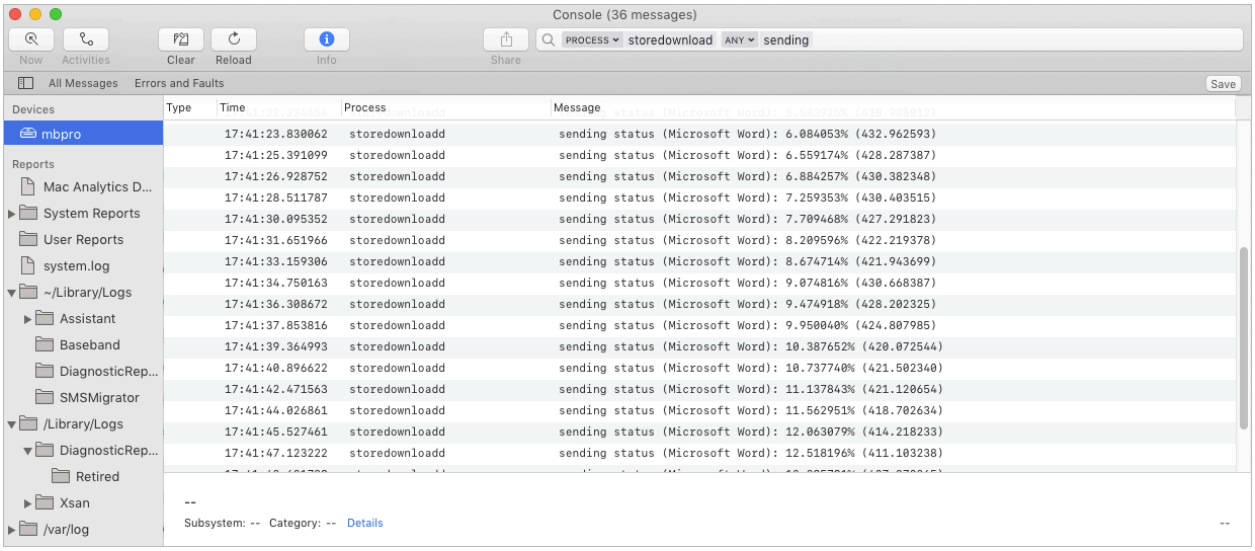

### Installing an "Available" application

To begin the installation, click the **Install** button. Please note that downloading and installing a large application may take some time. During that time the installation status is displayed in the area below the **Cancel** button, which is what the **Install** button is changed to once you click it. On successful installation, the status should say "Installed on:" followed by the date and time, as shown on the screenshot below.



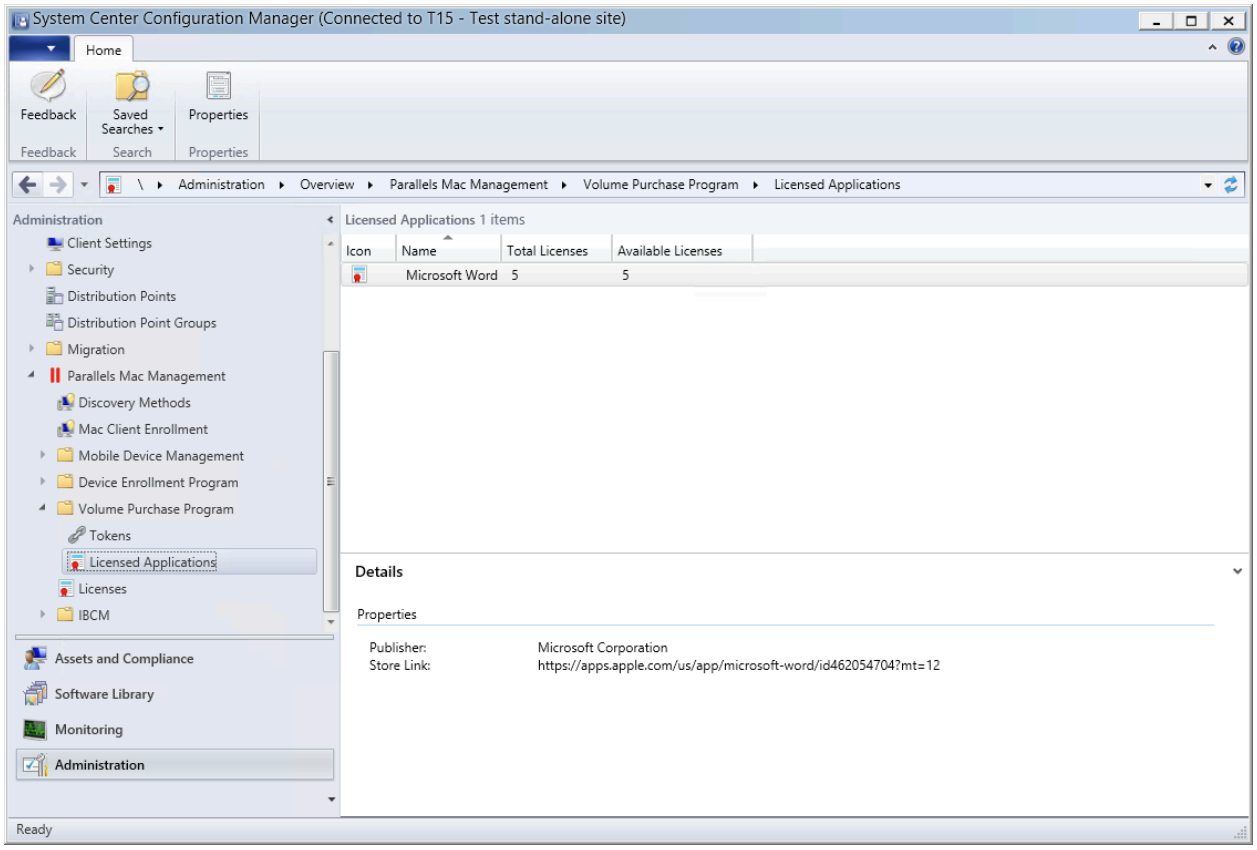
## Troubleshooting

If you believe that the installation takes longer than it should, you can look at the current processes in the Console application using these filters: "PROCESS=storedownload" and "ANY=sending" (see the screenshot below). To set a filter in the Console app, type "storedownload" in the Seach box, press Enter, and then select "Process" in the drop-down menu that will appear in the Search box. Repeat the same for the "sending" keyword.



# Managing assigned licenses

When you add a VPP application to Configuration Manager, the total number of licenses and the number of available licenses are displayed in the Configuration Manager console:




## License assignment

A license is assigned to a particular installation (a Mac computer or Apple mobile device) as follows:

- If the deployment is configured as **Available**, a license is claimed when a user initiates the installation on the device.
- If the deployment is configured as **Required** (silent installation), the license is claimed before the command to install the app is sent to a device.

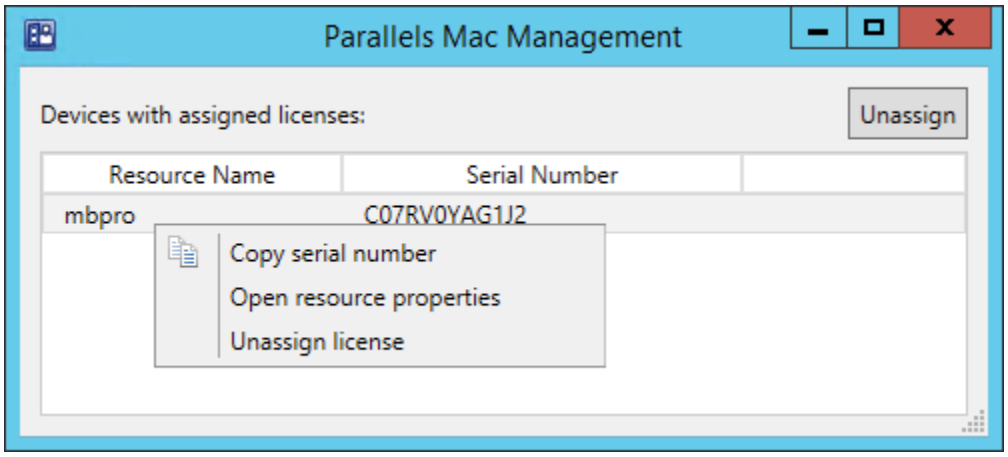
A license is always claimed from the location in the Apple Business Manager where the application resides.

### Unassigning a license

A license can be unassigned from an installation at any time if needed. To do so, right-click an application in the Configuration Manager console and choose **Properties**. This opens a dialog listing all of the devices on which the application is currently installed. Find a device from which you want to remove the license, right-click it and choose **Unassign license**. The license will be returned to the pool and the **Available Licenses** field in the **Licensed Applications** view (see the screenshot above) will be updated to reflect this.

### Viewing devices and corresponding resources

As was said above, you can see the list of devices on which a given application is installed by right-clicking the application and choosing **Properties**. If you need to locate a Configuration Manager resource corresponding to a device, do the same and then right-click a device and choose **Open resource properties.**




# Uninstalling VPP applications

To uninstall an application that was installed earlier, use the same Configuration Manager Application Deployment functionality.

To uninstall an application:

1. If the application you want to uninstall already exists as a Configuration Manager application, proceed to step 2 below. If not, create an application in Configuration Manager the same way as described earlier in this section (p. 121).
2. Deploy the application using the **Deploy Software Wizard (p. 124).** While doing so, specify the following:
   - Select **Uninstall** in the **Deployment Settings** > **Action** drop-down list.

- For a silent uninstallation, select **Required** in the **Purpose** field. Note that at the time of this writing, **Required** is the only supported option.
- Specify **Scheduling** and **User experience** settings as per your requirements. Note that **User experience** settings are not supported on Apple mobile devices and will be ignored.

When the policy is applied to a device, the application will be uninstalled at the time specified in the **Deploy Software Wizard** > **Scheduling** > **Installation deadline** setting.

**Note:** As part of the uninstallation process, the VPP license that was previously assigned to a device will be unassigned.

### Removing an application that is already deployed

If the application that you want uninstalled from specific devices still has an active deployment with an action of **Install**, you can do one of the following:

- Remove the **Install** deployment from the entire device collection.
- Exclude desired devices from the device collection that has the **Install** deployment.

When one of the above is done, you'll be able to deploy the application with an action of **Uninstall**.

### Visibility of the deployment with an action of Uninstall in Parallels Application Portal

A deployment with an action of **Uninstall** is visible in the Parallels Application Portal only if both of the following requirements are met:

- The deployment is active and does not conflict with the deployment with an action of **Install**.
- The deployed application is installed on a target device.

### Priorities of Install and Uninstall deployments which exist simultaneously

If an application is deployed twice to a device, once with an action of **Install** and once with an action of **Uninstall**, the application deployment with the action of **Install** will take priority. Note that this rule only applies if both deployments have a purpose of **Required**. If one of the deployments is configured as **Available**, the **Required** deployment takes priority. The following table lists all possible deployment combinations and the outcome:

| Deployments for an application that exist simultaneously | Deployment that takes priority |
|---|---|
| Install (Available) + Install (Required) | Equal (both are carried out) |
| Install (Required) + Uninstall (Required) | Install (Required) |
| Install (Available) + Uninstall (Required) | Uninstall (Required) |

CHAPTER 12

# macOS Software Update Management

## In This Chapter



# Overview

Parallels Device Management for Configuration Manager allows you to manage macOS software updates (patches) using the native Configuration Manager functionality. Using this functionality you can import the information about available macOS updates into Configuration Manager and then deploy the updates to Mac computers in your organization.

To use the macOS Software Update Management functionality you need:

- **Parallels OS X Software Update Point** installed. If you don't have it installed, run the Parallels Device Management installer again and install the component.
- By default, Mac computers will download deployed macOS updates from Apple's servers. On Mac computers running macOS prior to macOS Big Sur, you have an option to host updates on a local server. Please note that Parallels Device Management does not include functionality for hosting macOS updates. You will have to use the Apple's macOS Server or a third-party software for that.
- To manage software updates on Mac computers running macOS Big Sur or later, the computers must be enrolled in MDM.

# Configuration options

Parallels Device Management provides you with a number of configuration options that you can use to deploy macOS updates to Mac computers. This section describes these configurations.

## Download updates from Apple's servers

This is the default and the simplest configuration in which software update catalogs and packages are downloaded from Apple's servers over the Internet.

When this configuration is used, macOS updates are installed on Mac computers as follows:

1. Depending on the macOS version, the software update catalogs are build as follows:
   - For Mac computers running macOS prior to macOS Big Sure, Parallels OS X Software Update Point downloads software update catalogs from Apple's servers and then imports them into WSUS. The default URL for downloading macOS software update catalogs and packages is https://swscan.apple.com/content/catalogs/others/.
   - To manage software updates on Mac computers running macOS Big Sur or later, the computers must be enrolled in MDM. MDM continuously collects software update information from all enrolled Mac computers. Parallels OS X Software Update Point then builds a software update catalog by querying MDM every hour and publishes the catalog in WSUS.
2. WSUS is synchronized with Configuration Manager, so the administrator can view and deploy macOS updates using the Configuration Manager console.
3. The Configuration Manager administrator selects which updates they want to install on Mac computers and deploys them.
4. Mac computers download deployed updates from Apple's servers. Depending on the macOS version and enrollment type, the updates are installed as follows:
   - On all Mac computers except non-DEP enrolled Apple Silicon computers, the updates are installed silently. If an update requires a Mac restart, the Mac user will have a choice to postpone the installation.
   - On non-DEP enrolled Apple Silicon computers, a dialog is shown to the user asking them to install the updates manually. The user follows the instructions and opens System Preferences in macOS from where they can install the updates.
5. A Mac user can also check for updates available from Apple using the standard macOS functionality and install any of them.

For the information on how to configure Configuration Manager and deploy macOS updates to Mac computers, please see **Deploying macOS updates** (p. 140).

## Download updates from a local server

**Note:** The Parallels Device Management functionality described here does not support macOS 11 Big Sur.

The configuration described here allows you to download macOS software update catalogs and packages from a local server instead of going to Apple's servers. You may consider this scenario if you want to minimize the Internet traffic in your organization.

When this configuration is used, macOS updates are installed on Mac computers as follows:

1. macOS software update catalogs and packages are hosted by a local web server (see **Hosting macOS Update Locally and Setting the Download URL** below).

2. Parallels OS X Software Update Point downloads software update catalogs from the local web server and then imports them into WSUS.
3. WSUS is synchronized with Configuration Manager, so the administrator can view and deploy macOS updates using the Configuration Manager console.
4. The Configuration Manager administrator selects which updates they want to install on Mac computers and deploys them.
5. Mac computers download software update catalogs from Parallels OS X Software Update Point and then download software update packages from the local web server.
6. The deployed updates are silently installed on a Mac. If an update requires a Mac restart, the Mac user will have a choice to postpone the installation.
7. A Mac user can also check for available updates using the standard macOS functionality and install any of them. Please note that in this scenario the macOS Software Update service running on a Mac will use update catalogs that were downloaded from Parallels OS X Software Update Point (not the catalogs from Apple's servers). Software update packages will be downloaded from the local web server.

### Hosting macOS updates locally and setting the download URL

Parallels Device Management allows you to use locally hosted software update catalogs and packages, but does not include functionality that replicates them on a local server. To host software update catalogs and packages locally, you will need to use the Apple's macOS X Server or a third-party software that can replicate them. Replicated catalogs and packages can then be served by a local web server, so Mac computers can download them via HTTP.

Depending on the software that you are using to replicate software update catalogs and packages, the local URL for downloading them may be different. For example, if you are using the Apple's macOS Server (a physical Apple computer with macOS Server as the operating system), the URL may look like the following:

```
http://myhost.example.com:8088/index.sucatalog
```

A third-party software will typically allow you to replicate Apple's software update catalogs and packages in a folder on your local computer. You will then have to set up a local web server that will serve this folder, so the URL to it may look lise this:

```
http://myhost.example.dom/repo/custom-catalog/
```

Once you have software update catalogs and packages hosted locally and know the download URL, you need to configure Parallels OS X Software Update Point to use them:

1. Open the Windows registry editor (regedit.exe) on the computer where Parallels OS X Software Update Point is installed.
2. Navigate to one of the following depending on your Windows version:
   - 64-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Parallels\Parallels Mac Management for Microsoft SCCM\Sup

- 32-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Parallels\Parallels Mac Management for Microsoft SCCM\Sup

3 Add a String value to the **Sup** subkey and name it **SusCatalogBaseUrl**.

4 Assign the download URL as the **SusCatalogBaseUrl** value data. The URL will be used by Parallels OS X Software Update Point to download software update catalogs. Mac computers will download software update packages using the URL specified in the catalogs, which will also point to a location on the local web server (the URL inside a catalog is configured by the software that performs the replication).

