



Parallels Mac Management for Microsoft SCCM

Administrator's Guide

v8.7

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

Copyright © 1999-2020 Parallels International GmbH. All rights reserved.

This product is protected by United States and international copyright laws. The product's underlying technology, patents, and trademarks are listed at <http://www.parallels.com/about/legal/>.

Microsoft, Windows, Windows Server are registered trademarks of Microsoft Corporation.

Apple, Mac, the Mac logo, macOS, iPad, iPadOS, iPhone, iPod touch are trademarks of Apple Inc., registered in the US and other countries.

Linux is a registered trademark of Linus Torvalds.

All other marks and names mentioned herein may be trademarks of their respective owners.

Contents

Introduction	9
Parallels Mac Management Features Overview.....	9
About This Guide	10
Pre-Installation Procedures	11
Parallels Mac Management Component Overview.....	11
Pre-Installation Checklist	12
Installation Requirements	15
General Requirements.....	15
Parallels Configuration Manager Proxy Requirements.....	16
Parallels IBCM/MDM Proxy Requirements.....	18
Parallels NetBoot Server Requirements	22
Parallels OS X Software Update Point Requirements.....	22
The Reporting Functionality Requirements	23
User Rights Requirements.....	23
Permissions for Running Parallels ConfigMgr Proxy Configuration Wizard	24
Permissions for Running Parallels ConfigMgr Proxy Service	28
Permissions for Running Parallels OS X Software Update Point.....	30
Permissions for Running Parallels Netboot Service.....	30
Configuration Manager Boundaries	32
Integrating Parallels Mac Management with PKI	33
PKI Integration Overview	33
What This Section Does Not Cover	34
Creating Certificate Templates for Parallels ConfigMgr Proxy and Mac Computers	34
Creating a Security Group	36
Handling Expired Certificates.....	36
Installation and Configuration	38
Installation Overview.....	38
Install Parallels Mac Management.....	38
Configuring Parallels Configuration Manager Proxy.....	39
Step 1: SMS Provider Location	39
Step 2: Configuration Manager Proxy Service Account	39

Step 3: Prerequisites Check	40
Step 4: Parallels Client Certificate Management Settings	40
Step 5: Role-Based Security	41
Step 6: Configuration Manager Proxy Communication Ports	41
Step 7: Customer Experience Program	42
Step 8: Configuration Settings Summary	42
Verifying the Parallels ConfigMgr Proxy Service Certificate.....	42
Configuring Parallels IBCM/MDM Proxy	43
Configuring Parallels IBCM Proxy	44
Configuring Parallels MDM Proxy.....	45
Secure IBCM/MDM Proxy Website with Wildcard SSL Certificate	54
Configuring Parallels NetBoot Server	54
Configuring Parallels OS X Software Update Point.....	55
Adding or Removing Parallels Mac Management Components.....	56
Upgrading Parallels Mac Management to a Newer Version.....	56
License Activation	58
License Activation Overview	58
Online Activation	59
Offline Activation	59
View and Update License Information	61
Exceeding the License Limit	62
Deactivating Parallels Mac Management	63
Parallels Mac Client Deployment.....	65
Installation Options Overview.....	65
Installing Parallels Mac Client Using Discovery Methods	66
Enabling Remote Access on Mac Computers	66
Configuring Parallels Mac Client Push Installation Properties	67
Using Parallels Network Discovery.....	68
Using SCCM Active Directory System Discovery	71

Running Parallels Mac Client Installer on a Mac Computer	71
Installing Parallels Mac Client Using a Script	73
Push Install or Update Parallels Mac Client	74
Configuring the macOS Firewall	76
Verifying Parallels Mac Client Deployment	76
Updating Parallels ConfigMgr Proxy Connection URL.....	77
Uninstalling Parallels Mac Client	77
Upgrading Parallels Mac Client.....	78
Automatic Upgrade of Parallels Mac Client.....	78
Upgrading Parallels Mac Client via Software Distribution	79
Manually Upgrading Parallels Mac Client	79
Using Parallels Mac Client Tools.....	79
Viewing Parallels Mac Client Properties	79
Initiating Policy Retrieval	81
Sending an Inventory Update to Configuration Manager.....	82
Sending Problem Reports	82
Enrolling Apple Mobile Devices in SCCM.....	84
Prerequisites	84
User Initiated Enrollment.....	84
Mobile Device Resources in SCCM	86
MDM Management Scope	86
Mobile Device License Management	87
De-enroll an Apple Mobile Device.....	87
Managing Apple Mobile Devices.....	88
Parallels ConfigMgr Proxy and Site Migration	89
Migrating Parallels ConfigMgr Proxy to a New Server	89
Migrating Mac Computers to a New Site.....	91
Using Parallels Mac Management for Microsoft SCCM	94
Configuration Manager Admin Console	94
Device Collections in Parallels Mac Management	95
Mac Computer Collections	95
Apple Mobile Device Collection	96

Hardware and Software Inventory	96
Extending Hardware Inventory for Mac Computers	97
Reporting Mac User Logon Information	101
Software Metering.....	104
Compliance Settings	105
Creating a macOS Configuration Profile	106
Creating an Apple Mobile Device Configuration Profile	114
Enforcing FileVault 2 Encryption	115
Enforcing Parallels Desktop Preferences	130
Enforcing Parallels Desktop VM Settings	132
Using Discovery and Remediation Scripts	134
Deploying Configuration Baseline	138
Receiving Compliance Settings Reports	139
Deploying macOS and Executing Task Sequences	140
Prerequisites for Deploying macOS	141
Capturing a macOS Boot Image.....	141
Creating a Bootable USB Drive.....	144
Capturing a macOS System Image	145
Distributing the macOS System Image in SCCM	148
Creating a Task Sequence	150
Deploying a Task Sequence to a Collection.....	166
Running a Task Sequence on a Mac Computer	166
Non-Operating System Deployments	170
Deploying Software via SCCM Package Deployment	172
Creating a Software Package	172
Sending the Package to a Distribution Point.....	175
Deploying the Software	176
Viewing the Package Status	176
Deploying Software via SCCM Application Deployment.....	177
Choose the Installation Type.....	177
Prepare a Mac Application for Configuration Manager.....	178
Create a Configuration Manager Application.....	179
Configure the Deployment Type	180
Deploy the Application.....	182
Installing the Application on a Mac	183

Using Parallels Application Portal.....	185
Uninstalling Applications.....	186
macOS Software Update Management.....	188
Configuration Options.....	188
Configuring Parallels OS X Software Update Point.....	196
Configuring SCCM and Deploying macOS Updates.....	197
Configuring Maintenance Windows.....	202
Executing Scripts on Mac Computers.....	203
Enrolling Mac Computers via Apple DEP.....	204
Enable Parallels MDM.....	204
Establish a Connection to the Apple DEP Web Service.....	204
Create a Device Enrollment Profile.....	206
Deploy Mac Computers.....	208
Using Apple VPP.....	210
Prerequisites.....	210
Configuring Apple VPP Support.....	210
Adding an Application to Apple Business Manager.....	214
Creating an Application.....	217
Deploying the Application.....	223
Installing the VPP Application.....	225
Managing Assigned Licenses.....	227
Uninstalling VPP Applications.....	228
Remote Lock and Wipe.....	229
Prerequisites.....	229
Wipe a Mac Computer.....	230
Unlock a Mac.....	231
Lock an Apple Mobile Device.....	232
Wipe an Apple Mobile Device.....	233
Internet-Based Client Management.....	233
Enrolling Mac Computers.....	234
Testing Internet-Based Client Management.....	234
A Note about Software Updates.....	235

Deploying Parallels Desktop on Mac Computers	235
Deploying SCCM Client in Windows Running in a Virtual Machine	238
Remote Support for Mac Computers	240
Problem Reporting and Monitoring	242
Sending Problem Reports Using Configuration Manager Console	242
Sending Problem Reports Using a Standalone Reporting Utility	243
Sending Problem Reports from Parallels Mac Client	243
Using Problem Monitoring Utility	243
Initiating Policy Retrieval from SCCM	246
Appendices	248
Port Reference	248
Logging	251
Changing Log File Rotation Limits	254
Enforcing TLS 1.2	256
Parallels Mac Management Database	257
Index	258

CHAPTER 1

Introduction

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

In This Chapter

Parallels Mac Management Features Overview	9
About This Guide	10

Parallels Mac Management Features Overview

Parallels Mac Management adds the following Mac and Apple mobile device management features to Microsoft System Center 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 SCCM 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 SCCM 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 SCCM 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 if 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 Mac 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 deploy and use Parallels Mac Management for Microsoft SCCM.

The guide begins with the information on how to prepare your computing environment for the installation of Parallels Mac Management. It then describes in detail how to install and configure Parallels Mac Management components. The guide continues with the information on how to use Parallels Mac Management features. It concludes with appendices containing miscellaneous information.

CHAPTER 2

Pre-Installation Procedures

This chapter describes the pre-installation steps that ensure successful installation of Parallels Mac Management for Microsoft SCCM.

In This Chapter

Parallels Mac Management Component Overview	11
Pre-Installation Checklist	12
Installation Requirements.....	15
User Rights Requirements.....	23
Configuration Manager Boundaries	32
Integrating Parallels Mac Management with PKI	33

Parallels Mac Management Component Overview

Parallels Mac Management for Microsoft SCCM consists of the components described below.

Configuration Manager Console Extension

This component consists of a set of dynamic libraries that extend the Configuration Manager console to provide a graphical user interface enabling you to manage Mac computers. The component must be installed on the computer where the Configuration Manager console is running.

Parallels Configuration Manager Proxy

Sometimes spelled **Parallels ConfigMgr Proxy** in this guide. This is the core Parallels Mac Management component. It is a Windows service application that acts as a proxy between SCCM and Mac computers.

Parallels IBCM/MDM Proxy

A dual component that consists of two parts: **IBCM Proxy** and **MDM Proxy**. When you install the component, you have the ability to enable either IBCM Proxy or MDM Proxy (or both) on a given server.

- **IBCM Proxy** enables Internet-Based Client Management (IBCM) of Mac computers. It serves as a transparent proxy that passes requests between Parallels Mac Client and Parallels Configuration Manager Proxy.
- **MDM Proxy** enables IT administrators to deploy and enroll in SCCM new Mac computers using Apple Device Enrollment Program (Apple DEP). It is also used to enroll Apple mobile devices in SCCM. In addition, MDM Proxy is used to distribute configuration profiles to Mac computers and mobile devices and to use the Remote Lock and Wipe functionality.

Parallels NetBoot Server

NetBoot is a technology from Apple that enables Mac computers to boot from a network. You need to install this component if you plan to deploy macOS images to Mac computers.

Note: Parallels NetBoot Server does not support macOS 11 Big Sur.

Parallels OS X Software Update Point

This optional component allows you to manage Apple software updates (patches) for macOS using the native SCCM functionality.

Parallels Mac Client

A client software that must be installed on Mac computers in order to be managed in SCCM. The software enables communication between a Mac computer and SCCM via the Parallels Configuration Manager Proxy.

For installation requirements of individual components, see the following sections:

- **Pre-Installation Checklist** (p. 12)
- **Installation Requirements** (p. 15)

Pre-Installation Checklist

You can use the checklist below to help you prepare your Microsoft SCCM environment for the deployment of Parallels Mac Management. The **Reference** column contains links to topics describing how to accomplish a task.

Before reviewing the checklist, please also note that you can download the **Parallels Mac Management Prerequisites Check Wizard**, which you can use to verify whether your Microsoft SCCM infrastructure is ready for Parallels Mac Management deployment. To download the wizard, visit <https://www.parallels.com/products/mac-management/download/> and locate the **Utilities** section. When there, click the **Learn More** link to learn what **Prerequisites Checker** is and how to use it.

	Category	Task	Reference
<input type="checkbox"/>	General requirements	Check the requirements for supported SCCM, Windows, and macOS versions.	General Requirements (p. 15)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	Where to install Parallels Configuration Manager Proxy if you have secondary SCCM sites.	Installation Location (p. 16)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	The Distribution Point Role configuration.	Distribution Point Role Configuration (p. 16)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	Verify the IIS settings on the Distribution Point server.	IIS Settings on the Distribution Point Server (p. 16)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	Configuration Manager Boundaries.	Configuration Manager Boundaries Configuration (p. 32)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	Configure Windows firewall.	Port Reference (p. 248)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	Configure macOS firewall.	Configuring macOS Firewall (p. 76)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	Verify the network environment configuration.	Network Configuration (p. 17)
<input type="checkbox"/>	Parallels ConfigMgr Proxy	Check date and time synchronization.	Date and Time Synchronization (p. 17)
<input type="checkbox"/>	Parallels IBCM/MDM Proxy	<p>Optional component that serves two functions (each function can be enabled or disabled during the configuration step):</p> <ul style="list-style-type: none"> - Enables Internet-based client management (IBCM) for Mac computers. - Enables MDM enrollment, which is required to use Apple DEP, Apple mobile device enrollment and management, Remote Lock and Wipe, and distributing security sensitive configuration profiles. 	Parallels IBCM/MDM Proxy Requirements (p. 18)

<input type="checkbox"/>	<p>Migrate Parallels MDM Server</p>	<p>Parallels MDM Server is an older component used in Parallels Mac Management prior to version 8.5. Beginning with v8.5 it was split into Parallels IBCM/MDM Proxy (described above) and the new Parallels MDM service.</p> <p>When upgrading to Parallels Mac Management v8.5, you have the following options:</p> <ul style="list-style-type: none"> - Migrate the existing MDM setup to the new version. This can be done at the time of the upgrade or it can be done later, when the core Parallels Mac Management components are already upgraded and function properly. - Discard the existing MDM setup and then re-enroll Mac computers in MDM from scratch using the new Parallels MDM functionality. 	<p>See KB article https://kb.parallels.com/125034</p>
<input type="checkbox"/>	<p>Parallels NetBoot Server</p>	<p>Optional component. Needed for the macOS image deployment functionality.</p>	<p>Parallels NetBoot Server Requirements (p. 22)</p>
<input type="checkbox"/>	<p>Parallels OS X Software Update Point</p>	<p>Optional component. Needed for the macOS software update functionality.</p>	<p>Parallels OS X Software Update Point Requirements (p. 22)</p>
<input type="checkbox"/>	<p>Other</p>	<p>Verify Reporting Point Role. Optional but needed to view reports.</p>	<p>The Reporting Functionality Requirements (p. 23)</p>
<input type="checkbox"/>	<p>Other</p>	<p>Verify Report Viewer. Optional but needed to view reports.</p>	<p>The Reporting Functionality Requirements (p. 23)</p>
<input type="checkbox"/>	<p>Other</p>	<p>Review the ports used by Parallels Mac Management.</p>	<p>Port Reference (p. 248)</p>
<input type="checkbox"/>	<p>User rights</p>	<p>Verify user rights requirements.</p> <p>Note: This is an important step to ensure a successful installation of Parallels Mac Management for Microsoft SCCM.</p>	<p>User Rights Requirements (p. 23)</p> <p>The KB article at http://kb.parallels.com/121569 contains additional information on how to set up a service account for a proper Parallels Mac Management installation.</p>
<input type="checkbox"/>	<p>PKI integration</p>	<p>Optional, but needed if you would like to integrate Parallels Mac Management with a Public Key Infrastructure (PKI).</p>	<p>Integrating Parallels Mac Management with PKI</p>

Installation Requirements

Before proceeding, please read the subsequent sections to learn about system requirements for installing Parallels Mac Management for Microsoft SCCM. The topics include General Requirements and requirements for installing individual Parallels Mac Management components.

General Requirements

Supported SCCM versions

At the time of this writing, Parallels Mac Management has been tested with Microsoft System Center Configuration Manager 2012 R2 up to Configuration Manager 2010.

For the most up-to-date information about supported SCCM versions, please see <https://kb.parallels.com/124197>

Top-level domain requirement

Parallels Mac Management supports top-level domain structures only (e.g. .com, .edu, .mil, .gov, .net). Pseudo-top-level domains (e.g. .local) are not supported.

Supported Windows and MS SQL Server versions

Same requirements as for the SCCM version that you are using.

Supported macOS versions

- To be managed in SCCM, client Mac computers must be running macOS 10.8 Mountain Lion — macOS 11 Big Sur.
- To capture a boot image for macOS deployment, the reference Mac computer must be running macOS 10.11 El Capitan — macOS 10.15 Catalina. Please note that capturing a boot image is not available with macOS 11 Big Sur. For more info, see **Deploying macOS and Executing Task Sequences** (p. 140).

Supported Apple mobile devices

- iOS devices
- iPadOS devices

Parallels Configuration Manager Proxy Requirements

The subsequent sections describe Parallels Configuration Manager Proxy requirements. The configuration procedure is described in the **Configuring Parallels Configuration Manager Proxy** section. (p. 39)

Installation Location

Parallels Configuration Manager Proxy must be installed on each primary SCCM site. If you have secondary sites, you can choose from the following installation options:

- Installing Parallels Configuration Manager Proxy on the primary and secondary sites. This option allows you to better manage bandwidth utilization between Mac computers, the distribution point, and the management point. You must install Parallels Configuration Manager Proxy on the primary site and then on a secondary site (in that order).
- Installing Parallels Configuration Manager Proxy on the primary site only. If you use this option, Mac computers will communicate directly with the Configuration Manager Proxy installed on the primary site.

Distribution Point Role Configuration

Verify the Distribution Point role configuration:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Site Configuration / Servers and Site System Roles**.
- 2 Select your site in the right pane.
- 3 In the **Site System Roles** pane, right-click the **Distribution Point** role and then click **Properties** in the context menu.
- 4 In the **Distribution Point Properties** dialog set the following options:
 - On the **General** tab, select **HTTP** or **HTTPS** in the **Specify how client computers communicate with this distribution point** group. If you'll be using Public Key Infrastructure (PKI) for authentication, you need to select **HTTPS**. The PKI integration is described in the **Integrating Parallels Mac Management with PKI** section (p. 33).
 - If you've selected **HTTP**, check the **Allow clients to connect anonymously** option.

IIS Settings on the Distribution Point Server

To verify the Internet Information Services settings on the Distribution Point Server, do the following:

- 1 Open **Start > Administrative tools > Internet Information Services (IIS) Manager**.
- 2 Navigate to **Sites / Default Web Site**.
- 3 Click the **Default Web Site** and double-click **Authentication** in the **IIS** section.
- 4 Check that **Windows Authentication** is enabled.

- 5 Click the **Default Web Site** and double-click **Authorization Rules** in the **IIS** section.
- 6 Check that authorization is allowed to all users

Configuration Manager Boundaries Configuration

See **Configuring Configuration Manager Boundaries** (p. 32) for complete details.

Windows and macOS Firewall Configuration

See **Port Reference** (p. 248) and **Configuring macOS Firewall** (p. 76).

Network Configuration

For details on how your network environment should be configured, see the following KB article: <https://kb.parallels.com/118518>

In addition, verify that your Mac computers have network access to SCCM site servers. Use the `traceroute` command in macOS and `tracert` in Windows to verify network access. Access to the following servers needs to be checked:

- The server that will host Parallels Configuration Manager Proxy
- The Active Directory server
- The Management Point role server
- The Distribution Point role server

Check the IP address of the DNS server in macOS network preferences on a Mac:

- 1 In macOS, open **System Preferences / Network**.
- 2 Click the **Advanced** button.
- 3 Click the **DNS** tab.
- 4 In the **DNS Servers** section, add the DNS server address if it's missing.

Date and Time Synchronization

Date and time must be synchronized between servers running Configuration Manager, Parallels Configuration Manager Proxy, Active Directory, Management Point, Distribution Point, and all Mac computers that you want to manage. If date/time is out of sync, the Parallels Mac Client registration procedure and Mac management operations (specifically, policy downloading and updating) may not work correctly.

Parallels IBCM/MDM Proxy Requirements

Parallels IBCM/MDM Proxy is a dual component that consists of two parts: **IBCM Proxy** and **MDM Proxy**. When you install the component, you have the ability to enable either IBCM Proxy or MDM Proxy (or both) on a given server.

- **IBCM Proxy** enables Internet-Based Client Management (IBCM) of Mac computers. It serves as a transparent proxy that passes requests between Parallels Mac Client and Parallels Configuration Manager Proxy.
- **MDM Proxy** enables IT administrators to deploy and enroll in SCCM new Mac computers using Apple Device Enrollment Program (Apple DEP). It is also used to enroll Apple mobile devices in SCCM. In addition, MDM Proxy is used to distribute configuration profiles to Mac computers and mobile devices and to use the Remote Lock and Wipe functionality.

Note: Beginning with Parallels Mac Management for Microsoft SCCM v8.5, the Parallels MDM functionality has changed. The older Parallels MDM Server component is no longer used. It was split into Parallels IBCM/MDM Proxy (the Internet facing part) and the new Parallels MDM service (the Intranet part). When upgrading to Parallels Mac Management v8.5, you can migrate the existing MDM setup or you can discard it and then re-enroll Mac computers in MDM using the new functionality from scratch. For detailed information, please see KB article <https://kb.parallels.com/125034>

When you install Parallels IBCM/MDM Proxy, both IBCM Proxy and MDM Proxy are installed together (as was said earlier, they are essentially the same component with two functions). You do, however, have the ability to enable one or the other (or both) on a particular server when you configure the component. This means that you can have both proxies running on the same or different servers depending on your needs.

Parallels IBCM/MDM Proxy prerequisites are listed in the section that follows this one. IBCM and MDM specifics are described in subsequent sections.

Prerequisites

In order for Parallels IBCM/MDM Proxy to work, Parallels Mac Management must be configured for Public Key Infrastructure (PKI). For details please see **Integrating Parallels Mac Management with PKI** (p. 33).

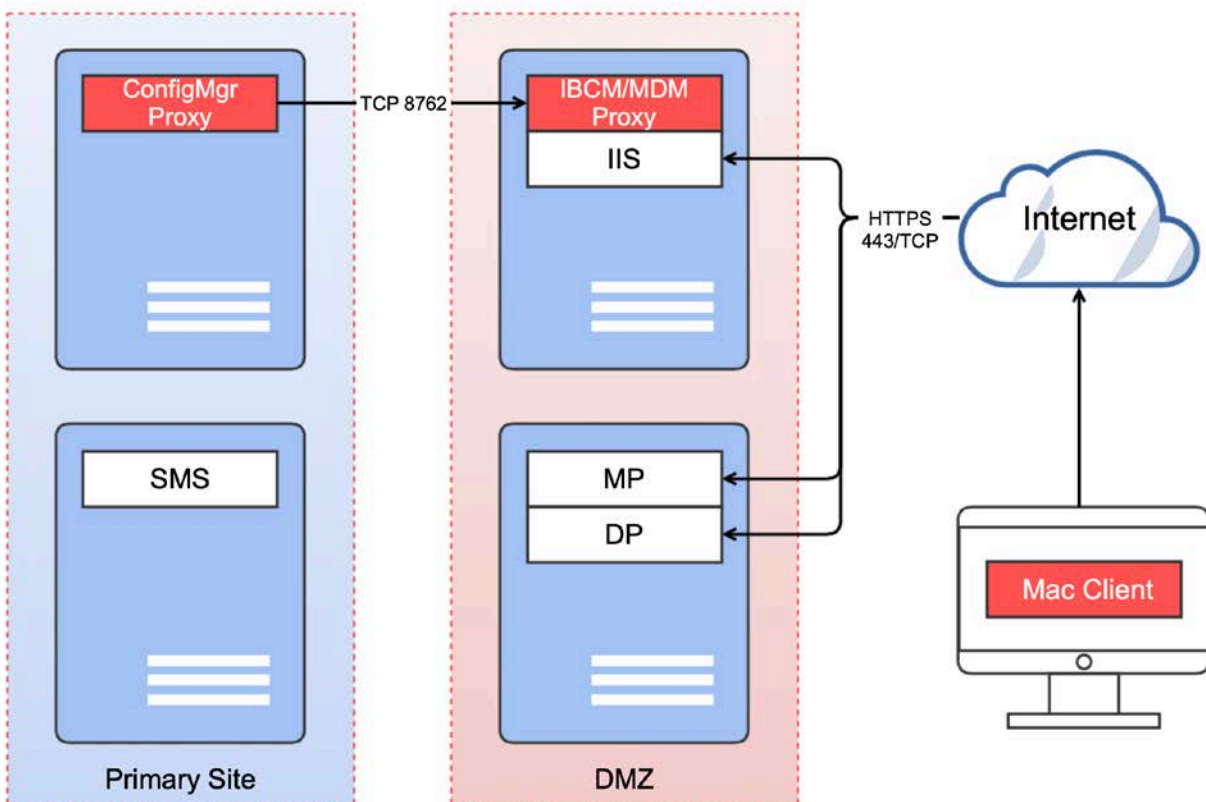
Other requirements for installing Parallels IBCM/MDM Proxy are:

- The server on which you'll be installing Parallels IBCM/MDM Proxy must be accessible from the server where Parallels ConfigMgr Proxy is installed (p. 16). Note that the Parallels ConfigMgr Proxy must be installed and configured before you install Parallels IBCM/MDM Proxy.
- The server must be accessible from the Internet. For increased security, the server should be located in DMZ.
- Ensure that a publicly available domain name is assigned to the server. Mac computers and Apple mobile devices will use this domain name to communicate with Parallels IBCM/MDM Proxy over the Internet.

- IIS 7.0 or above must be installed.
- IIS Web Server role must be installed.
- IIS Management script and tools must be installed.
- Placing Internet-enabled SCCM roles in DMZ is highly recommended (but not required).
- If you have multiple primary SCCM sites, a separate instance of Parallels IBCM/MDM Proxy must be deployed for each site.
- IBCM must be configured in SCCM with at least one Internet-enabled Management Point role and Distribution Point role. Planning and implementing the network infrastructure, as far as configuring native Internet-based client management in SCCM, is out of scope of this guide.

IBCM/MDM Proxy Architecture

A typical infrastructure used by Parallels IBCM/MDM Proxy is illustrated in the diagram below. Another diagram in the section that follows this one illustrates MDM specifics related to communications with Apple DEP and APNs services.



- Parallels IBCM/MDM Proxy serves as a transparent proxy that passes requests between managed devices (Mac computers and Apple mobile devices) and Parallels Configuration Manager Proxy.

- The connector is a plugin to IIS, which is also used by SCCM in the IBCM setup for communications between Mac computers on the Internet and Management Points / Distribution Points.
- A single instance of Parallels IBCM/MDM Proxy serves a single primary SCCM site. If you have multiple primary sites, then you will need to repeat the hierarchy shown above for each primary SCCM site.

Parallels Configuration Manager Proxy establishes a permanent SSL-secured link with Parallels IBCM/MDM Proxy, which is configured after the components are installed. Trust is established using the certificate pinning mechanism, when each party is configured to stick to a specific certificate of another party.

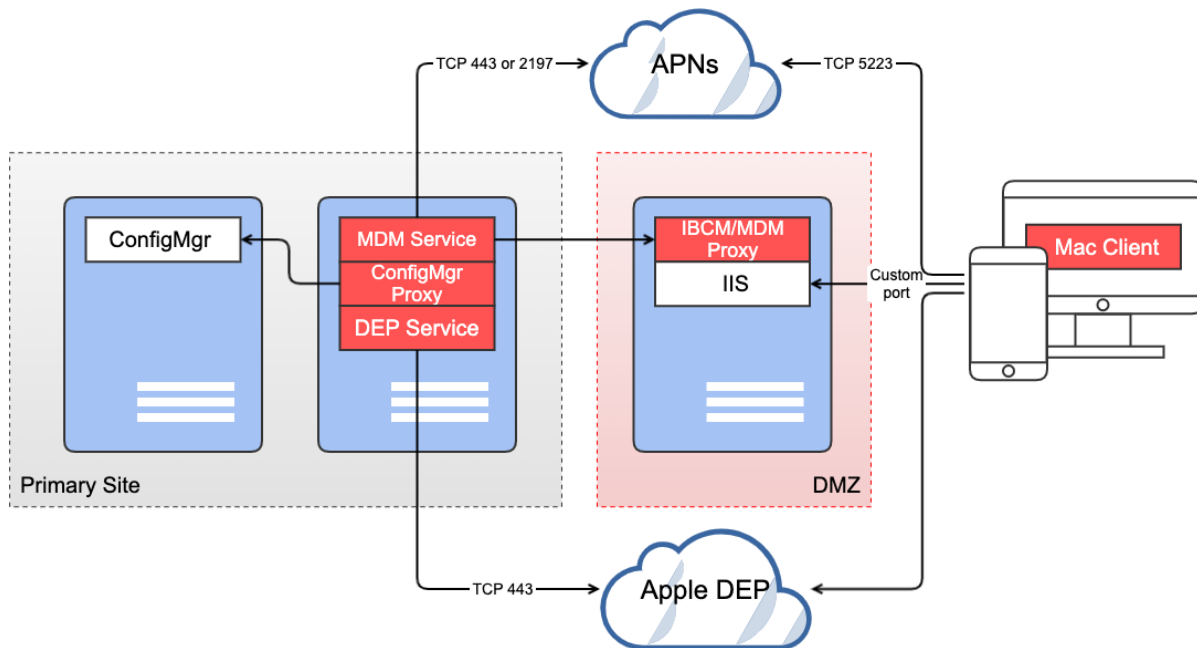
Each Mac computer enrolled in SCCM from the Intranet automatically obtains the public URL of the Parallels IBCM/MDM Proxy. When a computer or an Apple mobile device is enrolled over the Internet, the user enters the URL manually (the URL is obtained from the IT administrator). When a managed device needs to communicate with SCCM, it first connects to Parallels IBCM/MDM Proxy and obtains the necessary links to Management and Distribution Points which are accessible from the Internet.

Parallels IBCM Proxy configuration steps are described in detail in **Configuring Parallels IBCM Proxy** (p. 44).

For detailed port information, please see **Port Reference** (p. 248).

MDM Proxy Specifics

The following diagram shows components that participate in a Parallels Mac Management MDM configuration. It provides information on where the components are located and how they communicate with each other. Please also see the IBCM/MDM Proxy diagram in the previous section.



Please note that beginning with Parallels Mac Management v8.7, push notifications have been upgraded to the **HTTP/2-based Apple Push Notification service (APNs) provider API**. The legacy binary protocol is no longer used. The APNs connection is now established with the following Apple server:

```
api.push.apple.com:443
```

You can alternatively use port 2197 when communicating with APNs. You might do this, for example, to allow APNs traffic through your firewall but to block other HTTPS traffic. The port is changed in the registry as follows:

- Registry path: [HKEY_LOCAL_MACHINE\Software\Wow6432Node\Parallels\Parallels Mac Management for Microsoft SCCM\Mdm]
- To enable the alternative port, set the DWORD value to 1:
"UseAlternativeApnsPort"=dword:00000001
- To enable the standard port, set the DWORD value to 0:
"UseAlternativeApnsPort"=dword:00000000

Please also note that port numbers specified on the diagram are used for communications with Apple services and cannot be changed (apart from APNs server ports 443 and 2197 described above). Port numbers that are not specified (the Parallels IBCM/MDM Proxy ports) are configured when you run the Parallels IBCM/MDM Proxy Configuration Wizard.

Parallels MDM configuration steps are described in detail in the **Configuring Parallels MDM Proxy** section (p. 45).

For detailed port information, please see **Port Reference** (p. 248).

Parallels NetBoot Server Requirements

Note: Parallels NetBoot Server does not support macOS 11 Big Sur.

Parallels NetBoot Server must be installed on a server where the Distribution Point role is installed. The server must also meet the following requirements:

- Must be a PXE service point.
- Must have WDS installed and running. If both WDS and DHCP are installed on the same server, the **Do not listen on port 67** option must be selected in the WDS service properties.
- Background Intelligent Transfer Service (BITS) must be installed and enabled. Parallels Mac Management has been tested with BITS 4.0 and 5.0.

Additionally, the user account that you'll use to configure the Parallels NetBoot Server must have sufficient privileges. See the following KB article: <https://kb.parallels.com/117937>

Depending on your network topology, you may also need to configure UDP traffic forwarding, so DHCP broadcast packets from Mac computers can reach the DHCP server and the NetBoot server. For the complete information about setting up the network environment for NetBoot, please read the following KB article: <https://kb.parallels.com/118518>.