5 Finally, you need to restart the Parallels OS X Software Update Point service (`pmm_sup_service`) for the changes to take effect.

If later you decide to go back to the default configuration (downloading updates from Apple's servers), you can simply delete the **SusCatalogBaseUrl** value.

### Configure Parallels Mac Clients

You now need to configure Parallels Mac Clients to download software update catalogs from Parallels OS X Software Update Point. To do so, create a Configuration Item with discovery and remediation scripts (for instructions on how to use scripts in Configuration Items, please see Using discovery and remediation scripts (p. 91)). When adding scripts, use sample scripts below to create your own.

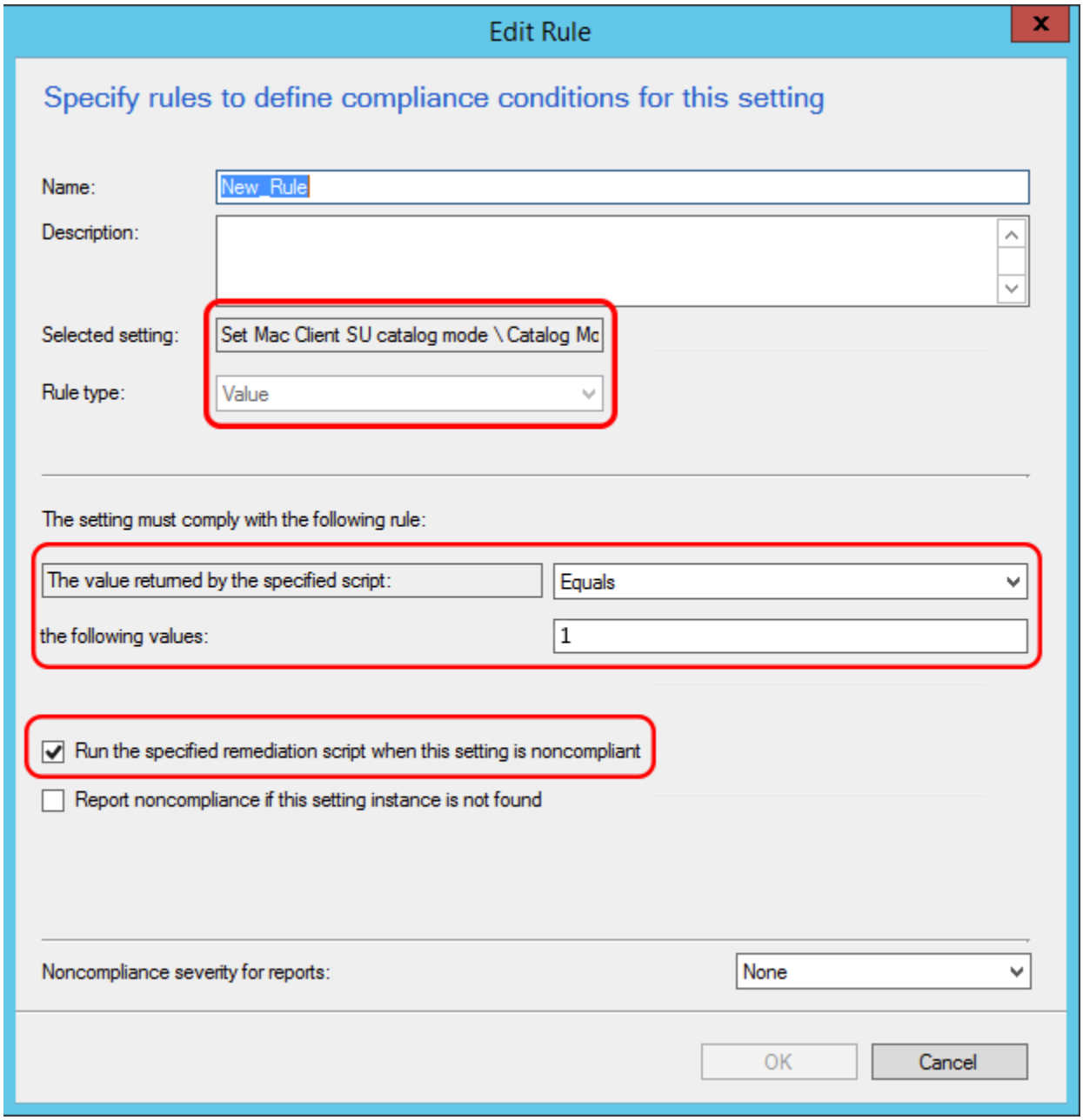
#### Discovery script:

```
#! /bin/bash
PLIST="/Library/Preferences/com.parallels.pma.agent.plist"
MODE=$(/usr/libexec/PlistBuddy -c "Print :SuCatalogMode" $PLIST 2>/dev/null)
if [ $? != 0 ]; then
  MODE=0
fi
echo $MODE
```

The script above determines which software update configuration the Parallels Mac Client running on a Mac is currently using. The MODE variable is assigned the value that we are looking for. If there's an error (e.g. the SuCatalogMode key is absent in the plist file), the MODE variable is assigned the value of 0 (zero). Finally, the value is returned as a string and passed to the compliance rule for evaluation.

**Compliance rule:**

The compliance rule must be set up as shown on the following screenshot (note the properties marked in red):




Note that the rule evaluates the value returned by the discovery script to be equal to 1 (one), which is the mode that we are setting up (see below for other possible modes). If the value complies, the Configuration Item simply exits without modifying anything. If the value doesn't comply (is not equal to 1), then the compliance rule executes the remediation script that will set it to 1.

The other possible catalog download modes are:

- 0 — catalogs are downloaded from Apple's servers (default).
- 1 — catalogs are downloaded from Parallels OS X Software Update Point.
- 2 — same as 1 above but gives you an ability to limit what a Mac user can install. More about this mode in the section that follows this one.

**Remediation script:**

```
#! /bin/bash -s -
PLIST="/Library/Preferences/com.parallels.pma.agent.plist"
MODE=1
/usr/libexec/PlistBuddy -c "Delete :SuCatalogMode" $PLIST 2>&1
/usr/libexec/PlistBuddy -c "Add :SuCatalogMode integer $MODE" $PLIST
```

The script above sets the value of the SuCatalogMode key to 1, thus configuring Parallels Mac Client to download software update catalogs from Parallels OS X Software Update Point.

When finished creating or modifying the Configuration Item, add it to a Configuration Baseline and then deploy it to a collection containing your Mac computers.

For the information on how to configure Configuration Manager and deploy macOS updates on a Mac, please see **Deploying macOS Updates** (p. 140).

## Restrict which updates a Mac user can install

**Note:** The Parallels Device Management functionality described here does not support macOS 11 Big Sur.

This configuration option allows you to restrict which updates a Mac user can see and install. Please note that this configuration allows you to download catalogs and packages from Apple's servers or a local web server.

When this configuration is used, macOS updates are installed on Mac computers as follows:

1. Parallels OS X Software Update Point downloads macOS update catalogs from Apple's servers or the local server (depending on the configuration) and then imports them into WSUS.
2. WSUS is synchronized with Configuration Manager, so the administrator can view and deploy macOS updates using the Configuration Manager console.
3. The Configuration Manager administrator selects which updates they want to install on Mac computers and deploys them.
4. Mac computers download full software update catalogs from Apple's servers or Parallels OS X Software Update Point (depending on the configuration). The catalogs are then filtered to include only the updates that the administrator has deployed in Configuration Manager. If a Mac user now checks for available updates using the standard macOS functionality, they will see only the updates that were deployed.

5 Mac computers download software update packages from the location specified in a catalog (Apple's servers or a local server).

6 The deployed updates are silently installed on a Mac. If an update requires a Mac restart, the Mac user will have a choice to postpone the installation.

7 If a Mac user now checks for updates using the standard macOS functionality, they will see only the updates that were deployed (or none at all if the updates have already been installed on this Mac).

### Configure Parallels Mac Clients

To configure Parallels Mac Clients to use this scenario, create a Configuration Item with discovery and remediation scripts (for instructions on how to use scripts in Configuration Items, please see Using discovery and remediation scripts (p. 91)). When adding scripts, use sample scripts below to create your own.

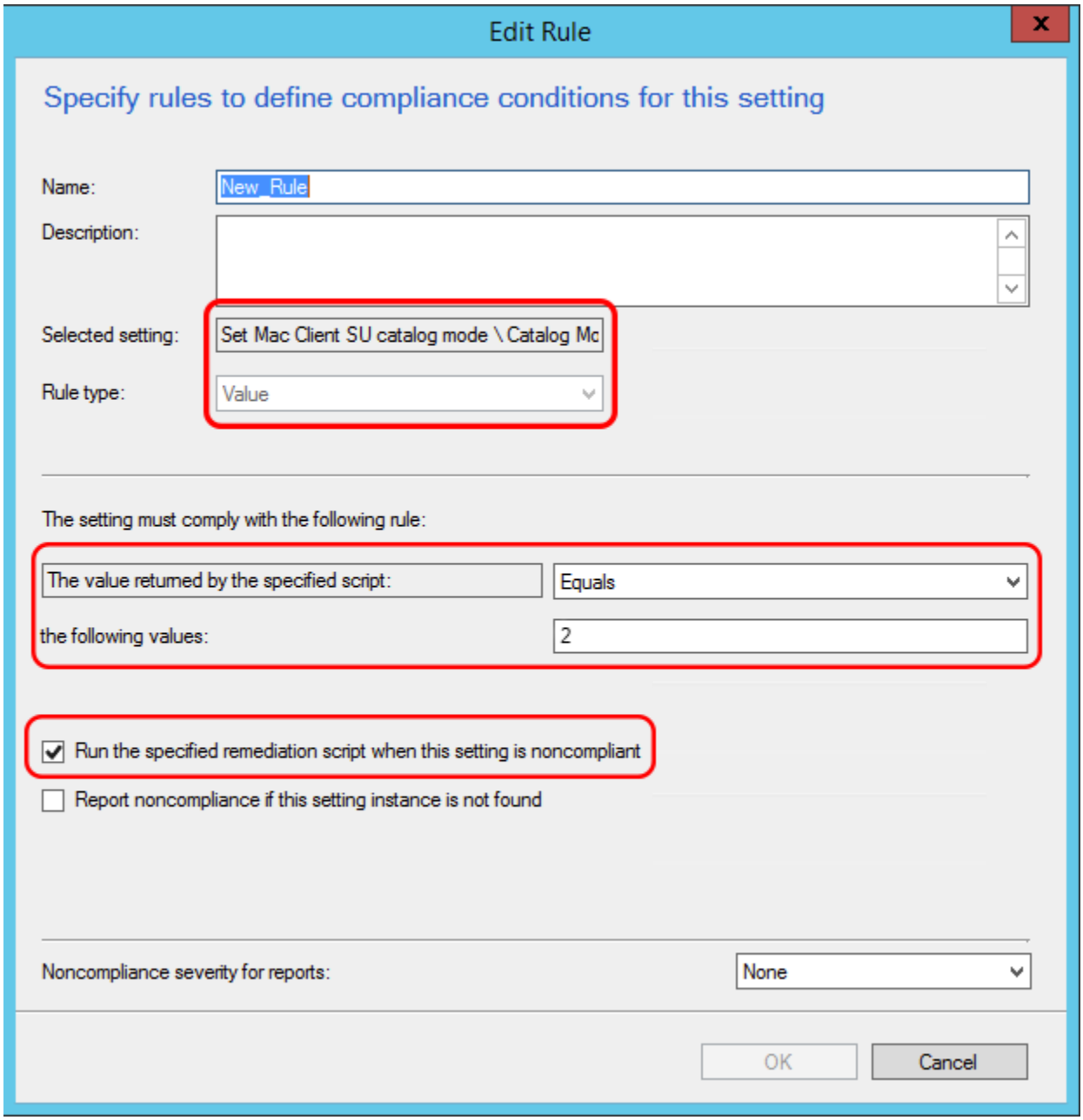
#### Discovery script:

```
#! /bin/bash
PLIST="/Library/Preferences/com.parallels.pma.agent.plist"
MODE=$(/usr/libexec/PlistBuddy -c "Print :SuCatalogMode" $PLIST 2>/dev/null)
if [ $? != 0 ]; then
  MODE=0
fi
echo $MODE
```

The script above determines which software update configuration the Parallels Mac Client running on a Mac is currently using. The MODE variable is assigned the value that we are looking for. If there's an error (e.g. the SuCatalogMode key is absent in the plist file), the MODE variable is assigned the value of 0 (zero). The value of the MODE variable is then returned as a string and passed to the compliance rule for evaluation.

**Compliance rule:**

The compliance rule must be set up as shown on the following screenshot (note the properties marked in red):




Note that the rule evaluates the value returned by the discovery script to be equal to 2 (two), which is the mode that we are setting up. If the value complies, the Configuration Item simply exits without modifying anything. If the value doesn't comply (is not equal to 2), then the compliance rule executes the remediation script that will set it to 2.

**Remediation script:**

```
#! /bin/bash -s -
PLIST="/Library/Preferences/com.parallels.pma.agent.plist"
MODE=2
/usr/libexec/PlistBuddy -c "Delete :SuCatalogMode" $PLIST 2>&1
/usr/libexec/PlistBuddy -c "Add :SuCatalogMode integer $MODE" $PLIST
```

The script above sets the value of the SuCatalogMode key to 2, thus configuring Parallels Mac Client to use the scenario described in this section.

When finished creating or modifying the Configuration Item, add it to a Configuration Baseline and then deploy it to a collection containing your Mac computers.

For the information on how to configure Configuration Manager and deploy macOS updates on a Mac, please see **Deploying macOS updates** (p. 140).

### Hosting macOS updates locally

Hosting software update catalogs and packages locally is optional when using the configuration described above. You may consider it if you want to minimize the Internet traffic in your organization.

Please note that Parallels Device Management allows you to use locally hosted update catalogs and packages, but does not include functionality that replicates them on a local server. To host catalogs and packages locally, you will need to use the Apple's macOS Server or a third-party software that can replicate OS X software update catalogs and packages on a local server. Replicated catalogs and updates can then be served by a local web server, so Parallels OS X Software Update Point and Mac computers can download them via HTTP.

Depending on the software that you are using to replicate software update catalogs and packages, the URL for downloading them may be different. For example, if you are using the Apple's macOS Server (a physical Apple computer with macOS Server as the operating system), the URL may look like the following:

`http://myhost.example.com:8088/index.sucatalog`

A third-party software will typically allow you to replicate macOS catalogs and packages in a folder on your local server. You will then have to set up a local web server that will serve this folder, so the URL to it may look lise this:

`http://myhost.example.dom/repo/custom-catalog/`

Once you have the updates hosted locally and know the download URL, do the following:

1. Open the Windows registry editor (regedit.exe) on the computer where Parallels OS X Software Update Point is installed.
2. Navigate to one of the following depending on your Windows version:

- 64-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Parallels\Parallels Mac Management for Microsoft SCCM\Sup
- 32-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Parallels\Parallels Mac Management for Microsoft SCCM\Sup

3 Add a String value to the **Sup** key and name it **SusCatalogBaseUrl**.

4 Assign the download URL as the **SusCatalogBaseUrl** value data.

5 Finally, you need to restart the Parallels OS X Software Update Point service (`pmm_sup_service`) for the changes to take effect.

If later you decide to go back to the default configuration (i.e. downloading updates from Apple's servers), you can simply delete the **SusCatalogBaseUrl** value.

# Configuring Parallels OS X Software Update Point

Parallels OS X Software Update Point has a number of configuration options that you can modify according to your needs. To modify these options, you need to make modifications in the Windows registry as follows:

Log into the computer where Parallels OS X Software Update Point is installed. Open the Registry Editor (regedit.exe) and navigate to the following key (choose your Windows version):

- 64-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Parallels\Parallels Mac Management for Microsoft SCCM\Sup
- 32-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Parallels\Parallels Mac Management for Microsoft SCCM\Sup

To modify the Parallels OS X Software Update Point configuration, you need to add the appropriate values to the **Sup** key as described in the following subsections.

## Specify the Web proxy server settings

If you are using a web proxy server in your organization, you need to specify its settings for Parallels OS X Software Update Point to access the Internet. To do so, add the following values to the **Sup** key:

| Value | Datatype | Description |
|---|---|---|
| NetProxyHost | String | Proxy server hostname |
| NetProxyPort | DWORD | Proxy server port number |
| NetProxyUserName | String | User name to connect to the proxy server (if required) |
| NetProxyUserPassword | String | User password (if required) |

## Set the HTTP server port number

When configuring a Mac computer for macOS updates, the Parallels Mac Client running on it needs to know the HTTP port number on which Parallels OS X Software Update Point listens for incoming connections. By default, the port is chosen dynamically. The Parallels Configuration Manager Proxy monitors the settings and updates its records when the port changes. When the Parallels Mac Client needs this info, it obtains it from the Parallels Configuration Manager Proxy. If you have a reason not to use a dynamic HTTP port, you can specify a static port number in the registry as follows:

1. Add a DWORD value to the **Sup** key and name it **HttpServerPort**.
2. Assign the static port number as the value data.