Please also see **Port Reference** (p. 248) for the list of ports used by the Parallels NetBoot Server.

Parallels NetBoot Server configuration steps are described in detail in the **Configuring Parallels NetBoot Server** section. (p. 54)

Parallels OS X Software Update Point Requirements

Note: Parallels OS X Software Update Point doesn't support CAS (Central Administration Site). In general, you may configure Parallels Software Update Point with CAS, but the feature may not work correctly.

In order to install Parallels OS X Software Update Point, the following requirements must be met:

- The server on which Parallels OS X Software Update Point will be installed must have the .Net Framework v4.0 or later installed.

- Windows Server Update Services (WSUS) must be installed and configured for local publishing of updates. Please see the following page on the Microsoft's website for more info:
<https://msdn.microsoft.com/library/bb902479>
On the web page, refer to the "To set up the update server for locally-published content" section for instructions.
- A user account must be configured for running the Parallels OS X Software Update Point service. The account must have administrative rights on the local sever and must be a member of the **WSUS Administrators** group.
- The WSUS signing certificate must be deployed and accessible by the user account that will be running the Parallels OS X Software Update Point service. Please see the following KB article for more information: <https://kb.parallels.com/123756>.

Parallels OS X Software Update Point configuration steps are described in detail in the **Configuring Parallels OS X Software Update Point** section (p. 55).

The Reporting Functionality Requirements

The Reporting Point role and report viewer described below are not required in order to install Parallels Mac Management, but are needed for the reporting functionality to work.

Reporting Point Role

To verify that the Reporting Point role is installed:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Site Configuration / Servers and Site System Roles**.
- 2 Verify that the **Reporting services point** role exists.
- 3 Navigate to **Monitoring / Reporting / Reports**.
- 4 Right-click any of the available reports and check that the **Run** item is available in the context menu.

Report Viewer

To verify that the Report Viewer is installed:

- 1 In the Configuration Manager console, click **Start > Control Panel > Programs and Features**.
- 2 Verify that **Microsoft Report Viewer Redistributable** is installed.

User Rights Requirements

To install, configure, and run Parallels Mac Management for Microsoft SCCM, you will need to create and configure user accounts with sufficient privileges to perform their respective tasks.

Permissions for Running Parallels ConfigMgr Proxy Configuration Wizard

A user that will be running the Parallels Configuration Manager Proxy Configuration Wizard must have specific permissions, which are described in this section.

The material presented in this section considers two possible scenarios:

- The Parallels Configuration Manager Proxy is configured for the first time.
- The Proxy has been previously configured and you want to reconfigure it using a different user account.

Some of the instructions apply to the first scenario only and some apply to both. Simply follow the instructions that correspond to your configuration and skip those that don't.

Note: When creating (or choosing) a user account that you will use to configure Parallels Configuration Manager Proxy, consider the following. If Parallels Configuration Manager Proxy and Active Directory will run on different computers, the described permissions must be granted directly to the user or to a custom group (not a built-in group, like Administrators) to which the user belongs. If Parallels ConfigMgr Proxy and AD will run on the same server, you can add the user to a built-in group.

Create a Domain User

The user configuring Parallels Configuration Manager Proxy must be a domain user. You can choose an existing domain user or create a new one.

Local Administrator Rights

The user must have administrative rights on the computer where the Parallels Configuration Manager Proxy will be installed:

- 1 Log into the computer that will run Parallels ConfigMgr Proxy.
- 2 Open Server Manager and navigate to **Configuration / Local Users and Groups / Groups**.
- 3 Right-click the Administrators group and select **Properties** in the context menu.
- 4 In the **Select Users** dialog, click **Add** and add the domain user you've created earlier. Click **OK** and then **OK** again.

DCOM Remote Activation Permission

The user must have the DCOM Remote Activation permission:

- 1 On the computer where the SMS Provider is installed, click **Start > Administrative Tools > Component Services**.

- 2 In the **Component Services** window, navigate to **Console Root / Component Services / Computers / My Computer / DCOM Config**. Scroll down to Windows Management and Instrumentation, right-click it, and then click **Properties** in the context menu.
- 3 Click the **Security** tab. The **Launch and Activation Permissions** section will have either the **Use Default** or the **Customize** option selected depending on your server configuration.
- 4 If the **Customize** option is selected, click the **Edit** button, then add the user to the list and grant the user the Remote Activation permission. You may skip the remaining steps.
- 5 If the **Use Default** option is selected, close this window and continue with the following steps.
- 6 In the **Component Services** window, navigate to **Console Root / Component Services / Computers**. Right-click **My Computer** and click **Properties** in the context menu.
- 7 Click the **COM Security** tab.
- 8 In the **Launch and Activation Permissions** section, click **Edit Default**.
- 9 Add the user to the list and grant the user Remote Activation permission.

Administrative Rights in SCCM

The user must have full administrator rights in Configuration Manager:

- 1 Log into the computer running the Configuration Manager console.
- 2 In the Configuration Manager console, navigate to **Administration / Overview / Security**.
- 3 Right-click **Administrative Users** and click **Add User or Group** in the context menu.
- 4 In the **Add User or Group** dialog, click **Browse**, find the domain user that you created earlier, and then click **OK**. The user will appear in the **User or group name** field in the **Add User or Group** dialog.
- 5 Click the **Add...** button in the **Assigned security roles** section.
- 6 In the **Available security roles** list, select **Full Administrator** and click **OK**.
- 7 Click **OK** to close the **Add User or Group** dialog.

Permissions in Active Directory

The user must have the necessary permissions in Active Directory. These permissions are required to create Parallels Mac Management-specific containers in AD and to manipulate data in these containers.

To grant the permissions:

- 1 Open ADSI Edit by clicking **Start > Administrative Tools > ADSI Edit**.
- 2 Verify that the following container exists: DC=<domain> / DC=<com> / CN=System / CN=ParallelsServices.

- 3 If the container above doesn't exist, grant the user the **Create All Child Objects** and **Read** permissions on the CN=System container. When granting these permissions to the user, apply it to **This object and all descendant objects**.
- 4 If the container exists, do the following:
 - Make sure the user have Read, Write, and Create All Child Objects permissions on it.
 - Make sure the user has the Full Control permission on the CN=ParallelsServices / PmaConfigMgrProxy-<site-code> container.
- 5 Verify that the DC=<domain> / DC=<com> / CN= Program Data / CN=Parallels container exists.
- 6 If the container above doesn't exist, grant the user the **Create All Child Objects** and **Read** permissions on the CN=Program Data container. When granting these permissions to the user, apply it to **This object and all descendant objects**.
- 7 If the CN=Parallels container exists, continue with the following steps.
- 8 Verify that the CN=Parallels / CN=Parallels Management Suite container exists. If it doesn't, grant the user the **Create All Child Objects** and **Read** permissions on CN=Parallels container.
- 9 If the CN=Parallels / CN=Parallels Management Suite container exists, make sure that the user has Read, Write, and Create All Child Objects permissions on it.

Permissions to Read/Write Service Principle Name

The user must have permissions to read/write Service Principle Name. These permissions are required for the RBAC functionality. The Parallels Configuration Manager Proxy service account must have a registered Service Principle Name (SPN) for Kerberos connections. By default (with some exceptions) users are not permitted to register SPN to their own accounts.

To grant the permissions:

- 1 Open ADSI Edit by clicking **Start > Administrative Tools > ADSI Edit**.
 - 2 Locate the required object:
 - If you specify a user as a service account during the configuration, you should locate this user object.
- Note:** The user object you select in this step must be the object of the user that will be used to run the service, not of the user that will be used to configure it. If you'll be using the same user to configure and to run the Parallels Configuration Manager Proxy service, then select the domain user object that you created in previous steps.
- If you choose LocalSystem as a service account during the configuration, you should locate the computer object you are running Proxy on.
 - 3 Right-click the object, select **Properties** in the context menu, and then click the **Security** tab in the user properties dialog.
 - 4 Add the user that will be configuring the Parallels Configuration Manager Proxy to the **Group or user names** list and then click the **Advanced** button.

- 5 In the **Advanced Security Settings** dialog, select the user that you added to the list in the previous step and click the **Edit** button.
- 6 In the **Permission Entry** dialog, click the **Properties** tab.
- 7 In the **Apply** to drop-down list, select **This object only**.
- 8 In the **Permissions** list, select the **Read servicePrincipalName** and **Write servicePrincipalName** permissions.
- 9 Close all dialogs.

Microsoft SQL Server Permissions

The user must have necessary permissions in Microsoft SQL Server. These permissions are needed to create and use a database storing the Parallels Mac Management data.

To grant the user the right to create databases in SQL Server, assign the user to the dbcreator role as follows:

- 1 Run SQL Server Management Studio.
- 2 Connect to the SQL server.
- 3 Verify that the user that will be configuring Parallels Configuration Manager Proxy exists in **Security / Logins**. If the user doesn't exist, add the user to the **Logins** list. To do so, right-click **Logins** and then click **New Login**. Select **Windows authentication** and specify the **Login name** as domain\username (or click **Search** to search for the user). Click **OK** when done.
- 4 Navigate to **Security / Server Roles**, right-click the **dbcreator** role, and then click **Properties** in the context menu.
- 5 In the **Server Role Properties** dialog, click **Add...**
- 6 In the **Select Logins** dialog, click **Browse** to search for and select the user that will configure Parallels Configuration Manager Proxy.
- 7 Close all dialogs.

If you have previously configured Parallels Mac Management Proxy on this site, then the Parallels Mac Management database should already exist in this SQL Server instance. To verify this, connect to the SQL Server and look for a database named "PMM_<side-code>" (where <side-code> is your SCCM site code). If a database with such a name exists, then perform the steps below. If the database doesn't exist, skip to the next section.

Assuming that the "PMM_<side-code>" database exists, grant the user the necessary permissions on it as follows:

- 1 In Microsoft SQL Server Management Studio, navigate to **Security / Logins**.
- 2 Right-click the user that will configure the Parallels ConfigMgr Proxy and click **Properties**.
- 3 In the left pane, click **User Mapping**.
- 4 In the right pane, select the "PMM_<side-code>" database (select the **Map** checkbox) and then select the following roles in the **Database role membership** list:

- db_datareader
- db_datawriter
- db_ddladmin
- db_securityadmin
- public

5 Click **OK**.

Administrative Rights in Authorization Manager

If Parallels Configuration Manager Proxy has been configured previously and the Authorization Store exists, the user configuring the Parallels ConfigMgr Proxy must be assigned to the Administrator role in Authorization Manager.

To assign the user to the Administrator role:

- 1 Start Microsoft Management Console (run mmc.exe).
- 2 In the MMC, click **File > Add/Remove Snap-in...**
- 3 Select **Authorization Manager** in the **Available snap-ins** list and click **Add**.
- 4 Click **OK**.
- 5 Right-click **Authorization Manager** and then click **Open Authorization Store...**
- 6 Select **Active Directory or Active Directory Application Mode (ADAM)** and click **Browse**.
- 7 Select CN=Authorization Store,CN=Parallels Management Suite,CN=Parallels,CN=Program Data, DC=<domain>,DC=<com>.
- 8 Click **OK** and **OK** again to close the dialogs.
- 9 Expand **Authorization Manager** in the left pane, right-click **Authorization Store**, and then click **Properties**.
- 10 Click the **Security** tab.
- 11 In the **Authorization Manager user role** drop-down list, select **Administrator**.
- 12 Click **Add** and add the user that will configure Parallels Configuration Manager Proxy to the **Users and groups that are assigned to this role** list.
- 13 Click **OK** to save the changes and close the dialog.

Permissions for Running Parallels ConfigMgr Proxy Service

Parallels Configuration Manager Proxy runs as a service in Windows. The user account under which it runs must have specific permissions. This article describes these permissions.

Note: When creating (or choosing) a user account that will be used to run the Proxy service, consider the following. If Parallel Configuration Manager Proxy and Active Directory will run on different computers, permissions must be granted directly to the user or to a custom group (not a built-in group, like Administrators) to which the user belongs. If the Proxy and AD will run on the same server, you can add the user to a built-in group.

The user account that will be used for running Parallels Configuration Manager Proxy must be a domain user. You can use an existing domain user or you can create a new one.

The user must be a local administrator on the computer running the Parallels Configuration Manager Proxy.

The user must have the DCOM Remote Activation permission. To grant the permission:

- 1 On the computer where the SMS Provider is installed, click **Start > Administrative Tools > Component Services**.
- 2 In the **Component Services** window, navigate to **Console Root / Component Services / Computers / My Computer / DCOM Config**. Scroll down to **Windows Management and Instrumentation**, right-click it, and then click **Properties** in the context menu.
- 3 Click the **Security** tab. The **Launch and Activation Permissions** section will have either the **Use Default** or the **Customize** option selected depending on your server configuration.
- 4 If the **Customize** option is selected, click the **Edit** button, then add the user to the list and grant the user the **Remote Activation** permission.
- 5 If the **Use Default** option is selected, close this window and continue with the following steps.
- 6 In the **Component Services** window, navigate to **Console Root / Component Services / Computers**. Right-click **My Computer** and click **Properties** in the context menu.
- 7 Click the **COM Security** tab.
- 8 In the **Launch and Activation Permissions** section, click **Edit Default**.
- 9 Add the user to the list and grant the user **Remote Activation** permission.

The user must have full administrator rights in Configuration Manager. To set the rights:

- 1 Log into the computer running the Configuration Manager console.
- 2 In the Configuration Manager console, navigate to **Administration / Overview / Security**.
- 3 Right-click **Administrative Users** and click **Add User or Group** in the context menu.
- 4 In the **Add User or Group** dialog, click **Browse**, find the domain user that you created earlier, and then click **OK**. The user will appear in the **User or group name** field in the **Add User or Group** dialog.
- 5 Click the **Add...** button in the **Assigned security roles** section.
- 6 In the **Available security roles** list, select **Full Administrator** and click **OK**.
- 7 Click **OK** to close the **Add User or Group** dialog.

- 8 If the CN=System / CN=ParallelsServices / CN=PmaConfigMgrProxy-<site-code> container exists in Active Directory, the user must have Read, Write, and Create All Child Objects permissions on it.

Permissions for Running Parallels OS X Software Update Point

A user account must be configured for running the Parallels OS X Software Update Point service. The account must meet the following requirements:

- Have administrative rights on the local server.
- Be a member of the **WSUS Administrators** group.

For additional information, please see **Parallels OS X Software Update Point Requirements** (p. 22).

Permissions for Running Parallels Netboot Service

To configure Parallels NetBoot Server, the user performing the configuration and the user account which will be used for running Parallels NetBoot service must have the following privileges:

- Administrator rights on the local computer
- Remote activation permissions
- Read access to SMS Provider

Create a Domain User

Users who will be configuring Parallels NetBoot Server and running Parallels NetBoot service must be domain users.

To create a domain user:

- 1 On a server running Active Directory, open Server Manager by clicking **Start > Administrative Tools > Server Manager**.
- 2 Expand **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > <domain-name>**.
- 3 Right-click **Users** and then click **New > User**.
- 4 In the **New Object – User** dialog, specify **Full name**, **User logon name**, and then click **Next**.
- 5 Type a password in the **Password** and **Confirm password** fields and click **Next**.
- 6 Click **Finish**.

Local Administrator Rights

Both users (for configuring and running the NetBoot service) must have administrative rights on the computer where the Parallels NetBoot Server will be installed.

To grant the administrative privileges to a user:

- 1 Log in to the computer that will run the NetBoot server.
- 2 Open Server Manager and navigate to **Configuration / Local Users and Groups / Groups**.
- 3 Right-click the **Administrators** group and select **Properties** in the context menu.
- 4 In the **Select Users** dialog, click **Add** and add the domain user you've created earlier. Click **OK** and click **OK** again.

DCOM Remote Activation Permission

Both users must have the DCOM Remote Activation permission:

- 1 On the computer where the SMS Provider is installed, click **Start > Administrative Tools > Component Services**.
- 2 In the **Component Services** window, navigate to **Console Root / Component Services / Computers / My Computer / DCOM Config**. Scroll down to **Windows Management and Instrumentation**, right-click it, and then click **Properties** in the context menu.
- 3 Click the **Security** tab. The **Launch and Activation Permissions** section will have either the **Customize** or **Use Default** option selected depending on your server configuration. Depending on the option selected, set the DCOM Remote Activation permission for the user as described in one of the following subsections.

Customize

If the **Customize** option is selected, click the **Edit** button, then add the user to the list and grant the user the **Remote Activation** permission.

Use Default

If the **Use Default** option is selected, close the window and do the following:

- 1 In the **Component Services** window, navigate to **Console Root / Component Services / Computers**.
- 2 Right-click **My Computer** and click **Properties** in the context menu.
- 3 Click the **COM Security** tab.
- 4 In the **Launch and Activation Permissions** section, click **Edit Default**.
- 5 Add the user to the list and grant the user **Remote Activation** permission.

Read Rights in SCCM

The user must have **Read-only Analyst** rights in Configuration Manager:

- 1 Log in to the computer running the Configuration Manager console.

- 2 In the Configuration Manager console, navigate to **Administration / Overview / Security**.
- 3 Right-click **Administrative Users** and click **Add User or Group** in the context menu.
- 4 In the **Add User or Group** dialog, click **Browse**, find the domain user that you created earlier, and then click **OK**. The user will appear in the **User or group name** field in the **Add User or Group** dialog.
- 5 Click the **Add...** button in the **Assigned security roles** section.
- 6 In the **Available security roles** list, select **Read-only Analyst** and click **OK**.
- 7 Click **OK** to close the **Add User or Group** dialog.

Configuration Manager Boundaries

Before deploying Parallels Mac Client on Mac computers, you need to configure Configuration Manager Boundaries. Boundary is a network location on the Intranet that can contain one or more Mac computers that you want to manage. Mac computers are assigned as clients to SCCM according to the boundaries configured in the Configuration Manager console.

Note: Please make sure that you complete all of the steps described below or you will not be able to enroll your Mac computers in Configuration Manager.

Create a Boundary

To create new (or modify an existing) boundary:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Hierarchy Configuration / Boundaries**.
- 2 To create a new boundary, right-click **Boundaries** and click **Create Boundary**. To modify an existing boundary, right-click it and select **Properties** from the context menu.
- 3 On the **General** tab page, select the desired boundary type and specify the value(s) in such a way that IP addresses of your Mac computers lie within this boundary. Please note that Parallels Mac Management supports the following boundary types:
 - IP subnet
 - IP address range
 - Active Directory site

Create a Boundary Group

After you create a boundary, you need to create a boundary group, add the boundary to it, and associate a site system server with the group.

To create a new or modify an existing boundary group:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Hierarchy Configuration / Boundary Groups**.
- 2 To create a new boundary group, right-click **Boundary Groups** and click **Create Boundary Group**. To modify an existing boundary, right-click it and select **Properties** from the context menu.
- 3 On the **General** tab page, specify a boundary name and optional description.
- 4 Click the **Add** button and select a boundary from the list. Click **OK**.
- 5 On the **References** tab page, select the **Use this boundary group for site assignment** option.
- 6 Select your site in the **Assigned site** drop-down box.
- 7 In the **Content location** section, click the **Add** button and select a site system server to associate with this boundary group. Click **OK**.
- 8 Click **OK** to save the boundary group and close the window.

Integrating Parallels Mac Management with PKI

Parallels Mac Management for Microsoft SCCM can be directly integrated with Public Key Infrastructure (PKI). Such integration enables the use of certificates for advanced user authentication and secure access to SCCM.

If you would like to integrate Parallels Mac Management with PKI, you need to complete the steps described in the following subsections prior to installing Parallels Mac Management. If not, you can skip this section and continue with **Installing Parallels Mac Management for Microsoft SCCM** (p. 38). You can perform the PKI integration at any time later by completing the steps described in this section and then reconfiguring Parallels Mac Management. The reconfiguration involves running the **Configuration Manager Proxy Configuration Wizard** (described later in this guide) and specifying the appropriate options on the **Parallels Client certificate management settings** page of the wizard.

PKI Integration Overview

The integration of Parallels Mac Management for Microsoft SCCM with PKI enables the following security features:

- Obtaining security certificates for assigned Mac computers from a certificate authority trusted by SCCM.
- Securing communications between Mac computers and SCCM by using mutual authentication and encrypted data transfers.

Parallels Mac Management supports certificate authority certificates on the following versions of Windows:

- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note: Integration is provided for Microsoft Certificate Services only. No third-party certificate services are supported

What This Section Does Not Cover

The material presented in this section does not cover any of the concepts behind PKI design and implementation. It describes what needs to be done in order to integrate Parallels Mac Management with an existing PKI installation. If you would like to learn more about PKI, you can read the **Securing Public Key Infrastructure (PKI)** content on the Microsoft's website, which can be found at the following URL:

<https://technet.microsoft.com/library/dn786443.aspx>

Creating Certificate Templates for Parallels ConfigMgr Proxy and Mac Computers

To enable Mac connectivity to HTTPS-enabled SCCM infrastructure, a Mac must obtain digital certificates from the certificate authority (CA) trusted by SCCM. Digital certificates secure the communication between Mac computers and the Configuration Manager site by using mutual authentication and encrypted data transfers.

Creating a Certificate Template for Parallels Configuration Manager Proxy

To create a certificate template:

- 1** In Windows, click **Start > Administrative Tools > Certification Authority**.
- 2** Expand the tree of your Certification Authority.
- 3** Right-click **Certificate Templates** and click **Manage**. The **Certificate Template Console** opens.
- 4** In the template list, locate **Web Server**, right-click it and then click **Duplicate Template**. The **Properties of New Template** dialog opens.
- 5** On the **Compatibility** tab page, select **Windows Server 2008** as **Certification Authority** and **Windows 7 / Server 2008 R2** as **Certificate recipient**.
- 6** On the **General** tab page, specify a template name.
- 7** On the **Cryptography** tab page:

- Set **Minimum key size** to 2048.
 - Set **Provider Category** to **Legacy Cryptographic Service Provider**.
 - Set **Algorithm** to **Determined by CSP**.
- 8** On the **Request Handling** tab page, select the **Allow private key to be exported** option.
 - 9** On the **Subject Name** tab page, select the **Supply in the request** option and the **Use subject information from existing certificates for autoenrollment renewal requests** option.
 - 10** On the **Extension** tab page, double-click the **Application Policies** extension, then click **Add** and select **Client Authentication** from the list. Click **OK** and then **OK** again. The **Client Authentication** description should appear in the **Description of Application Policies** list.
 - 11** On the **Security** tab page, add the server that hosts Parallels Configuration Manager Proxy and the user account under which the Proxy is running. Grant them **Enroll** and **Autoenroll** permissions. Please note that if the Proxy is running under the LocalSystem account, then you only need to add the computer name.
 - 12** Click **OK** to close the **Properties of New Template** dialog.
 - 13** Close the **Certificate Template Console**.
 - 14** Back in the **Certification Authority** window, right-click **Certificate Templates** again and choose **New > Certificate Template to Issue**.
 - 15** Select the template that you created in the previous steps and click **OK** to enable it.

Creating a Certificate Template for Mac Computers

To create a certificate template:

- 1** In Windows, click **Start > Administrative Tools > Certification Authority**.
- 2** Expand the CA tree, right-click **Certificate Templates** and click **Manage**.
- 3** The **Certificate Template Console** opens.
- 4** In the template list, locate **Workstation Authentication**, right-click it and then click **Duplicate Template** in the context menu.
- 5** On the **Compatibility** tab page, select **Windows Server 2008** as **Certification Authority** and **Windows 7 / Server 2008 R2** as **Certificate recipient**.
- 6** On the **General** page, specify a template name.
- 7** On the **Cryptography** tab page:
 - Set **Minimum key size** to 2048.
 - Set **Provider Category** to **Legacy Cryptographic Service Provider**.
 - Set **Algorithm** to **Determined by CSP**.
- 8** On the **Request Handling** tab page, select the **Allow private key to be exported** option.
- 9** On the **Subject Name** tab page, select the **Supply in the request** option. The **Certificate Templates** message box will pop. Click **OK** to close it.

- 10** On the **Subject Name** tab page, select **Use subject information from existing certificates for autoenrollment renewal requests** option.
- 11** On the **Extension** tab page, make sure that **Client Authentication** is displayed in the **Description of Application Policies** list. If it's not, add it.
- 12** On the **Security** tab page, add the server that hosts Parallels Configuration Manager Proxy and the user account under which the Proxy is running. Grant them **Enroll** and **Autoenroll** permissions. If the Proxy is running under the LocalSystem account, then you only need to add the computer name.
- 13** Click **OK** to close the **Properties of New Template** dialog.
- 14** Close the **Certificate Templates Console**.
- 15** In the **Certification Authority** window, right-click **Certificate Templates** and click **New > Certificate Templates to Issue**.
- 16** In the **Enable Certificate Templates dialog**, select the template that you created in the previous steps and click **OK** to enable it.

Creating a Security Group

Create a dedicated security group and grant it the rights to request certificates from the certificate authority. The following users must be added to this group:

- An administrator who will be installing and configuring Parallels Configuration Manager Proxy. This is needed because the Parallels ConfigMgr Proxy configuration utility will request the certificate for the Proxy.
- An account under which the Parallels Configuration Manager Proxy service will run. This is needed because the Proxy will be requesting certificates for Mac computers.

Handling Expired Certificates

Parallels Configuration Manager Proxy can automatically handle a situation when digital certificates issued to Mac computers or the proxy itself expire. It can also determine if a signing certificate of the certification authority (CA) has changed, thus invalidating current certificates. The following describes how Parallels Configuration Manager Proxy handles these events:

- When the proxy needs to communicate with a Mac, it first examines the digital certificate of the Parallels Mac Client running on it. If a certificate has expired or will expire soon, it will automatically renew the certificate.
- Parallels Configuration Manager Proxy will also check if the signing certificate of the currently used certification authority matches the one used by the Parallels Mac Client's certificate. If it's not, a new certificate will be issued for the Parallels Mac Client using the current CA.

- The proxy validates its own digital certificate at preset intervals. If a certificate is not valid, a log entry is created in the `isv_proxy_service.log` file and in the Windows event log. The relevant log entries can be viewed in the `%WINDIR%\Logs\pma_isv_proxy_service.log` file and in the Windows event viewer (**eventvwr**) by navigating to **Windows Logs > Application** and searching for "Parallels Mac Management for Microsoft SCCM" entries.

Note: Parallels Mac Management v8.5 does not support automatic renewal of the Parallels Configuration Manager Proxy certificate. This functionality may become available in a later version of Parallels Mac Management. For the instructions on how to renew the certificate manually, please read <https://kb.parallels.com/123836>.

CHAPTER 3

Installation and Configuration

This chapter will take you through the installation of Parallels Mac Management for Microsoft SCCM.

In This Chapter

Installation Overview	38
Install Parallels Mac Management	38
Configuring Parallels Configuration Manager Proxy	39
Configuring Parallels IBCM/MDM Proxy	43
Configuring Parallels NetBoot Server	54
Configuring Parallels OS X Software Update Point	55
Adding or Removing Parallels Mac Management Components	56
Upgrading Parallels Mac Management to a Newer Version	56

Installation Overview

All server-side Parallels Mac Management components are installed using the same setup wizard. If you are installing individual Parallels Mac Management components on different servers, run the setup wizard on each server and select only the component(s) that you want installed on that server.

Before running the installation and configuration wizards, please make sure that you have read Installation Requirements (p. 15) for each component that you are planning to install.

You can also download the **Parallels Mac Management Prerequisites Check Wizard**, which you can use to verify whether your Microsoft SCCM infrastructure is ready for Parallels Mac Management deployment. To download the wizard, visit <https://www.parallels.com/products/mac-management/resources/> and locate the **Utilities** section. When there, click the **Learn More** link to learn what **Prerequisites Checker** is and how to use it.

Install Parallels Mac Management

To install Parallels Mac Management, run the setup wizard, select the components you wish to install on a given server and follow the onscreen instructions. The installation is automatic and will prompt you once it has completed.

Once the selected components are installed, you will need to configure them using configuration wizards, which will be opening automatically after the setup wizard exits. Each Parallels Mac Management component has its own configuration wizard. For example, if you choose to install all of the components on the same server, all configuration wizards will run automatically one after another. As soon as you complete one wizard, the next one will open after a short delay. You must complete each configuration wizard before you can use Parallels Mac Management.

Read on to learn how to use configuration wizards to configure Parallels Mac Management components.

Configuring Parallels Configuration Manager Proxy

The **Parallels Configuration Manager Proxy Configuration Wizard** starts automatically after the Parallels Mac Management setup wizard is completed. You can also run the wizard manually by going to **Apps > Parallels** and double-clicking the **SCCM Proxy Configuration Utility** application.

Note: Before running the wizard, please make sure that you've read the **Parallels Configuration Manager Proxy Requirements** section (p. 16).

To configure the Parallels Configuration Manager Proxy, complete the wizard as described in the subsequent sections.

Step 1: SMS Provider Location

On the **SMS Provider location** page, specify the hostname or IP address of the server where the SMS Provider is installed. Make your selection based on the following conditions:

- If the SMS Provider and the Configuration Manager Proxy are installed on the local server, select the **Local server** option.
- If the SMS Provider is installed on a different server, select the **Remote server** option and enter the server hostname or IP address.

Step 2: Configuration Manager Proxy Service Account

On the **Configuration Manager Proxy service account** page, specify the user account under which the Configuration Manager Proxy service will run:

- The account must have read/write access to the SMS Provider.
- Select the **Local System account** option to use the standard Windows LocalSystem account.
- Select **This account** to specify a domain account or a local user account.
- In the **Password** field, specify the account password.

Step 3: Prerequisites Check

The **Prerequisites Check** page displays a list of prerequisites for Parallels Configuration Manager Proxy and verifies if they are met. The prerequisites include the following:

- Current user access rights for configuring the Proxy service. If the user has insufficient right, you cannot proceed and will need to either set the necessary rights or use a different user.
- Access rights of the user you specified in the previous step for running the Proxy service. If the rights are insufficient, grant the rights or go back and specify a different user.
- Proxy-related Active Directory data (containers with values), which are required to configure and run the Proxy service. If the verification indicates a failure, make the appropriate modifications to Active Directory.

If one or more prerequisites are not met, you cannot advance to the next wizard page until you make the necessary adjustments. The instructions are provided on the screen for each prerequisite that's not met (you may need to scroll the list to the right to see them). You can also read the **User Rights Requirements** section (p. 23) for the complete list of requirements. You don't have to quit the wizard at this point. Simply make the required changes and then click the **Rerun** button. If the fixes were sufficient (all prerequisites are met), the **Next** button becomes enabled and you can continue to the next wizard page.

Step 4: Parallels Client Certificate Management Settings

On the **Parallels Client certificate management settings** page, select the protocol (HTTP or HTTPS) that the Parallels Configuration Manager Proxy and Mac computers will use to communicate with management points and distribution points. If your distribution points or management points are configured to use HTTPS, then the HTTP option will not be available.

The options described below allow you to integrate Parallels Mac Management with Windows Public Key Infrastructure (PKI). If you don't use PKI, you don't have to configure these options.

- The **Certificate Authority** field is automatically populated with the name of a Certificate Authority (CA) detected by the wizard. To specify a CA manually, click the **Browse** button.
- The **Parallels Proxy certificate template** field is used to specify a certificate template for the Parallels Configuration Manager Proxy. Click the **Browse** button to select a template. If you followed the instructions in the **Creating Certificate Templates for Parallels Proxy and Mac Computers** (p. 34) section, you should see the Parallels Configuration Manager Proxy certificate template that you created.
- The **Mac client certificate template** field is used to specify a certificate template for Mac computers. Click the **Browse** button to select a template.

Note: If you are reassigning a certificate template on this site, the newly enrolled Mac computers will use the new template. Previously assigned Mac computers will continue using the certificates that was issued using the old template.

If the Parallels Configuration Manager Proxy has already been configured not to use PKI and if there are Mac computers assigned to the site, then the Proxy certificate will be re-issued.