To switch back to a dynamic port, delete the **HttpServerPort** value from the key.

## Set the interval to notify Parallels ConfigMgr Proxy of software update configuration changes

When any of the connection settings of the update server or the Parallels OS X Software Update Point change, the Parallels Configuration Manager Proxy must be notified, so it can relay this information to Parallels Mac Clients running on Mac computers. By default, the interval is set at 1800 seconds (30 minutes). If needed, you can set a custom time interval as follows:

1. Add a DWORD value to the **Sup** key and name it **InfoUpdateIntervalSeconds**.
2. Assign the desired time interval (in seconds) as the value data.

## Set the interval to check for macOS catalog updates

When a macOS catalog is updated on the update server (global or local), the Parallels OS X Software Update Point service must update its records accordingly. By default, the service checks with the update server for available updates every 24 hours. If needed, you can set a custom time interval as follows:

1. Add a DWORD value to the **Sup** key and name it **CatalogRefreshIntervalSeconds**.
2. Assign the desired time interval (in seconds) as the value data. For example, the default value of 24 hours would be specified in seconds as 86400.

# Deploying macOS updates

This section describes how to deploy available macOS updates on Mac computers. For additional information about importing macOS updates into Configuration Manager and synchronizing Configuration Manager with WSUS, please also see the **Parallels Device Management for Configuration Manager Deployment Guide**.

## Deploying updates

To deploy the updates, create a Software Update Group and then deploy it to a collection of Mac computers. Mac computers will process policies according to the policy polling interval. On all Mac computers except non-DEP enrolled Apple Silicon computers, the Parallels Mac Client will evaluate assignments and install assigned updates if necessary. If an update requires a restart, the Mac user will have a choice to postpone the installation. A restart will not be performed without user's approval, even if the deadline for an assignment has been reached. On non-DEP enrolled Apple Silicon computers, the updates are not installed automatically. A user will be shown a dialog asking to installed updates. The user will follow the instructions and open System Preferences in macOS from where they can installed the updates.

## Limitations and known issues

The Software Update Management functionality has the following limitation:

- Updates imported into WSUS will not be updated again if the update information is changed in the catalog downloaded from Apple.

CHAPTER 13

# Configuring Maintenance Windows

Automatic installation of software packages, applications, and updates may severely interrupt the work of Mac users. To avoid such an interruption, you can configure maintenance windows to define the time during which Configuration Manager can apply software deployments to Mac computers.

Maintenance windows can be used with the following Mac software deployment types:

- Software deployment, both Application and Package models.
- Software updates deployment.

Maintenance windows are ignored in the following cases:

- When a Mac user initiates an application installation from Parallels Application Portal, the application is installed immediately.
- If an application deployment configured as **Required** has reached its installation deadline, it is installed in the nearest maintenance window.
- The same rules as above apply to software updates.
- Compliance Settings ignore maintenance windows.

If several maintenance windows overlap, they are treated as a single maintenance window on Mac computers.

To configure a maintenance window:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Device Collections**.
2. Right-click a collection (e.g. All Mac OS X Systems) and choose **Properties** in the context menu.
3. In the **Properties** dialog, select the **Maintenance Windows** tab page.
4. To add a maintenance window, click the star icon.
5. The **<new> Schedule** dialog opens. Follow the instructions below to define a schedule for the maintenance window:
   - Specify a maintenance window name.
   - In the **Time** section, specify the effective date, start and end time, and duration. Software deployments will only be applied to Mac computers according to these settings.
   - In the **Recurrence pattern** section, configure the recurrence schedule.

- Use the **Apply this schedule to** drop-down list to select a deployment type to which this maintenance window applies:

  **All deployments** — use this type for software distribution and required applications.

  **Software updates** — use this type for software updates.

  **Task sequences** — this option is not used by Parallels Device Management.

6 Click **OK** when done.

CHAPTER 14

# Executing Scripts on Mac Computers

With Parallels Device Management you can easily deploy and execute scripts on Mac computers right from the Configuration Manager console. This can be helpful, for example, if you have a Mac with an issue that can be easily resolved using a script written in Shell or Python.

A Mac doesn't have to be enrolled in Configuration Manager to deploy a script to it. A connection with a Mac is established vis SSH regardless of whether it is enrolled in Configuration Manager or not.

To deploy and execute a script:

1. In the Configuration Manager console, navigate to the collection containing your Mac computers.
2. Select a Mac or multiple Mac computers using the **Ctrl** key, or select the entire collection if needed. Right-click the selection and choose **Execute Script** in the context menu.
3. The **Execute Script On Macs** dialog opens.
4. Browse for and select a script file to be deployed or enter the script into the **Edit script** box.
5. Click **Next**.
6. On the next screen, specify whether you want to run the script on a Mac with administrative privileges and the timeout value.
7. Click **Next**.
8. The next screen allows you to configure an SSH connection. You need to specify a user account that should be used to establish a connection with individual Mac computers. You have the following choices:
   - **Use account from Parallels Mac Client Push Installation properties**. With this option selected, an SSH connection will be established using the account that you specified in Parallels Mac Client push installation properties (p. 29).
   - **Use this account**. Select this option and then specify an account name and password.
9. Click **Next** to deploy the script.
10. A dialog will open displaying a progress bar (number of processed Mac computers). If a connection with a Mac cannot be established, the information about it can be viewed by clicking the **Details** button. The list that opens will contain only the Mac computers that could not be reached. You can right-click a Mac in the list for more options, which include viewing Mac computers properties and copying the Mac information to the clipboard.
11. You can click **Hide** to hide the progress dialog and continue the deployment process in the background. To cancel deployment, click **Cancel**.

CHAPTER 15

# Remote Lock and Wipe

When a Mac or an Apple mobile device is lost or stolen, the leak of the stored confidential information may lead to severe business risks. Parallels Device Management provides you with the ability to remotely lock and wipe a device if it's lost or stolen.

## In This Chapter



# Prerequisites

Remote wiping and locking of Mac computers and Apple mobile devices is done via MDM enrollment. To use MDM, you must have the Parallels IBCM/MDM Proxy component installed and Parallels MDM configured.

Please note that if you are using Apple DEP (Device Enrollment Program), you should have Parallels IBCM/MDM Proxy already installed and configured. Mac computers that were enrolled via Apple DEP should also be already enrolled in MDM. If you have Mac computers that were enrolled in Configuration Manager outside of Apple DEP, you need to enroll them in MDM before you can wipe and lock them.

Apple mobile devices must also be enrolled in MDM to use the Lock and Wipe functionality on them. MDM enrollment is done when you enroll a mobile device in Configuration Manager.

Once your Parallels IBCM/MDM Proxy is installed and configured and your Mac computers and Apple mobile devices are enrolled in MDM, you can set up the Remote Lock and Wipe functionality in the Configuration Manager console. Read on to learn how to do it.

# Wipe a Mac computer

Once a Mac computer is enrolled in MDM, it can be remotely wiped and locked if needed.

To wipe a Mac remotely:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Devices**.
2. Right-click a Mac computer that you want to wipe and choose **Parallels Device Management Tools** > **Wipe Mac** > **Wipe Mac**. Please note that you cannot wipe multiple Mac computers at the same time. If the Mac you are trying to wipe is not enrolled in MDM, you will see an error message. If the wipe command has already been executed on the selected Mac, you will also see a corresponding message.
3. If the selected Mac computer is enrolled in MDM, the **Wipe Mac** dialog opens. In the dialog, type a 6-digit unlock code of your choice. This code will be saved in the Parallels Device Management database and can be used later to unlock the wiped Mac computer. You can see the code later by looking at the Mac properties in the Configuration Manager console (the **Wipe/Lock** tab page in the **Mac Properties** dialog).
4. When ready, click the **Wipe** button. This sends the wipe command to the target Mac using the Apple Push Notification service (APNs). Note that after sending the wipe command, the Mac computer remains enrolled in Configuration Manager, so you can monitor its status as described below.

After sending the wipe command to the Mac computer, you can monitor its status in the Configuration Manager console. The wipe status is updated when the MDM service reports status changes.

To see the Remote Wipe status:

1. Locate the Mac computer in the Configuration Manager console.
2. Right-click the Mac and choose **Properties**.
3. See the value of the **Retire/Wipe Status** property on the **General** tab. You can also see additional information on the **Wipe/Lock** tab page, including the Mac's hardware ID, serial number, wipe/lock status, and the unlock code that you've entered earlier.

### Canceling a wipe operation

You can only cancel a pending wipe operation if it hasn't been pushed to the Mac computer already.

To cancel a pending wipe operation:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Devices**.
2. Right-click the Mac of interest and choose **Parallels Device Management Tools** > **Wipe Mac** > **Cancel Wipe**.
3. If it's too late to cancel the wipe, you will see a message saying so. If canceling a wipe is still possible, you will see a confirmation dialog. Click **Cancel Wipe** to proceed with the cancelation.

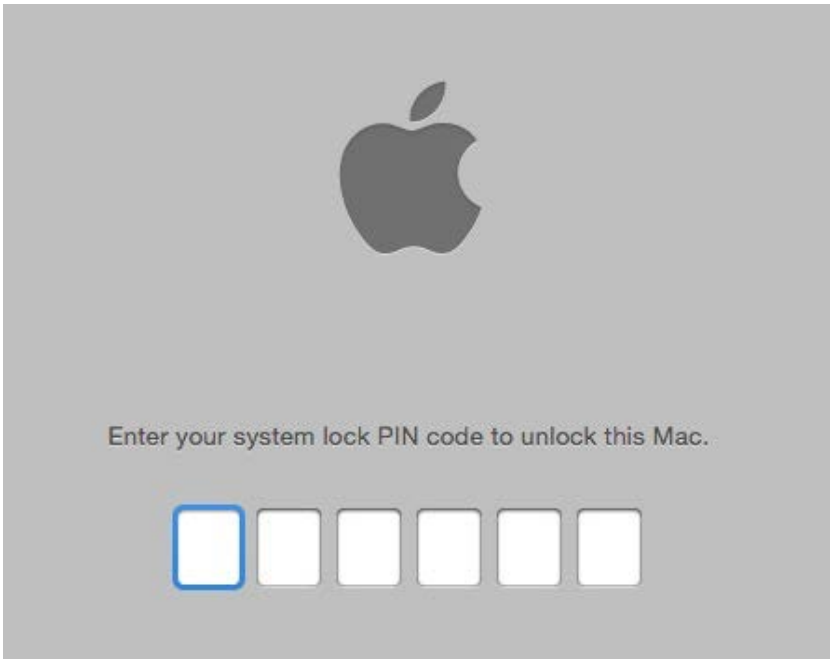
After you cancel the wipe operation, the status in the Mac properties dialog is changed to **Wipe Canceled**.

# Unlock a Mac

After a Mac has been wiped, it cannot be used by anybody until it is unlocked with the code you've specified when you wiped it.

To obtain the unlock code, locate the Mac in the Configuration Manager console, open its **Properties** dialog and see the **Unlock Code** property value on the **Wipe/Lock** tab page.

To unlock a Mac (if you have it in your possession), turn it on and type the unlock code when asked to enter the system lock PIN:




The Mac will be unlocked and you can reinstall macOS on it and enroll it back in Configuration Manager if desired. Please note that the **Unlock Code** and **Wipe/Lock status** properties in the **Mac Properties** dialog in the Configuration Manager console will not change their values immediately upon unlocking a Mac. These properties will be updated when the Mac is enrolled back in Configuration Manager and Parallels Mac Client reports its status to Parallels Configuration Manager Proxy.

### Recovering the unlock code

If a locked Mac is no longer assigned to the Configuration Manager site (i.e. you can't find it in any of the device collections), you can still retrieve the unlock key from the Parallels Device Management database. Unlock keys are never deleted even for Mac computers that are no longer assigned to a Configuration Manager site.

To retrieve the unlock key:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Parallels Device Management / Extended Device Information**.
2. Right-click the **Extended Device Information** item in the right pane and choose **Properties** in the context menu.
3. In the dialog that opens, enter the Mac's serial number or hardware ID and then click **Search**.
4. If the Mac is found, another dialog will open with the **Wipe/Lock** tab page selected. The **Unlock Code** field will contain the unlock code for this Mac computer.

# Lock an Apple mobile device

To lock an Apple mobile device:

1. In the Configuration Manager console, navigate to the mobile device collection.
2. Right-click a mobile device and choose **Parallels Device Management** > **Lock**.
3. The **Lock a Mobile Device** dialog opens.
4. In the dialog, specify the information that will help to return the device to its owner (both fields are required in order to continue):
   - **Lock screen message:** Enter a message that will be displayed on the device.
   - **Phone number:** Enter a phone number to call if the device is found.

   Please note that the two messages above are supported on iOS 7 and later.
5. Click the **Lock** button.
6. The lock command will be sent to the device. You will see a progress bar indicating the progress of the lock operation.

Once the lock command executes successfully, the device will be locked and signed off the Apple ID. The user will still be able to unlock it with a Passcode, Touch ID, or Face ID.

# Wipe an Apple mobile device

**Note**: You can only wipe an institutionally owned Apple mobile device. You cannot wipe a personally owned device.

To wipe an Apple mobile device:

1. In the Configuration Manager console, navigate to the mobile device collection.
2. Right-click a mobile device and choose **Parallels Device Management** > **Wipe**.
3. The **Wipe a Mobile Device** dialog opens.
4. In the dialog, specify the following options:

- **Preserve data plan**: If a cellular data plan is available on the device, it is preserved after the factory reset.
- **Disallow Quick Start**: For the first device start after the factory reset, skip the Quick Start step in the Setup Assistant that allows the user to transfer content from another mobile device.

Please note that the **Preserve data plan** option is supported on iOS 11 and later. **Disallow Quick Start** option is supported on iOS 11.3 and later.

5 Click the **Wipe** button. The device will be immediately wiped, even if it's currently locked. The device user will not be warned. You will see a progress bar indicating the progress of the wipe operation.

Once the device is wiped, all data on it will be erased. The device owner will still be able to set up the device from scratch.

CHAPTER 16

# Internet-Based Client Management

Beginning with Parallels Device Management for Configuration Manager v7.0, you have the ability to enroll and manage Mac computers that are not connected to the corporate network. It extends the Configuration Manager native Internet-based client management functionality (IBCM) to Mac computers managed with Parallels Device Management. To use this functionality, you need Parallels IBCM/MDM Proxy installed and configured for IBCM.

## In This Chapter



# Enrolling Mac computers

Internet-based client management (IBCM) allows you to enroll and manage Mac computers in Configuration Manager via the Internet. With IBCM configured, your Mac users don't have to be connected to your local network in order to enroll their computers in Configuration Manager and for you to manage them.

To be managed via the Internet, a Mac computer must be enrolled in Configuration Manager first. The enrollment itself can be done locally (when a computer is connected to your organization's local network) or over the Internet. In both scenarios, the Parallels Mac Client needs to know the public URL of the Parallels IBCM/MDM Proxy through which it will communicate with Configuration Manager. The differences between the two scenarios a outlined below:

- When a Mac computer is enrolled from the local network, Parallels Mac Client automatically obtains the public URL of Parallels IBCM/MDM Proxy. When Parallels Mac Client needs to communicate with Configuration Manager, it first connects to Parallels IBCM/MDM Proxy using its public URL and then obtains the necessary links to Management Points and Distribution Points which are accessible from the Internet.
- Enrolling over the Internet is performed during the Parallels Mac Client installation procedure. A Mac user first runs the Parallels Mac Client installer and installs it. When the enrollment wizard opens, the user selects the **Enroll over the Internet** option on the **Introduction** page and then manually enters the public URL of the Parallels IBCM/MDM Proxy. This means that the administrator must give the user this URL in advance.

Mac computers enrolled in Configuration Manager with Parallels Device Management v7.0 or later are automatically prepared for the Internet-based client management. This includes the following:

- PKI certificate is delivered to each Mac computer (in older versions of Parallels Device Management, the certificates resided on the Parallels Configuration Manager Proxy host).
- The URL of Parallels IBCM/MDM Proxy is saved in the configuration of Parallels Mac Client installed on a Mac computer.

**Note:** Parallels Mac Client that was installed on previously enrolled Mac computers must be upgraded to the current version to be able to connect to Parallels IBCM/MDM Proxy from the Internet.

To see if a Mac computer is configured for Internet-Based Client Management, go to the **System Preferences** > **Parallels Device Management** pane and examine the value of the **SCCM Proxy Internet URL** field. See the section that follows this one for more details.

# Testing Internet-based client management

A Mac computer will be able to connect to Configuration Manager over the Internet immediately after the enrollment. When Parallels Mac Client detects that the computer is placed outside the corporate network, it starts communicating with Parallels IBCM/MDM Proxy using its public URL. You can check this URL in the **System Preferences** > **Parallels Device Management** panel.

At this point you can either wait for Parallels Mac Client to connect to Parallels IBCM/MDM Proxy and request policies (once every hour by default). Or you can click the "gear" drop-down menu in the lower left corner and then choose **Connect** to initiate policy retrieval manually. If the connection is successful, the **Connected to SCCM Proxy** field will be updated with the last connection time. The text in braces will be either "(Internet)" or "(Intranet)", depending on where the Mac computer was located at that time.

**Note:** If after clicking **Connect** the connection fails (e.g. Parallels Mac Client cannot locate the proxy), a dialog will open asking the user to enter his or her credentials. The credentials will be used to read the current proxy location from Active Directory. Once the location information is obtained, it will be stored in the Parallels Mac Client configuration, so you will not have to enter it again.

If IBCM is not configured, or if Parallels Mac Client couldn't obtain the IBCM settings, the **SCCM Proxy Internet URL** field will say "Not assigned".

# A note about software updates

This note is about installing macOS software updates using the Parallels Software Update Point functionality. The functionality can be configured to host software updates on a local server to reduce Internet traffic. If you use such a configuration, please note that this will not affect Mac computers managed via IBCM. These computers will always download software updates from the Apple servers over the Internet regardless of how the Parallels Software Update Point is configured. You can read more about software updates in **macOS Software Update Management** (p. 130).

CHAPTER 17

# Task Sequences

## In This Chapter



# Overview

**Note:** The Parallels Device Management functionality described here does not support macOS 11 Big Sur.

Task sequences can be used to automate steps in a Configuration Manager environment. Parallels Device Management allows you to use task sequences to deploy a macOS image to a destination Mac computer and perform non-operating system deployments.

### macOS image deployments

macOS image deployment consists of the following steps:

1. Prepare to boot your Mac computers in order to deploy the operating system on them by doing one of the following:
   - Capture a macOS boot image using the image builder utility included with Parallels Device Management.
   - Prepare a bootable USB drive (flash drive or HDD) using a special utility supplied with Parallels Device Management.
2. Capture a macOS system image using a task sequence or the image builder utility.
3. Distribute the boot image (if you are planning to boot from the network) and the system image to a distribution point.

4 Create a task sequence that will deploy the macOS system image and optionally execute other task sequence steps.

5 Deploy the task sequence to a collection of Mac computers.

6 Boot a Mac from the network or the USB drive and execute the task sequence on it.

7 When you deploy macOS on a Mac computer, the task sequence will also automatically install Parallels Mac Client on it and will enroll the computer in Configuration Manager.

For detailed information about macOS image deployment, please read the sections that follow this one.

### Non-operating system deployments

Parallels Device Management also supports task sequences for non-operating system deployments (non-OSD). These task sequences do not deploy the operating system on a destination Mac computer and do not change the format of any storage. You can use them to install a package or an application, to join a Mac computer to a domain, execute a script, apply a configuration profile, etc. For more information, see **Non-operating system deployments** (p. 181).

# Prerequisites for deploying macOS

Before using the macOS deployment functionality, please verify that the following requirements are met:

- Parallels NetBoot Server must be installed and configured.
- If the NetBoot Server and target Mac computers are running in different subnets, DHCP forwarding must be set up. For the complete information about setting up the network environment for NetBoot, please read the following KB article: https://kb.parallels.com/118518.
- The reference Mac computers that will be used to capture macOS images must have a Recovery HD partition.

# Capturing a macOS boot image

A macOS boot image is used to boot a Mac from the network using the Parallels NetBoot Server. This section explains how to capture a boot image and how to distribute it in the Configuration Manager.

**Note:** The reference Mac must be running macOS 10.11 El Capitan or newer.

If you are planning on booting Mac computers from a USB drive you may skip to **Creating a bootable USB drive** (p. 156).

# Capture a macOS boot image

To capture a macOS boot image, you first need to download the Image Builder utility as follows:

1. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **Mac Client Enrollment**.
2. In the **Mac Client Enrollment** list, right-click the **Mac Client installation package download URL** item and then click **Properties** in the context menu.
3. Copy and paste the URL into a text editor. Replace the "pma_agent.dmg" part with "PmmOsdImageBuilder.dmg".
4. On the reference Mac, open the resulting URL in a web browser to download the `PmmOsdImageBuilder.dmg` file. When done, mount the image in macOS.

## Using the Image Builder utility

To use the `PmmOsdImageBuilder.dmg` utility to capture a NetBoot image, open Terminal and change directory to the `PmmOsdImageBuilder.dmg` image mount point (e.g. `/Volumes/Parallels OSD Image Builder 7.0.xxxx.yyyyyy`) and execute the following command:

```
$ sudo ./pmm_osd_image_builder netboot -n PATH [-h] [-s SOURCE]
                  [--ssh-authkeys PATH] [--ntp-servers SERVERS]
                  [--ignore-version-mismatch]
```

where:

- `-n PATH, --nbi-root PATH` is the path where to save the NetBoot image.
- `-h, --help` displays the command help.
- `-s SOURCE, --source SOURCE` is the source volume mount point, disk identifier, or device node. Default is '/'.
- `--ssh-authkeys PATH` is a path to the file with an SSH public key in the authorized_keys format. The key will be installed in the NetBoot image for root SSH access.
- `--ntp-servers SERVERS` is a list of comma-separated NTP server hostnames or IP addresses.
- `--ignore-version-mismatch` will ignore macOS version mismatch between the source volume and the Recovery HD partition. NOTE: Doing so may cause issues, such as malfunctioning of the boot image.

After executing the command, copy the entire resulting directory to a location on the computer running the Configuration Manager console, so you can add it later to Configuration Manager.

## Add the boot image to Configuration Manager

To add the macOS boot image to Configuration Manager, do the following:

1. In the Configuration Manager console, navigate to **Software Library / Overview / Operating Systems / Operating System Images**.
2. Right-click **Operating System Images** and then click **Add OS X Boot Image**.
3. The **Add OS X Boot Image** dialog opens.
4. In the **Path to the OS X boot image directory** field, specify the path to the macOS boot image folder. The other field should contain name and path where you want the image file (`.wim`) to be created.
5. Click **Next**.
6. Specify a macOS image name and version and click **Next**.
7. Wait for the image to be converted to the `.wim` format.
8. Click **Finish**.

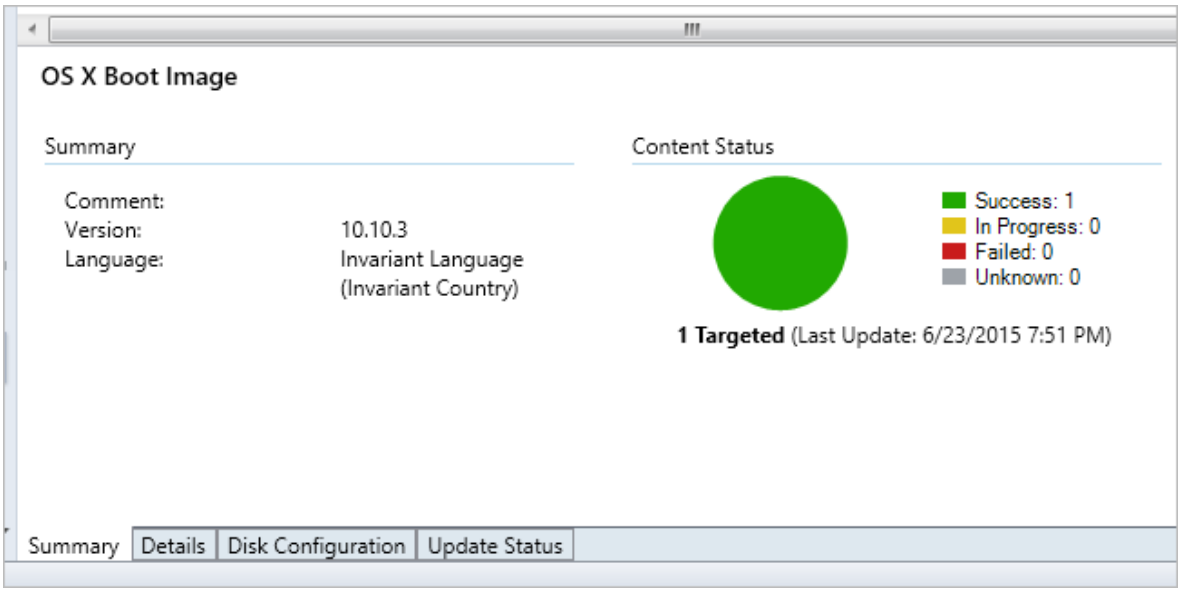
## Distribute content of the boot image

The macOS boot image must now be distributed to the computer running the Parallels NetBoot server.

To distribute the image:

1. In the Configuration Manager console, right-click the boot image item and choose **Distribute Content** in the context menu.
2. In the **Distribute Content** wizard, select the distribution point where the Parallels NetBoot server is installed and complete the wizard.

3 You can monitor the content status in the NetBoot image **Summary** pane. You must wait for the circle to turn green (as shown in the picture below) before proceeding to the next step. Press **F5** to refresh the view.




## Verify the macOS boot image deployment

To verify that the macOS boot image has been deployed successfully, log into a Mac connected to your network and open **System Preferences** > **Startup Disk**. The macOS boot image should be included in the **Select the system you want to use to start up your computer** list.

# Creating a bootable USB drive

If for any reason you can't use a network boot during operating system deployment, you can create a bootable USB drive (flash drive or HDD) and boot each Mac computer from it.

To create a bootable drive, you first need to download the Image Builder utility to a Mac computer as follows:

1 In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **Mac Client Enrollment**.

2 In the **Mac Client Enrollment** list, right-click the **Mac Client installation package download URL** item and then click **Properties** in the context menu.

3 Copy and paste the URL into a text editor. Replace the "pma_agent.dmg" part with "PmmOsdImageBuilder.dmg".

4 On a Mac computer, open the resulting URL in a web browser to download the `PmmOsdImageBuilder.dmg` disk image file.

5 After downloading the disk image file, mount it in macOS. You are now ready to use the utility to create a bootable USB drive.

The utility allows you to create two kinds of bootable drives:

- Regular bootable drive
- Bootable drive with SSH access

To continue, open Terminal and change directory to the `PmmOsdImageBuilder.dmg` image mount point (e.g. `/Volumes/Parallels OSD Image Builder 7.0.xxxx.yyyyyy`).

To create a bootable USB drive, execute the following command in Terminal:

```
$ sudo ./pmm_osd_image_builder usbboot -t TARGET
        [-h] [-s SOURCE] [--ssh-authkeys PATH]
        [--ntp-servers SERVERS] [--ignore-version-mismatch]
        [--noprompt] [--volname NAME]
```

where:

- `-t TARGET, --target TARGET` is the USB drive volume mount point, disk identifier, or device node.
- `-h, --help` displays the command help.
- `-s SOURCE, --source SOURCE` is the source volume mount point, disk identifier, or device node. Default is '/'.
- `--ssh-authkeys PATH` is the path to a file with an SSH public key in the authorized_keys format. The key will be installed in the NetBoot image for root SSH access.
- `--ntp-servers SERVERS` is the comma-separated NTP server hostnames or IP addresses.
- `--ignore-version-mismatch` will ignore OS X version mismatch between the source volume and the Recovery HD partition. NOTE: Doing so may cause issues, such as malfunctioning of the boot image.
- `--noprompt` will suppress the prompt which is normally displayed before the target volume is erased.
- `--volname NAME` is the boot media name used in the firmware-based OS picker.

# Capturing a macOS system image

Parallels Device Management provides you with two methods that can be used to capture a macOS system image:

- Using a task sequence. (p. 158) The main advantage of this method is that you can capture an image from an active partition. The procedure consists of configuring a task sequence, distributing it in Configuration Manager, and then running it on a Mac to capture the image.
- Using the Image Builder utility provided by Parallels (p. 160). With this method you cannot capture an image from an active partition, so the reference Mac must have an additional bootable partition. The actions that you must take here include booting a Mac from a different partition, downloading the Image Builder utility to the reference Mac and then running it to capture the image.

We suggest using the task sequence method, but you can choose a method that you prefer.

## Capturing a macOS image using a task sequence

A macOS system image can be captured using a task sequence, which is configured to execute the Capture OS X Image step. Before using this functionality, please review the information below:

- To capture a macOS system image, you need a Mac computer with macOS 10.10 Yosemite or newer installed.
- The image can be captured from an active partition.
- The reference Mac doesn't have to be assigned to Configuration Manager.

**Note:** If you already have a macOS boot image that you created with Parallels Device Management 4.0 or earlier, you need to create a new boot image using the current Parallels Device Management version. Older boot images are incompatible with this functionality.

### Create a task sequence for capturing a macOS system image

To create a task sequence for capturing a macOS system image:

1. In the Configuration Manager console, navigate to **Software Library / Overview / Operating Systems / Task Sequences.**
2. Right-click **Task Sequences** and choose **Create Task Sequence for Macs**. The **Task Sequence Editor for Macs** dialog opens.
3. On the **General** tab page, specify a task sequence name and an optional description.
4. Click the **Steps** tab and then click **Add** > **Capture OS X Image**.
5. On the **Properties** tab page, specify the network path where the captured image will be stored (see **Free Disk Space Requirements** below), the account that can write to the specified network path, and the account password.
6. Click the **Verify** button next to the **Password** field. If everything checks out, the red icon next to the button (and the red icon in front of the task sequence name) will change to the green check mark icon.
7. Click **OK** to close the dialog. The new task sequence will appear in the task sequence list (press F5 to refresh the list).

If you need to modify the task sequence, right-click it and choose **Edit Task Sequence for Macs** in the context menu.

### Free disk space requirements

When specifying a network path for the image file, the required free disk space can be calculated as a combined size of the used space on the source volume and the Recovery HD volume, multiplied by two. Consider the following example:

1. The used space on the source volume from which you capture the macOS image is 15 GB.
2. The Recovery HD volume size is about 650 MB.
3. (15 GB + 0.65 GB) * 2 = 31.3 GB. This is what your network drive should have available to store the macOS image on it.

### Using task sequence variables

You can use the following variables when configuring the **Capture OS X Image** step.

| Variable | Description | Example | Status |
|---|---|---|---|
| OSDCaptureAccount | Specifies a Windows account name that has permissions to save the captured image on a network share. | guest<br>pmm12.dom\Administrator | PUBLIC |
| PmmOSDCaptureAccountPassword | Specifies the password for the Windows account used to store the captured image on a network share. | secret | PUBLIC |
| OSDCaptureDestination | Specifies the destination network share for the image directory. | \\server\files | PUBLIC |
| PmmOSDCaptureDestinationDir | Specifies the name of the directory for storing the captured image. | OSX-10.11-C12L3390FFT0 | PUBLIC |
| PmmOSDSourceDisk | Specifies the device node of the source disk that has macOS installed. | /dev/disk0s2 | INTERNAL |

## Capture a macOS image

To capture a macOS image, do the following:

1. Deploy the task sequence that you created in the previous steps to the collection of Mac computers that contains the reference Mac.
2. Boot the reference Mac from the network.

3 When the Mac boots, select the task sequence that you deployed in step 1 and execute it.

4 The task sequence will run and will capture the macOS image to the network share that you specified when you created the task sequence.

For the complete details on how to deploy and execute a task sequence, please see **Deploying a task sequence to a collection** (p. 178) and **Running a task sequence on a Mac** (p. 178).

# Capturing a macOS image using the Image Builder utility

A macOS system image can also be captured using the Image Builder utility, which is included with Parallels Device Management for Configuration Manager. This method has a limitation that the image cannot be captured from an active partition. This means that you need another partition on the Mac's hard drive from which it can boot.

### Supported macOS versions

The source partition on a reference Mac must have macOS 10.10 Yosemite or newer installed.

## Boot a reference Mac from a different partition

Before using the Image Builder utility, you must create an additional bootable partition on your Mac's hard drive and install macOS on it. The partition must have macOS 10.10 Yosemite or newer installed. The inactive partition from which you'll capture the image must have macOS 10.10 Yosemite or newer.

## Capture a macOS system image

To capture a macOS system image:

1 In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **Mac Client Enrollment**.

2 In the right pane, right-click the **Mac Client installation package download URL** item and then click **Properties**.

3 Copy and paste the URL into a text editor. Replace the "pma_agent.dmg" part with "PmmOsdImageBuilder.dmg".

4 On the reference Mac, open the resulting URL in a web browser to download the `PmmOsdImageBuilder.dmg` file. When done, mount the image in macOS.