Step 5: Role-Based Security

The **Role-based security** page allows you to configure the Configuration Manager Proxy role-based access control. The roles are created during the Parallels Mac Management installation and include the following:

- **Problem Monitor Users.** Members of this role are allowed to run the Problem Monitor, view problem reports, delete reports, and perform some other related tasks. See **Using Problem Monitoring Utility** (p. 243) for more info.
- **FileVault Key Administrators.** This role grants read rights to the Parallels Mac Management SQL Server database (p. 257). The database is used to store FileVault 2 recovery information for Mac computers. Users and groups that have read access will be able to retrieve and view the recovery keys for Mac computers in the Configuration Manager console. By default, only the Domain Admins group is granted access to the database. The Parallels Configuration Manager Proxy account is granted access automatically. To grant access to other users, add them to this role.
- **Administrator.** Members of this role have full access to all Parallels Mac Management features.
- **Enrollers.** Members of this role can only enroll Mac computers in SCCM.

You can select a role and see the default users and groups for it. To remove a group, select it and click the "-" button. To add a group or a user click the "+" button and use the standard **Select Users, Computers, Service Accounts, or Groups** dialog to specify a user or a group.

Step 6: Configuration Manager Proxy Communication Ports

The **Configuration Manager Proxy communication ports** page allows you to specify the TCP ports that Parallels Configuration Manager Proxy will use to communicate with the Configuration Manager console and Mac computers.

Parallels Configuration Manager Proxy uses these ports to serve requests from the Configuration Manager console and Parallels Mac Client running on Mac computers. The Proxy publishes its current port configuration in Active Directory and the DNS so that managed Mac computers can discover it if the port configuration changes.

The default ports that you see on the page should only be changed if they are used by some other processes/applications running on the same server as the Configuration Manager Proxy.

Step 7: Customer Experience Program

The **Customer Experience Program** page allows you choose whether to participate in the Parallels Customer Experience Program (CEP) aimed at improving the quality of Parallels Mac Management for Microsoft SCCM.

If you choose to participate in the program, all sites (primary and secondary) will participate. The information about the Parallels Mac Management that you are using will be sent to Parallels once every two weeks. Please note that no sensitive information of any kind will be collected. If you decide not to participate in the program, you can join the program later by reconfiguring the Parallels Configuration Manager Proxy on the primary site and selecting this option.

Step 8: Configuration Settings Summary

On the **Configuration Settings Summary** page, review the settings. If everything is correct, click **Finish**. Wait for the settings to be applied and for the Configuration Manager Proxy service to start. A message box will be displayed informing you of the result.

If you need to reconfigure the Parallels Configuration Manager Proxy later, you can run the configuration wizard again and repeat the steps described above. After you update the Proxy configuration, the Configuration Manager Proxy service must be restarted for changes to take effect.

Read on to learn how to verify the Parallels Configuration Manager Proxy service certificate.

Verifying the Parallels ConfigMgr Proxy Service Certificate

When the Configuration Manager Proxy service settings are applied, a certificate is deployed for it on the local computer. The Configuration Manager Proxy service account that you specified on the second page of the wizard is granted Read access to the certificate. If you change the account later, you have to make sure that the new account has access to the certificate store and can read the Configuration Manager Proxy certificate private key. Use the instructions below to verify the store and account permissions.

To view the certificate store permissions

- 1 Run regedit.exe on the computer where the Configuration Manager Proxy is installed.
- 2 Navigate to **HKLM\Software\Microsoft\SystemCertificates**.
- 3 Right-click **SystemCertificates** and select **Permissions** from the context menu.
- 4 In the **Permissions for SystemCertificates** dialog, verify that the user that you use to run the Configuration Manager Proxy service has the **Read** permission selected.

To verify that the Configuration Manager Proxy service account has permissions to read the certificate private key

- 1 Open the Microsoft Management Console (MMC) from the **Start** menu by clicking **Run** and then typing "mmc".
- 2 In the **File** menu, select **Add/Remove Snap-in...**
- 3 In the **Add or Remove Snap-ins** dialog, find and select Certificates in the **Available snap-ins** list. Click **Add**.
- 4 In the **Certificate snap-in** dialog, select **Computer account** and then select **Local computer**.
- 5 Click **OK** in the **Add or Remove Snap-in** dialog.
- 6 In the snap-in tree, navigate to **Certificates (Local Computer)\Personal\Certificates** and expand it to view the available certificates.
- 7 Make sure that the **Configuration Manager Proxy** certificate exists. If it doesn't, run the Configuration Manager Proxy configuration utility.
- 8 Right-click the **Configuration Manager Proxy** certificate, point to **All Tasks**, and then click **Manage Private Keys**.
- 9 In the **Permissions for Configuration Manager Proxy private keys** dialog, verify that the user (or a group to which the user belongs) has **Read** access to the certificate's private key.

Configuring Parallels IBCM/MDM Proxy

Important: Beginning with Parallels Mac Management for Microsoft SCCM v8.5, the Parallels MDM functionality has changed. The older Parallels MDM Server component is no longer used. It was split into Parallels IBCM/MDM Proxy (the Internet facing part) and the new Parallels MDM service (the Intranet part). When upgrading to Parallels Mac Management v8.5, you can migrate the existing MDM setup or you can discard it and then re-enroll Mac computers in MDM using the new functionality from scratch. For detailed information, please see KB article <https://kb.parallels.com/125034>

If you choose to install the **IBCM/MDM Proxy** component, the **Parallels IBCM/MDM Proxy Configuration Wizard** starts automatically after the installation. You can also run the wizard manually by navigating to **Apps > Parallels** and double-clicking **IBCM/MDM Proxy Configuration Utility**.

Before using the wizard, please make sure that you've read the **Parallels IBCM/MDM Proxy Requirements** section (p. 18).

Parallels IBCM/MDM Proxy is a dual component that consists of two parts: IBCM Proxy and MDM Proxy. The same wizard is used to configure both, but there are differences in preparation steps that must be completed outside of the wizard, as well as some post-configuration steps that must be performed. Therefore, the configuration instructions are described in two separate sections, one for IBCM Proxy and the other for MDM Proxy.

Configuring Parallels IBCM Proxy

This section describes IBCM specifics when configuring Parallels IBCM/MDM Proxy.

Step 1: Prepare to Enable Trust Between Proxies

In this step, you need to enable trust between Parallels IBCM/MDM Proxy and Parallels Configuration Manager Proxy. This must be done before you configure Parallels IBCM/MDM Proxy because it affects the configuration procedure.

To enable trust:

- 1 Log in to the computer where Parallels Configuration Manager Proxy is installed and export the certificate named **Parallels Configuration Manager Proxy** from the **Local Computer / Personal** certificate store. Do not export the private key. To export the certificate, open the **Certificates** snap-in (run the `certlm` command), then navigate to **Local Computer / Personal / Certificates**, locate the **Parallels Configuration Manager Proxy** certificate, right-click it and choose **All Tasks > Export**.
- 2 Now log in to the computer where Parallels IBCM/MDM Proxy is installed and import the certificate from the previous step into the **Local Computer / Personal** certificate store. When running the **Certificate Import Wizard**, select **Place all certificates in the following store** and choose **Personal** in the drop-down list.

Continue to the next step.

Step 2: Run the Configuration Wizard

When the **Parallels IBCM/MDM Proxy Configuration Wizard** opens, complete it as described below:

- 1 On the first page, specify the port for incoming Parallels Configuration Manager Proxy connections. Make sure that this port is open for incoming connections.
- 2 On the next page, specify the Parallels Configuration Manager Proxy certificate that you imported earlier. (p. 44) Click **Browse** to select the certificate.
- 3 Click **Next** to go to the next page of the wizard.
- 4 On the **Choose Web Sites for Parallels IBCM/MDM Proxy** page, select **IBCM Proxy** (this will enable IBCM Proxy on this computer) and then select an IIS web site from the drop-down list.
- 5 On the **Prerequisites Check** page, verify that all of the requirements are met (all items have a green check mark). If not, resolve the issues and click the **Rerun** button (you can also go back or you can close the wizard and run it again later).
- 6 Click **Next** and then click **Finish** to close the wizard.

Continue to the next step.

Step 3: Configure IBCM Link

The last step is to configure the IBCM link so that Parallels Configuration Manager Proxy can communicate with Parallels IBCM/MDM Proxy.

To configure the link:

- 1** In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / IBCM / IBCM Link**.
- 2** Right-click the **IBCM link** item in the right pane and choose **Properties**.
- 3** In the **IBCM Link Properties** dialog, click the **Configure** button to open the **Parallels IBCM Proxy Link Configuration Wizard**.
- 4** On the first page of the wizard, enter the Parallels IBCM/MDM Proxy location information, including:
 - The hostname of the computer where Parallels IBCM/MDM Proxy is running.
 - The port number on which Parallels IBCM/MDM Proxy is listening for Parallels Configuration Manager Proxy requests. This is the port you specified when you configured Parallels IBCM/MDM Proxy.
- 5** Click **Next**.
- 6** On the second page, a test connection will be established and you will see the details of the certificate provided by the remote party.
- 7** Review the details of the certificate and confirm that it is the certificate that belongs to Parallels IBCM/MDM Proxy. If it is, click **Accept** and wait for the configuration settings to be applied. After that, click **Finish** to close the wizard. When the link is configured, its settings will be displayed in the preferences dialog.

At this point the mutual trust between Parallels IBCM/MDM Proxy and Parallels Configuration Manager Proxy is established. From this point forward, Parallels Configuration Manager Proxy and IBCM/MDM Proxy begin communicating with each other.

For the information on how to enroll and manage Mac computers via the Internet, see **Internet-based Client Management** (p. 233).

Conclusion

Your Parallels IBCM/MDM Proxy is now fully configured for IBCM and can be used for Internet-based Client Management (p. 233).

Configuring Parallels MDM Proxy

This section described MDM specifics when configuring Parallels IBCM/MDM Proxy.

Step 1: Prepare to Enable Trust

In this step, you need to enable trust between Parallels IBCM/MDM Proxy and Parallels MDM service that runs on the server where Parallels Configuration Manager Proxy is installed. This must be done before you configure Parallels IBCM/MDM Proxy because it affects the configuration procedure.

To enable trust:

- 1 Log in to the computer where Parallels Configuration Manager Proxy is installed and export the certificate named **Parallels Configuration Manager Proxy** (without the private key) from the **Local Computer / Personal** certificate store. To export the certificate, open the **Certificates** snap-in (run the `certlm` command), then navigate to **Local Computer / Personal / Certificates**, locate the **Parallels Configuration Manager Proxy** certificate, right-click it and choose **All Tasks > Export**. Use the DER or Base-64 encoding.
- 2 Now log in to the computer where Parallels IBCM/MDM Proxy is installed and import the certificate from the previous step into the **Local Computer / Personal** certificate store. When running the **Certificate Import Wizard**, select **Place all certificates in the following store** and choose **Personal** in the drop-down list.

Continue to the next step.

Step 2: Run the Configuration Wizard

When the **Parallels IBCM/MDM Proxy Configuration Wizard** opens, complete it as described below:

- 1 On the first page, specify the port for incoming Parallels Configuration Manager Proxy connections. Make sure that this port is open for incoming connections.
- 2 On the next page, specify the Parallels Configuration Manager Proxy certificate that you have imported earlier. (p. 46) Click **Browse** to select the certificate.
- 3 Click **Next** to go to the next page of the wizard.
- 4 On the **Choose Web Sites for Parallels IBCM/MDM Proxy** page, select **MDM Proxy** (this will enable MDM Proxy on this computer) and then select an IIS web site from the drop-down list.
- 5 On the **Prerequisites Check** page, verify that all of the requirements are met (all items have a green check mark). If not, resolve the issues and click the **Rerun** button (you can also go back or you can close the wizard and run it again later).
- 6 Click **Next** and then click **Finish** to close the wizard.

Continue to the next step.

Step 3: Configure the MDM Link

The last step is to configure the MDM link so that Parallels MDM Service can communicate with Parallels IBCM/MDM Proxy.

To configure the link:

- 1** In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / Mobile Device Management / MDM Proxy**.
- 2** Right-click **MDM Proxy Link** in the right pane and choose **Properties**.
- 3** In the **MDM Proxy Link Properties** dialog, click the **Configure** button.
- 4** The configuration wizard opens. On the first page of the wizard, specify the Parallels MDM Proxy location information:
 - **Service host:** The hostname of the server where Parallels IBCM/MDM Proxy is installed.
 - **Service port:** Port number that Parallels MDM Service must use to connect to Parallels IBCM/MDM Proxy.
 - **Internet FQDN:** Internet FQDN that clients (Mac computers) must use to connect to Parallels IBCM/MDM Proxy.
 - **Internet port:** Port number for incoming Internet connection.
 - **The MDM Proxy server is behind an HTTPs proxy that does not pass through client certificates:** With this option enabled, clients will be authenticated using additional HTTP headers named MDM-Signature. Please keep in mind that this option consumes a significant amount of data, so use it only if necessary. See more details in the **MDM Protocol Reference** document, section **Passing the Client Identity Through Proxies:** <https://developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf>

If you've selected **The MDM Proxy server is behind an HTTPs proxy that does not pass through client certificates** (see above), you also need to do the following:

- a** Log in to the machine where MDM Proxy is installed.
 - b** Open the Internet Information Services (IIS) Manager.
 - c** Go to *server-name* > **Sites** > *site-name* > **ParallelsMacManagement.MDM**.
 - d** Double click on **SSL Settings**.
 - e** In **Client certificates**, choose the **Accept** option and click **Apply**.
- 5** Click **Next**. The wizard will try to connect to Parallels IBCM/MDM Proxy using the specified parameters. If the connection fails, verify that the information on the previous page is entered correctly and that the Parallels Configuration Manager Proxy certificate has been imported to the IBCM/MDM Proxy server (p. 46).
 - 6** On successful connection, the next page of the wizard opens displaying the Parallels IBCM/MDM Proxy certificate information. You need to accept it to continue. If you do, the certificate thumbprint is stored and will be used to verify future connections to Parallels IBCM/MDM Proxy. If the certificate is changed for any reason in the future, you will need to run this wizard again.

Continue to the next step.

Step 4: Configure APNs Certificate

Parallels Mac Management uses Apple Push Notification Service (APNs) to send push notifications for MDM functions, which include Parallels Mac Client push installations and some others. To enable push notifications, you need to obtain a corporate APNs push certificate and make it available to Parallels IBCM/MDM Proxy.

To configure APNs:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / Mobile Device Management / MDM Service**.
- 2 Right-click on **MDM Service** in the right pane and choose **Configure APNs**.
- 3 In the **APNs Certificate Properties** dialog, click **Configure**.
- 4 The **APNs Certificate Configuration Wizard** opens. Complete the wizard as described below.

An APNs certificate must be obtained on the Apple Push Certificates Portal. To obtain it, you need a certificate signing request (CSR) signed by Parallels. The first page of the **APNs Certificate Configuration Wizard** gives you the following two options to obtain a CSR signed by Parallels:

- **Obtain a CSR from Parallels automatically.** This option allows you to obtain a signed CSR from Parallels directly from this wizard. You can only use this option if your local server can access the Parallels certificate signing service (pmm.parallels.com) over the Internet. If your local server has limited Internet access (e.g. it is limited to certain domains), you can add pmm.parallels.com to the allowed domain list if your security policy allows it. When using this option, you must also specify your Parallels Mac Management license key in the **License key** field.
- **Save the CSR file locally and then sign it using the Parallels certificate signing service.** This option allows you to save a CSR file locally and then sign it on the Parallels certificate signing service manually. Select this option if your local server can't access the Parallels certificate signing service (pmm.parallels.com) over the Internet.

After making your selection, click **Next** to continue. Depending on the option selected, please read the corresponding subsection below:

- Obtain a CSR from Parallels automatically (p. 48)
- Save the CSR file locally and then sign it using the Parallels certificate signing service (p. 49)

Obtain a CSR from Parallels automatically

When you select this option and click **Next**, the following will happen:

- 1 A progress bar will appear indicating the CSR preparation progress. During this time, the wizard will do the following in the background
 - a Create a certificate signing request (CSR) and the associated private key.

Important Note: The private key associated with this CSR will not be known to Parallels at any time.

- b** Connect to the Parallels certificate signing service over the Internet and sign the CSR with Parallels MDM Signing Certificate.
- 2** Once the signed CSR is ready, the next page opens where you need to specify a local folder where you want to save it.
- 3** After the CSR file is saved, another page opens with instructions to proceed to the Apple Push Certificates Portal. Do not click **Next** yet and do the following instead:
 - a** Open the Apple Push Certificates Portal in a web browser and log in using your Apple ID and password.
 - b** **Important:** If this is the first time you are creating a certificate, click the **Create a Certificate** button. If you are renewing an existing certificate, find it in the **Certificates for Third-Party Servers** list and click the **Renew** button. After that, follow the onscreen instructions and upload the signed CSR file when asked.
 - c** Download the created APNs certificate file named “MDM_<VendorName>_Certificate.pem” to your local computer.
- 4** Back in the wizard, click **Next** to proceed to the page where you need to upload the APNs certificate file to the local server. Click **Browse** to browse for a target folder.
- 5** When done, click **Next** to upload the APNs file.

Continue to **Step 6: Configure Signing** (p. 50)

Save the CSR file locally and then sign it using the Parallels certificate signing service

When you select this option and click **Next**, the following will happen:

- 1** The configuration wizard creates a CSR and the associated private key.

Important Note: The private key associated with this CSR will not be known to Parallels at any time.

- 2** A page opens where you can specify a local folder for saving the CSR and the private key files. Specify the folder and click **Next**.
- 3** Another page opens with instructions on how to proceed with signing the CSR and obtaining an APNs certificate from Apple. Do not click **Next** yet and do the following instead:
 - a** Visit Parallels My Account at <https://my.parallels.com>. Sign in using your email address and password (if you don't have a Parallels account, you must register for one; a Parallels account is required to activate Parallels Mac Management and to use other services, such as certificate signing).
 - b** Once signed in, click **MDM Certificate** inside the **Parallels Mac Management** product card.

- c** Follow the instructions on the **MDM Certificate Signing** page and upload the CSR file that you saved in step 2 above. When instructed, download the signed CSR to your local computer.
 - d** Open the Apple Push Certificates Portal in a web browser and log in using your Apple ID and password.
 - e Important:** If this is the first time you are creating a certificate, click the **Create a Certificate** button. If you are renewing an existing certificate, find it in the **Certificates for Third-Party Servers** list and click the **Renew** button. After that, follow the onscreen instructions. When asked, upload the signed CSR file that you obtained from Parallels My Account earlier.
 - f** Download the created APNs certificate file named “MDM_<VendorName>_Certificate.pem” to your local computer.
- 4** Back in the wizard, click **Next** to proceed to the page where you need to upload the APNs file to the local server. Click **Browse** to browse for a target folder.
 - 5** When done, click **Next** to upload the APNs file.

Step 5: Configure MDM Profile Signing

In this step, you can optionally sign the MDM profile. When a signed profile is installed on a user device during MDM enrollment, the device will be able to verify the chain of trust and will display the MDM profile as "Verified".

To sign the profile:

- 1** In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / Mobile Device Management / MDM Service**.
- 2** Right-click **MDM Service** in the right pane and choose **Configure Signing**.
- 3** The **Signing Certificate Properties** dialog opens. In the dialog, click the **Configure** button.
- 4** The **Signing Certificate Configuration Wizard** opens.
- 5** On the first page of the wizard, select the **Enable Signing** option.
- 6** In the **Certificate file** field, specify a certificate file. If the certificate file is password-protected, specify the password.
- 7** Select the **Ensure that the certificate can be verified on a Mac computer** to install the root certificate of the signing certificate as trusted on a Mac computer or Apple mobile device during MDM enrollment. If the certificate that you are using is from a publicly-trusted CA, then the root certificate should be already installed on a device, in which case you don't have to install it.
- 8** Click **Next** and complete the wizard.

Please note that previously enrolled devices will not get the signed profiles automatically. The existing profiles will continue to function, but will be displayed on a device as "Not verified".

This completes the main part of the Parallels MDM Proxy configuration procedure. However, you still need to perform some additional steps before you can use it. These steps are described in the section that follows this one.

Post-Configuration Steps

Post-configuration steps described in this section must be performed after you configure Parallels MDM Proxy and before you try to use it.

Import MDM Service Certificate

For devices to be able to enroll in MDM, you need to import the Parallels MDM service certificate to the certificate store on the Parallels IBCM/MDM Proxy server.

Note: Parallels MDM service and Parallels IBCM/MDM Proxy are two different components. MDM service is a part of Parallels Configuration Manager Proxy. It performs the actual processing of MDM tasks on the SCCM side. IBCM/MDM Proxy is a standalone component, which is installed separately and which is used to receive requests from Mac computers over the Internet. The MDM service certificate is required on the IBCM/MDM Proxy side for client devices to enroll in MDM.

To import the certificate:

- 1 Log in to the computer where Parallels Configuration Manager Proxy is installed and export the certificate named **Parallels MDM Service** (without the private key) from the **Local Computer / Personal** store. To export the certificate, open the **Certificates** snap-in (run the `certlm` command), then navigate to **Local Computer / Personal**, locate the **Parallels MDM Service** certificate, right-click it and choose **All Tasks > Export**.
- 2 Now log in to the computer where Parallels IBCM/MDM Proxy is installed and import the certificate from the previous step into the **Computer / Trusted Root Certificates** store. When running the **Certificate Import Wizard**, select **Place all certificates in the following store** and choose **Trusted Root Certificates** in the drop-down list.

Configure Automatic Mac Enrollment in MDM

Note: This is an optional step, which only needs to be performed if you are not using Apple DEP or if some of your Mac computers were not enrolled in SCCM through DEP.

Your Mac computers must be enrolled in MDM before you can use MDM features on them. MDM enrollment is done automatically during Apple DEP enrollment. However, if you are not using Apple DEP or if some of your Mac computers were not enrolled in SCCM through DEP, you need to enroll them in MDM yourself. This is done by configuring automatic MDM enrollment as described below.

To configure automatic MDM enrollment:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / Mobile Device Management / MDM Service**.
- 2 Right-click **MDM Service** in the right pane and choose **Enrollment Properties**. The **Parallels Mac Client MDM Enrollment Properties** dialog opens.
- 3 Select the **Enable automatic enrollment of Macs into Parallels MDM service** option and then choose one of the following:

- **Enroll all Mac resources.** All Mac computers that are enrolled in SCCM will be automatically enrolled in MDM (computers that are already enrolled in MDM via Apple DEP are excluded).
- **Enroll Mac resources from following collections.** Only the Mac resources from the specified collection(s) will be enrolled. Select this option and click the **[+]** icon to select a collection and add it to the list (you can add more than one collection).

4 Prompt user to approve the MDM profile — select this option to prompt a Mac user to approve and install the MDM profile. This must be done because of the following requirements:

- Apple requires user-approved MDM when delivering security-sensitive payloads. If you will be delivering such payloads to Mac computers via MDM, you need to select this option.
- User approved MDM is required when delivering configuration profiles to macOS Big Sur. If target Mac computers run macOS Big Sur, you need to select this option.

For more information, see **Creating a macOS Configuration Profile** (p. 106). Please also note the following:

- MDM approval can only be done personally by a Mac user. With this option enabled, the user will see a dialog when Parallels Mac Client receives a policy update. The dialog informs the user that their computer must be enrolled in MDM and contains instructions on how to do it. The user should follow the instructions and install the MDM profile. If the user simply closes the dialog, it will be shown again on each policy update until the MDM profile is installed. Please also see macOS Big Sur notes below.
- As an IT administrator, you have the ability to determine whether the user has approved and installed the MDM profile. For details, see the **Reporting UAMDM Status** section. (p. 53)

5 Click **OK** so save your changes and close the dialog.

The next time a Mac computer requests policy updates, it will receive enrollment settings and will be enrolled in MDM.

macOS 11 Big Sur notes

When a Mac computer receives the MDM enrollment policy, the user will see a notification dialog asking them to enroll the computer in MDM. The user should do the following:

- 1** In the notification dialog, click the **Open System Preferences** button.
- 2** The **System Preferences** dialog opens with the **Profiles** pane selected.
- 3** Clicks **Install** and follow the onscreen instructions to install the profile.

Note that the MDM profile will be available in System Preferences for 8 minutes, after which it will be removed from the **Profiles** pane by macOS. The user can click the **Open System Preferences** button in the notification dialog again (the dialog stays open) to re-add the profile. Once the profile is installed, the notification dialog closes by itself within a minute.

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. If you haven't read the previous section of this guide, please read it before you continue: **Configure Automatic Mac Enrollment in MDM** (p. 51). In that section, the **Prompt user to approve the MDM profile** option enables the UAMDM mechanism on the client side. 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. 97). Once you understand how 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. 97).

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.

Conclusion

Your Parallels MDM Proxy is now fully configured and can be used to perform the following tasks:

- **Enrolling Mac Computers via Apple DEP** (p. 204)
- **Enrolling Apple Mobile Devices in SCCM** (p. 84)
- **Using Apple VPP** (p. 210)
- **Delivering security-sensitive configuration profiles to Mac computers** (p. 106)
- **Remote Lock and Wipe** (p. 229)

Secure IBCM/MDM Proxy Website with Wildcard SSL Certificate

Parallels IBCM/MDM Proxy uses an IIS website to receive HTTP/HTTPS requests. You can optionally secure the website with a wildcard SSL certificate, so you don't have to purchase a separate certificate for each Internet-facing host.

To use a wildcard certificate:

- 1 On the server where you have Parallels IBCM/MDM Proxy installed, open the IIS Manager.
- 2 Open the **Site Bindings** dialog for the site with installed Parallels IBCM/MDM Proxy.
- 3 Select an https binding and press the **Edit** button.
- 4 Select a wildcard SSL certificate using the **Select** button.
- 5 Press the **OK** button to save changes.

Configuring Parallels NetBoot Server

If you choose to install the NetBoot Server component, the **Parallels NetBoot Configuration Wizard** will automatically open after the installation. You can also run the wizard manually by going to **Apps > Parallels** and double-clicking the **NetBoot Server Configuration Utility**.

Note: Before running the wizard, please make sure that you've read **Parallels NetBoot Server Requirements** (p. 22) and **Permissions for Running NetBoot Service** (p. 30) sections.

To configure the Parallels NetBoot server, complete each wizard page as described below.

SMS Provider location

On the **SMS Provider location** page, specify the hostname or IP address of the server where the SMS Provider is installed. If the SMS Provider and the NetBoot server are installed on the local server, select the **Local server** option. If the SMS Provider is installed on a different server, select the **Remote server** option and enter the server hostname or IP address.

Parallels NetBoot Server service account

On this page, specify a user account for running the NetBoot service:

- The account must have read/write access to the SMS Provider.
- Select the **Local System account** option to use the standard Windows LocalSystem account.
- Select **This account** to specify a domain account or a local user account.
- In the **Password** field, specify the account password.

The LocalSystem account is normally used when the SMS Provider is located on the same server as the NetBoot service. A specific account may also be used to manage access rights of the NetBoot service. When running on different computers, the NetBoot service must have DCOM Remote Activation permissions. Permissions on the WMI namespace can be set using **Server Manager > Configuration > WMI Control** snap-in. Permissions for DCOM remote activation can be set via `dcomcnfg.exe` on a computer where the SMS provider is running.

NetBoot images path

Specify a folder where the NetBoot server will store `.dmg` images.

Configuration progress

The **Configuration progress** page display the progress bar while the NetBoot server is being configured. Once the process is complete, review the result of each operation and click **Finish** to exit the wizard.

If you need to reconfigure the Parallels NetBoot Server later, you can run the configuration utility again and repeat the steps described above.

Configuring Parallels OS X Software Update Point

If you choose to install the **OS X Software Update Point** component, the **Parallels OS X Software Update Point Configuration Wizard** automatically opens after the installation. You can also run the wizard manually by going to **Apps > Parallels** and double-clicking the **OS X Update Point Configuration Utility**.

Note: Before running the wizard, please make sure that you've read the **Parallels OS X Software Update Point Requirements** section (p. 22).

To configure Parallels OS X Software Update Point:

- 1 On the first page of the wizard, specify a user account to run the Parallels OS X Software Update Point service. The account you choose must have administrative rights on the local server and must be a member of the **WSUS Administrators** group.

- 2 On the **Prerequisites Check** page, verify that all of the requirements are met. If one or more of the requirements are not met, you need to resolve them before proceeding. For the complete list of the requirements, see **Parallels OS X Software Update Point Requirements** (p. 22).
- 3 On the **Configuration settings summary** page, review the installation summary. If satisfied, click **Finish** to apply the settings and close the wizard.

Adding or Removing Parallels Mac Management Components

If you would like to add or remove one or more Parallels Mac Management components, do the following:

- 1 Run the Parallels Mac Management setup wizard and advance to the **Select Components** page.
- 2 On the **Select Components** page, select the components you want to install and clear the components you don't want installed. Depending on your selection, the following will happen:
 - If a selected component is not installed on this computer, it will be installed. If the component is already installed, it will not be reinstalled (provided it's the same Parallels Mac Management version).
 - If a component is cleared and is already installed on this computer, it will be removed.
- 3 Click **Next** and complete the wizard. If you've installed a new component, the configuration wizard will open allowing you to configure it.

Upgrading Parallels Mac Management to a Newer Version

To upgrade Parallels Mac Management to a newer version, you don't need to uninstall or reconfigure it. Simply run the new version of the setup wizard on every server where you have Parallels Mac Management components installed. The only exception is the Parallels MDM Server component when you are upgrading to Parallels Mac Management v8.5 from an earlier version (see the important note below). Please note that all of the components must be upgraded at the same time to avoid issues due to version mismatch.

Note: Beginning with Parallels Mac Management for Microsoft SCCM v8.5, the Parallels MDM functionality has changed. The older Parallels MDM Server component is no longer used. It was split into Parallels IBCM/MDM Proxy (the Internet facing part) and the new Parallels MDM service (the Intranet part). When upgrading to Parallels Mac Management v8.5, you can migrate the existing MDM setup or you can discard it and then re-enroll Mac computers in MDM using the new functionality from scratch. For detailed information, please see KB article <https://kb.parallels.com/125034>

To upgrade Parallels Mac Management to a newer version:

- 1** Run the Parallels Mac Management setup wizard and advance to the **Select Components** page.
- 2** On the **Select Components** page, the installed components will be preselected. When the installation runs, the components will be upgraded to the new version and their current configurations will remain unchanged. If you clear any of the selected components, they will be uninstalled.
- 3** Click **Next** and complete the setup wizard.

Please note that after upgrading Parallels Mac Management, you need to upgrade Parallels Mac Client on each managed Mac. See **Upgrading Parallels Mac Client** (p. 78) for more information.

CHAPTER 4

License Activation

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

In This Chapter

License Activation Overview	58
Online Activation.....	59
Offline Activation.....	59
View and Update License Information.....	61
Exceeding the License Limit	62
Deactivating Parallels Mac Management.....	63

License Activation Overview

To enroll and manage Mac computers and Apple mobile devices in SCCM, 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 Mac Management installation, please make sure that:

- you have registered for a Parallels account (<https://my.parallels.com>);
- you have purchased a Parallels Mac 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 Mac Management licensing and Parallels My Account, please refer to the **Parallels Mac Management for SCCM 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 Mac 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 Mac Management installation using the online activation method:

- 1 Open the Configuration Manager console.
- 2 Navigate to **Administration / Overview / Parallels Mac 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 SCCM 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 Mac 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 SCCM console changes to **Activated**.

Your Parallels Mac 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 Mac Management:

- 1 Open the Configuration Manager console.
- 2 Navigate to **Administration / Overview / Parallels Mac 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 SCCM 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 Mac Management** card.
- 3 On the **Parallels Mac 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 SCCM console changes to **Activated**.

Your Parallels Mac 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 Mac 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 Mac 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 Mac 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 Mac Management installations (if you have more than one) in one place.

Note: If you activated Parallels Mac 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 Mac 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 Mac 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 Mac Management** card.
- 6 On the **Parallels Mac 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 an SCCM 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 SCCM 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 SCCM.
- If the Parallels Mac 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 Mac 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 Mac Management

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

To deactivate a Parallels Mac Management installation:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac 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 Mac Management connects to Parallels cloud and deactivates your Parallels Mac Management installation. Your 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 Mac 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 Mac Management** card.
 - 8** On the **Parallels Mac 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 Mac Management is now fully deactivated and the license key can be used to activate a different installation.