5 Open Terminal and change directory to the `PmmOsdImageBuilder.dmg` image mount point (e.g. `/Volumes/Parallels OSD Image Builder 7.0.xxxx.yyyyyy`).

6 Execute the following command in Terminal:

```
sudo ./pmm_osd_image_builder netrestore -s [source-vol] –o [output-dir]
```

where `[source-vol]` is the source volume mount point; `[output-dir]` is a path where you want to create the image file.

7 Copy the resulting image file to a location on the server running the Configuration Manager console.

# Distributing the macOS system image in Configuration Manager

### Add the image to Configuration Manager

After you captured the macOS image, you need to add it to Configuration Manager. To do so:

1 In the Configuration Manager console, navigate to **Software Library / Overview / Operating Systems / Operating System Images**.

2 Right-click **Operating System Images** and then click **Add OS X Image**.

3 The **Add OS X Image** dialog opens.

4 In the **Path to the OS X image directory** field, specify the folder containing the macOS system image. The other field should contain name and path where you want the image file (`.wim`) to be created.

5 Click **Next**.

6 Specify a macOS image name and version and click **Next**.

7 Wait for the image to be converted to the `.wim` format.

8 Click **Finish**.

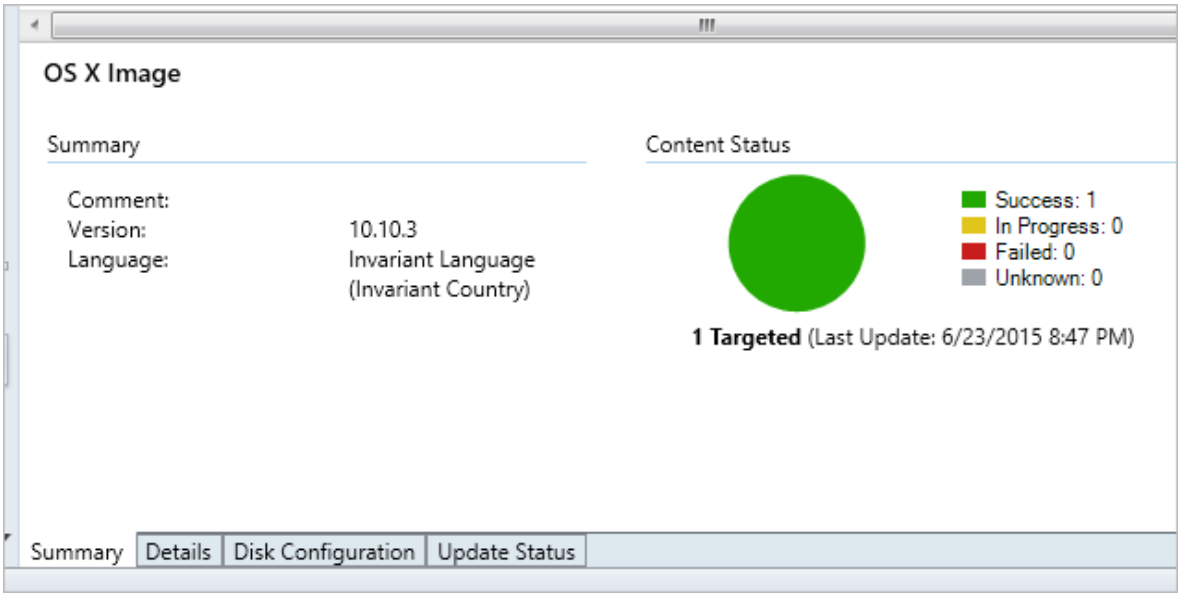
### Distribute the image to a Distribution Point

You now need to distribute the macOS image to a distribution point:

1 In the Configuration Manager console, right-click the macOS system image and then click **Distribute Content**.

2 In the **Distribute Content** wizard, select the distribution point where the Parallels NetBoot server is installed and complete the wizard.

3 You can monitor the content status in the macOS image **Summary** view. You must wait for the circle to turn green (as shown in the picture below) before proceeding to the next step. Press **F5** to refresh the view.




Once the image is distributed, the Parallels NetBoot service will create a corresponding package in the location specified during the NetBoot configuration process.

### Verify the image

Processing of a macOS system image takes some time. Before deploying the image to Mac computers, you can verify that the image is ready. To do so, on the computer running the Parallels NetBoot server, navigate to the `C:\Windows\Logs\pmm` directory and open the `pma_netboot_service.log` file. A successful image processing should have the "New image distributed: xxxxx" entry at the end (or close to it) in the file.

Once the image is distributed, you need to create a task sequence that will deploy the macOS image on Mac computers. Read on to learn how to do it.

# Creating a task sequence

### OSD and non-OSD task sequences

Task sequences can be used to deploy a macOS image (operating system deployment, or OSD) or they can be used for a non-operating system deployment (non-OSD). The difference between the two scenarios is one deploys an operating system and the other does not. The other difference is, some of the task sequence steps can be used only with a non-operating system deployment (these steps are marked in this documentation with an appropriate note). For additional information, please see **Non-operating system deployments** (p. 181).

## Creating a task sequence

After you distribute a macOS system image to a distribution point, you need to create a task sequence to deploy the image on Mac computers.

To create a task sequence:

1 In the Configuration Manager console, navigate to **Software Library / Overview / Operating Systems / Task Sequences.**

2 Right-click anywhere in the **Task Sequences** pane and choose **Create OS X Task Sequence**. The **Task Sequence Editor for Macs** dialog opens.

3 On the **General** tab page, specify a task sequence name and an optional description.

4 You now need to add one or more steps to the task sequence. You must add at least the **Apply OS X Image** task sequence step, which will deploy the operating system image on Mac computers. Other steps are optional, but you will probably use at least some of them. The **Task sequence steps** section (p. 165) describes each available step in detail.

> **Note:** There's one step that deserves a special attention. It is the **Format and Partition Disk** step. If you want to format a disk (or disks) on a destination Mac computer before you install macOS on it, you must add this step to the task sequence before any other step, including **Apply OS X Image**. For complete details see **Format and Partition Disk** (p. 165).

5 To add the **Apply OS X Image** step, select the **Steps** tab page and then click **Add** > **Apply OS X Image**.

6 Click the **Browse** button and select the macOS system image that you distributed earlier.

7 Use the **Destination** drop-down list to specify a partition on a destination Mac computer for the macOS image deployment. Choose from the following options:

- **Next available formatted partition**. If a destination disk has a single partition, it will be used for deployment. If a destination disk has multiple partitions, the image will be deployed on a partition suitable for macOS deployment. The task sequence will go through all available partitions and pick the first one it finds suitable.
- **Specific disk and partition**. Use this option to select a specific disk and partition. The disk number normally corresponds to the bay in a Mac computer with multiple disks.
- **Partition identifier stored in a variable**. If you've already added the **Format and Partition Disk** step to the task sequence (see the **Note** above) and specified the **Partition identifier variable** in it, you can enter the variable name here. The operating system image will be installed on the partition to which this variable refers. For more info, please see **Format and Partition Disk** (p. 165).

> **Note:** The **Destination** option was introduced in Parallels Device Management v6.0. If you have existing task sequences that were created in earlier versions of Parallels Device Management, you should update them to use this option. Simply open a task sequence for editing and specify the destination partition. For additional information, please see **Updating legacy task sequences** (p. 165).

8 At this point, you can add other steps to the task sequence as described in the **Task sequence steps** section (p. 165) or you can click **OK** to close the dialog and add additional steps later.

The new task sequence will appear in the task sequence list in the Configuration Manager console (press F5 to refresh the list if necessary).

## Modifying a task sequence

To modify a task sequence, right-click it and choose **Edit Task Sequence for Macs** in the context menu. This opens the same **Task Sequence Editor for Macs** dialog that you used to create a task sequence. The following describes some of the editing options that you can use while creating or modifying a task sequence.

**Copy and paste a task sequence step**. Right-click a task sequence step and choose **Copy** in the context menu (or press Ctrl+C). To paste the step inside the same task sequence, right-click anywhere in the left pane and choose **Paste** (or press Ctrl+V). To copy the step to an existing task sequence group (p. 173), select the group, right-click it and choose **Paste**. To paste the step to a different task sequence, open the task sequence and paste it as described above. Note that if you are copying a task sequence group, the group will be copied with all the steps (and other groups if any) that it contains. Please also note that when you copy a step or a group, all of their properties, including names, remain exactly the same.

**Cut and paste a task sequence step**. The cut and paste option works exactly like copy and paste described above with the exception that the selected step is removed from its original location after you paste it to a new location. To cut a step, right-click it and choose **Cut** in the context menu (or press Ctrl+X). Then select a different location in the same or different task sequence and paste it there. Note that the original step will remain in its original location until you paste it to a different location.

**Copy all task sequence steps**. This option allows you to copy all existing task sequence steps at once and paste them to the same or different task sequence. To do so, right-click anywhere in the left pane and choose **Copy All** in the context menu. Then select a location in the same or a different task sequence and paste all copied steps there.

**Remove a task sequence step**. To remove a step, select it and click **Remove** at the top of the list. You can also right-click a step and choose **Remove** in the context menu or press Delete on the keyboard.

**Move steps up or down**. To move a step up or down the list, select it and then click the Move Up or Move Down icons at the top of the list. You can also right-click a step and click **Move Up** or **Move Down** in the context menu, or press Ctrl+Up or Ctrl-Down on the keyboard. Please note that if you have groups in your task sequence, the step that you are moving will be placed in or out of a group as it moves through them.

## Updating legacy task sequences

If you have existing task sequences that were created in Parallels Device Management v5.0 or earlier, you should update them to use the new **Destination** [partition] option. You specify this option when you create a task sequence.

The ability to specify a destination partition for macOS image deployment in a task sequence was introduced in Parallels Device Management v6.0. Earlier versions didn't have it. Because of this, when an older task sequence is executed on a Mac, the user has to select a destination volume for macOS image deployment. Starting with Parallels Device Management v6.0, the destination volume is preconfigured in a task sequence, so the user doesn't have to select it when the task sequence is executed on a Mac.

To update an existing task sequences to use the new **Destination** option:

1. In the Configuration Manager console, navigate to **Software Library / Overview / Operating Systems / Task Sequences.**
2. Right-click a task sequence and choose **Edit Task Sequence for Macs** in the context menu.
3. When the **Task Sequence Editor for Macs** dialog opens, you should see a message saying that the **Destination** option is not set in the **Apply OS X Image** step. The option will be automatically set to the **Next available formatted partition**, which is the default value.
4. Select a desired option in the **Destination** drop-down list.
5. Click **OK** to save the updated task sequence.

## Task sequence steps

This section describes task sequence steps that can be added to a task sequence to perform various tasks when the task sequence is executed.

### Format and Partition Disk

The **Format and Partition Disk** task sequence step allows you to format and partition a specified disk on the destination Mac computer.

Please note that if a destination Mac has more than one disk that you want to format and partition, you need to create a separate **Format and Partition Disk** step for each disk.

To add the step to a task sequence:

1. In the **Task Sequence Editor for Macs** dialog, select the **Steps** tab page.
2. Click **Add** and choose **Format and Partition Disk**.

Specify the step properties as follows:

**Name:** Specify a step name.

**Description:** Specify a step description (optional).

**Disk number:** Select the target disk (0 or 1). This is normally the bay number in a Mac with more than one disk.

**Partitions:** Use this section to specify how the disk should be partitioned. You must specify at least one partition for the step to be valid. To add a partition, click the "Add Partition" icon (the star), which opens the **Partition Properties** dialog. Specify the partition properties as follows:

- **Partition name**. Specify a partition name.
- **Format**. Select a format from the drop-down list.
- **Use percentage of remaining free space.** Select this option to specify the partition size as a percentage of the remaining free space on the disk.
- **Use specified size**. Select this option to specify the partition size in kilobytes, megabytes, gigabytes, or terabytes.
- **Partition identifier variable**. This field allows you to declare a variable which will store the identifier of the created partition when the task sequence is executed on a Mac computer. You can use this variable when specifying a destination partition in the **Apply OS X Image** step. For more info, see **Creating a task sequence** (p. 162).

When done, click **OK** to save the partition information and close the **Partition Properties** dialog.

To modify a partition, click the "Edit" icon (paper and pencil).

To delete a partition, click the "Delete" icon.

To rearrange partitions, use the "Up" and "Down" icons on the right side of the partition list.

To create a step to format and partition another disk on a destination Mac, repeat all of the steps described above.

## Join Domain

The **Join Domain** task sequence step allows you to add a Mac to a domain after a macOS image has been deployed on it.

To add the **Join Domain** step to the task sequence:

1. In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.
2. Click **Add** > **Join Domain**.
3. On the **Properties** tab page, specify a step name and an optional description.
4. In the **Domain** field, click **Browse** and then select a domain to join.
5. If you want your Mac computers to be a part of an organizational unit, click **Browse** in the **Organizational unit** field and select an OU container.
6. Specify an account that has permissions to join the domain and the account password.

7 To grant domain users and groups administrative privileges on a Mac, add them to the **Allow administration for groups** list.

8 Select the **Create mobile accounts at login** option to create a mobile account. An account will be created when a Mac user logs into a Mac for the first time using a domain account.

When you select this option, you can also select or clear the **Require confirmation before creating a mobile account** option. If you select it, a user will be asked to confirm the account creation. If you clear it, an account will be created silently.

9 You may customize the step on the **Options** tab page where you can define conditions and other options. For more info about conditions, see **Task sequence variables** (p. 174).

## Install Application

The **Install Application** task sequence step is used to install applications on a Mac as part of a task sequence execution.

If you are using the Application Deployment model to deploy software on Mac computers and already have applications in Configuration Manager, you can use the **Install Application** task sequence step to install these applications as part of a task sequence execution.

This section describes how to add the **Install Application** step to a task sequence. For the information on how to prepare and create macOS applications in Configuration Manager, please refer to **Deploying Software via Application Deployment** (p. 103). Specifically, the following topics contain instructions on how to prepare an application which can be used in a task sequence:

- **Prepare a Mac application for Configuration Manager** (p. 105)
- **Create a Configuration Manager application** (p. 105)
- **Configure the deployment type** (p. 107)

Please note that some of the instructions in the above sections refer to Parallels Application Portal, which is only relevant if you are using the Configuration Manager Application Deployment. When installing an application via a task sequence, those settings can be ignored. The instructions also include a step when you deploy an application to a collection of Mac computers. When using a task sequence, you only need to distribute an application to a distribution point. However, if you've already deployed an application, you don't have to do anything because it has been distributed to a distribution point already.

### Add the Install Application task sequence step

To add the **Install Application** task sequence step:

1 In the **Task Sequence Editor for Macs** dialog, click **Add** and choose **Install Application**.

2 Specify a step name and an optional description.

3 Click **Browse** and select an application. For an application to appear in this list, it must exist in Configuration Manager and must be distributed to a distribution point (see above).

You may customize the step on the **Options** tab page where you can define conditions and other options. Specifically, you may want to select the **Continue on error** option. The reason for this is described below.

When an application is downloaded and installed on a Mac, the task sequence executor begins indexing files on the file system. This process may take some time, which is difficult to predict. In some cases, this time may not be sufficient to accurately evaluate detection rules, which may cause the task sequence executor to conclude that the application installation has failed. To prevent the abortion of the entire task sequence, you may want to enable the **Continue on error** option for the **Install Application** step.

### Kernel extension approval

If the application that you specified in the **Install Application** task sequence step uses third-party kernel extensions, the extensions need to be approved on a target Mac computer. This can be done using one of the following options:

- Applying a configuration profile that contains the Kernel Extension Policy payload. This can be done using the **Apply Configuration Profile** task sequence step. When configuring the step, select the **Install via MDM server** option. For more information, please see **Apply Configuration Profile** (p. 170).
- Using the **Kernel Extensions** task sequence step (p. 171) that gives you the ability to create a Kernel Extensions Policy payload using a built-in editor.

Since kernel extension approval is typically used with software deployments, it should normally be done prior to installing a corresponding application or package. In such cases, the most useful option would be to use the **Kernel Extensions** task sequence step, but you can use an option that works best for you.

## Install Package

The **Install Package** task sequence step is used to install software packages on a Mac as part of a task sequence execution.

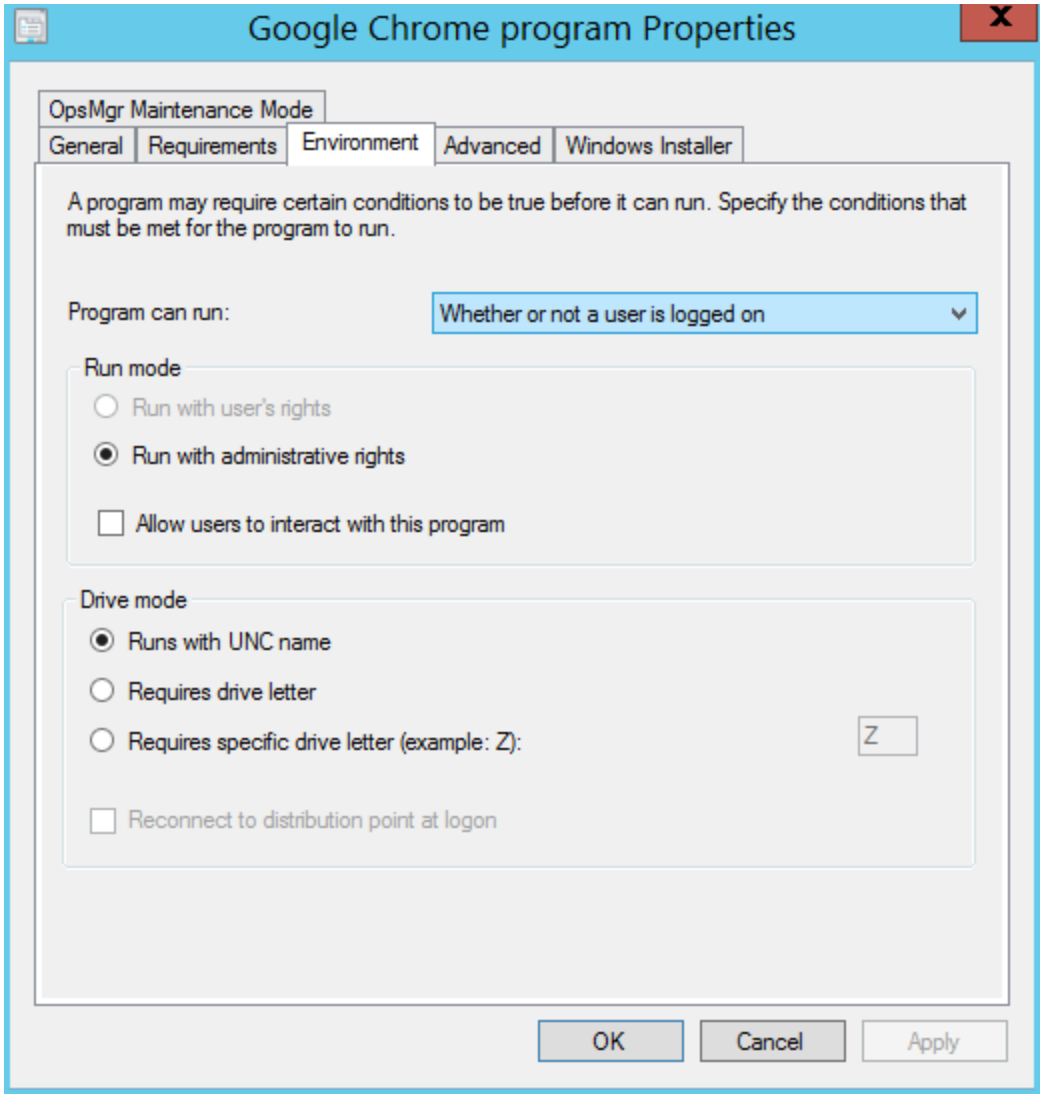
Before adding this step to a task sequence, you need to create a software package as described in the **Creating a software package** section (p. 98). When preparing a software package to be used in a task sequence, the program within a package must meet the requirements as described below.

To view and modify the program properties:

1. In the Configuration Manager console, navigate to **Software Library** / **Overview** / **Application Management** / **Packages**.
2. Select the software package that you want to include in a task sequence and then click the **Programs** tab at the bottom of the **Packages** view.
3. Right-click the program in the list (in the lower pane) and then click **Properties**.

4 Click the **Environment** tab and set the following options:

- Set the **Program can run** option to **Whether or not a user is logged on**.
- Set the **Run mode** option to **Run with administrative rights.**
- Clear the **Allow users to interact with this program** option.




## Add the Install Package step to the task sequence

To add the **Install Package** step to the task sequence:

1 In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.

2 Click **Add** > **Install Package**.

3 Specify a step name and an optional description.

4 In the **Package** field, specify the software package that the step should install.

5 You may customize the step on the **Options** tab page where you can define conditions and other options. For more information about conditions, please see **Task sequence variables** (p. 174).

## Set Hostname

You can use the **Set Hostname** task sequence step to set a Mac's hostname.

To add the **Set Hostname** step to a task sequence:

1 In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.

2 Click **Add** > **Set Hostname**.

3 Specify a name for the step and an optional description.

4 In the **Hostname** field, specify a hostname to be assigned to Mac computers. To assign a unique hostname to each individual Mac, you can use a task sequence variable as a value. For example, you may use the `%OSDComputerName%` built-in variable. Before using the variable here, you must assign it to a device collection or to individual Mac resources. If you leave the value of the variable blank, a Mac user will be prompted to enter a hostname when the step is executed on a Mac. If you assign a value, it will be used to set the Mac's hostname.

5 You may customize the step on the **Options** tab page where you can define conditions and set other options. For more info about conditions, please read **Task sequence variables** (p. 174).

## Apply Configuration Profile

You can use the **Apply Configuration Profile** task sequence step to configure Mac computers using a configuration profile. A configuration profile can be created using an external configuration profile editor or you can use the iMazing Profile Editor from DigiDNA, which can optionally be installed when you install Parallels Device Management.

To add the **Apply Configuration Profile** step to a task sequence:

1 In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.

2 Click **Add** > **Apply Configuration Profile**.

3 Specify a name for the step and an optional description.

4 Click the **Import** button to import an existing configuration profile or click the **Edit** button to open the iMazing Profile Editor from DigiDNA. If the iMazing Profile Editor is not installed, you will be asked to install it. For more information about using the iMazing Profile Editor from DigiDNA, please see Creating a macOS/iOS configuration profile (p. 62). Please note that if you don't installed the iMazing Profile Editor, you will need to use an external profile editor and then use the **Import** button to import the profile.

5 You may customize the step on the **Options** tab page where you can define conditions and set other options. For more information about conditions, please read **Task sequence variables** (p. 174).

### Install via MDM

The **Install via MDM server** option gives you the ability to deliver a profile to Mac computers via MDM. While you can optionally use this delivery method with any profile, you have to use it when a profile contains a security-sensitive payload, as required by Apple. This specifically applies to Kernel Extension Policy and Privacy Preferences Policy Control payloads. If your configuration profile contains any of these payloads, you need to select the **Install via MDM server** option.

**Important:** The **Install via MDM server** option can only be used in Non-OSD task sequences.

To use this functionality, you need Parallels IBCM/MDM Proxy installed and your Mac computers must be enrolled in MDM. Consider the following possible options:

- If you are using Apple DEP to enroll your computers in Configuration Manager, you should already have your Mac computers enrolled in MDM. If you do, you can simply use the **Install via MDM server** option without any additional steps. You can read more about the DEP support in **DEP enrollment** (p. 20).
- If you are not using DEP, you need to install and configure Parallels IBCM/MDM Proxy and then enroll your Mac computers in MDM. You will also need to make sure that the MDM is approved by each individual Mac user because this is an Apple's requirement for computers enrolled in MDM outside of DEP.

## Kernel Extensions

If you are deploying applications that use third-party kernel extensions, the extensions need to be approved on a Mac computer where the application will be installed. The **Kernel Extensions** task sequence step allows you to you create a Kernel Extensions Policy payload, which will be applied on a Mac computer when the task sequence is executed.

**Important:** The **Kernel Extensions** task sequence step can only be used in Non-OSD task sequences.

To add the **Kernel Extensions** step to a task sequence:

1. In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.
2. Click **Add** > **Kernel Extensions**.
3. On the **Properties** tab page, specify a step name and optional description.
4. Specify the following properties:
   - **Allow user overrides**. Select this option to allow users to approve additional kernel extensions, which are not explicitly allowed by this payload.
   - **Allowed team identifiers**. Specify one or more signed kernel extensions that will be allowed to load.
   - **Allowed kernel extensions**. Specify one or more Bundle Identifier and Team Identifier pairs defining kernel extensions that will be allowed to load. Use an empty Team Identifier for unsigned legacy kernel extensions.

5 You may customize the step on the **Options** tab page where you can define conditions and set other options. For more info about conditions, please read **Task sequence variables** (p. 174).

### MDM requirement

Kernel Extensions Policy is a security-sensitive payloads. As such, it must be delivered via a user-approved MDM as required by Apple. What this means is to execute a task sequence containing the **Kernel Extensions** step, you need Parallels IBCM/MDM Proxy installed and your Mac computers must be enrolled in MDM. Consider the following possible options:

- If you are using Apple DEP to enroll your computers in Configuration Manager, you should already have your Mac computers enrolled in MDM. You can read more about the DEP support in **DEP enrollment** (p. 20).
- If you are not using DEP, you need to install and configure Parallels IBCM/MDM Proxy and then enroll your Mac computers in MDM. You will also need to make sure that the MDM is approved by each individual Mac user because this is an Apple's requirement for computers enrolled in MDM outside of DEP.

## Execute Script

You can use the **Execute Script** task sequence step to run a script of your choice on Mac computers during the task sequence execution.

To add the **Execute Script** step to a task sequence:

1 In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.

2 Click **Add** > **Execute Script**.

3 Specify a name for the step and an optional description.

4 Enter a script into the **Script** box (type or paste it) or click **Load Script** and select a file containing your script. Please note that the total size of the script that you can enter is limited to 16 KB.

5 You may customize the step on the **Options** tab page where you can define conditions and set other options. For more information about conditions, please read **Task sequence variables** (p. 174).

When you click **OK** in the **Task Sequence Editor for Macs** dialog, the script is saved in the task sequence. If you need to modify the script later, simply open the dialog again and change it according to your needs.

### Specifying the interpreter

Te **Execute Script** step does not use a default script interpreter, so you must specify it explicitly. To do so, use a shebang at the beginning of a script:

```
#! /bin/bash
```

```
#! /bin/sh

#! /usr/bin/python

#! /usr/bin/perl

#! /usr/bin/ruby
```

etc.

### Modifying task sequence variables from a script

If you need to modify a task sequence variable from your script, please use the examples below.

To read the current value of a variable:

```
ComputerName=$("$PMM_TS_VARIABLE_UTIL" --get OSDComputerName)
```

To set the value of a variable:

```
"$PMM_TS_VARIABLE_UTIL" --set OSDComputerName="MyMac"
```

## Using groups in a task sequence

A task sequence group allows you to combine multiple steps within a task sequence. Groups are useful when adding task sequence steps that share a common condition. Groups can contain a mixture of subgroups and individual task sequence steps.

To add a task sequence group:

1. In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.
2. Click **Add** > **Group**.
3. Specify a name for a group and an optional description.
4. If you want to disable a group and all steps in it, select **Disable this step** on the **Options** tab page.
5. To continue to the next task sequence step outside the group when one of the steps within a group fails, select the **Continue on error** option. Please note that if a step within a group fails and you want to continue to the next step in the same group, the first step must have **Continue on error** selected, otherwise the task sequence will continue to the next step outside the group.
6. To add an existing step or a group to an existing group, select the step (or a group) and use the Move Up and Move Down icons.
7. To add a new step or a subgroup to an existing group, select the group and then click **Add** > <*step_type*> or **Add** > **Group**.
8. You can define conditions for the group on the **Options** tab page. For more info about conditions, please read **Task sequence variables** (p. 174).

# Task sequence variables

Task sequence variables enable you to configure settings for task sequence steps and to configure conditions that must be evaluated before running a task sequence step or a group.

A task sequence has many settings that are stored as task sequence variables. Configuration Manager has built-in task sequence variables that you can evaluate or modify in a task sequence, and you can create your own task sequence variables.You can define task sequence variables for a device collection, an individual device, or you can add a variable to a task sequence using the **Set Variables** task sequence step.

Task sequence variables in Configuration Manager don't inherit values from their ancestors, which means that a device collection variable overrides the built-in Configuration Manager variable with the same name; an individual device variable overrides the device collection variable; and a variable that is defined in a task sequence overrides them all.

When you define a variable for a collection, individual device, or task sequence, you can specify a value for it or you can leave it blank. Leaving the value blank is useful if you want Mac users to specify their own values when a task sequence is executed on a Mac. If you use a variable in a task sequence that has no value, the Mac user will be prompted to specify it during the task sequence run.

When specifying a variable in the **Task Sequence Editor for Macs**, enclose the variable name by percent sign, i.e `%OSDJoinDomainName%`.

## Specifying task sequence step properties using variables

When you add a step to a task sequence, you can specify certain step properties using task sequence variables. This enables you to define variables with different values for different device collections or individual devices and automatically use those values when the task sequence is deployed to a particular collection or a device.

The following tables list task sequence properties that you can specify using task sequence variables. The **Built-in Variable** column lists the corresponding task sequence variables that are defined in Configuration Manager. When specifying one of the listed task sequence properties using a variable, you can use these built-in variables. Ultimately, you can define your own variables for a device collection, device, or a task sequence.

### Join Domain Task Sequence Step

| Property | Built-in Variable |
|---|---|
| Domain | OSDJoinDomainName |
| Organizational Unit | OSDJoinDomainOUName |

| | |
|---|---|
| Account with permissions to join the domain | OSDJoinAccount |
| Password | PmmOSDJoinPassword |
| Allow administration for groups | PmmOSDAdminGroups |
| Create mobile accounts at login | PmmOSDCreateMobileAccounts |

**Set Hostname Task Sequence Step**

| Property | Built-in Variable |
|---|---|
| Hostname | OSDComputerName |

Built-in variables are defined in Configuration Manager, but in order for them to be available in a task sequence, you have to define them for a device collection, individual device, or for the task sequence itself.

For example, to define the `OSDJoinDomainName` built-in variable for the **Unknown Mac OS X Systems** collection:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Device Collections**.
2. Right-click the **Unknown Mac OS X Systems** collection and click **Properties**.
3. In the **Unknown Mac OS X Systems Properties** dialog, click the **Collection Variables** tab.
4. Click the **New** icon.
5. In the **<New> Variable** dialog, enter `OSDJoinDomainName` as the variable name.
6. To hide the value, select the **Do not display this value in the Configuration Manager console** option.
7. Specify the value in the **Value** field or leave it blank. If you leave it blank, the task sequence will prompt the Mac user to supply it during the task sequence run. This might be useful for such properties as Hostname (the **Set Hostname** task sequence step) or any other where you want the users to enter the value themselves.
8. Click **OK**.

The following example demonstrates how you can use the `OSDJoinDomainName` variable in a task sequence after it's been defined for the collection:

1. In the Configuration Manager console, navigate to **Software Library / Overview / Operating Systems / Task Sequences.**
2. Right-click the task sequence and then click **Edit Task Sequence for Macs** in the context menu.
3. In the **Task Sequence Editor for Macs**, click **Add** > **Join Domain**.
4. On the **Properties** tab page, specify the domain name as `%OSDJoinDomainName%`.
5. Specify the rest of the properties as you wish.
6. When this step runs on a Mac, the Mac will be added to the domain specified in the `OSDJoinDomainName` variable.

## Using conditions in task sequence steps

You can add conditional statements to a task sequence step using task sequence variables. If a conditional statement evaluates to True, the task sequence step will run. If the statement evaluates to False, the step will not run.

To add a conditional statement to a step:

- In the **Task Sequence Editor for Macs**, select a step (or create a new one) and then click the **Options** tab.
- Click **Add** > **If Statement**. This must be the first statement in every condition.
- In the drop-down list, select **any**, **all**, or **none** depending on the logic that you consider.
- Click **Add** > **Task Sequence Variable.**
- In the **Task Sequence Variable** dialog, specify a variable name, a condition (logical operator), and a value. The variable that you specify must exist either on a device collection level, individual device level, or in the **Set Variables** step in the task sequence.
- To add another variable at the same level, click **Add** > **Task Sequence Variable**.
- To nest a condition in a condition, select an **If** statement and click **Add** > **If Statement**. The new condition will appear as nested in the first one.
- To move statements and variables up and down the list, use the Move Up and Move Downs icons.

Using the provided logical statements and operators you can create conditional statements as complex as you desire.

One thing to remember is that before you use a variable in a condition, you must make sure that the variable will be within a scope of the task sequence when it runs. This specifically applies for the variables defined in the **Set Variables** step.

## Set Variables task sequence step

In addition to defining task sequence variables for device collections and devices, you can define a variable for a task sequence. If the variable is defined for a device collection or an individual device, the value that you specify here will override the other two.