Parallels Mac Client Deployment

Parallels Mac Client is a macOS application that enables communication between a Mac computer and the Parallels Configuration Manager Proxy. Before you can manage a Mac computer in SCCM, you need to install Parallels Mac Client on it and enroll the computer in Configuration Manager.

In This Chapter

Installation Options Overview.....	65
Installing Parallels Mac Client Using Discovery Methods	66
Running Parallels Mac Client Installer on a Mac Computer.....	71
Installing Parallels Mac Client Using a Script	73
Push Install or Update Parallels Mac Client	74
Configuring the macOS Firewall.....	76
Verifying Parallels Mac Client Deployment.....	76
Updating Parallels ConfigMgr Proxy Connection URL.....	77
Uninstalling Parallels Mac Client.....	77
Upgrading Parallels Mac Client	78
Using Parallels Mac Client Tools	79

Installation Options Overview

Parallels Mac Client can be installed on Mac computers using one of the following methods:

- **Parallels Network Discovery** (p. 66). Discovers Mac computers on the network, push installs Parallels Mac Client on them, and then enrolls each Mac in Configuration Manager.
- **SCCM Active Directory System Discovery** (p. 66). Discovers domain joined Mac computers and adds them as resources to Configuration Manager. The Parallels Configuration Manager Proxy then identifies the discovered resources as Mac computers, push installs Parallels Mac Client on them, and enrolls Mac computers in Configuration Manager.
- **Running Parallels Mac Client installer on a Mac** (p. 71). Log in to a Mac and manually install Parallels Mac Client by running the installation package.
- **Using an installation script** (p. 73). Use a script to install Parallels Mac Client on a Mac. The script can be executed manually on each Mac or it can be distributed to and executed on Mac computers using Apple Remote Desktop or a similar remote management software.
- **Push install or update Parallels Mac Client** (p. 74). If a Mac computer is already enrolled in SCCM or has been added to it as an unmanaged resource, you can push install or update Parallels Mac Client on it right from the Configuration Manager console.

Installing Parallels Mac Client Using Discovery Methods

Parallels Mac 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
- SCCM 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 SCCM 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 SCCM 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 SCCM 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. 66) 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 SCCM 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 SCCM 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 Mac 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. 67) 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. If you haven't configured boundaries and boundary groups in SCCM, you need to do it as described in the **Configuring Configuration Manager Boundaries** section (p. 32).

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 SCCM 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 Mac Management in one organization and is brought in to another organization that also uses Parallels Mac 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. For more information, see **Collections in Parallels Mac Management** (p. 95).

Using SCCM Active Directory System Discovery

SCCM AD System Discovery can discover domain-joined Mac computers. You can configure and run the AD System Discovery using the standard SCCM functionality. Once the Mac resources are discovered, Parallels Mac 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 Mac 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. 67).

Running Parallels Mac Client Installer on a Mac Computer

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

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 Mac 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 Mac 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 Mac 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. 233).

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 SCCM

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. 233). 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. For more information, see **Configuring Parallels IBCM/MDM Proxy** (p. 43).

- 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 SCCM 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 (p. 77).

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 SCCM.
- The Mac inventory is collected and saved in SCCM.
- 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.

Installing Parallels Mac Client Using a Script

A special script is supplied with Parallels Mac 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 Mac Management for Microsoft SCCM\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 **Manually Installing Parallels Mac Client**.
- `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 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).

Push Install or Update Parallels Mac Client

You can push install or update Parallels Mac Client on Mac computers that are already enrolled in SCCM 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. 67).
 - **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. 66) 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**.

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 Mac 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. The possible reasons for this are described in **Using Parallels Network Discovery** (p. 68).

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 SCCM 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.

Updating Parallels ConfigMgr Proxy Connection URL

If you migrate Parallels Configuration Manager Proxy to a different server, its connection URL record must be updated on managed Mac computers. Parallels Mac Client is capable of making this update automatically as described below.

Parallels Mac Client running on a Mac connects to the Parallels Configuration Manager Proxy using the connection URL that it obtains from the Active Directory during the Parallels Mac Client installation. If at some point the client fails to establish a connection with the proxy, it will try to recover the connection as follows:

- 1 First, it will try to access DNS records for the location of the Configuration Manager Proxy. If it finds the new connection URL in DNS, it will use it to connect to the Configuration Manager Proxy.
- 2 If the location cannot be found in DNS at this time, the client will keep trying to connect to the Proxy and to find the new location in DNS for a period of one week.
- 3 If after a week the connection still cannot be establish, a dialog box will be displayed in macOS asking the Mac user to enter the Active Directory credentials. The client will then connect to the Active Directory and try to retrieve the Configuration Manager Proxy connection URL from it. If succeeded, the client will use the URL to connect to the Configuration Manager Proxy. If it fails again, it will display an error message to the Mac user advising them to contact the system administrator.

For additional information about migrating the Configuration Manager proxy to a different server, please see **Migrating Configuration Manager Proxy** (p. 89).

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/Resources/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.

Upgrading Parallels Mac Client

When you upgrade Parallels Mac Management for Microsoft SCCM, you also need to upgrade Parallels Mac Client on every Mac computer on which it is installed. This task can be accomplished using one of the following methods:

- 1 Enabling the Automatic Parallels Mac Client Update option in the Configuration Manager console. This will upgrade Parallels Mac Client on every managed Mac automatically without requiring the administrator to take any extra steps.
- 2 Distributing the client installation package to Mac computers using the standard SCCM software distribution functionality.
- 3 Manually uninstalling Parallels Mac Client from a Mac and then installing a new version.

Each method is described in detail in the following subsections.

Automatic Upgrade of Parallels Mac Client

Parallels Mac Client can be upgraded automatically when you upgrade Parallels Mac Management to a newer version.

To use this functionality, the **Automatic Parallels Mac Client Upgrade** option must be enabled in the Configuration Manager console as described below:

- 1 Navigate to **Administration / Site Configuration / Sites**.
- 2 Right-click the **Sites** node and choose **Hierarchy Settings**. The **Hierarchy Settings Properties** dialog opens.
- 3 Click the **Automatic Mac Client Upgrade** tab and select the **Upgrade client automatically when new client updates are available** option.

After you enable this option, Parallels Mac Client running on a Mac will begin to periodically check whether it needs to be upgraded. If you upgrade Parallels Mac Management to a newer version while this option is enabled (or prior to enabling it), Parallels Mac Client will be automatically upgraded on all managed Mac computers. The Parallels Mac Client registration parameters will be inherited from the existing registration file, so you don't have to configure it again.

Note: It may take up to an hour (or more) for Mac computers to upgrade after Parallels Mac Management is upgraded.

Upgrading Parallels Mac Client via Software Distribution

To upgrade Parallels Mac Client on Mac computers via Software Distribution, do the following:

- 1 Obtain the Parallels Mac Client installation image file as described in **Manually Installing Parallels Mac Client**.
- 2 Distribute the client installation image to Mac computers. The **Deploying Software via SCCM Package Deployment section** (p. 172) describes how to accomplish this task.

Note that when creating a program for the distribution package, the **Command Line** property should be specified as follows:

```
:pma_agent.dmg/Parallels Mac Management for Microsoft SCCM.pkg::
```

When you install Parallels Mac Client via software distribution, the client registration parameters will be inherited from the existing registration file, so you don't have to configure the client again.

Manually Upgrading Parallels Mac Client

If you need to upgrade Parallels Mac Client on a single Mac, you can do it manually as follows:

- 1 Uninstall Parallels Mac Client from a Mac. See **Uninstalling Parallels Mac Client** (p. 77). This is a necessary step. Please note that when upgrading Parallels Mac Client using the automatic upgrade option or the software distribution functionality (described above), the client is uninstalled automatically.
- 2 Download the Parallels Mac Client installation image and run the installation program as described in **Manually Installing Parallels Mac Client**.

Using Parallels Mac Client Tools

Parallels Mac Client includes useful tools that can be run from System Preferences. This chapter describes how to use them.

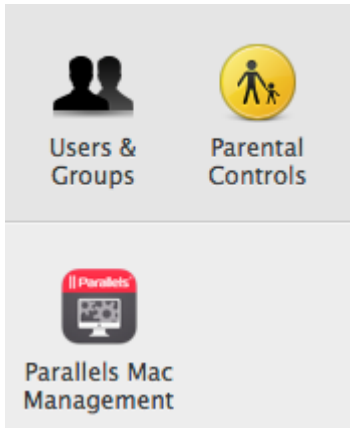
Viewing Parallels Mac Client Properties

The Parallels Mac Client properties window allows you to see the client properties and perform some tasks which are described below.

To open the Parallels Mac Client properties window:

- 1 Open **System Preferences**.

- 2 Click the **Parallels Mac Management** icon (or click **View > Parallels Mac Management for Microsoft SCCM**).



- 3 The **Parallels Mac Management for Microsoft SCCM** 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 SCCM 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.
 - **SCCM Proxy Internet URL.** Displayed if a Mac computer is managed via the Internet (i.e. connects to SCCM via the Parallels IBCM/MDM Proxy).
 - **SCCM 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 contains the following choices:
 - **Connect.** Connects to the Parallels Configuration Manager Proxy and downloads the latest policy from SCCM. For details, see **Initiating Policy Retrieval** (p. 81).
 - **Report Inventory.** Sends an inventory update to Configuration Manager. For details, see **Sending an Inventory Update to Configuration Manager** (p. 82).
 - **Send Problem Report.** Sends a problem report to the IT administrator. For details, see **Sending Problem Reports** (p. 82).

Initiating Policy Retrieval

Parallels Mac Client downloads policies from Configuration Manager on a schedule. You can download policies ahead of schedule if needed. You can do this from the Parallels Mac Client properties window or from the command line.

Using the Client Properties Dialog to Initiate Policy Retrieval

In System Preferences, click the **Parallels Mac Management** icon (or click **View > Parallels Mac Management for Microsoft SCCM**). 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.

Initiate 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
```

Sending an Inventory Update to Configuration Manager

Hardware and software inventory is collected automatically by Configuration Manager. If needed, you can also send an inventory update directly from a Mac computer.

To send an inventory update to Configuration Manager:

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

You can also send an inventory update 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.

Sending Problem Reports

If you are experiencing a problem with Parallels Mac Client, you can generate a problem report and then send it to your IT administrator.

To generate a report:

- 1** In System Preferences, click the **Parallels Mac Management** icon (or click **View > Parallels Mac Management for Microsoft SCCM**).
- 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.

Enrolling Apple Mobile Devices in SCCM

This chapter describes how to enroll Apple mobile devices in SCCM.

In This Chapter

Prerequisites	84
User Initiated Enrollment.....	84
Mobile Device Resources in SCCM	86
MDM Management Scope	86
Mobile Device License Management	87
De-enroll an Apple Mobile Device	87
Managing Apple Mobile Devices.....	88

Prerequisites

In contrast to Mac computers, Apple mobile devices don't need Parallels Mac Client in order to be managed in SCCM. The enrollment and management is done entirely via MDM. To enable MDM functionality, you need to install Parallels IBCM/MDM Proxy. When configuring the component, you need to enable MDM Proxy (select a corresponding option in the configuration wizard). For complete details, please see the following sections:

- **Configuring Parallels IBCM/MDM Proxy** (p. 43)
- **Configuring Parallels MDM Proxy** (p. 45)

User Initiated Enrollment

The 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 Mac Management / Mobile Device Management / MDM Proxy**.
- 2** Select an MDM Proxy Link for the desired SCCM 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 SCCM. Note that the URL contains the site code of the primary SCCM 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. 86).

- 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.

Mobile Device Resources in SCCM

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

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 SCCM, you need an active license of type **Mobile** in the primary SCCM site. For details about activating a license, see **License Activation** (p. 58).

When an Apple mobile device is enrolled in SCCM, 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. 87).

De-enroll an Apple Mobile Device

To de-enroll an Apple mobile device from SCCM, 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 SCCM. The corresponding SCCM resource, however, will remain in the Configuration Manager database.

Managing Apple Mobile Devices

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

- **Compliance Settings** (p. 105) allow you manage configuration and compliance of Apple mobile devices in your organization.
- **Hardware and Software Inventory (p. 96)** lets you collect inventory information about Apple mobile devices.
- **Remote Lock and Wipe** (p. 229) allows you to lock and wipe a managed mobile device if it's lost or stolen.
- **De-enroll an Apple Mobile Device** (p. 87) so it's no longer managed in SCCM.

Parallels ConfigMgr Proxy and Site Migration

This chapter describes how to migrate Parallels Configuration Manager Proxy to another server and how to migrate Mac computers to a new SCCM site.

In This Chapter

Migrating Parallels ConfigMgr Proxy to a New Server	89
Migrating Mac Computers to a New Site	91

Migrating Parallels ConfigMgr Proxy to a New Server

If you decide to migrate the Parallels Configuration Manager Proxy to a different server on the same SCCM site, you need to transfer the Proxy certificate to the new server before you install the Proxy on it.

The Parallels Configuration Manager Proxy migration procedure consists of the following steps::

- 1 Export the Parallels Configuration Manager Proxy certificate from the Windows certificate store on the current server.
- 2 Uninstall the proxy from the current server.
- 3 Import the certificate into the Windows certificate store on the new server.
- 4 Install the Parallels Configuration Manager Proxy on the new server.

The rest of this section describes how to export and import the certificate. The installation procedures are described in the **Installation and Configuration** chapter (p. 38).

Exporting the certificate from the Windows certificate store

To export the certificate from the current server:

- 1 Open the Microsoft Management Console (`mmc.exe`).
- 2 In the console, click **File > Add/Remove Snap-in** to open the **Add or Remove Snap-ins** dialog.

- 3 Click **Certificates** in the **Available snap-ins** list.
- 4 Click the **Add** button. Select the **Computer account** option and click **Next**.
- 5 On the **Select Computer** page, select **Local computer** and click **Finish**. Click **OK** to close the **Add or Remove Snap-ins** dialog.
- 6 In the Microsoft Management console, click **Console Root / Certificates(Local computer) / Personal / Certificates**.
- 7 Right-click the Parallels Configuration Manager Proxy certificate and then click the **All Tasks > Export...** option in the context menu. The **Certificate Export Wizard** opens.
- 8 Click **Next** on the **Welcome** page.
- 9 Select **Yes, export the private key** and click **Next**.
- 10 On the **Export File Format** page, select the following options:
 - **Personal Information Exchange - PKCS #12 (.PFX)**
 - **Include all certificates in the certification path if possible**
 - **Export all extended properties**
- 11 Click **Next**.
- 12 On the **Password** page, type and confirm a password (you'll be asked for it when importing the certificate on the new server). Click **Next**.
- 13 Type a path and filename for the target certificate file (e.g. `C:\sccm_proxy.pfx`) and click **Next**.
- 14 Review the export summary and click **Finish** to complete the wizard.
- 15 Copy the certificate file to the server where you want to migrate the Configuration Manager Proxy.

Importing the certificate into the Windows certificate store

To import the certificate into the new server:

- 1 Open the Microsoft Management Console (`mmc.exe`).
- 2 In the console, click **File > Add/Remove Snap-in** to open the **Add or Remove Snap-ins** dialog.
- 3 Click **Certificates** in the **Available snap-ins** list.
- 4 Click the **Add** button. Select the **Computer account** option and click **Next**.
- 5 On the **Select Computer** page, select **Local computer** and click **Finish**.
- 6 Click **OK** to close the **Add or Remove Snap-ins** dialog.
- 7 In the Microsoft Management console, click **Console Root / Certificates(Local computer)**.
- 8 Right-click the **Personal** node and then click the **All Tasks > Import...** item in the context menu. The **Certificate Import Wizard** opens.

- 9 Click **Next**.
- 10 On the **File to Import** page, click the **Browse** button and select the “.pfx” certificate file that you exported earlier (make sure to change the filter in the **Open** dialog to .pfx). Click **Next**.
- 11 On the **Password** page, type the password that you entered when you exported the certificate and select the **Mark this key as exportable...** option.
- 12 Click **Next**.
- 13 On the **Certificate Store** page, select the **Place all certificates in the following store** option. Make sure that the **Certificate store** field is set to **Personal** (if it doesn't, click the **Browse** button and select **Personal** from the list).
- 14 Click **Next**.
- 15 Review the import summary and click **Finish** to complete the wizard.
- 16 Install and configure Configuration Manager Proxy on the new server by running the Parallels Mac Management for Microsoft SCCM installer.
- 17 Mac computers will automatically discover the new Parallels Configuration Manager Proxy and will update their own local Proxy connection records. For more information, please see **Updating Proxy Connection URL** (p. 77).

Migrating Mac Computers to a New Site

This section describes how to migrate Mac computers enrolled in SCCM from one site to another.

Creating a new SCCM site may be a necessity when you upgrade your system to a new version of Configuration Manager or when you want to combine two separate SCCM sites into a single one (or for any other reason). In either case, you need to migrate Mac computers, which are enrolled in your current site(s), to the new site. This can be accomplished using a migration package provided by Parallels and the standard SCCM software deployment functionality. Follow the instructions below to migrate your Mac computers to a new site.

First, you need to prepare the migration script:

- 1 On the server where you have the old (the one you are migrating) Parallels Configuration Manager Proxy installed, open the following folder:

```
C:\Program Files (x86)\Parallels\Parallels Mac Management for  
Microsoft SCCM\sitemigration\pkgsrsc
```

The folder contains files that will be used on Mac computers to migrate them to a new site.

- 2 Open the `migrate_pmm_to_new_site.sh` file in a text editor that supports Unix-style line endings (e.g. Notepad++). This is the script that will migrate Parallels Mac Client to a new SCCM site when you run it on a Mac computer.
- 3 In the script, modify the values of the following variables:

- `TARGET_SITE_CODE` must contain the site code of the new Parallels Configuration Manager Proxy.
Example: `TARGET_SITE_CODE = "T16"`
- `CM_PROXY_URL` must contain the URL of the new Parallels Configuration Manager Proxy.
Example: `CM_PROXY_URL = "https://win2012r2.pmm12.dom:8760/isvproxy/rpc"`

4 Save the `migrate_pmm_to_new_site.sh` file and close the text editor.

Once you have the migration script ready, do the following:

- 1** Make sure your new SCCM site has boundaries configured the same way they are configured in the old site. See **Configuring Configuration Manager Boundaries** for more info (p. 32).
- 2** Import all Parallels Configuration Manager Proxy certificates from the server running the old proxy into the server running the new proxy. For instructions, please see this KB article: <https://kb.parallels.com/117220>.
- 3** Log in to the server running the new Parallels Configuration Manager Proxy and open the Windows registry editor. Find a key and add a parameter to it as specified below:
 - **Key (64-bit Windows):**
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Parallels\Parallels Mac Management for Microsoft SCCM\CmProxy`
 - **Key (32-bit Windows):** `HKEY_LOCAL_MACHINE\SOFTWARE\Parallels\Parallels Mac Management for Microsoft SCCM\CmProxy`
 - **Parameter:** `TrustedPmmSites` (type `REG_MULTI_SZ`). The parameter should contain the list of site codes from which you are migrating Mac computers.
- 4** Save the register changes and restart the Parallels Configuration Manager Proxy service for the changes to take effect.
- 5** Open the Configuration Manager console in the old site and create a software package as follows:
 - Source should be the path to the folder described in step 1 above. The folder should contain the modified `migrate_pmm_to_new_site.sh` file together with the rest of the files. If needed, copy the entire folder to a location where it can be accessed from the Configuration Manager console in the old site.
 - Command line should be `chmod u+x ./install.sh && ./install.sh`General info about package deployment is available in the **Deploying Software via SCCM Package Deployment** section (p. 172).
- 6** Deploy the package to the collection of Mac computers that you want to migrate to the new site.

After the package is deployed on a Mac, Parallels Client will automatically register with the new Parallels Configuration Manager Proxy. To verify that registration was successful, open System Preferences on a Mac computer and examine the SCCM Proxy URL value. The migration operation log file can be viewed at `/Library/Logs/pmm_site_migration.log`.

CHAPTER 8

Using Parallels Mac Management for Microsoft SCCM

This chapter describes how to use the Parallels Mac Management features.

In This Chapter

Configuration Manager Admin Console	94
Device Collections in Parallels Mac Management.....	95
Hardware and Software Inventory.....	96
Software Metering	104
Compliance Settings	105
Deploying macOS and Executing Task Sequences.....	140
Deploying Software via SCCM Package Deployment.....	172
Deploying Software via SCCM Application Deployment	177
macOS Software Update Management	188
Configuring Maintenance Windows	202
Executing Scripts on Mac Computers	203
Enrolling Mac Computers via Apple DEP	204
Using Apple VPP	210
Remote Lock and Wipe.....	229
Internet-Based Client Management	233
Deploying Parallels Desktop on Mac Computers	235
Deploying SCCM Client in Windows Running in a Virtual Machine	238
Remote Support for Mac Computers.....	240
Problem Reporting and Monitoring	242
Initiating Policy Retrieval from SCCM	246

Configuration Manager Admin Console

Parallels Mac Management for Microsoft SCCM extends the Configuration Manager console with support for Mac computers and Apple mobile devices. The Configuration Manager console is the primary interface to manage Mac computers and Apple mobile devices in your enterprise. After you install Parallels Mac Management, the Mac and mobile device specific GUI elements are integrated into the console.

Device Collections in Parallels Mac 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.

Mac Computer Collections

Parallels Mac 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 SCCM, 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 **Operating System Deployment** (p. 140).

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 is enrolled in SCCM. To see the properties of resource, right-click it and choose **Properties**. For additional info, see **Mobile Device Resources in SCCM** (p. 86).

Hardware and Software Inventory

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 SCCM directly from a Mac computer. To do so:

- 1 Log in to the Mac computer.
- 2 Open **System Preferences** and click the **Parallels Mac Management** icon.
- 3 In the **Parallels Mac Management for Microsoft SCCM** 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 SCCM silently with no additional user interaction required.

You can also send an inventory update to SCCM 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 SCCM 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 SCCM'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 SCCM using the class above:

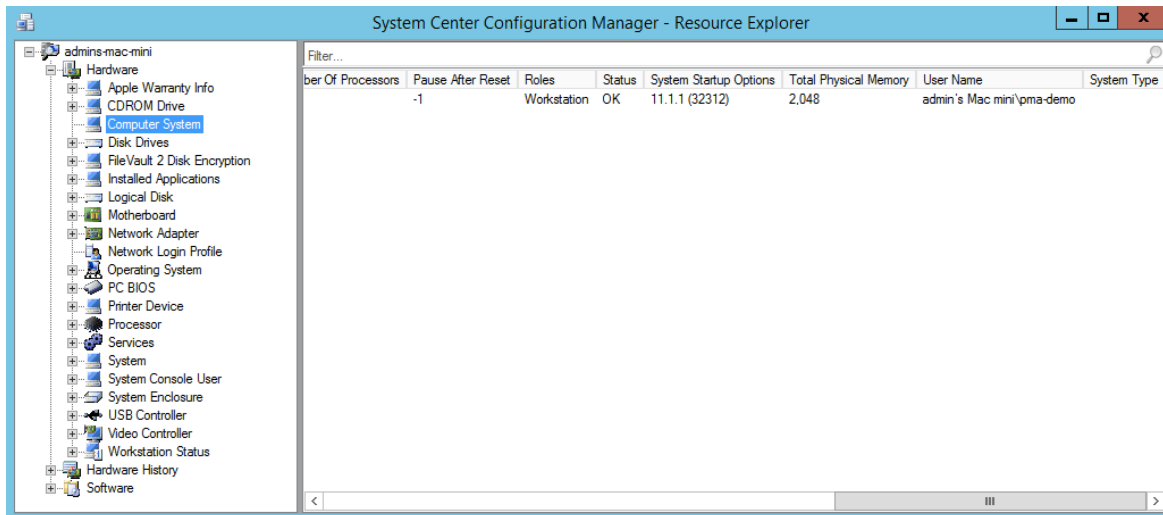
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"https://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
  <dict>
    <key>IsApplicable</key>
    <false/>
    <key>IsReady</key>
    <false/>
  </dict>
</array>
</plist>
```

Reporting Mac User Logon Information

Mac user logon details are reported by Parallels Mac Client to SCCM 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.

The screenshot shows the 'System Center Configuration Manager - Resource Explorer' window. The left pane displays a tree view of system components, with 'Network Login Profile' selected. The right pane shows a table with the following data:

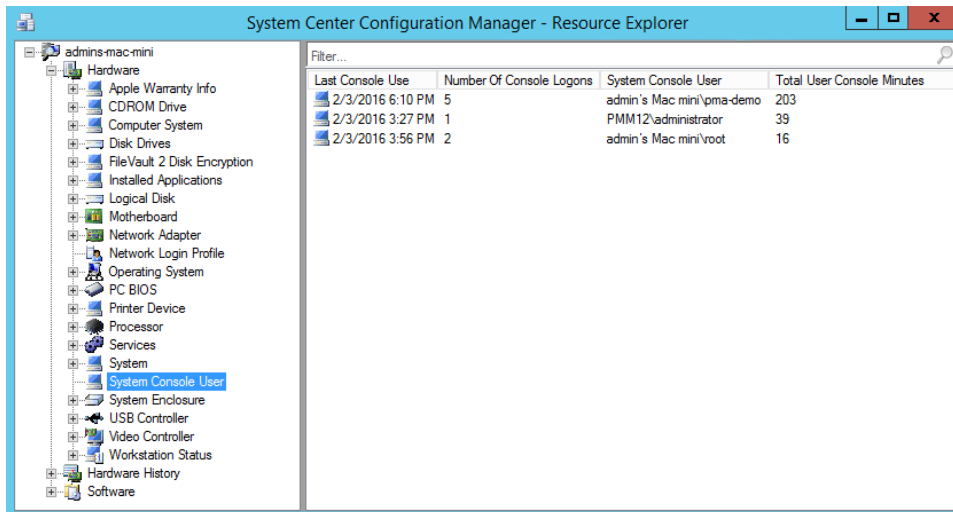
Name	Full Name	Home Directory	Last Logoff	Last Logon	Logon Server	Number Of Logons
admin's Mac mini\pma-demo	pma-demo	/Users/pma-demo	2/3/2016 2:50 PM	2/3/2016 2:39 PM	*	3
admin's Mac mini\root	System Administrator	/var/root			*	0
admin's Mac mini\admin	admin	/Users/admin			*	0
admin's Mac mini\user	user	/Users/user			*	0
PMM12\administrator		/Users/administrator	2/3/2016 2:50 PM	2/3/2016 2:47 PM	*	1

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.



The screenshot shows the System Center Configuration Manager - Resource Explorer window. The left pane displays a tree view of hardware and software resources for 'admins-mac-mini'. The right pane shows a table with the following data:

Last Console Use	Number Of Console Logons	System Console User	Total User Console Minutes
2/3/2016 6:10 PM	5	admin's Mac mini\pma-demo	203
2/3/2016 3:27 PM	1	PMM12\administrator	39
2/3/2016 3:56 PM	2	admin's Mac mini\root	16

Software Metering

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.

Compliance Settings

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. Please note that creating a configuration profile item for Mac computers and Apple mobile devices are described separately in the following sections:

- Creating a macOS Configuration Profile (p. 106)
- Creating an Apple Mobile Device Configuration Profile (p. 114)

Creating a macOS Configuration Profile

First, you need to create a macOS configuration profile using one of the following options:

- **Using the macOS Profile Editor** (p. 107): The editor is provided by Parallels Mac Management and is integrated into the Configuration Manager console.
- **Importing a Profile from a File** (p. 112): Import a device configuration profile from a file (.mobileconfig) created with an external profile editor.

Installing configuration profiles via MDM

As per Apple requirements, configuration profiles can only be installed via MDM 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 install any configuration profile via MDM, even if it's not a requirement.

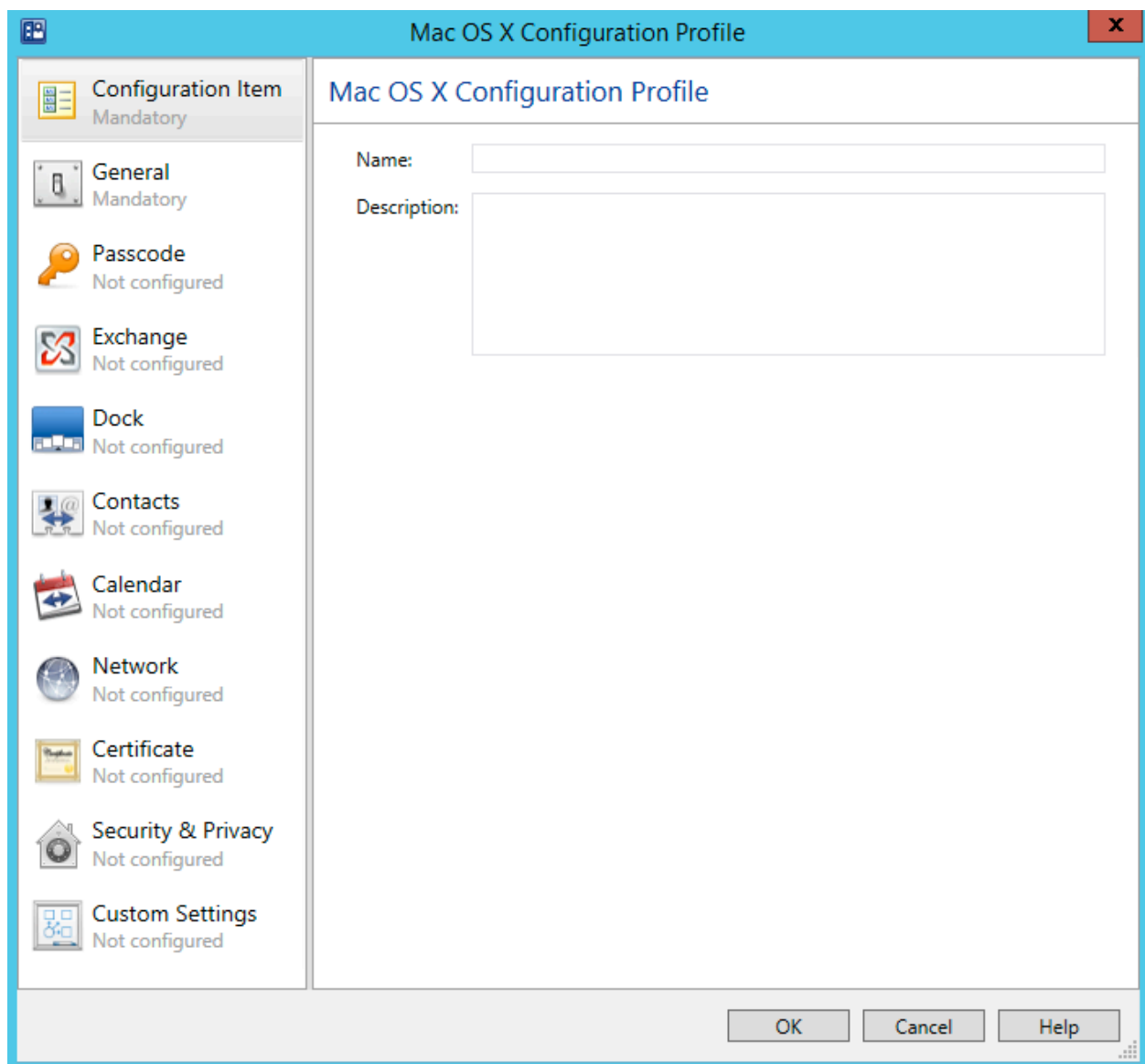
To install a configuration profile via MDM, you need Parallels IBCM/MDM Proxy installed and your Mac computers must be enrolled in MDM. Consider the following possible scenarios:

- If you are using Apple DEP to enroll your computers in SCCM, 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. For instructions on how to install and configure Parallels IBCM/MDM Proxy and enroll Mac computers in MDM, read the entire **Configuring Parallels IBCM/MDM Proxy section** (p. 43). Please note that when configuring Parallels IBCM/MDM Proxy, you need to enable MDM Proxy (select a corresponding option in the configuration wizard). This step is described in **Configuring Parallels MDM** (p. 45).

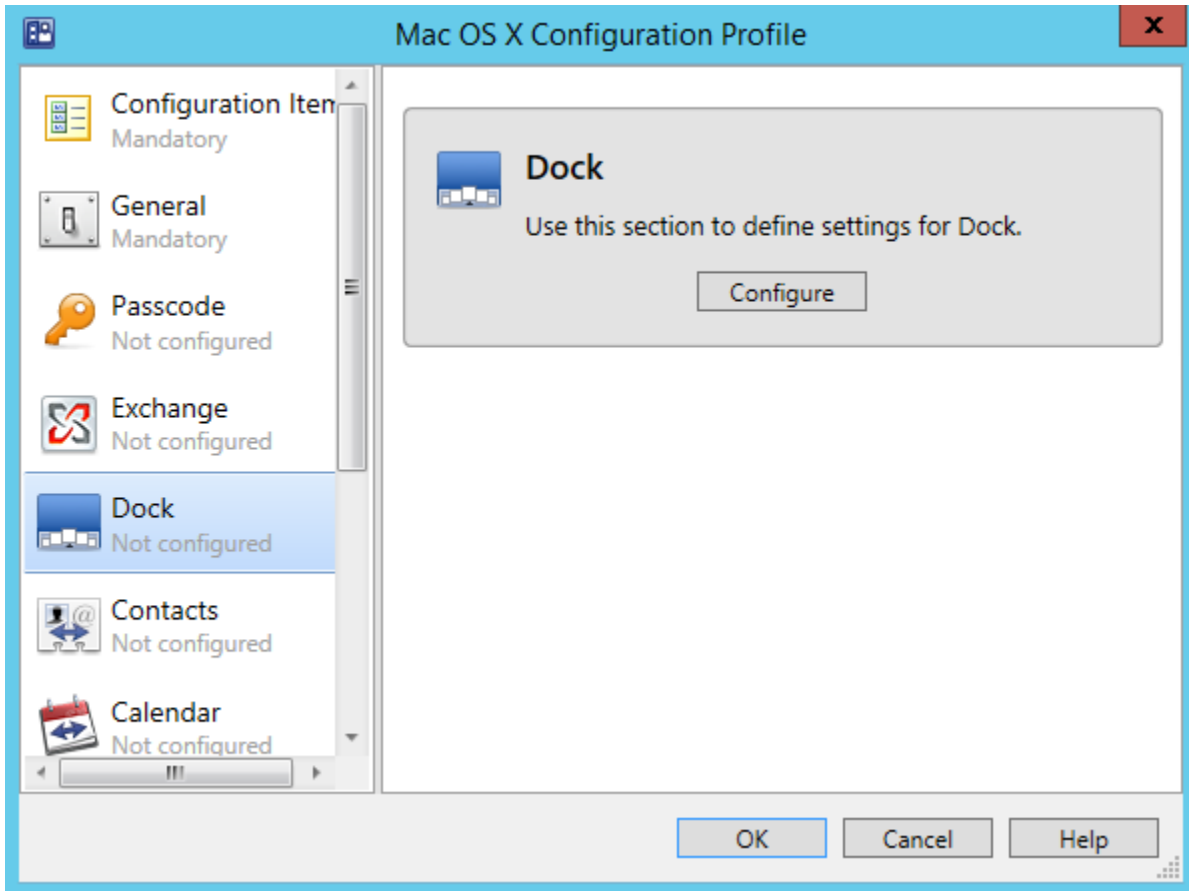
Using the macOS Profile Editor

To create a macOS configuration profile using the built-in profile editor:

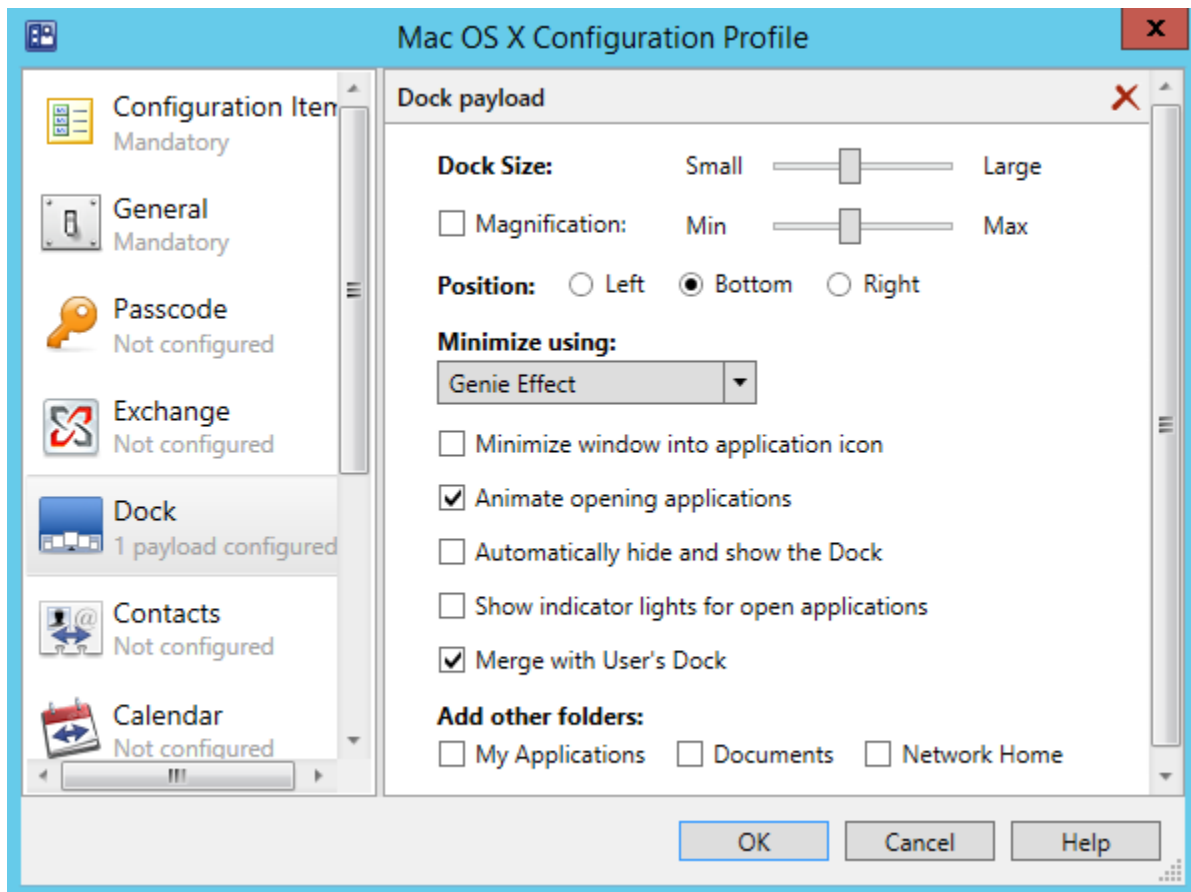
- 1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings / Configuration Items**.
- 2 Right-click **Configuration Items**, point to **Create Parallels Configuration Item**, and then click **Mac OS X Configuration Profile**.
- 3 The **Mac OS X Configuration Profile** dialog opens.



The left pane of the dialog 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 SCCM. 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. 111).

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. 138) 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 **Creating macOS Configuration Profile Using the Profile Editor** (p. 107).
- 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 .plist 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. For additional information, please see the **Saving the Configuration Profile** subsection in **Creating macOS Configuration Profile Using the Profile Editor** (p. 107).

Importing a Profile from a File

To create a configuration profile and save it to a file, you need to use one of the external configuration profile editors, which are available from Apple and from third-party vendors, including:

- Apple Configurator 2
- Apple Profile Manager
- iMazing Profile Editor (<https://imazing.com/guides/how-to-create-or-edit-apple-configuration-profiles>)
- ProfileCreator (<https://github.com/ProfileCreator/ProfileCreator>)

Use the profile editor of your choice to create a profile and save it as a `.mobileconfig` file.

Once you have the file, do the following:

- 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 **Import Configuration Profile from File**.
- 3 In the dialog that opens, enter a configuration item name and description and then select the profile type from the options described below.

User profile

Select the **User profile** option if you want to install the configuration profile using the current user's security context.

Note: The System Policy Control payload (designated by specifying `com.apple.systempolicy.control` as the `PayloadType`) 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.

System profile

Use the **System profile** option if you want to install the configuration profile as `root`. To install a configuration profile via MDM, select the **Install via MDM server** option.

Specify a configuration profile file

After making selections describe above, click the **Browse** button and select a `.mobileconfig` file that you would like to import. The profile can be signed, encrypted, or both signed and encrypted. When done, click **OK** to save your changes. The new configuration item is created with the XML content of the configuration profile embedded into it. Press **F5** to refresh the **Configuration Items** list to see the new item.

Editing a profile

To edit the profile, right-click it and choose **Edit Parallels Configuration Item**. The **Mac OS X Configuration Profile** dialog will now have the **Import from .mobileconfig** and **Export to .mobileconfig** buttons. Using these two buttons, you can export the profile to a file, edit it in an external profile editor and then import it back into the configuration item.

The import operation performs the following validations of the profile data:

- The profile type (User or System) must be the same as the original.
- If this is a signed profile, the payload identifier must be the same as the original.
- If the profile is not signed but the payload identifier differs from the original, a message box containing this information will be displayed. You'll have an option to cancel or continue the importing operation.

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. 138) for more information.

Creating an Apple Mobile Device Configuration Profile

To create an Apple mobile device configuration profile, you need to use one of the external configuration profile editors, which are available from Apple and from third-party vendors, including:

- Apple Configurator 2
- Apple Profile Manager
- iMazing Profile Editor (<https://imazing.com/guides/how-to-create-or-edit-apple-configuration-profiles>)
- ProfileCreator (<https://github.com/ProfileCreator/ProfileCreator>)

Use the profile editor of your choice to create a profile and save it as a `.mobileconfig` file.

Once you have the configuration profile file, do the following:

- 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 **Import Configuration Profile from File**.
- 3** In the dialog that opens, enter a configuration item name and description.
- 4** Select the **System profile** and **Install via MDM server** options. Please note that to use this functionality, you need Parallels MDM Proxy installed and configured. For details, please read the entire **Configuring Parallels IBCM/MDM Proxy** section (p. 43).
- 5** Click the **Browse** button and select the `.mobileconfig` file that you created earlier using an external editor. When done, click **OK** to save your changes.

The new configuration item is created with the XML content of the configuration profile embedded into it. Press **F5** to refresh the **Configuration Items** list to see the new item.

Editing a profile

To edit the profile, right-click it and choose **Edit Parallels Configuration Item**. The dialog will now have the **Import** and **Export** buttons. Using these two buttons, you can export the profile to a file, edit it in an external profile editor and then import it back into the configuration item.

The import operation performs the following validations of the profile data:

- The profile type (i.e. System) must be the same as the original.
- If this is a signed profile, the payload identifier must be the same as the original.

- If the profile is not signed but the payload identifier differs from the original, a message box containing this information will be displayed. You'll have an option to cancel or continue the importing operation.

To evaluate Apple mobile devices for compliance, you need to add the configuration item to a baseline and then deploy it to the **All Mobile Devices** collection. See **Deploying Configuration Baseline** (p. 138) for more information.

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 SCCM site (p. 257). 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. 115)
- **FileVault 2 Encryption with Personal Recovery Key** (p. 123)

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 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. 123).

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

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

- Enter a configuration item name and description.
- 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.
- 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. 138) 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 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 Mac Management has saved in its database (p. 257). 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 Mac Management database (p. 257). 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 Mac 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 Mac 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 **LVGUID**, **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.

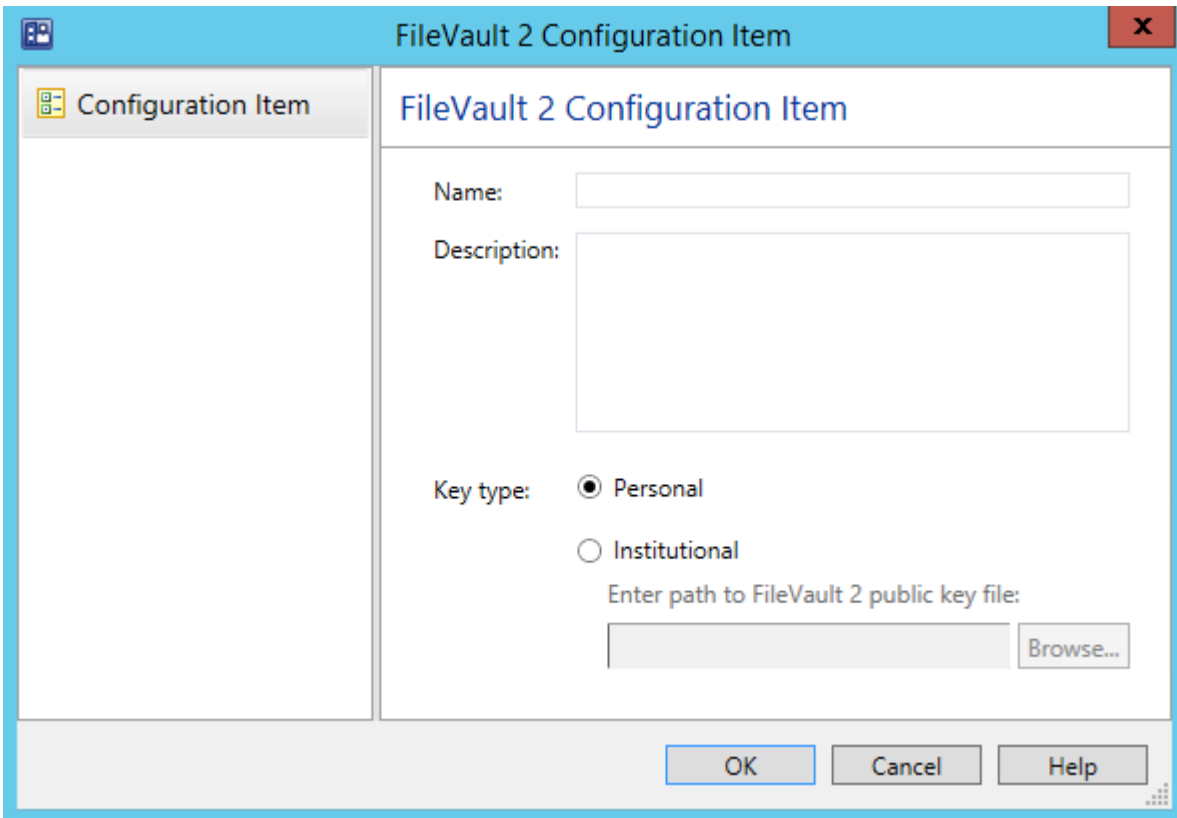
Creating FileVault 2 Configuration Item

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. 115).

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. 138) 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 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 Mac Management database (p. 257) 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. 121).

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 Mac Management database (p. 257). 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 Mac 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 **LVGUID**, **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 Mac 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
```

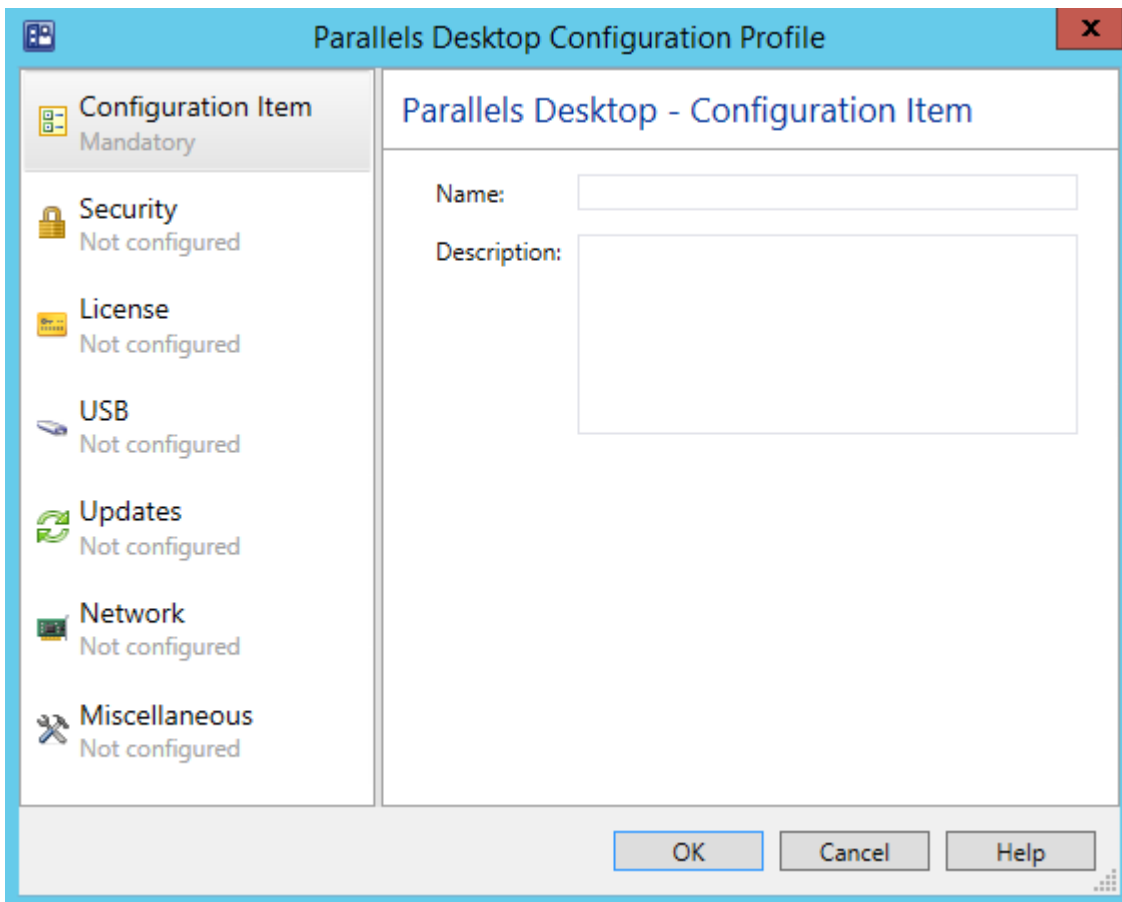
Enforcing Parallels Desktop Preferences

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 an 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. 138) for more information.

Enforcing Parallels Desktop VM Settings

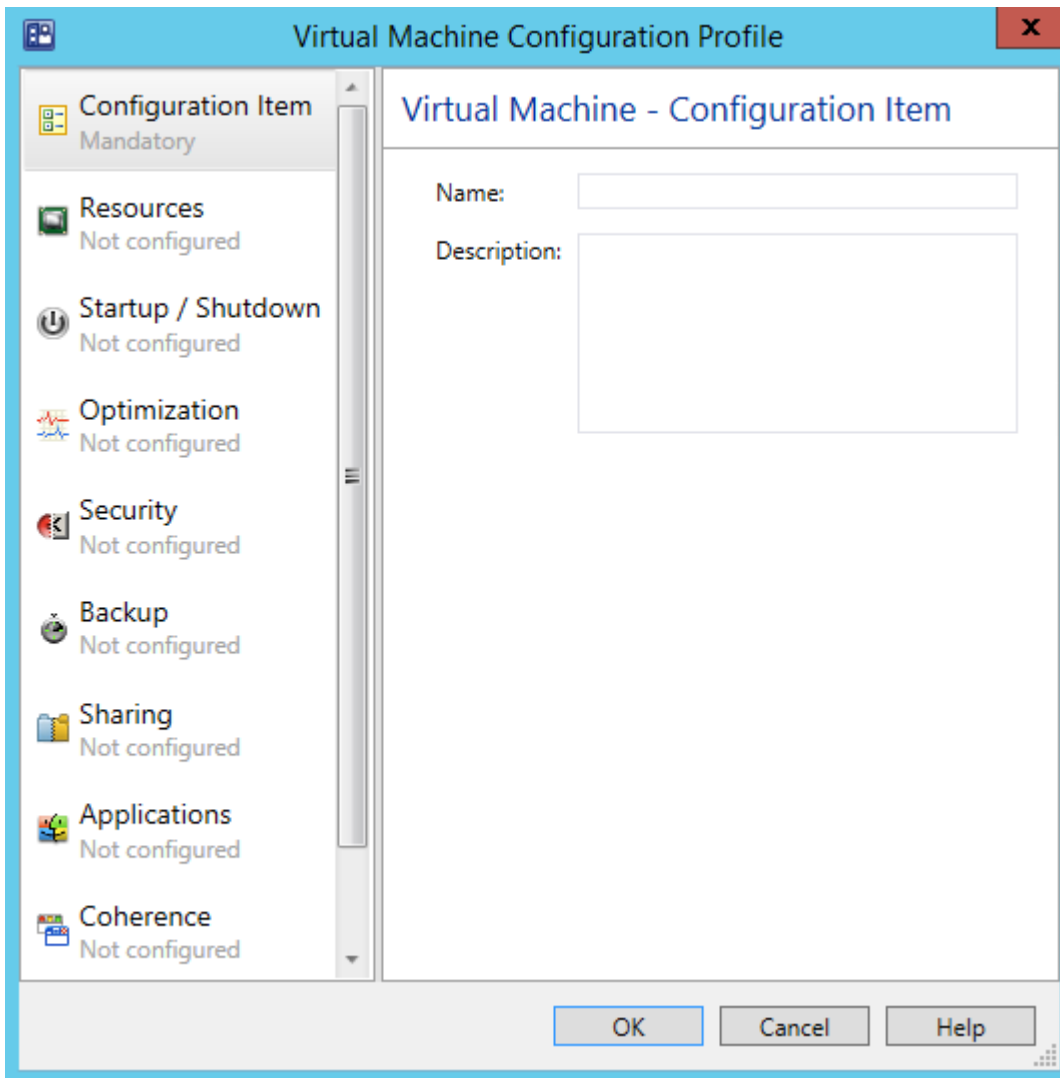
A Parallels Desktop virtual machine has numerous configuration options that can be customized according to your organization requirements. To monitor Mac computers for virtual machine configuration compliance you need to create a virtual machine configuration item specifying the desired configuration 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. 138) 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 SCCM 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 SCCM. 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. 134)
- Create a discovery script (p. 136)
- Create a remediation script (p. 136)
- Specify the script interpreter to be used (p. 137)
- Define Compliance Rules (p. 137)

Creating a Configuration Item

To use scripts to assess compliance, you need to create a standard SCCM 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 Page

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 Page

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 Mac 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 Page

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 Discovery Script** (p. 136) 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 Remediation Script** (p. 136) 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. 137) 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 Page

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 Pages

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. 138) 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. 134).

The script can be written in any scripting language supported by macOS, such as Bash, Python, Apple Script, etc. See **Specifying Script Interpreter** (p. 137) 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. 136), 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 SCCM.

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. 134).

The script can be written in any scripting language supported by macOS, such as Bash, Python, Apple Script, etc. See **Specifying Script Interpreter** (p. 137) 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 SCCM.

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. 134).

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.

Deploying macOS and Executing Task Sequences

Note: The Parallels Mac Management functionality described here does not support macOS 11 Big Sur.

Parallels Mac Management provides you with the ability to deploy macOS on Mac computers using task sequences. The 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 Mac Management.
 - Prepare a bootable USB drive (flash drive or HDD) using a special utility supplied with Parallels Mac 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 (p. 152).
- 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 SCCM.

Non-operating system deployments

Parallels Mac Management also 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. 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. 170).

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. For details, please see **Parallels NetBoot Server Requirements** (p. 22).
- 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. 144).

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 Mac 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 SCCM.

Add the macOS 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.

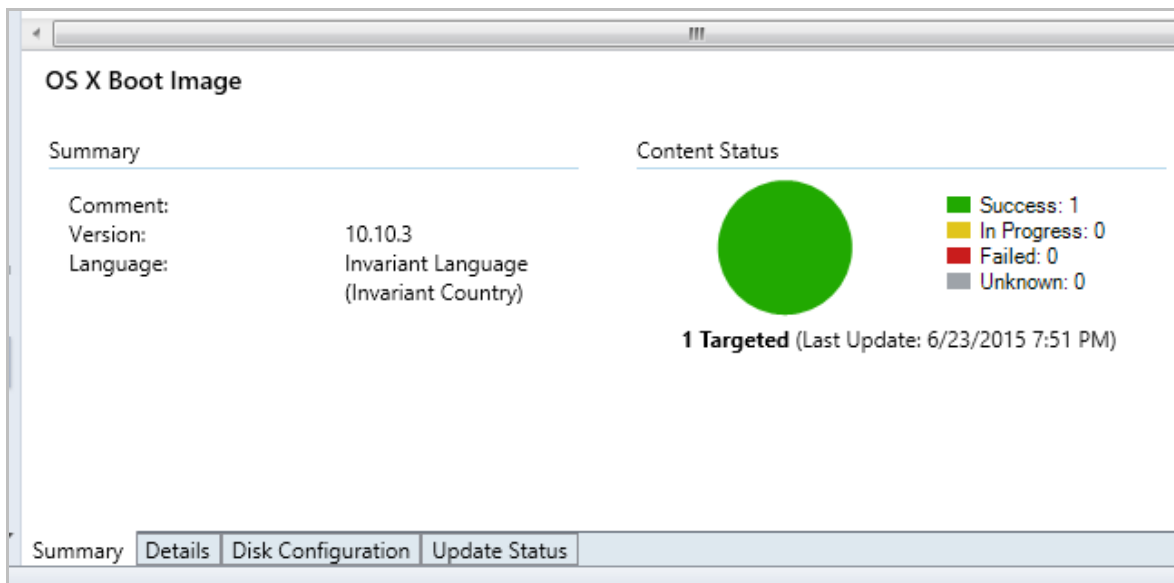
- 5 Click **Next**.
- 6 Specify a macOS image name and version and click **Next**.
- 7 Wait for the image to be converted to the .wim format.
- 8 Click **Finish**.

Distribute Content of the macOS 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 Mac 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 Mac Management provides you with two methods that can be used to capture a macOS system image:

- Using a task sequence. (p. 145) 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 SCCM, and then running it on a Mac to capture the image.
- Using the Image Builder utility provided by Parallels (p. 147). 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 10.8 Mountain Lion 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 Mac Management v4.0 or earlier, you need to create a new boot image using the current Parallels Mac 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 $(15 \text{ GB} + 0.65 \text{ GB}) * 2 = 31.3 \text{ GB}$. 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 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. 166) and **Running a Task Sequence on a Mac** (p. 166).

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 Mac Management for Microsoft SCCM. 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 10.8 Mountain Lion 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 10.9 Mavericks or newer installed. The inactive partition from which you'll capture the image must have macOS 10.8 Mountain Lion or newer.

Capture a macOS System Image

To capture a macOS system image:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac 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 SCCM

Add the Image to Configuration Manager

After you captured the macOS image, you need to add it to Configuration Manager. To do so:

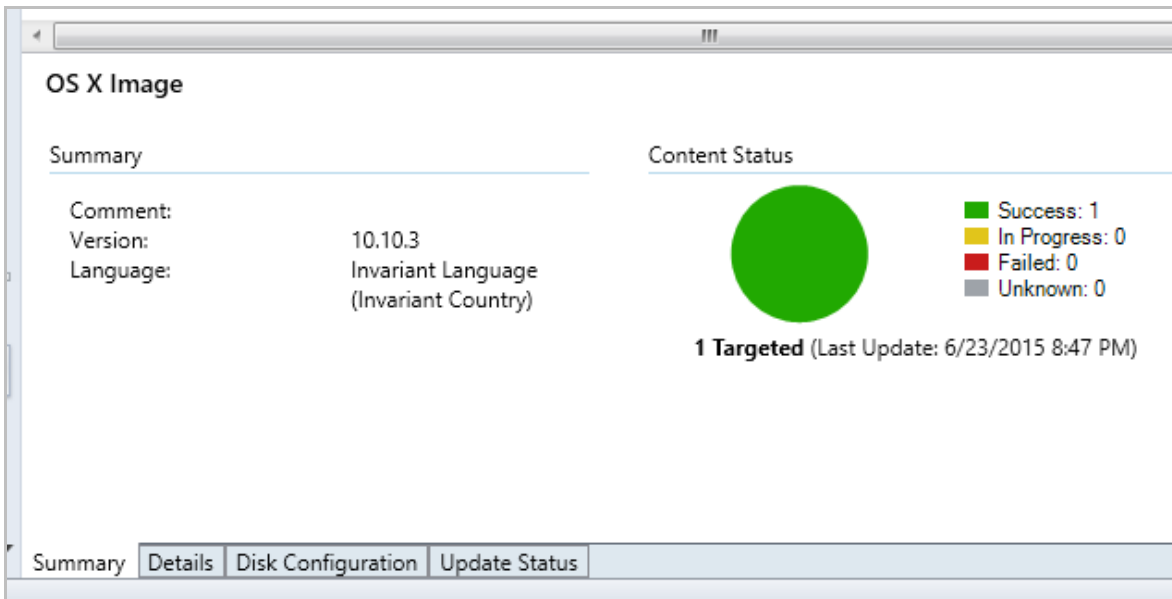
- 1 In the Configuration Manager console, navigate to **Software Library / Overview / Operating Systems / Operating System Images**.
- 2 Right-click **Operating System Images** and then click **Add OS X Image**.
- 3 The **Add OS X Image** dialog opens.
- 4 In the **Path to the OS X image directory** 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` 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. 170).

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. 152) 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. 152).

- 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. 152).

Note: The **Destination** option was introduced in Parallels Mac Management v6.0. If you have existing task sequences that were created in earlier versions of Parallels Mac 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. 152).

- 8 At this point, you can add other steps to the task sequence as described in the **Task Sequence Steps** section (p. 152) 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. 161), 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 Mac 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, as described in **Creating a Task Sequence for Deploying macOS** (p. 150).

The ability to specify a destination partition for macOS image deployment in a task sequence was introduced in Parallels Mac 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 Mac 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. 150).

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, please see **Using Task Sequence Variables** (p. 161).

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 SCCM, 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 SCCM Application Deployment** (p. 177). 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. 178)
- **Create a Configuration Manager Application** (p. 179)
- **Configure the Deployment Type** (p. 180)

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 SCCM 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. 157).
- Using the **Kernel Extensions** task sequence step (p. 159) 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.

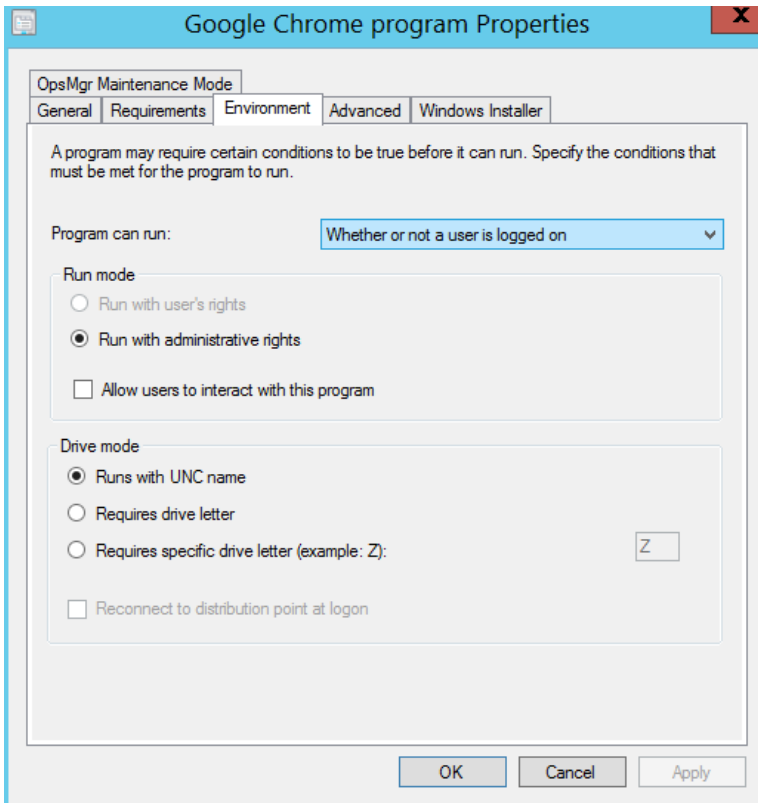
Install Package

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. 172). 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 **Using Task Sequence Variables** (p. 161).

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 **Using Task Sequence Variables** (p. 161).

Apply Configuration Profile

You can use the **Apply Configuration Profile** task sequence step to configure Mac computers using a configuration profile created in advance. A configuration profile is created using an external configuration profile editor. It is an XML file with the ".mobileconfig" extension that contains the macOS configuration settings that your organization requires.

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 a description. The description is optional but highly recommended. See **Configuration profile data** at the end of this section for the explanation.
- 4 Click the **Import Profile** button and select a configuration profile (a file with the ".mobileconfig" extension).
- 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 **Using Task Sequence Variables** (p. 161).

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 (p. 169).

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 SCCM, 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 **Enrolling Mac Computers via Apple DEP** (p. 204).
- 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. For instructions on how to install and configure Parallels IBCM/MDM Proxy and then enroll Mac computers in MDM, read the entire **Configuring Parallels IBCM/MDM Proxy** section (p. 43). Please note that when configuring Parallels IBCM/MDM Proxy, you need to enable the MDM Proxy (select a corresponding option in the configuration wizard). This step is described in **Configuring Parallels MDM** (p. 45).

Configuration profile data

After you import a configuration profile into the task sequence step and click **OK** in the **Task Sequence Editor for Macs** dialog, the profile data is saved in the task sequence. Please note that when you open the dialog later, no functionality is provided to preview the configuration profile data. For this reason, you should enter a meaningful description when creating an **Apply Configuration Profile** task sequence step. You can also click the **Export Profile** button to export the profile saved in the task sequence to a file. This can come handy if you don't have the original .mobileconfig file anymore, but would like to review the settings stored in the profile. Once you export the profile, you can open the resulting .mobileconfig file in an external configuration profile editor.

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 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 (p. 169).

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 **Using Task Sequence Variables** (p. 161).

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 SCCM, you should already have your Mac computers enrolled in MDM. You can read more about the DEP support in **Enrolling Mac Computers via Apple DEP** (p. 204).

- 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. For instructions on how to install and configure Parallels IBCM/MDM Proxy and enroll Mac computers in MDM, please read the entire **Configuring Parallels IBCM/MDM Proxy** section (p. 43). Please note that when configuring Parallels IBCM/MDM Proxy, you need to enable the MDM Proxy (select a corresponding option in the configuration wizard). This step is described in **Configuring Parallels MDM** (p. 45).

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 **Using Task Sequence Variables** (p. 161).

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

The **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 **Using Task Sequence Variables** (p. 161).

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 Step Properties Using Task Sequence 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 that you are defining has been defined for a device collection or 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 Mac Management for Microsoft SCCM.
- 2 Create a Configuration Manager software package (p. 172) containing the script.
- 3 Add the software package as the **Install Package** task sequence step (p. 156).

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
```

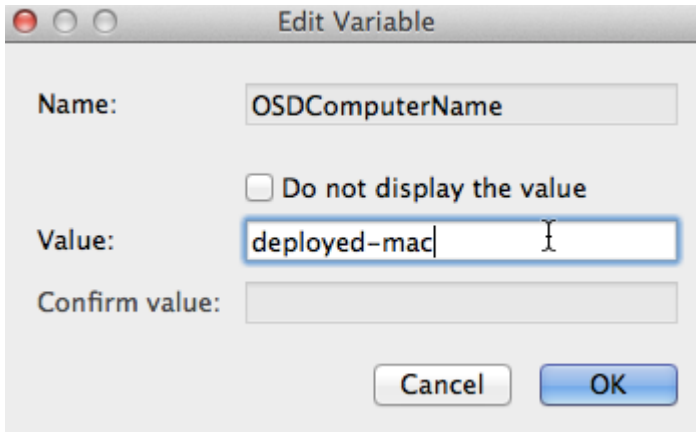
Prompting Users to Set Empty Variables During Task Sequence Execution

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 Mac 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 (p. 141) or a bootable USB drive that you prepared earlier (p. 144).
- 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 (p. 144) 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

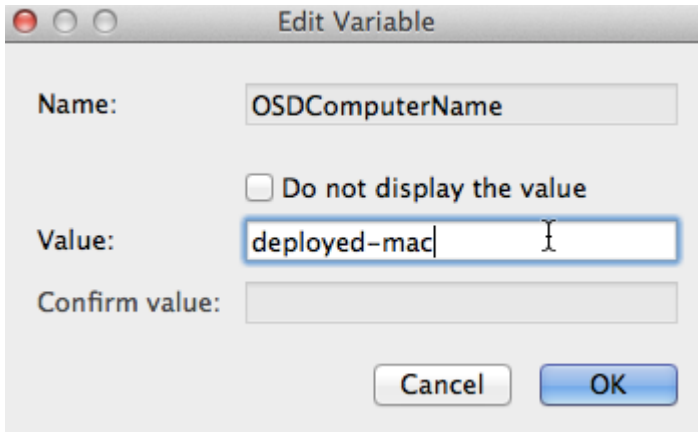
If you have configured a macOS boot image (p. 141) to boot your Mac computers from the network, do the following:

- 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 SCCM, 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. 157) 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 Mac Management:
 - In Parallels Mac 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.