To add the **Set Variable** task sequence step:

1. In the **Task Sequence Editor for Macs** dialog, click the **Steps** tab.
2. Click **Add** > **Set Variables**.
3. On the **Properties** tab page, click **Add Variable**.
4. Specify the variable name and value.
5. Select the **Secret value** field if you want to hide it in the dialogs.
6. You can add more than one variable to a single **Set Variables** step.

7 Use the **Options** tab page to define conditional statements for the step.

## Running Shell scripts as part of a task sequence step

You can create a shell script that will run as part of a task sequence. This is especially useful when you want to read or modify task sequence variables when the task sequence runs on a Mac.

To run a shell script, you need to do the following:

1 Write a script that will utilize a special command-line utility provided by Parallels Device Management for Configuration Manager.

2 Create a Configuration Manager software package (p. 98) containing the script.

3 Add the software package as the **Install Package** task sequence step (p. 168).

### Using the Command-line utility to access task sequence variables

The command-line utility will run inside the task sequence runtime environment.

The path to the utility is made available using the `PMM_TS_VARIABLE_UTIL` environment variable.

The following is a Bash script example:

```
echo "Path to variable utility = ${PMM_TS_VARIABLE_UTIL}" >>
/tmp/script.log
```

To read task sequence variables, add the `--get` argument to the command:

```
a=`"${PMM_TS_VARIABLE_UTIL}" --get a`
```

The following command reads two variables at once (it can be more than 2):

```
eval `"${PMM_TS_VARIABLE_UTIL}" --get a b`
```

To modify a variable, use the `--set` argument:

```
"${PMM_TS_VARIABLE_UTIL}" --set b="$a"
```

The following command modifies the values of two variables at once (it can be more than two):

```
"${PMM_TS_VARIABLE_UTIL}" --set b="$a" a=123
```

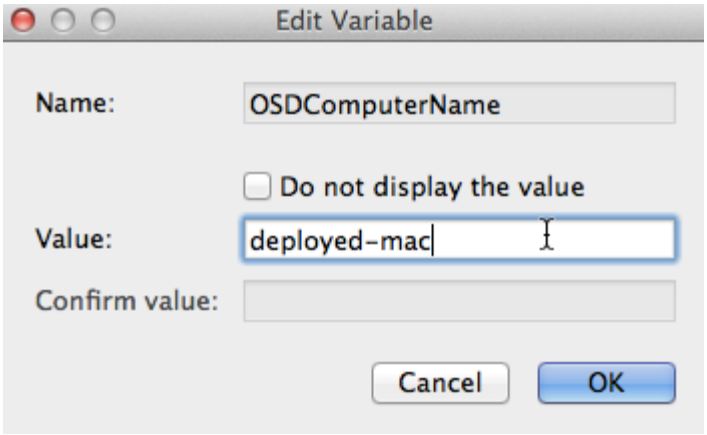
## Prompting a user to set empty variables during a task sequence execution

As we mentioned earlier, you can specify a property of a task sequence step using a variable that has no value. When the task sequence is executed on a Mac, the Mac user will be prompted to specify a value for such a variable.

Here's how it will look on a Mac during the task sequence execution:

1 The **Edit Task Sequence Variables** dialog opens. The list contains the task sequence variables with empty values.

2 Double click a variable to assign a value to it.




3 Click **OK** and then click **Continue.**

The task sequence will continue executing and will use the values that you specified.

# Deploying a task sequence to a collection

When you are done configuring a task sequence, you need to deploy it to a collection of Mac computers.

To deploy a task sequence to a collection:

1 In the Configuration Manager console, right-click the task sequence and then click **Deploy**.

2 The **Deploy Software Wizard** opens.

3 On the **General** page, click the **Browse** button next to the **Collection** field and select the target device collection. If you are deploying macOS on computers that are not enrolled in Configuration Manager, select the **Unknown Mac OS X Systems** collection.

4 Click **Next**.

5 Use the default values on the rest of the pages and complete the wizard.

# Running a task sequence on a Mac computer

Executing a task sequence on a Mac computer consists of the following steps:

1 Start up a Mac from the network or a bootable USB drive that you prepared earlier.

2 After the computer starts, select a task sequence to run.

3 Follow the **Parallels Task Sequence Wizards** instructions and deploy the macOS image on the Mac.

4 The Mac will reboot. When it does, follow the **Parallels Task Sequence Wizard** instructions again and execute the remaining task sequence steps.

5 When all is done, the Mac is enrolled in Configuration Manager and you'll be prompted to log in to it.

The following topics describe each step in detail.

## Start up a Mac and execute a task sequence

### Booting from a USB drive

If you have prepared a bootable USB drive to boot your Mac computers, do the following:

1 Connect the bootable drive to a Mac computer.

2 Power on the computer while holding the **Option** key (Alt). EFI boot screen will show the available boot volumes.

3 Select the volume named "Parallels Mac OSD" and press Enter.

### Booting from the network

If you have configured a macOS boot image to boot your Mac computers from the network, do the following:

1 Start up a Mac to boot from the network (hold down the **N** key on the keyboard while the Mac boots).

2 If you've added more than one macOS boot image to Configuration Manager, you'll be prompted to choose the one to boot from.

### Executing the task sequence

1 Upon successful boot, the **Parallels Task Sequence Wizard** will start (some delay is possible while the Mac establishes a network connection).

2 On the **Log In** page, enter your AD domain name and login credentials.

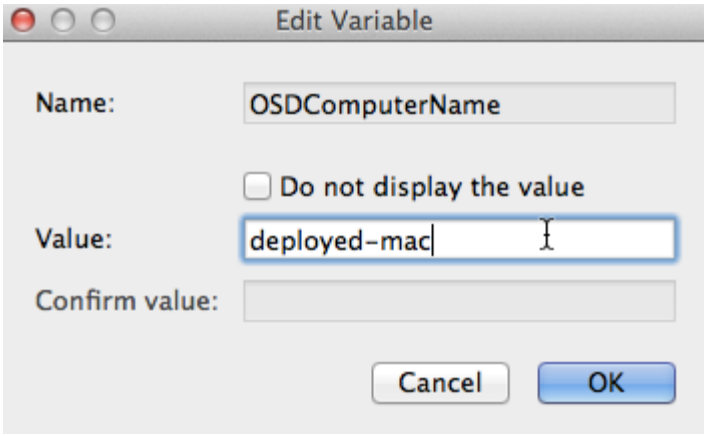
3 Click **Continue**.

4 On the **Select a Task Sequence** page, select the task sequence to execute. If the list is empty, make sure that you deployed the task sequence to the correct collection.

5 Click **Continue**.

6 The **Edit Task Sequence Variables** pages will only show up if one or more task sequence variables that are used in a task sequence step have empty values (see **Set Hostname** (p. 170) for the example).

7 Double click the variable to assign a value to it.




8 Click **OK** and then click **Continue**.

9 At this point, the **Select a Destination** page may or may not appear depending on whether the task sequence was created with the latest or an earlier version of Parallels Device Management:

- In Parallels Device Management v6.0 and newer, you have the ability to specify the target partition for the macOS image deployment when you configure the task sequence in the Configuration Manager console.
- In earlier versions, no such option existed. If you haven't done so already, you should update your existing task sequences to conform to the new design. To do so, simply open an existing task sequence for editing in the Configuration Manager console, select the **Apply OS X Image** step and set the **Destination** option.

If you see the **Select a Destination** page, select a destination volume for the macOS image deployment. Please note that clicking **Continue** on this page will start the macOS image deployment immediately. You cannot go back!

10 The task sequence is now ready to execute the first step. If the first step is **Format and Partition Disk**, it will be executed and the disk specified in it will be formatted and partitioned.

11 The task sequence will now deploy the macOS system image according to the settings specified in the **Apply OS X Image** step.

Once the image is deployed, the Mac will be automatically rebooted from the volume to which the macOS image was applied. Once it boots back up, the task sequence execution will continue with the rest of the task sequence steps.

Read on to learn how to execute other task sequence steps and how to verify the deployment.

## Executing task sequence steps

When a Mac reboots after the macOS system image deployment, it may take a few seconds for it to configure network access. You may see the **Starting Task Sequence** screen with the "Please wait..." message in it.

After the network is configured, the **Parallels Task Sequence Wizard** will run once again. Follow the instructions and complete the wizard.

Once the task sequence run is complete, you'll be prompted to log in to macOS. After logging in, you can verify that the Mac has been enrolled in Configuration Manager as part of macOS deployment. To do so, open System Preferences, then click the **Parallels Device Management** icon.

In the dialog that opens, view the Parallels Mac Client properties. If the enrollment was successful, all properties should have actual values.

## Troubleshooting

The following log becomes available when a Mac boots from the network:

- `/Library/Logs/pmm_tswizard.log`

  You can view the log file in Terminal which can be opened from the **Utilities** menu. Please note that after the macOS image is deployed and the Mac is rebooted, the log file will be moved to the deployed OS partition.

The following logs become available when the Mac is rebooted after the macOS image deployment step:

- `/Library/Logs/pmm_launchd_helper.log`
- `/Library/Logs/pmm_ts_executor.log`

  The logs are finalized when the task sequence execution completes. You can view them when you log into the Mac. To view these logs while the task sequence is executing, connect to the Mac via SSH and view the logs in the SSH terminal.

# Non-operating system deployments

Parallels Device Management supports task sequences for non-operating system deployments (also known as non-OSD). These task sequences do not deploy the operating system on a Mac computer and do not change the format of any storage. A non-OSD task sequence can be deployed to Mac computers for either silent or user-initiated execution.

**Note:** Please note that non-OSD task sequences are supported in Parallels Device Management v7.0 or later. In earlier versions, only the operating system deployment task sequences (OSD) are supported.

# Creating a non-OSD task sequence

Non-OSD task sequences are created the same way the OSD task sequences are created. The difference is, when creating a non-OSD task sequence, you don't use the "Apply OS X Image" task sequence step (and some others). For the list of steps that can and cannot be used, see below.

The following task sequence steps can be used in a non-OSD task sequence:

- Install Package
- Install Application
- Join Domain
- Execute Script
- Set Hostname
- Apply Configuration Profile
- Set Variable
- Kernel Extensions

The following task sequence steps cannot be used in a non-OSD task sequence (using any of these steps will prevent the task sequence from executing on a Mac computer):

- Install Parallels Mac Client
- Apply OS X Image
- Capture OS X Image
- Format and Partition Disk

## Customizing task sequence properties

After you create a task sequence, you can customize some of its properties according to your needs. To do so, in the Configuration Manager console, right-click a task sequence and choose **Properties**. This opens the standard Configuration Manager task sequence properties dialog. The following list describes the properties that are supported by Parallels Device Management:

- On the **General** tab, you can modify **Name**, **Description**, **Category**, and **Download size** properties.
- On the **Advanced** tab page, you can select or clear the **Disable this task sequence on computers where it is deployed** option. If selected, the task sequence will not be executed on those computers. You can also modify the **Maximum allowed run time** property according to your needs.

When done, click **OK** to save the task sequence.

## Deploying a non-OSD task sequence

After creating a non-OSD task sequence, you need to deploy it to a collection of Mac computers.

To deploy a task sequence to a collection:

1. In the Configuration Manager console, right-click the task sequence and then click **Deploy**.
2. The **Deploy Software Wizard** opens.
3. On the **General** page, click the **Browse** button next to the **Collection** field and select the target device collection.
4. Click **Next**.
5. On the **Deployment Settings** page, specify whether the task sequence should be executed on Mac computers automatically (silently) or whether the execution should be initiated by a user. Select one of the following from the **Purpose** drop-down list:
   - **Required** for automatic execution.
   - **Available** for user-initiated execution.
6. Click **Next**.
7. On the **Scheduling** page, specify the schedule for the deployment. Set the date when the deployment should become available and when it should expire. Once it expires, it will no longer be available in the Parallels Application Portal on a Mac computer. You can also set the **Rerun behavior** property according to your needs.
8. Click **Next**.
9. On the **User Experience** page, you can only set the **Allow users to run the program independently of assignment** option. This option is always selected (and cannot be cleared) if the deployment **Purpose** (see above) is "Available". For "Required" deployments, you can select or clear it depending on whether you want the user to be able to install it manually. The automatic execution will still be performed, so this setting essentially affects whether the **Install** button will be enabled or disabled in the Parallels Application Portal on a Mac computer.
10. Use the default values on the rest of the pages and complete the wizard.

## Running a non-OSD task sequence during DEP enrollment

After you deploy a task sequence to a device collection (as described in the previous section), the task sequence is delivered to a destination Mac computer and runs on it. If you are enrolling your Mac computers via Apple DEP, the delivery of a task sequence to a Mac can be significantly delayed for newly enrolled computers. To avoid this delay, you can specify a desired task sequence when you create an enrollment profile, in which case a task sequence will run on a Mac immediately after the enrollment is completed.

For complete information, please see **DEP enrollment** (p. 20) and **Create an enrollment profile for Mac computers (p. 20).**

## Manually running task sequences

If you specified the deployment as "Available", the user will need to manually run the task sequence. To do so, the user opens the Parallels Application Portal and locates the task sequence in it. Non-OSD task sequences are treated as applications in Parallels Application Portal and are listed together with other applications (if any were deployed). Note that a task sequence becomes available in the Parallels Application Portal according to its availability date (see how to specify the schedule in the previous section).

To run a task sequence, the user clicks the **Install** button (just like for applications). The task sequence is then executed in the background with no user interaction required.

CHAPTER 18

# Deploying Parallels Desktop on Mac Computers

## In This Chapter



# Overview

Parallels Desktop for Mac Business Edition is a virtualization software that allows you to run Windows and other operating systems on a Mac computer alongside macOS.

Parallels Device Management for Configuration Manager enables you to deploy Parallels Desktop to Mac computers. Deploying Parallels Desktop is similar to deploying other software: you create a distribution package, add a program to it, copy the package to a distribution point, and create an advertisement (see **Deploying Software via Package Deployment** (p. 98)). Parallels Desktop deployment adds a few extra steps, which are described below.

**Note:** The instructions in this chapter describe the Mass Deployment feature, which is only supported by Parallels Desktop for Mac Business Edition. Parallels Desktop Standard and Pro editions do not support it.

# Preparing the deployment package

Parallels provides a special software package that can be used to mass deploy Parallels Desktop to many Mac computers at once.

To prepare the deployment package:

1 Download the package to your Windows server where the Configuration Manager console is running using the following URL:

https://download.parallels.com/desktop/tools/pd-autodeploy.zip

2 Unzip the file. You should see the `Parallels Desktop Business mass deployment package vx.x.x` folder (where x.x.x is the package version number).

3 Open the folder and navigate to `Parallels Desktop Autodeploy.pkg\Parallels` folder, which should contain the `deploy.cfg` file.

4 Open the file in WordPad (or other advanced text editor), find the `License` section and type your Parallels Desktop license number as a value of the `license_key` variable. Save the file.

5 Copy the Parallels Desktop installation disk image (.dmg file) to the `Parallels Desktop Autodeploy.pkg\Parallels` folder where the `deploy.cfg` file is residing.

# Adding virtual machines to the deployment package

If you would like to distribute one or more virtual machines together with Parallels Desktop, you have to add them to the deployment package. To include a virtual machine, locate the virtual machine bundle (the file with the .pvm extension) and copy it to the `Parallels Desktop Autodeploy.pkg\Parallels` folder.

Parallels Desktop and a source virtual machine can be configured before deployment in a number of ways according to your requirements. This includes the general virtual machine configuration parameters, such as the number of CPUs, available RAM, hard disk size, etc., as well as additional configuration options. For the complete information on how to customize Parallels Desktop and virtual machines before the deployment, please read the **Parallels Desktop Business Edition for IT Administrators** guide.

# Creating a software distribution package

The Parallels Desktop deployment package is distributed to Mac computers using the standard Configuration Manager functionality:

1 In the Configuration Manager console, navigate to **Software Library / Overview / Application Management / Packages**.

2 On the toolbar, click **Create Package**. Use the **Create Package and Program Wizard** to create a software distribution package and program.

3 On the **Package** page, specify the package name and an optional description, manufacturer, language, and version information. Select the **This package contains source files** option and click **Browse**. Select the folder that contains the `Parallels Desktop Autodeploy.pkg` folder. Please note that you must select the parent folder of the `Parallels Desktop Autodeploy.pkg` folder, not the `.pkg` folder itself.

4 Click **Next**.

5 On the **Program Type** page, select the **Standard program** item and click **Next**.

6 On the **Standard Program** page, specify the information about the program. You can create a package that will require user interaction or a package that will install automatically.

- To create a package requiring user interaction, type the following in the **Command line** field:

  ```
  chmod 700 "Parallels Desktop
  Autodeploy.pkg/Contents/Resources/postflight" &&
  /System/Library/CoreServices/Installer.app/Contents/MacOS/Installe
  r "Parallels Desktop Autodeploy.pkg"
  ```

  Specify the **Run mode** as **Run with administrative rights** and select the **Allow user to view and interact with the program installation** option.