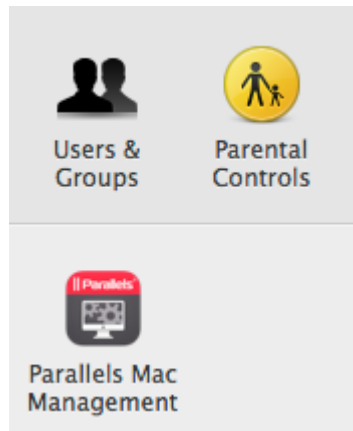
Read on to learn how to execute other task sequence steps and how to verify the deployment.

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 Mac 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 Mac 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 Mac 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. For the information about creating a task sequence, please see **Creating a Task Sequence for Deploying macOS** (p. 150). 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 SCCM task sequence properties dialog. The following list describes the properties that are supported by Parallels Mac 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.

Initiating Task Sequence Execution by a User

If you specified the deployment as "Available", the user will need to initiate the task sequence execution manually. To do so, the user opens the Parallels Application Portal and locates the task sequence in it. Non-OSD task sequences are treated as application 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 execute a task sequence, the user clicks the **Install** button (just like for applications). The task sequence execution is then performed in the background with no user interaction required.

Deploying Software via SCCM Package Deployment

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

Please note that Parallels Mac Management supports Configuration Manager Package and Application deployment models. This section describes how to distribute software via SCCM Package deployment. For Application deployment, please see **Deploying Software via SCCM Application Deployment**. (p. 177)

Parallels Mac Management also supports software deployment via task sequences. For details, see **Non-Operating System Deployments** (p. 170).

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.

See also **Create Package and Program Wizard**

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.

Please make sure that the distribution point is properly configured as described in the **Configuring a Distribution Point** section.

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.

Deploying Software via SCCM Application Deployment

Applications are similar to SCCM packages (p. 172) but contain more information to support smart deployment. Parallels Mac Management natively supports the Application Management feature of SCCM and allows you to deploy applications on Mac computers.

Please also note that in addition to Packages and Applications, Parallels Mac Management supports software deployment via task sequences. For details, see **Non-Operating System Deployments** (p. 170).

The steps to create and deploy a Mac application are:

- 1 Choose the installation type (install an application on a Mac silently or interactively) (p. 177)
- 2 Prepare a Mac application for Configuration Manager (p. 178)
- 3 Create a Configuration Manager application (p. 178)
- 4 Configure the Deployment Type (p. 180)
- 5 Deploy the application (p. 182)

The following topics in this section describe how the application is installed on a Mac and how to use the Parallels Application Portal.

- Installing Application on a Mac (p. 183)
- Using Parallels Application Portal (p. 185)

The Application Deployment section concludes with the instructions on how to **Uninstall Applications** (p. 186).

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. 185).

Prepare a Mac Application for Configuration Manager

Before you can deploy a native macOS software package (.app, .dmg etc.) in SCCM, 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.

CMAAppUtil 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:

```
./CMAAppUtil <properties>
```

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

```
./CMAAppUtil -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 **CMAAppUtil** 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** — click **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 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

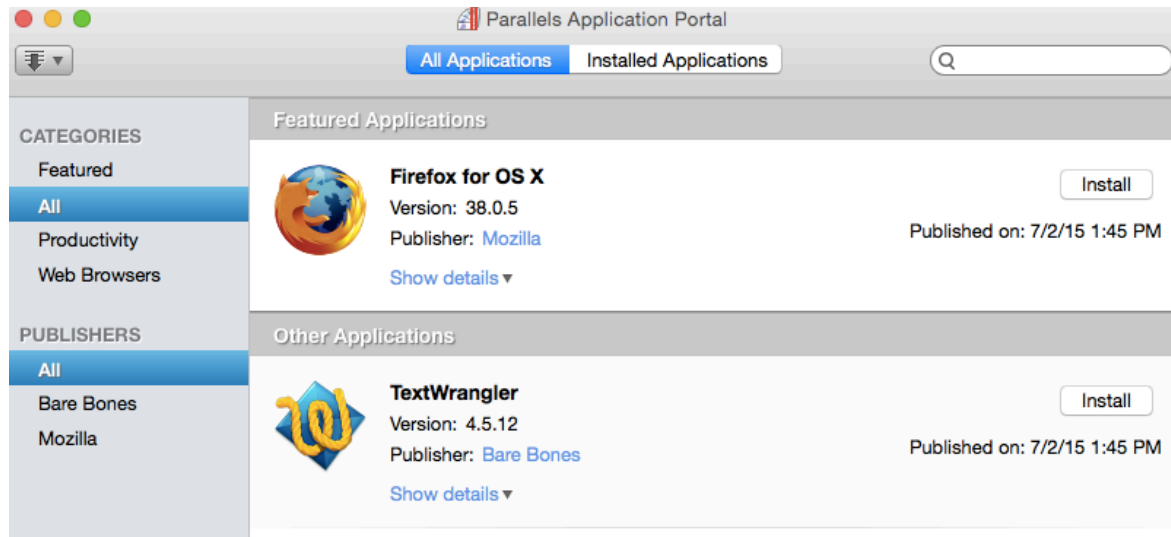
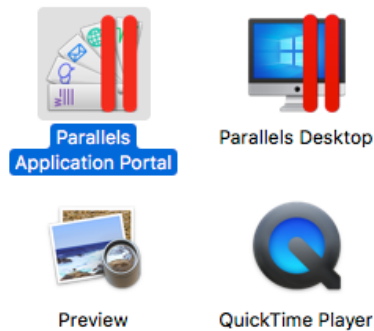
If the installation type was specified as silent (the **Deploy Software Wizard** > **User Experience page** > **Hide in Software Center and all notifications** option was selected), no message asking the user to install the application will be displayed, and the installation will be performed silently 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 Mac Management for Microsoft SCCM 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 SCCM Application Deployment** (p. 177).

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. 179). 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. 180).

Uninstalling Applications

To uninstall an application that was installed earlier, use the same SCCM 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 SCCM the same way as described earlier in this section (p. 179).
- 2 Configure the Deployment Type (p. 180) and specify the uninstallation command for the application in the **Programs > Installation program** field.
- 3 Deploy the application using the **Deploy Software Wizard (p. 182)**. 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 Mac Management

Using the functionality described above, you can also uninstall applications that were not installed via Parallels Mac 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)

macOS Software Update Management

Parallels Mac Management for Microsoft SCCM allows you to manage macOS software updates (patches) using the native SCCM functionality. Using this functionality you can import the information about available macOS updates into SCCM 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 Mac Management installer again and install the component. Before you do, please don't forget to read **Parallels OS X Software Update Point Requirements** (p. 22) and make sure the requirements are met or you will not be able to configure Parallels OS X Software Update Point.
- By default, Mac computers will download deployed macOS updates from Apple's servers. If you want to minimize Internet traffic, you may prefer to host macOS updates on a local server. Please note that Parallels Mac 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. For more information, please refer to the documentation that comes with the software of your choice.

Configuration Options

Parallels Mac 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. The default URL for downloading macOS software update catalogs and packages is <https://swscan.apple.com/content/catalogs/others/>.

When this configuration is used, macOS updates are installed on Mac computers as follows:

- 1 Parallels OS X Software Update Point downloads software update catalogs from Apple's servers and then imports them into WSUS.
- 2 WSUS is synchronized with SCCM, so the administrator can view and deploy macOS updates using the Configuration Manager console.
- 3 The SCCM administrator selects which updates they want to install on Mac computers and deploys them.
- 4 Mac computers download deployed updates from Apple's servers, after which the updates are silently installed on them. If an update requires a Mac restart, the Mac user will have a choice to postpone the installation.

- 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 SCCM and deploy macOS updates to Mac computers, please see **Configuring SCCM and Deploying macOS Updates** (p. 197).

Download Updates From a Local Server

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 SCCM, so the administrator can view and deploy macOS updates using the Configuration Manager console.
- 4 The SCCM 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 Mac 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 like this:

`http://myhost.example.com/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\SOFTWAREWow6432Node\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 an SCCM Configuration Item with discovery and remediation scripts (for instructions on how to use scripts in Configuration Items, please see **Using Scripts to Assess Compliance** (p. 134)). 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):

Edit Rule

Specify rules to define compliance conditions for this setting

Name:

Description:

Selected setting:

Rule type:

The setting must comply with the following rule:

the following values:

Run the specified remediation script when this setting is noncompliant

Report noncompliance if this setting instance is not found

Noncompliance severity for reports:

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 SCCM and deploy macOS updates on a Mac, please see **Configuring SCCM and Deploying macOS Updates** (p. 197).

Restrict Which Updates a Mac User Can Install

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 SCCM, so the administrator can view and deploy macOS updates using the Configuration Manager console.
- 3** The SCCM 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 SCCM. 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 an SCCM Configuration Item with discovery and remediation scripts (for instructions on how to use scripts in Configuration Items, please see **Using Scripts to Assess Compliance** (p. 134)). 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):

The screenshot shows the 'Edit Rule' dialog box with the following configuration:

- Name: New Rule
- Description: (empty)
- Selected setting: Set Mac Client SU catalog mode \Catalog Mc
- Rule type: Value
- The setting must comply with the following rule:
 - The value returned by the specified script: Equals
 - the following values: 2
- Run the specified remediation script when this setting is noncompliant
- Report noncompliance if this setting instance is not found
- Noncompliance severity for reports: None

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 SCCM and deploy macOS updates on a Mac, please see **Configuring SCCM and Deploying macOS Updates** (p. 197).

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 Mac 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 like this:

```
http://myhost.example.com/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.

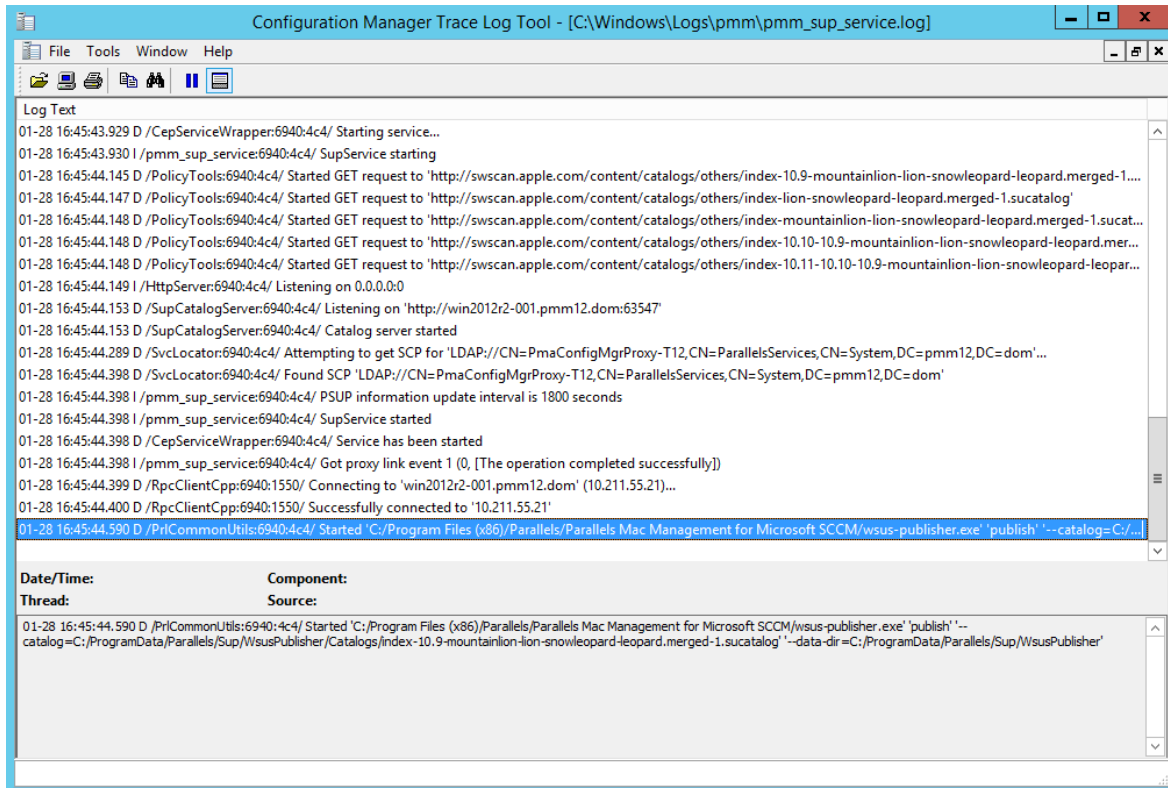
Configuring SCCM and Deploying macOS Updates

This section describes how to import the information about available macOS updates into SCCM and how to deploy updates to Mac computers.

Import macOS Software Updates

macOS software update catalogs must be imported into SCCM before you can deploy them to Mac computers. The steps below explain how the import is done.

- 1 Once you've installed and configured Parallels OS X Software Update Point, it automatically begins downloading software update catalogs, which contain information about available macOS updates.
- 2 It then imports catalog metadata into WSUS using the local publishing API. Please note that update packages (binaries) are not downloaded and are not present in WSUS.
- 3 You can view the import process log by opening the following log file:
`%Windir%\Logs\pmm\pmm_sup_service.log` file.



Configure Synchronization of SCCM with WSUS

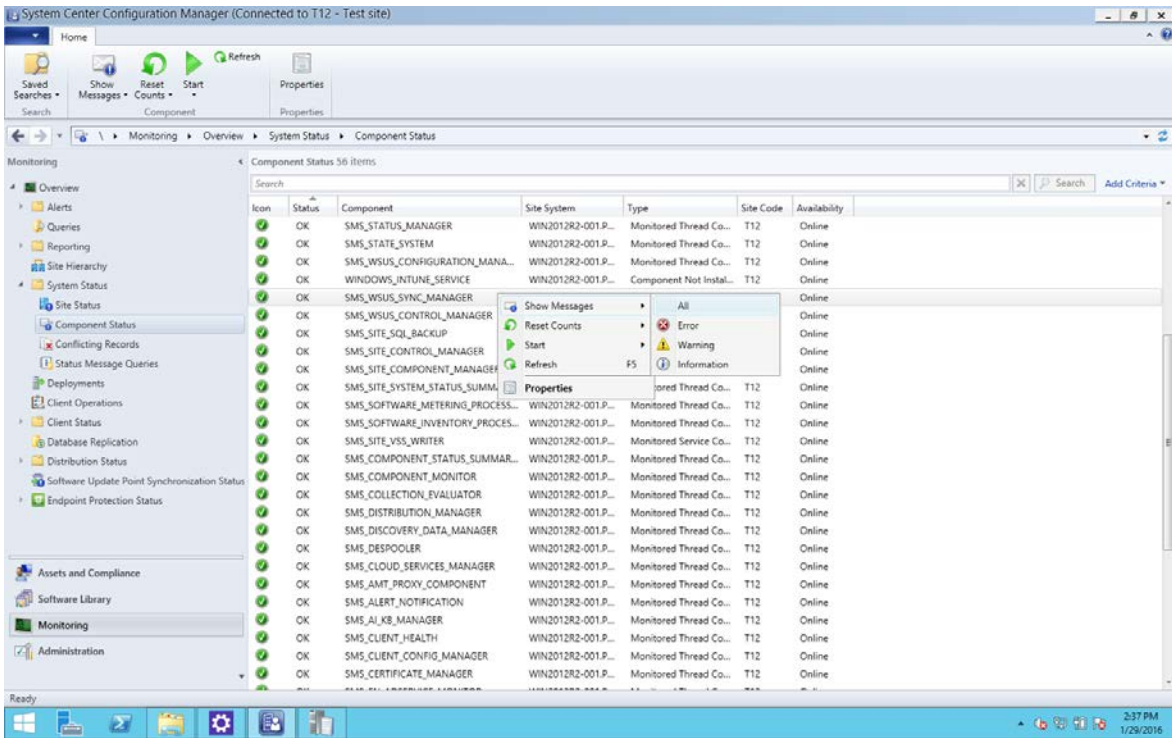
In order for the information about available macOS updates to become available in SCCM, you need to synchronize SCCM with WSUS. The steps described here must be performed only once. The synchronization itself is done by the SCCM Software Update Point role.

If you already have a synchronization scheduled, you can either wait for it to complete or you can start it manually. This is necessary for the **Apple** option to appear in the **Software Update Point Component Properties** dialog, as you will see later in this topic.

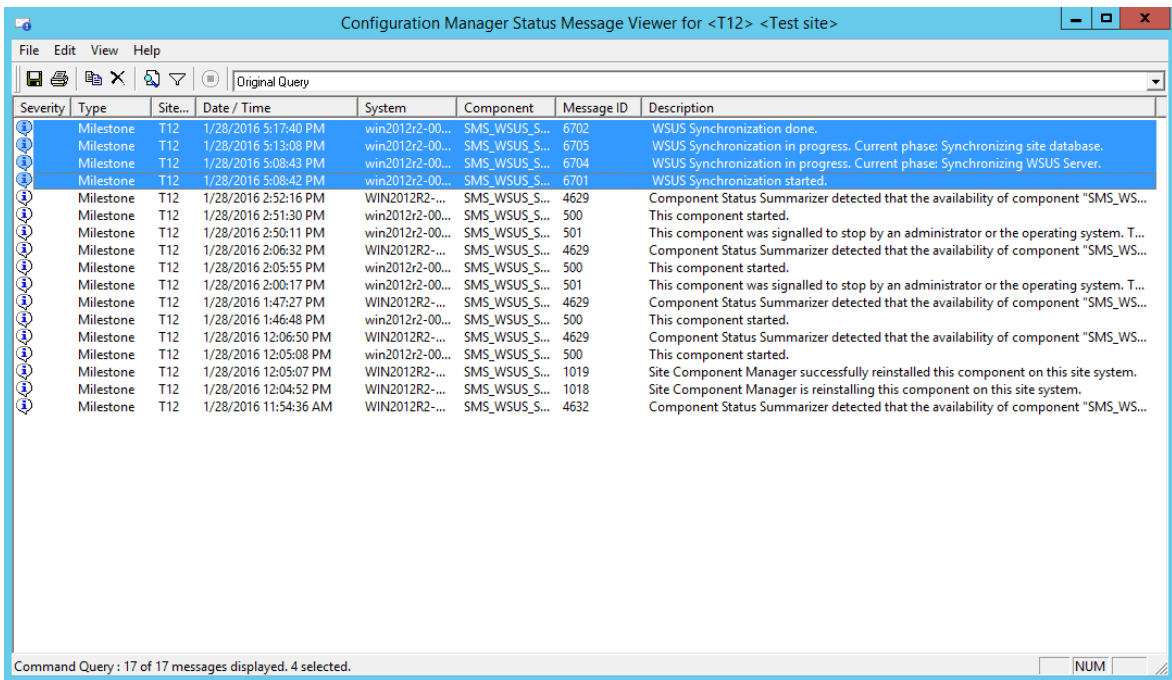
Configure Synchronization Settings

- 1 In the Configuration Manager console, navigate to **Software Library / Software Updates**.
- 2 Right-click **All Software Updates** and choose **Synchronize Software Updates**.

- Wait for the synchronization to complete. You can monitor the process in the **Monitoring / Overview / System Status / Component Status / SMS_WSUS_SYNC_MANAGER**.



- In the message viewer, you will see the "WSUS Synchronization done" record.



Configure the Software Update Point Role

You now need to configure the Software Update Point role to synchronize Apple software updates. To do so, follow these steps:

- 1 Navigate to **Administration / Overview / Site Configuration / Sites**.
- 2 Right-click your site and choose **Configure Site Component > Software Update Point**.
- 3 On the **Classifications** tab page, select the **Updates** option.
- 4 On the **Products** tab page, select **Apple** and click **OK**.

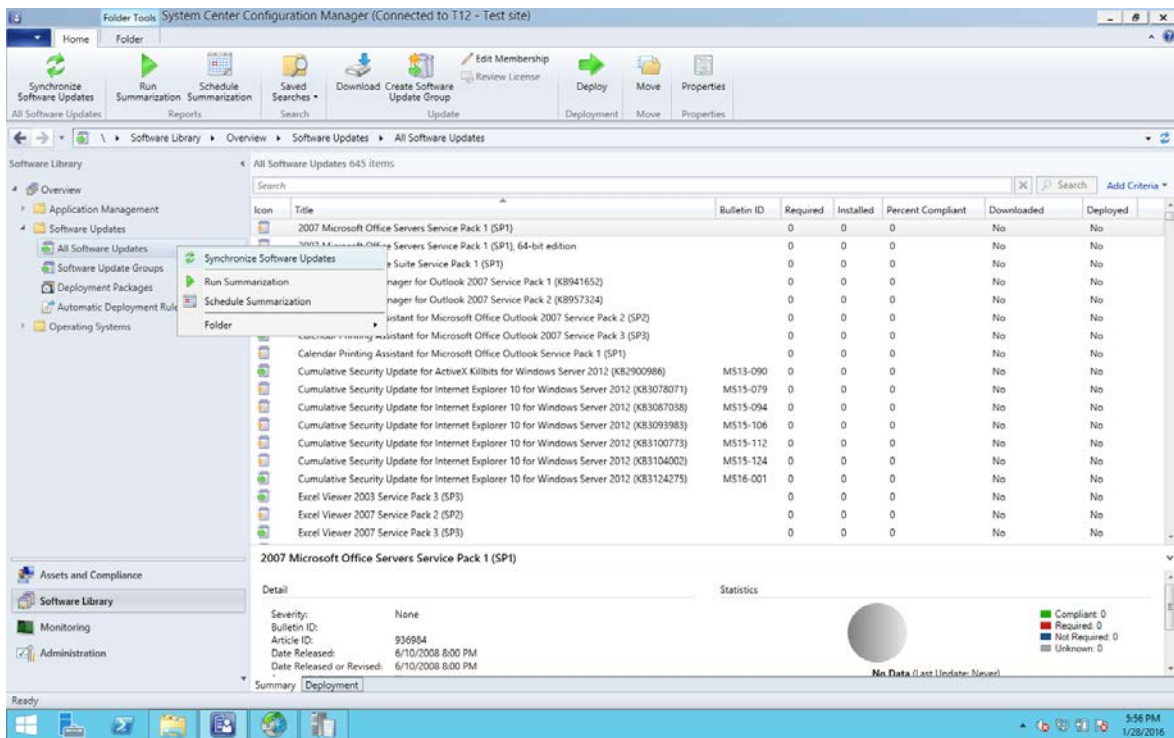
Note: If the **Apple** product is not present on the **Products** tab page it's because the software update point did not synchronize with WSUS after the Apple software updates were imported. In such a case try repeating the steps described in this topic from the beginning.

Synchronize SCCM with WSUS

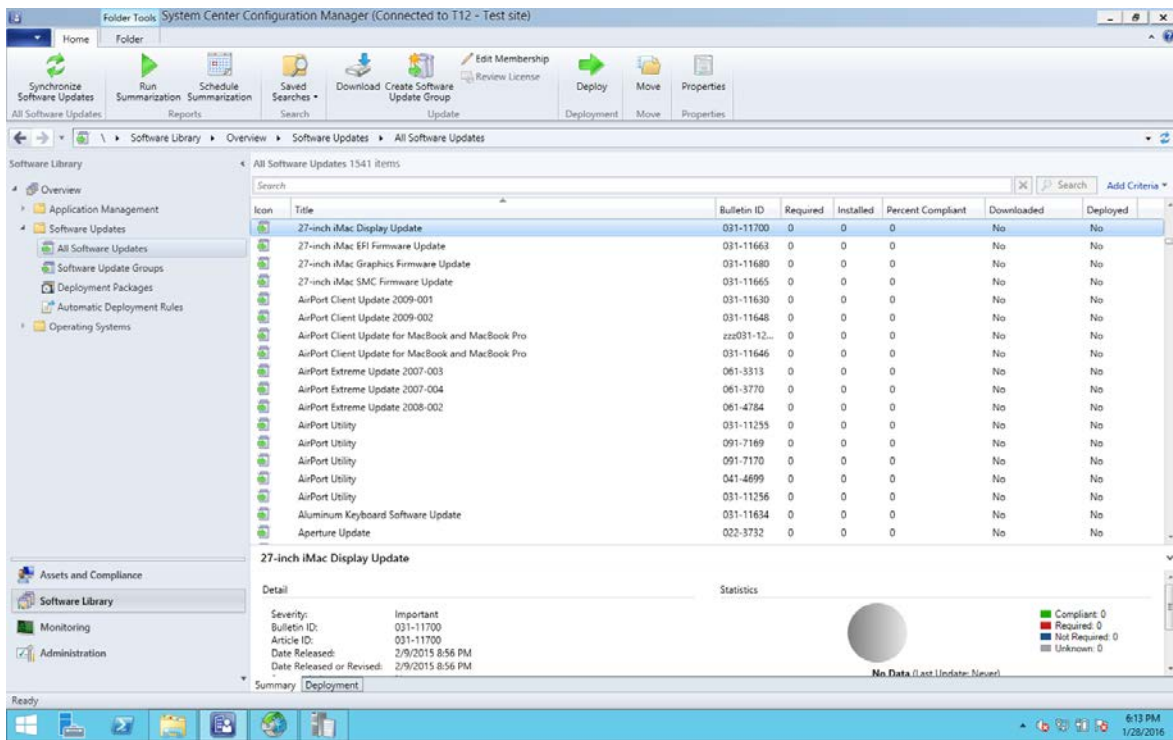
Once the synchronization settings are configured, you need to perform the actual synchronization. You can schedule the synchronization or you can perform it manually. The manual synchronization procedure is described below. If you want to run it on a schedule, please refer to the SCCM documentation.

To synchronize SCCM with WSUS manually:

- 1 Run the WSUS synchronization again.



2 You will see available macOS updates in the **Software Library / Overview / Software Updates / All Software Updates**.



Deploy Updates to Mac Computers

When macOS updates are displayed in the **All Software Updates** list, you can deploy them using the standard Configuration Manager functionality.

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. When policies with software update assignments are delivered to a Mac, the Parallels Mac Client running on it 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.

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.

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 Mac Management.

6 Click **OK** when done.

Executing Scripts on Mac Computers

With Parallels Mac 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 SCCM to deploy a script to it. A connection with a Mac is established via SSH regardless of whether it is enrolled in SCCM 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. 67).
 - **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**.

Enrolling Mac Computers via Apple DEP

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 Mac Management for Microsoft SCCM supports DEP and provides you with the ability to automatically enroll new Mac computers in SCCM during the initial DEP setup procedure.

To use the DEP functionality, you must be enrolled in Apple Deployment Programs. For more information, please refer to the Apple DEP guide:

https://www.apple.com/education/docs/DEP_Guide.pdf

Enable Parallels MDM

To enable the DEP functionality in SCCM, 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 following topics:

- **Parallels IBCM/MDM Proxy Requirements** (p. 18)
- **Install Parallels Mac Management** (p. 38)
- **Configuring Parallels IBCM/MDM Proxy** (p. 43)

Please read the above topics carefully as all of the requirements and configuration steps must be completed for Parallels MDM Proxy to function properly.

Once Parallels MDM Proxy is installed and configured, you can set up the DEP functionality in the Configuration Manager console. Read on to learn how to do it.

Establish a Connection to the Apple DEP Web Service

During Parallels Mac Management installation, a local Parallels DEP service is automatically installed on the same server where you install Parallels Configuration Manager Proxy. The Parallels DEP service is used to communicate with the local Parallels MDM Proxy and the virtual MDM server on the Apple DEP website. To enable these communications, a link for each connection must be configured. The local MDM link is created when you configure Parallels MDM Proxy (p. 45). The link to the virtual MDM server is created as described below.

Configure a link from Parallels DEP service to a virtual MDM server

First, you need to obtain the PEM-encoded X.509 certificate from the server where Parallels Configuration Manager Proxy and the Parallels DEP service are running. To do so:

- 1** In the Configuration Manager console, navigate to **Administration / Parallels Mac Management / Device Enrollment Program / DEP Links**.

- 2 Right-click a DEP link in the right pane and choose **Properties**. The **DEP Link Properties** dialog opens.
- 3 Click **Configure** to open the **DEP Link Configuration Wizard**.
- 4 Click the **Download Certificate** button to save the PEM-encoded X.509 certificate containing the PEM public key of the MDM key pair on the local computer. Specify a location and file name. The certificate is needed to create a virtual MDM server on the Apple DEP website. The public/private key pair is generated and stored securely on a server when you configure the local Parallels MDM Proxy.

You now need to upload the certificate to the Apple DEP website. To do so:

- 1 Visit the Apple DEP website and log in using your Apple ID and password.
- 2 Create a virtual MDM server. Please note that you need a virtual MDM server for each primary SCCM site in which you'll be enrolling Mac computers via DEP.
- 3 Upload the PEM-encoded X.509 certificate that you obtained earlier.
- 4 Download the S/MIME encrypted token file from the Apple DEP website.

Now that you have the S/MIME token, you need to add it to the local server. To do so:

- 1 Return to the **DEP Link Configuration Wizard** in the Configuration Manager console.
- 2 Click **Browse** and select the server token file that you've downloaded in the previous step.
- 3 Click **Next**.
- 4 The server token will now be decrypted and stored to be used for communication between Parallels Mac Management and the Apple DEP website. Wait for the decryption process to complete (you'll see a progress indicator).
- 5 When the settings are applied, Parallels Mac Management will try to connect to the local Parallels MDM Proxy and the virtual MDM server. Depending on the result, the following will happen:
 - If both connections are successful, the **Finish** button on the wizard page becomes enabled.
 - If a connection cannot be established, a message box is displayed describing the problem. You will have to resolve any issues before you can continue.
- 6 Click the **Finish** button to close the wizard.

The **DEP Link Properties** dialog is refreshed with the new information retrieved from the Apple DEP website. Review the information and close the dialog.

Assign Mac computers to the virtual MDM server

Assign your Mac computers to your virtual MDM server on the Apple DEP website. For more information, please see the Apple Device Enrollment Program Guide:
https://www.apple.com/business/docs/DEP_Guide.pdf

View Mac computers assigned to DEP

In the Configuration Manager console, navigate to **Administration / Parallels Mac Management / Device Enrollment Program / Devices**. The list of Mac computers assigned to the virtual MDM server will now be retrieved from your Apple DEP account and displayed in the **Devices** pane. We'll talk more about managing devices in the **Deploy Mac Computers** section (p. 208).

View DEP link properties

To view properties of a DEP link, right-click it and choose **Properties**. The **DEP Link Properties** dialog opens displaying the information.

If you need to reconfigure a DEP link to pair with another virtual MDM server, click the **Configure** button on the **DEP Link Properties dialog**. A warning message will be displayed to prevent accidental changes. You can then repeat the steps described above to reconfigure the link.

You now need to create an enrollment profile and assign it to Mac computers. Read on.

Create a Device Enrollment Profile

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 Mac 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 Mac Management / Device Enrollment Program / Enrollment Profiles**.
- 2 Right-click anywhere in the right pane and choose **New Enrollment Profile**. The **New Device Enrollment Profile** wizard opens.

Complete the wizard as described below.

General Information

On the **General Information** 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 select, 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.

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 SCCM, 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** to close the wizard.

Please note that you cannot edit an existing device enrollment profile, because editing is not supported by the Apple DEP website.

If needed, you can create multiple enrollment profiles and then assign different profiles to different groups of Mac computers according to your needs.

Manage Enrollment Profiles

To view an existing device enrollment profile:

- 1** In the Configuration Manager console, navigate to **Administration / Parallels Mac Management / Device Enrollment Program / Enrollment Profiles**.
- 2** Right-click a profile and choose **Properties**. The **Device Enrollment Profile Properties** 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.

Note that except for downloading a profile, you cannot change any settings in this dialog. The reason for this is Apple doesn't support editing of existing device enrollment profiles.

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.

Deploy Mac Computers

To deploy Mac computers via Apple DEP and enroll them in SCCM, you need to complete the following steps:

- 1 Assign an enrollment profile that you created earlier to Mac computers.
- 2 Deploy a Mac computer using the Apple Device Enrollment Program, which will also automatically enroll the Mac computer in SCCM.

Read on to learn how to perform these tasks.

View Mac Computers Assigned to a Site

To view Mac computers assigned to a site:

- 1 In the Configuration Manager console, navigate to **Administration / Parallels Mac 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 by default, Mac computers are assigned to the primary SCCM site. You can also assign Mac computers to a secondary site (if you have one) as follows:

- 1 Select one or more Mac computers, then right-click on the selection and choose **Assign Site**. The **Device Site Assignment** dialog opens.
- 2 Select a desired site in the list and click **OK** to assign the selected devices to this 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 SCCM.
 - c **Enrolled** — a profile is assigned and the device is enrolled in SCCM.

- **d Disowned** — the device disowned and removed from SCCM (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

You now need to assign an enrollment profile to Mac computers that you plan to deploy using the Device Enrollment Program.

To assign an enrollment profile:

- 1 In the Configuration Manager console, navigate to **Administration / Parallels Mac Management / Device Enrollment Program / Devices**.
- 2 Selects one or more Mac computers, then right-click on the selection and choose **Assign Enrollment Profile**. The **Assign Enrollment Profile** 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.

Deploy Mac Computers

Your Mac computers are now ready to be deployed and enrolled in SCCM. 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 SCCM.
- 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 SCCM 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 SCCM.

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

Using Apple VPP

Parallels Mac Management for Microsoft SCCM v8.0 and newer includes support for Apple Volume Purchase Program (VPP). Using this functionality you can deploy licensed AppStore applications and automatically track the number of consumed licenses.

Prerequisites

To use the Apple VPP functionality, the following prerequisites must be met:

- Parallels IBCM/MDM Proxy must be installed and configured for MDM.
- A Mac computer on which you will be installing VPP applications must be enrolled in MDM.

For details about MDM enrollment see **Configuring Parallels IBCM/MDM Proxy** (p. 43) and **Configure Automatic Mac Enrollment in MDM** (p. 51).

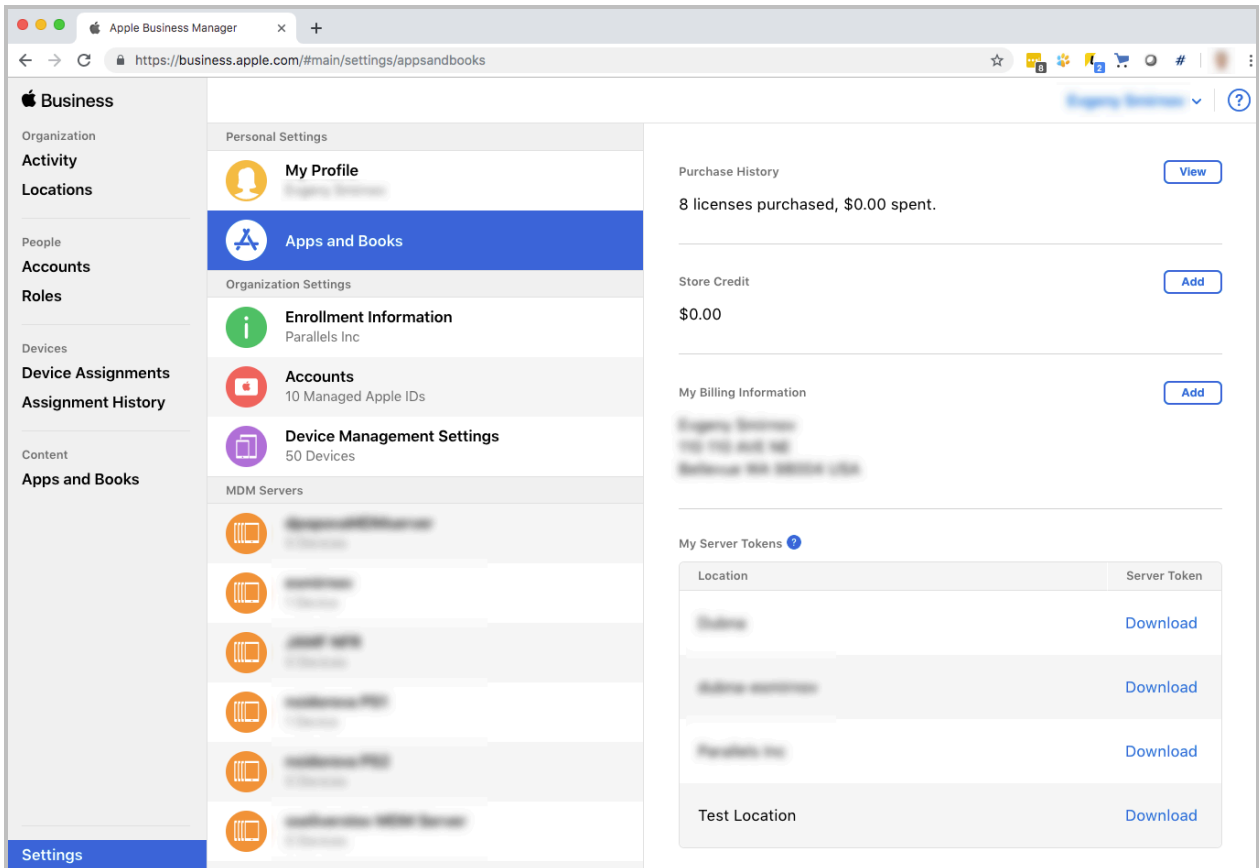
Configuring Apple VPP Support

To configure the Apple VPP support you need to add one or more VPP tokens to Parallels Mac Management.

To add a VPP token:

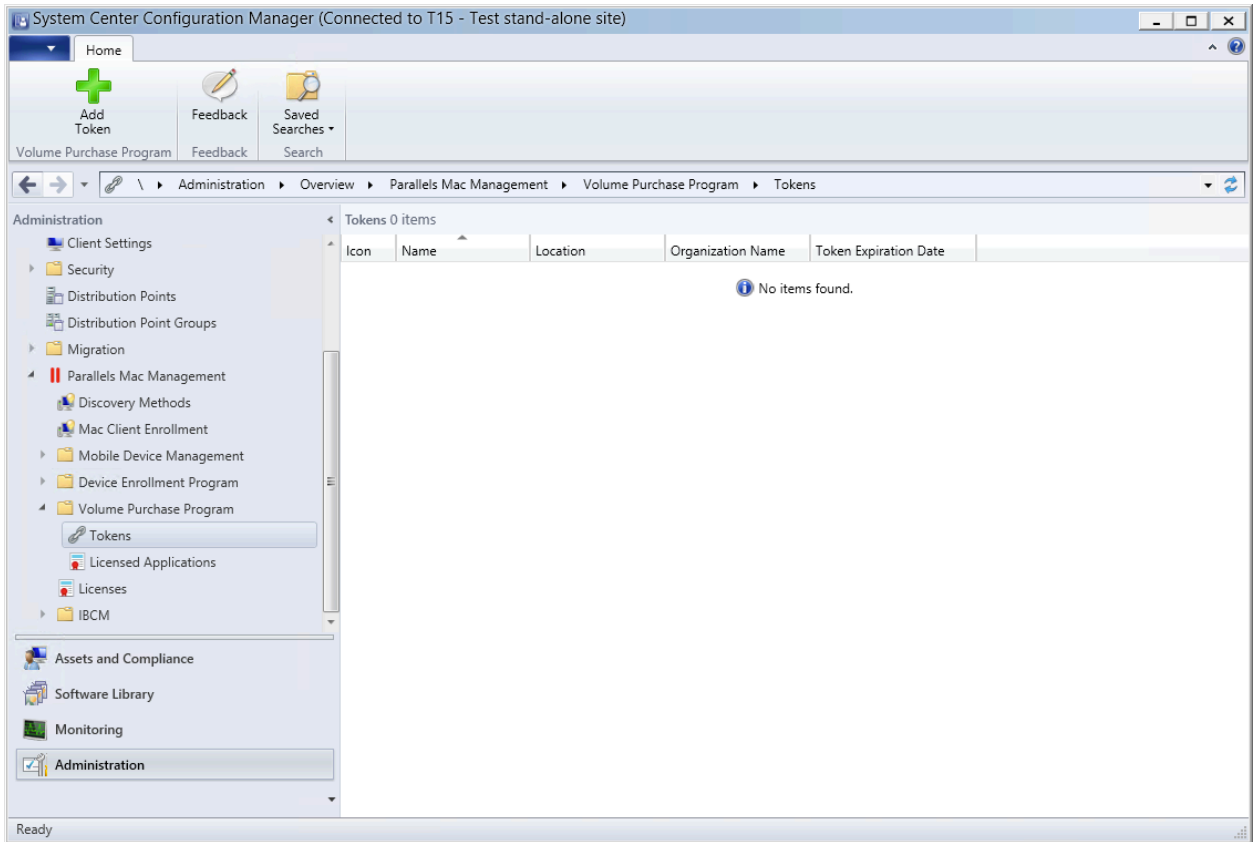
- 1 In a web browser, enter the Apple Business Manager URL: `business.apple.com`

- 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:

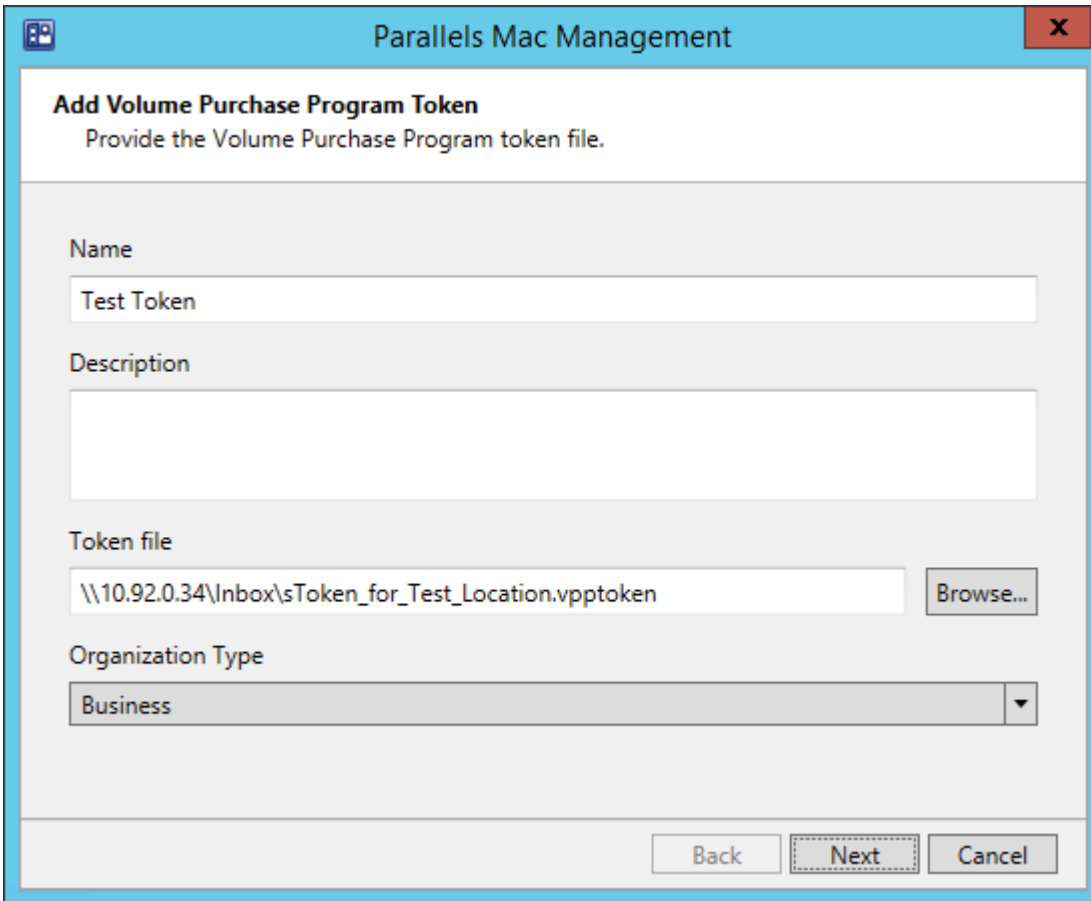


- Click the **Download** link next to the location name to download the VPP token and save it locally.

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



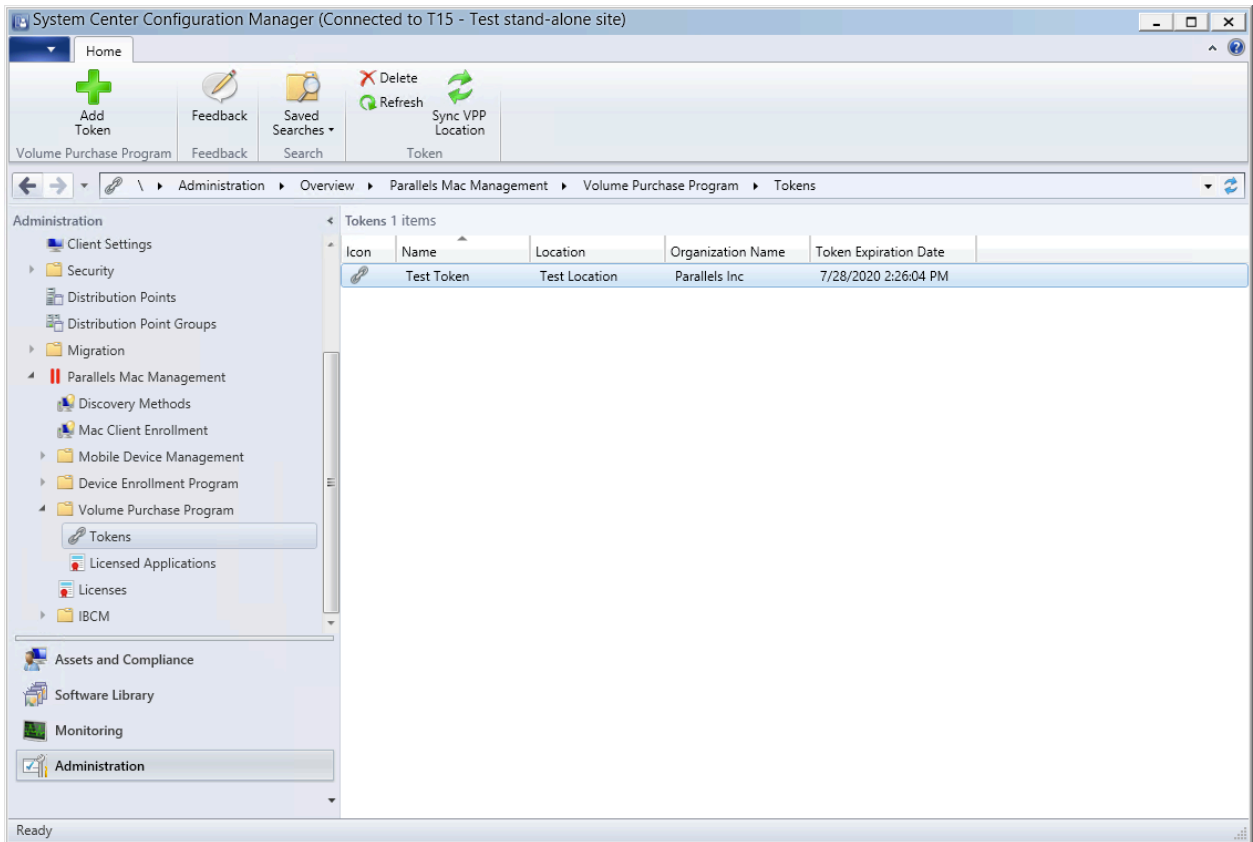
- 5 Click **Add Token** on the toolbar. The **Add Volume Purchase Program Token** wizard opens.



The screenshot shows a window titled "Parallels Mac Management" with a red close button in the top right corner. The main content area is titled "Add Volume Purchase Program Token" and contains the instruction "Provide the Volume Purchase Program token file." Below this, there are four input fields: "Name" with the text "Test Token", "Description" (empty), "Token file" with the path "\\10.92.0.34\Inbox\Token_for_Test_Location.vpptoken" and a "Browse..." button, and "Organization Type" with a dropdown menu set to "Business". At the bottom right, there are three buttons: "Back", "Next" (highlighted with a dashed border), and "Cancel".

- 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**.

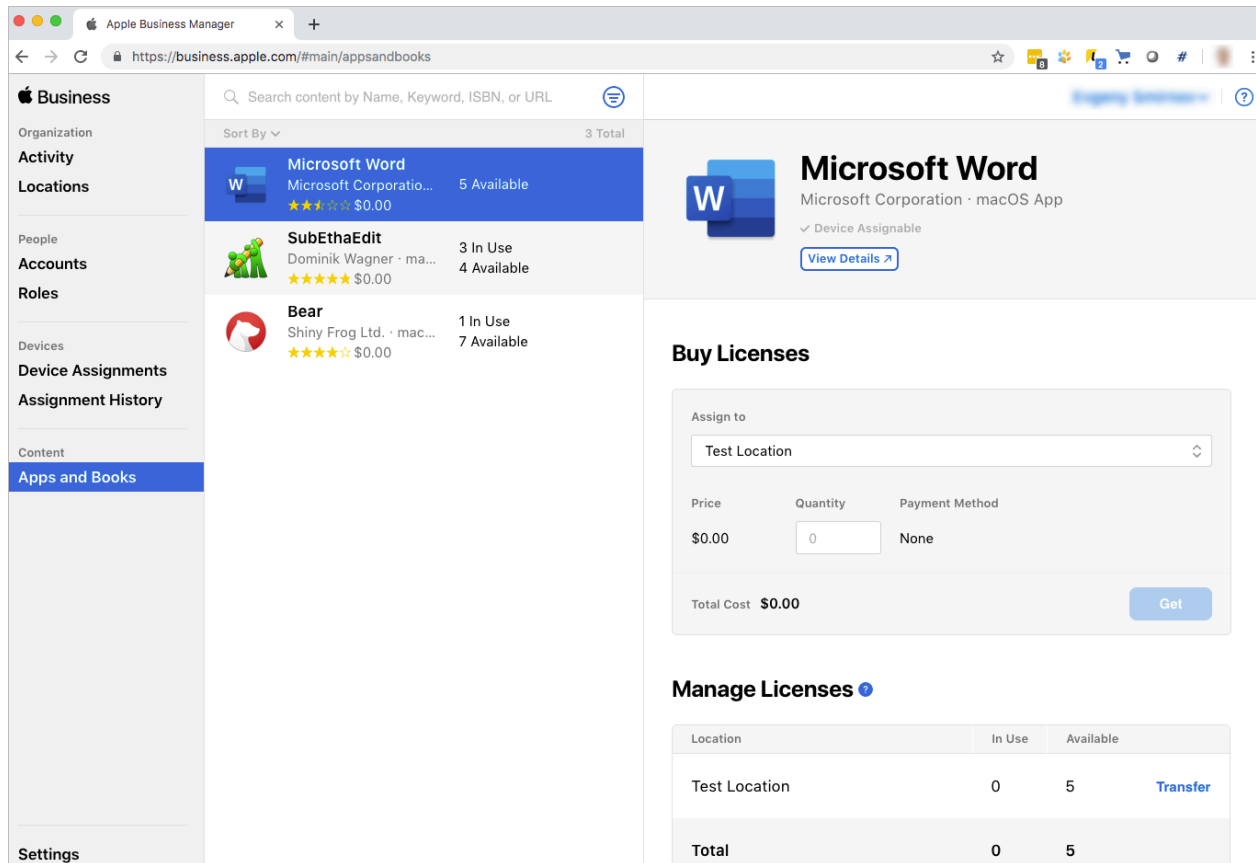
9 The newly added token should now appear in the Configuration Manager console:



Adding an Application to Apple Business Manager

To use the Apple VPP functionality in Parallels Mac Management, you need one or more applications in the location that you are using. If you don't have any applications, you need to purchase one to continue. If you have applications in other locations, you can transfer some licenses from them to this location.

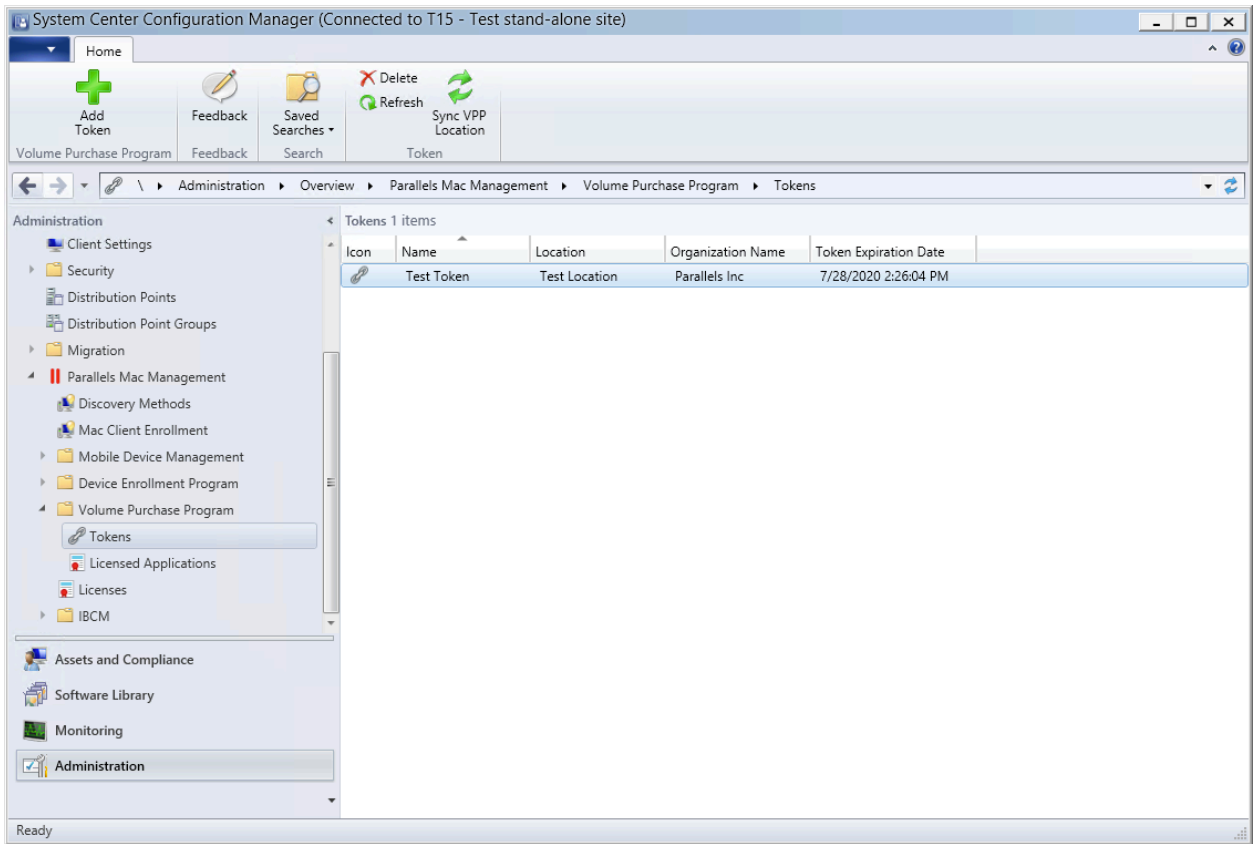
In this this section we'll use Microsoft Word as a sample application, as shown on the screenshot below:



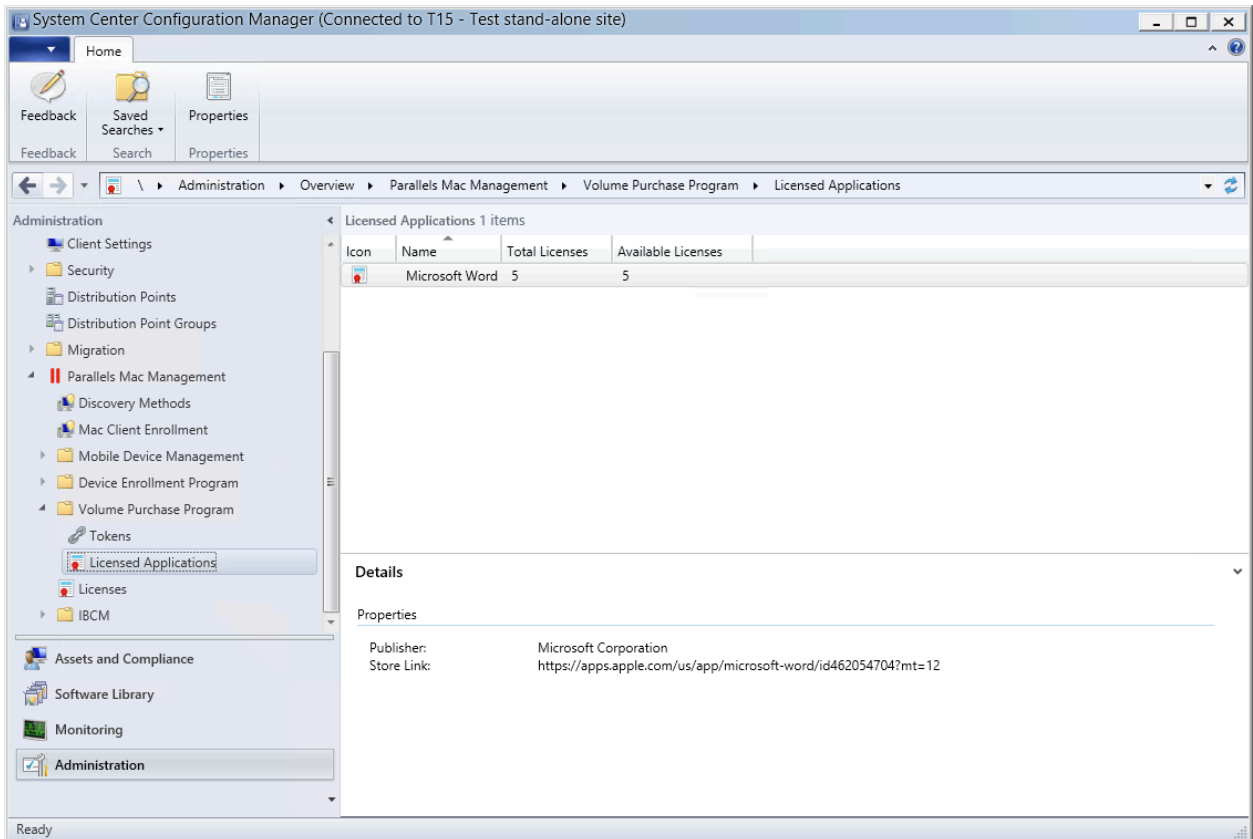
Please note that if you added an application to your location *after* adding the token to the Configuration Manager, the VPP information needs to be synchronized. Configuration Manager performs this synchronization periodically, so it will not happen immediately. If you don't want to wait, you can manually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