- To create a package that will install automatically, the command line should be:

  ```
  chmod 700 "Parallels Desktop
  Autodeploy.pkg/Contents/Resources/postflight" && installer -pkg
  "Parallels Desktop Autodeploy.pkg" -target /
  ```

  DO NOT select the **Allow user to view and interact with the program installation** option.

7 When done specifying the program information, click **Next**.

8 Click **Next** on the **Requirements** page.

9 Review the summary and click **Next** to create the package.

# Sending the package to a distribution point

To send a copy of the package to a distribution point, right-click the package of interest and click **Distribute Content** in the context menu. Use the **Distribute Content Wizard** to specify a distribution point to which you want to send the package. Please make sure that the distribution point is properly configured.

# Deploying Parallels Desktop

To deploy Parallels Desktop:

1 In the Configuration Manager console, right-click the package and then click **Deploy** in the context menu. The **Deploy Software Wizard** opens.

2 On the **General** page, click the **Browse** button next to the **Collection** field and select the collection containing the desired Mac resources (e.g. **All Mac OS X Systems**). Click **OK** and then click **Next.**

3 On the **Content** page, verify the distribution point info and click **Next**.

4 Click **Next** on the **Deployment Settings** page.

5 On the **Scheduling** page, specify the schedule for this deployment. Click **New** to specify the assignment schedule. When done, click **Next**.

6 Use the default values on the rest of the wizard pages and complete the wizard.

The package will be advertised to Mac computers in the specified collection and will be distributed to them according to the schedule that you specified.

See also **Viewing the package status** (p. 102) for the information on how to see the package distribution results.

CHAPTER 19

# Remote support for Mac computers

You can provide remote support for Mac computers by temporarily connecting to a remote Mac computer as administrator. A remote connection can be established right from the Configuration Manager console with both managed and unmanaged Mac computers.

To use the Remote Assistance feature, open the Configuration Manager console, find a Mac that you want to connect to and right-click it. In the context menu, point to **Parallels Management Tools**, and click one of the following connection options:

- **Connect via VNC**. This option uses the Virtual Network Computing graphical desktop sharing system, which lets you remotely control the macOS desktop.
- **Connect via SSH**. This option uses the Secure Shell (SSH) protocol to access a shell account on a remote Mac and execute commands in macOS.

Parallels Device Management uses third-party VNC and SSH client utilities that are installed in Windows automatically when you install the Configuration Manager Console Extension component. A VNC server and an SSH server are included in every edition of macOS and are installed on a Mac by default.

**Note:** In both scenarios, VNC and SSH, Parallels Device Management for Configuration Manager uses administrative credentials to connect to administrative profiles. Administrators cannot interact live with end-user sessions. There is no connection to the end-user's active profile for screen sharing.

The following describes how to set up and use each connection option.

## Connect via VNC

Before using this feature, the macOS Remote Management service must be enabled on each individual Mac.

To enable macOS Remote Management:

1. Log into a Mac.
2. Open System Preferences.
3. Choose **View > Sharing**, or click Sharing.
4. In the Service list, select Remote Management and enable it by selecting the On checkbox.
5. Click the **Computer Settings** button and then select the **VNC viewers may control screen with password** checkbox.

6 Choose a VNC password and enter it in the field provided. You will later use the password to establish a VNC connection with the Mac. Whether you choose the same VNC password for all Mac computers in your organization (for simplicity) or a unique password on each Mac depends on your security policies.

7 Click **OK**.

8 Close System Preferences.

When you select the **Connect via VNC** option in the Configuration Manager console, the VNC viewer application starts and asks you to enter the Mac user ID and the VNC password. If the credentials are valid, a window is displayed where you can remotely control the macOS desktop.

### Connect via SSH

Before using this feature, the SSH service must be enabled on each individual Mac.

To enable SSH in macOS:

1 Log into a Mac.

2 Open System Preferences.

3 Choose **View > Sharing**, or click Sharing.

4 In the Service list, select Remote Login and enable it by selecting the On checkbox.

5 Close System Preferences.

When you select the **Connect via SSH** option in the Configuration Manager console, the SSH client application starts and asks you to enter the Mac user ID and password. If the credentials are valid, an SSH window opens where you can type and execute commands in macOS.

CHAPTER 20

# Problem Reporting and Monitoring

The problem reporting functionality helps you to gather system information for the Parallels Configuration Manager Proxy, Configuration Manager Console Extension, and managed Mac computers. The collected information can then be sent to Parallels Support. The following subsections describe how to use the Parallels Device Management problem reporting tools and utilities.

## In This Chapter



# Sending problem reports using Configuration Manager Console

To generate a report and send it to Parallels Support:

1. In the Configuration Manager console, navigate to the Mac you're having a problem with (or any Mac if you can't pinpoint it), right-click it and select **Parallels Management Tools > Send Problem Report**.
2. In the **Problem Report for Parallels Device Management for Configuration Manager** dialog, type a message that will be appended to the report and then click **Send Report**.
3. A window with a progress bar will open informing you of the information gathering progress.

The problem report data gathering consists of the following steps (transparent to the user):

1. The Configuration Manager Console Extension information is collected and is sent to the Parallels Configuration Manager Proxy together with the selected Mac identifier.
2. The Parallels Configuration Manager Proxy collects its own data and then requests the data from the specified Mac computer.
3. The Parallels Mac Client collects its data and sends it back to the Configuration Manager Proxy.
4. The Configuration Manager Proxy merges individual reports into a single one and sends it to Parallels Support.

The final report will contain combined information gathered from all three components: Parallels Configuration Manager Proxy, Console Extension, and the Mac that was selected. After the problem report is sent to Parallels, a dialog will open displaying the report ID. If you would like to request help with the issue, you can submit a ticket to Parallels Support and include this ID for reference.

If you receive an error while using the reporting feature, make sure that the Configuration Manager Proxy and the Mac are running and accessible. If for some reason you cannot start or access the Configuration Manager Proxy or the Mac, you can use the available standalone reporting utilities, which are described in the following section.

# Sending problem reports using a standalone reporting utility

You can also send a problem report using a standalone reporting utility. Compared to the Configuration Manager console reporting feature, this utility will collect information for individual Parallels Device Management components. For example, if you run the utility on the computer where the Parallels Configuration Manager Proxy is installed, the information will be gathered for the Configuration Manager Proxy only. If you run it on the computer where the Configuration Manager Console Extension is installed, the information will be gathered for the Console Extension. If both components are installed on the same computer, both will be included in the report.

To run the utility, go to **Start** > **Apps** > **Parallels** and click the **Send Problem Report** application. The **Send Problem Report** dialog opens and the data gathering process begins. Once the report is generated, a message is displayed in the dialog specifying a temporary location on the local hard drive where the report file was saved. In the dialog, do one of the following:

- Click the **Send** button to send the report to Parallels Support. After the report is sent, a message box containing the problem report number is displayed. You can use this number for future reference. The report file is automatically deleted from the temporary location.
- Click **Cancel** to close the dialog without sending the report. If the utility is run on the computer where the Parallels Configuration Manager Proxy is installed, the report file will be forwarded to Configuration Manager Proxy, which will notify the Problem Monitor about it. You can then use the Problem Monitor to view the report summary and to send it to Parallels Support. For the information about Problem Monitor, see **Using Problem Monitoring utility** (p. 193). If the utility is run on the computer where only the Configuration Manager Console Extension is installed, the report file will be deleted from the temporary directly and no other actions will be performed.

# Sending problem reports from Parallels Mac Client

If a Mac user is experiencing a problem with Parallels Mac Client, they can generate a problem report and then send it to the IT administrator.

To generate a report:

1. On a Mac computer, in System Preferences, click the **Parallels Device Management** icon (or click **View** > **Parallels Device Management for Configuration Manager)**.
2. Click the "gear" drop-down menu in the lower left corner and choose **Send Problem Report**. The **Send Problem Report** dialog opens and the report data gathering process begins.
3. Once the report file is generated, a message is displayed in the dialog specifying its location on the local hard drive. Clicking the **Send** button will send the report to the Parallels Configuration Manager Proxy, which will notify the IT administrator through the Problem Monitoring utility. The Problem Monitor can then be used to view the report summary and to send it to Parallels Support if needed.

The problem reporting utility can also be run from Finder as follows:

1. Open Finder and navigate to the `/Library/Parallels/` folder.
2. Locate the `pma_agent.app` package, right-click it and select **Show Package Contents**.
3. In the package, navigate to the `Contents/MacOS` folder and double-click the `pma_report_tool` file. The **Send Problem Report** dialog opens. This is the same dialog as the one described above.

# Using the Problem Monitoring utility

Parallels Device Management for Configuration Manager provides a utility that allows you to monitor the system in real time for possible problems. The utility is installed together with Parallels Device Management and can be accessed on computers where the Parallels Configuration Manager Proxy or the Configuration Manager Console Extension are installed.

The problem monitor runs in the background with a notifier in the Windows taskbar notification area (also called the "system tray"). It receives problem report notifications from the Configuration Manager Proxy and notifies the IT administrator when the reports are available.

The following list describes how the monitor interacts with the Configuration Manager Proxy and the administrator:

1. If there's a problem with Parallels Device Management, the Parallels Configuration Manager Proxy generates a report, saves it to a local file, and sends a notification to the problem monitor that a new report is available.
2. The problem monitor receives the notification and displays a balloon tip in the notification area informing the administrator of a new report.
3. The administrator can open the problem report list, which is populated with the names of the available reports and some basic info about them.
4. The administrator can then send a report to Parallels Support, delete it, or close the list and return to it later.

The rest of this section describes how to use the problem monitor.

### Starting and stopping the Problem Monitor

The monitor starts automatically after you complete the Parallels Device Management installation. It also starts automatically when the computer is rebooted and a user logs in to Windows. If the user is not authorized to access the computer where the Parallels Configuration Manager Proxy is running, a dialog is displayed asking the user to enter a user name and password. After the problem monitor is connected to the Configuration Manager Proxy, it adds a notifier to the taskbar notification area.

To terminate the problem monitor, right click its icon in the notification area and select **Exit** from the context menu. To manually start the monitor, go to **Start** / **Apps** / **Parallels** and click **Problem Monitor**. When the monitor starts, it immediately requests problem report information from the Configuration Manager Proxy. If there are new problem reports, a balloon tip is displayed.

### Receiving Problem Monitor notifications

By default the problem report icon in the notification area is hidden. To make it always appear, right-click the notification area and select **Customize notification icons** in the context menu. Change the behavior of the Problem monitor utility to "Show icons and notifications".

Depending on the problem monitor status, its icon will be one of the following:

-  indicates that there are no new problem reports.
-  indicates that one or more new problem reports are available.
-  indicates that the problem monitor cannot communicate with the Parallels Configuration Manager Proxy. This can happen if the Configuration Manager Proxy is down or if there's a network problem.

The problem monitor communicates with the Configuration Manager Proxy every one minute. If there's a new problem report, the proxy notifies the monitor. Once the notification is received, the problem monitor displays a balloon tip in the notification area and its icon changes accordingly.

### Viewing the problem report list

To view the problem report list, click the balloon to open the **Problem Reports** dialog. If the balloon is not currently displayed, right-click the problem monitor icon and select **Show Problem Reports** from the context menu (or you can simply click the icon).

Each row in the list contains information about an individual report and has the following columns:

- **Created** — contains the date and time when the report was created.
- **Proxy info** — if set to "Yes", indicates that the report contains the information related to the Parallels Configuration Manager Proxy.
- **Mac info** — if set to "Yes", indicates that the report contains the information related to a managed Mac computer.
- **Description** — specifies whether the report was generated automatically or manually by a user.

If there are no problem reports on the server, the list will be empty.

To perform an action on a report, select the report of interest from the list and click one of the available buttons:

- Click **Send** to send the selected problem report to Parallels Support. After the report is sent, it is removed from the server on which it resides.
- Click **Delete** to delete the selected report from the list and the server on which it resides.
- Click **Close** to closes the dialog. The reports will remain in the problem monitor report list and the report files will remain in their original locations.

### Viewing the problem report activity log

The problem monitor maintains an activity log, which contains the information about the operations that were performed on the reports. To view the problem report activity log, right-click the problem monitor icon in the notification area and select **Problem Reports Log** from the context menu. The **Problem Report Operations Log** dialog opens. Each entry in the log describes an individual operation that was performed on a report. This is a read-only information provided as a reference. If a report operation included sending it to Parallels Support, the entry will include the report ID, which can be used when following up on the report with Parallels Support.

CHAPTER 21

# Initiating Policy Retrieval

Managed Mac computers download client policies from Configuration Manager automatically according to a schedule. There may be a need to download the latest policy before the scheduled download occurs. This is especially helpful when you test or debug something. Policy retrieval can be initiated from an individual Mac computer or it can be initiated for multiple Mac computers from the Configuration Manager console.

## In This Chapter



# Initiating policy retrieval from a Mac computer

In System Preferences, click the **Parallels Device Management** icon (or click **View** > **Parallels Device Management for Configuration Manager)**. In the client properties window, click the "gear" drop-down menu in the lower left corner and choose **Connect**. Depending on the result, the following will happen:

- If the connection was successful, the **Policies received** field in the property list will specify how many policy updates have been received.
- If the connection fails (e.g. Parallels Mac Client cannot locate the proxy), a dialog will open asking the user to enter his or her credentials. The credentials will be used to read the current proxy location from Active Directory. Once the location information is obtained, it will be stored in the Parallels Mac Client configuration, so you will not have to enter it again.

### Initiating policy retrieval from the command line

To initiate policy retrieval from the command line, open Terminal, change directory to `/Library/Parallels/pma_agent.app/Contents/MacOS` and type the following command:

```
$ ./pmmctl get-policies
```

On completion, the command returns one of the following XML documents depending on the result.

If policy retrieval fails:

```
<plist version="1.0">
    <dict>
        <key>ErrorCode</key>
        <integer>3</integer>
        <key>ErrorMessage</key>
        <string>Operation timed out</string>
    </dict>
</plist>
```

where the `<integer>` element contains the error code, and the `<string>` element contains the error description.

If policy retrieval was successful:

```
<plist version="1.0">
    <dict>
        <key>ErrorCode</key>
        <integer>0</integer>
        <key>ErrorMessage</key>
        <string>No error</string>
       <key>NumberOfPolicyUpdates</key>
       <integer>5</integer>
    </dict>
</plist>
```

where the `<integer>` value of the `<NumberOfPolicyUpdates>` key contains the number of policy updates retrieved.

To obtain the list of possible error codes with descriptions, use the following command:

```
$ pmmctl error-info
```

The command returns the following list:

```
0: No error
1: Invalid command
2: Operation failed
3: Operation timed out
4: Connection aborted
5: Unknown error code 5
```

# Initiating policy retrieval from the Configuration Manager console

To initiate policy retrieval for multiple Mac computers:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Overview** / **Device Collections.**
2. You can initiate policy retrieval for the entire collection or for selected Mac computers:
   - To select individual Mac computers, double-click the collection containing your Mac computers and then select the desired computers.

- To initiate policy retrieval for the entire collection, simply select the collection without opening it (alternately, you can navigate to **Overview** / **Devices** and select the collection in the left pane).

While the collection or individual Mac computers are selected, right-click on them and then click **Parallels Management Tools** > **Machine Policy Retrieval and Evaluation Cycle** in the context menu**.**

3 The **Requesting Mac Clients to Download Policies** dialog opens and the policy retrieval initiation operation begins automatically. The progress bar informs you of how many Mac computers have been processed.

4 While the operation is in progress, you can hide the dialog by clicking the **Hide** button or by simply closing the dialog. The policy retrieval operation will continue to run in the background. If you want to cancel the operation, click **Cancel**.

5 You can initiate another policy retrieval operation while the current operation is still in progress. To do so, simply repeat the steps above. Additional Mac computers that you select this time will be added to the list of the currently processed Mac computers and the operation will continue uninterrupted.

6 When all Mac computers are processed, you can view the results of the operation by clicking the **Details** button. If the button is disabled, it means that all Mac computers were processed successfully. This means that the policy retrieval operation has been initiated on all selected Mac computers. If the button is enabled, clicking it displays the list of Mac computers that the Parallels Configuration Manager Proxy was unable to connect to. The **Status** column of the list will contain one of the following:

- Offline — the Mac is turned off or unreachable.
- Connection refused — the Mac was reachable but the connection was refused by it.
- No client installed — the Mac doesn't have the Parallels Mac Client installed on it.
- Not a Mac — the resource is not a Mac computer.

You can sort the list by Resource Name or Status by clicking the corresponding column header.

# Index

**E**



**F**



**H**



**I**



**J**



**K**



**L**



**M**



**N**

## O



## P



## R



## S



## T



## U

## V



## W