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

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



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



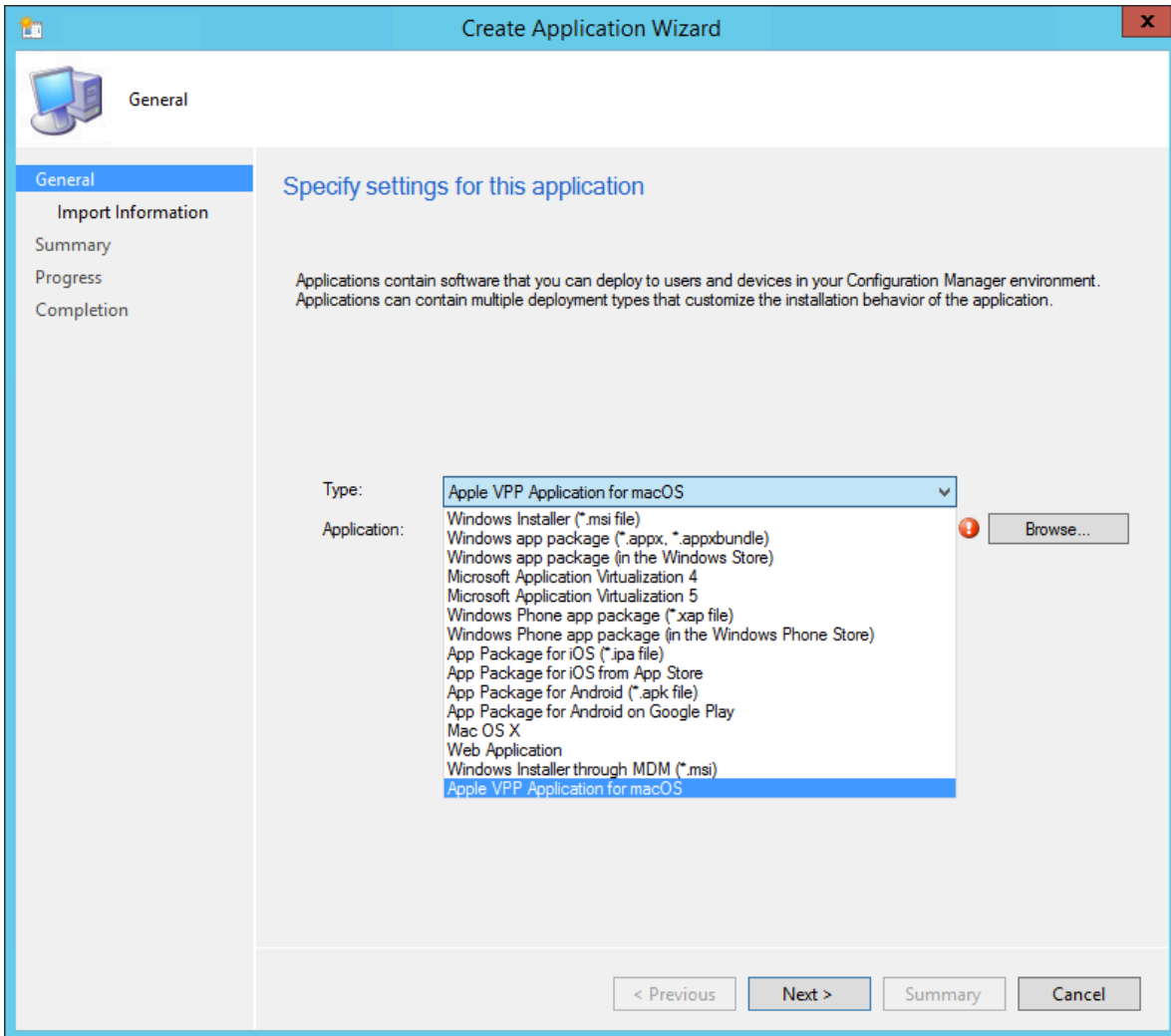
Creating an Application

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

To create an application in SCCM:

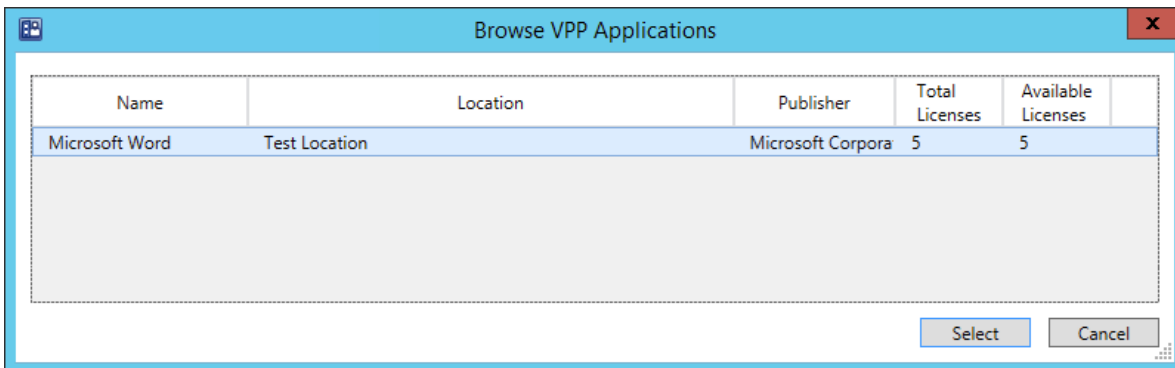
- 1 In the Configuration Manager console, navigate to **Software Library / Overview / Applications**:

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

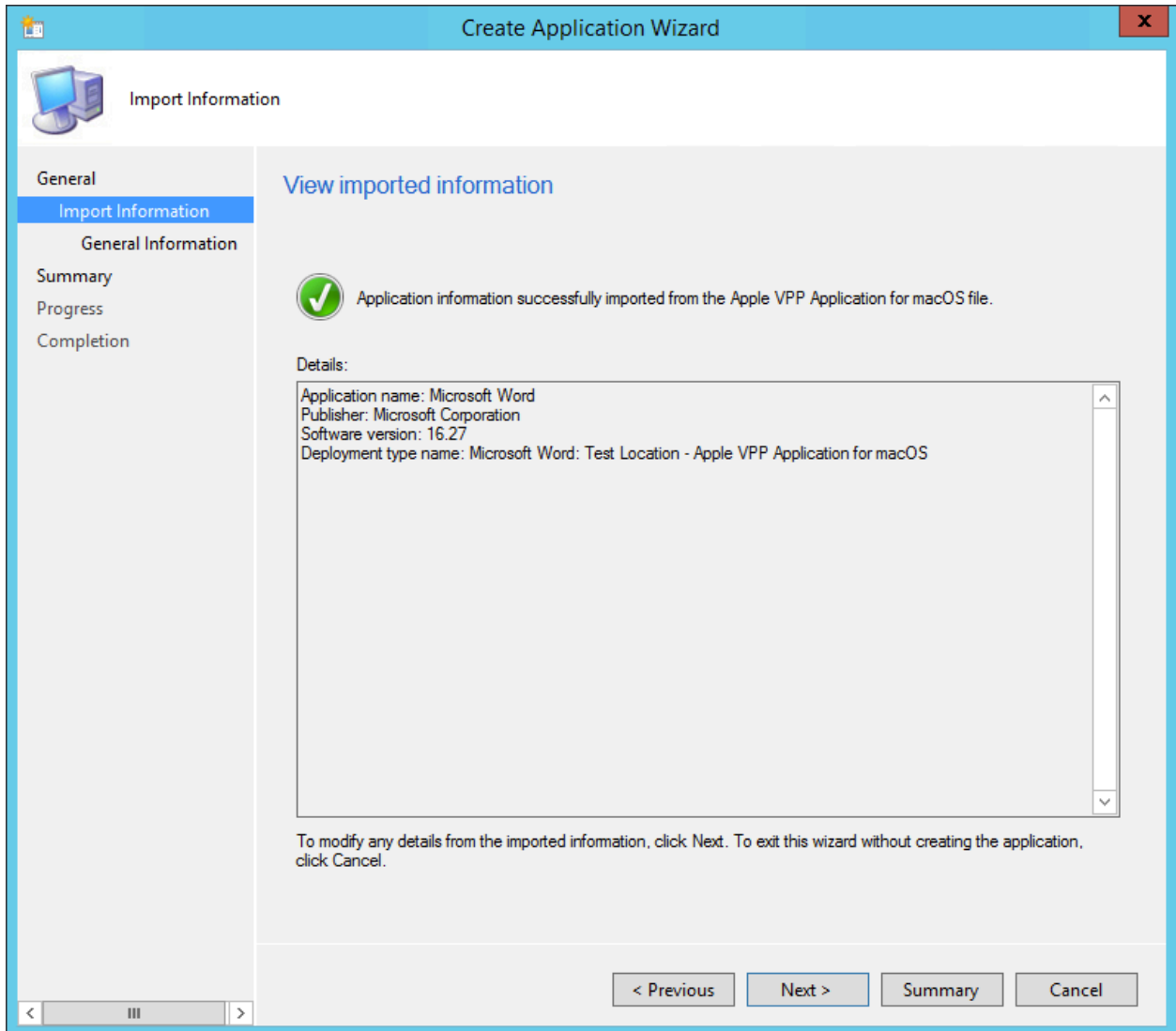


3 On the **General** page, in the **Type** drop-down list, select **Apple VPP Application for macOS** (see the screenshot above).

4 Click the **Browse** button. This opens the **Browse VPP Applications** dialog containing the list of VPP applications for which you have licenses:

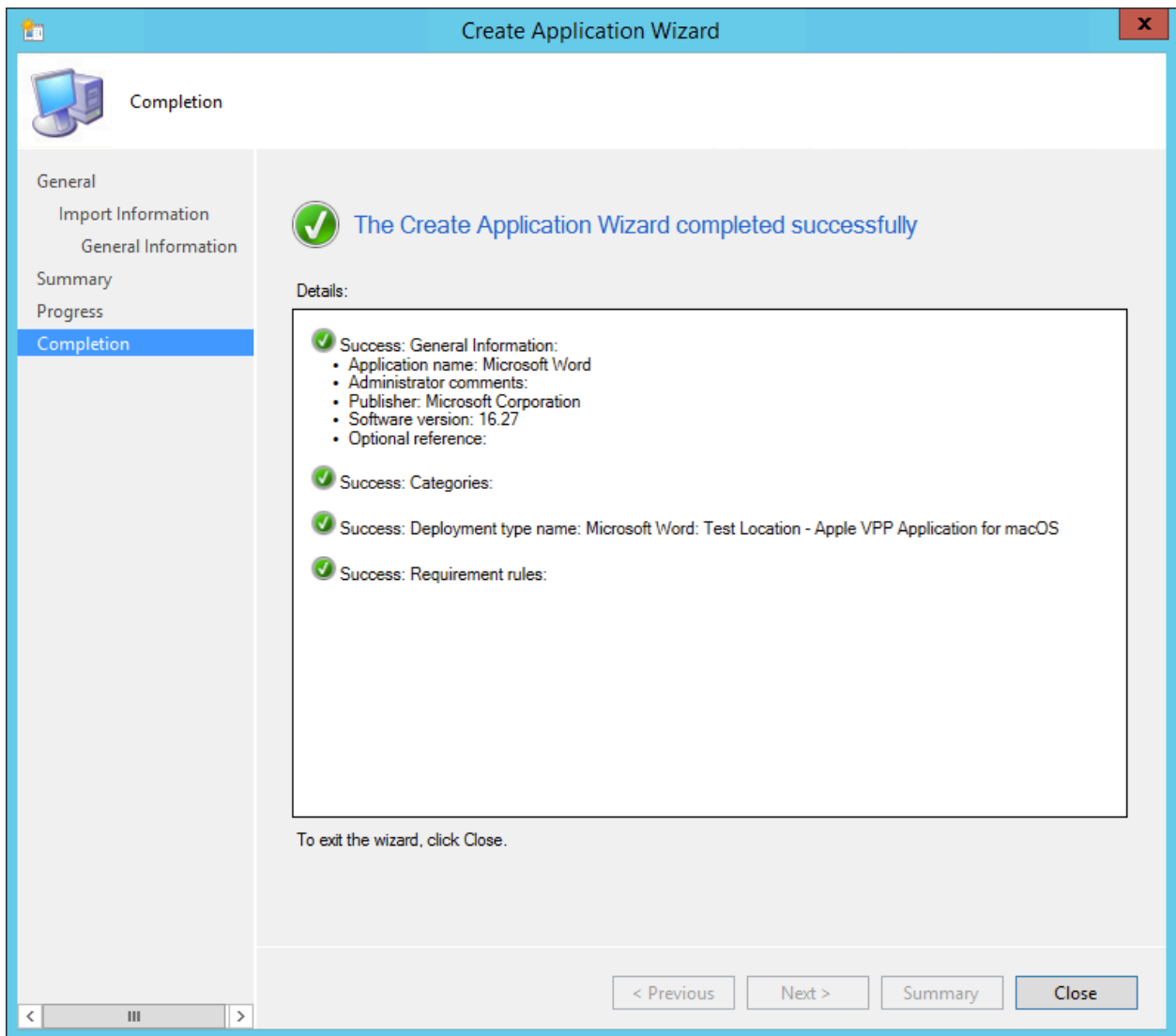


- 5 Select an application and click the **Select** button. The application information will be obtained from VPP data and used in the subsequent wizard pages. The following screenshot shows the **Import Information** page containing the application details that were automatically imported.

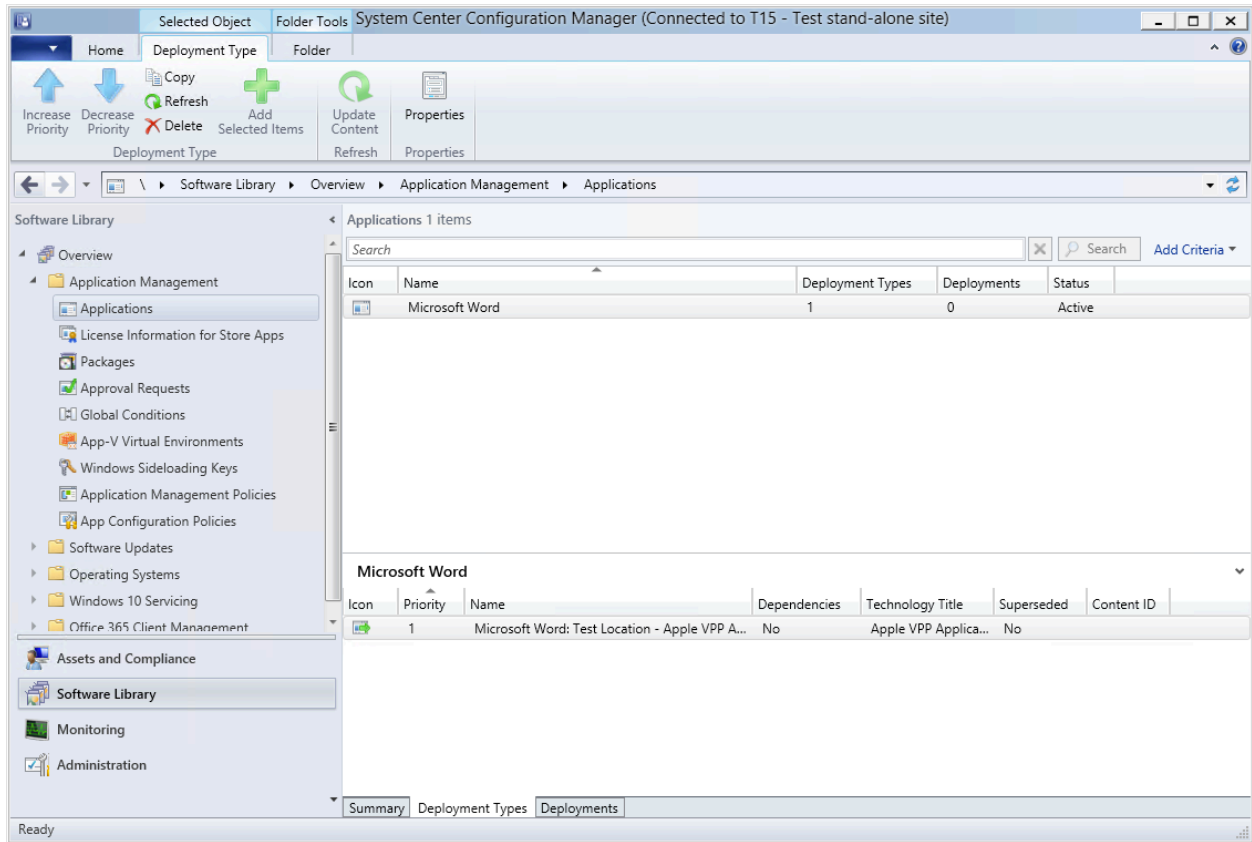


- 6 For the simplest scenario you can keep the imported information and simply click **Next** on every subsequent page.

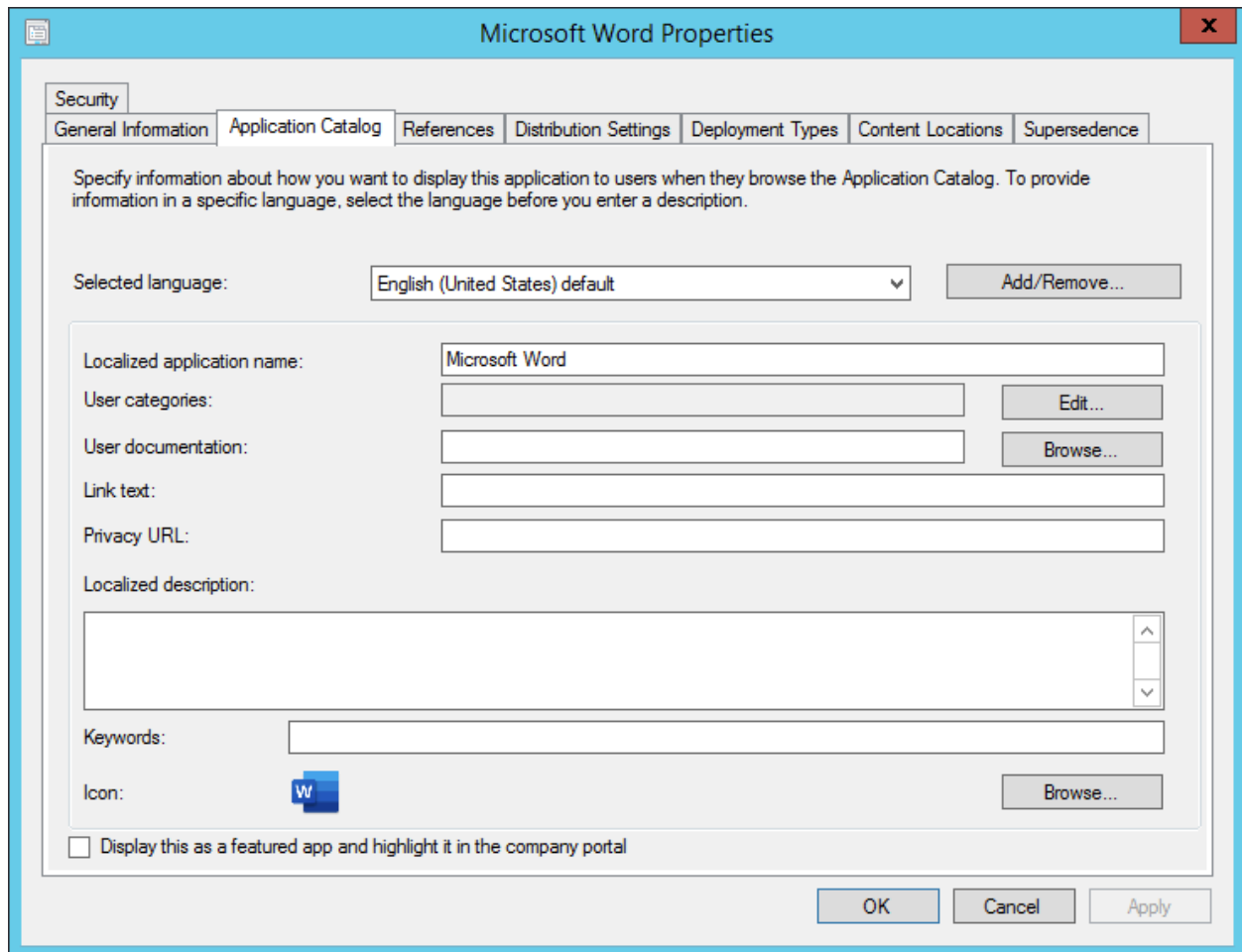
- 7 On the **Completion** page (the last page of the wizard) verify that the application was created successfully and click **Close** to exit the wizard:



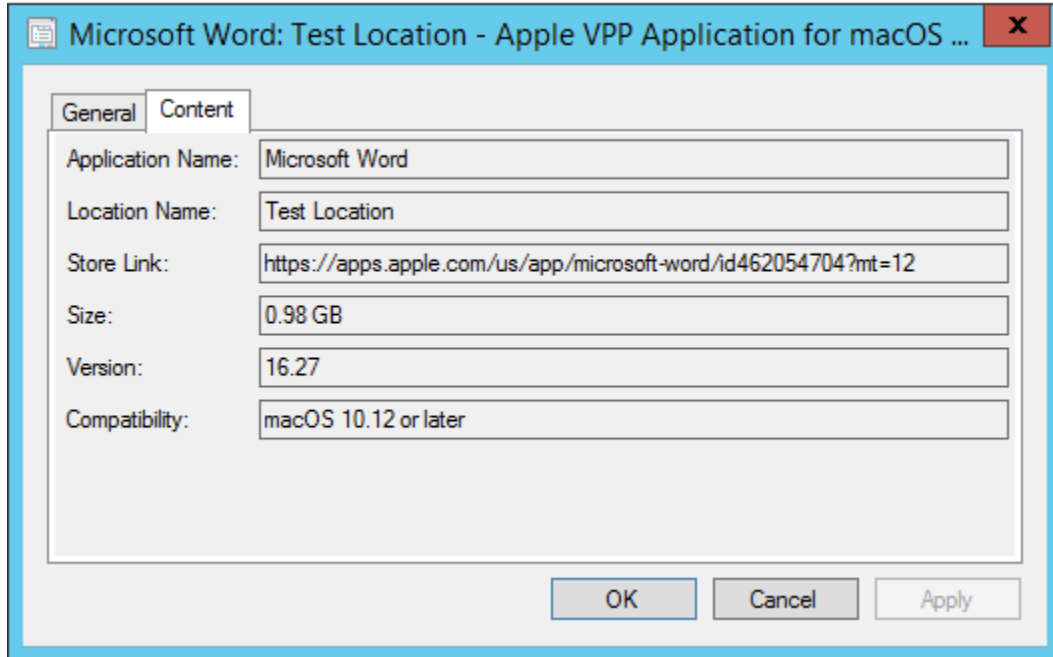
When the wizard is closed, the application that you've just created will be displayed in the Configuration Manager console:



If you view the application properties (right-click > **Properties**), you can see the information that was added to it automatically:



To see more information, go back to the Configuration Manager console and 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:

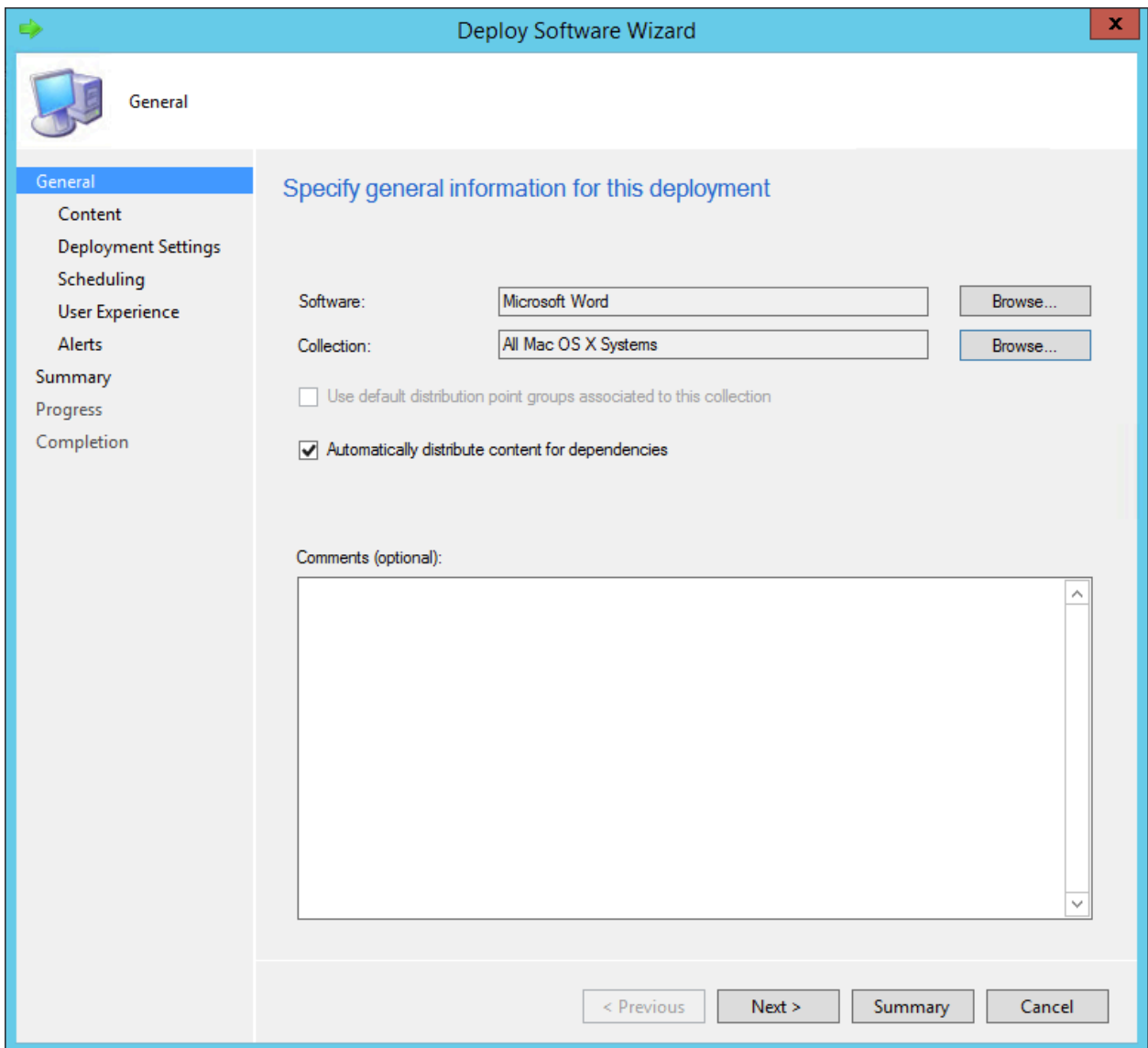


Deploying the Application

After creating an application in SCCM, you need to deploy it. This is done using the regular SCCM deployment procedure, which is described in **Deploying Software via SCCM Application Deployment** (p. 177).

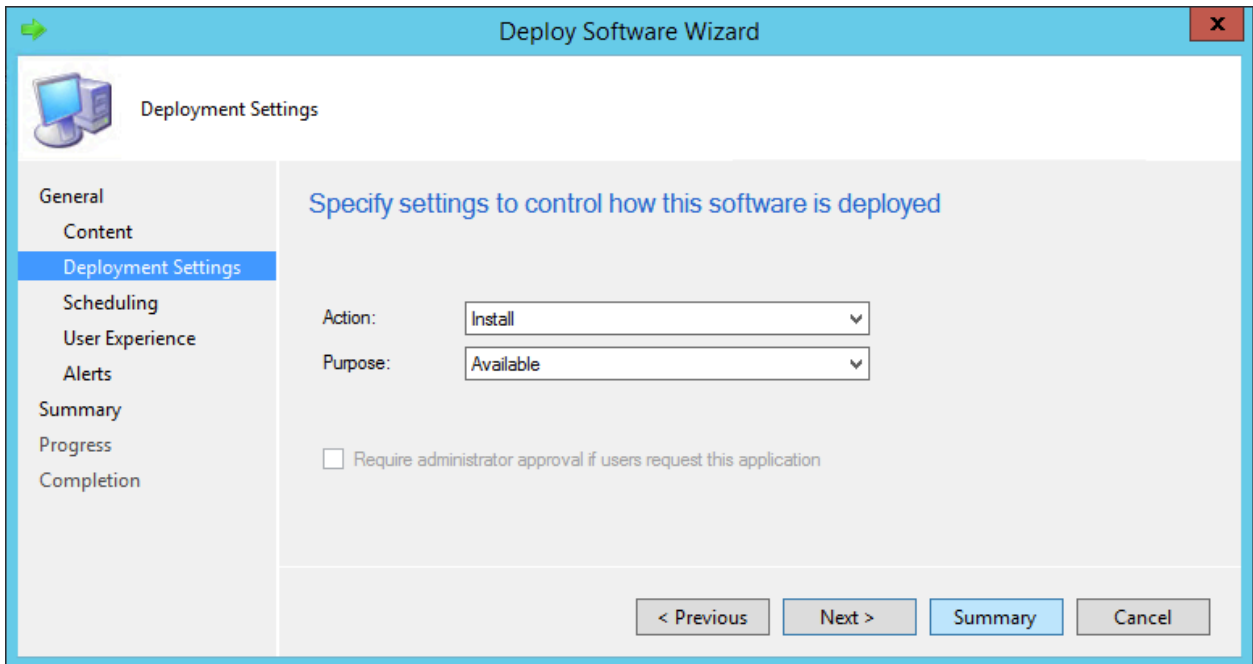
In this demonstration, we will deploy our sample Microsoft Word application:

- 1 In the Configuration Manager console, right-click the application and click **Deploy**. The **Deploy Software Wizard** opens:



- 2 Click **Next**.

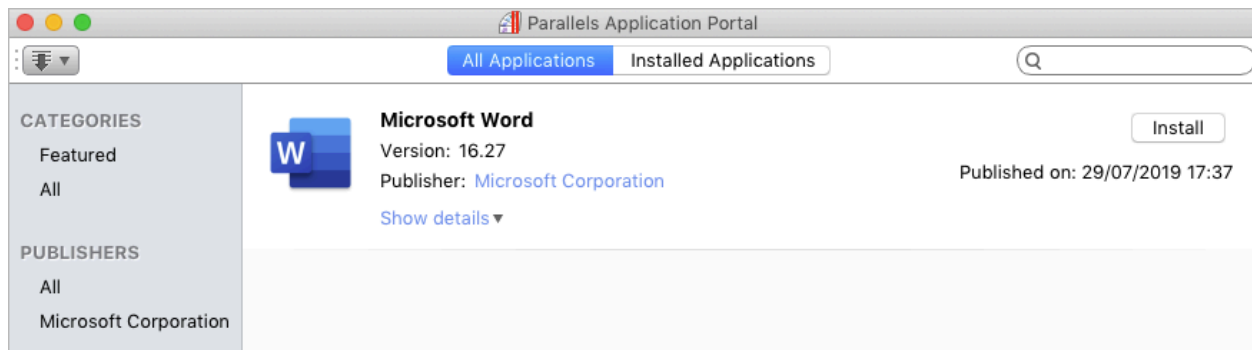
- 3 On the **Deployment Settings** page select "Install" in the **Action** field and select "Available" in the **Purpose** field:



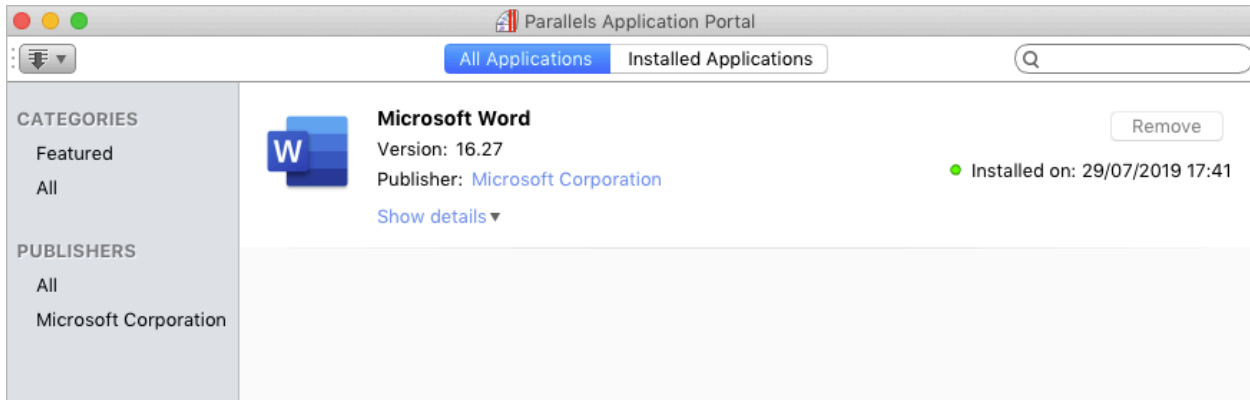
- 4 For the simplest scenario, you can keep default settings on all subsequent pages of the wizard. Simply click **Next** to get to the last page and then close the wizard.

Installing the VPP Application

After the VPP application is deployed in SCCM, it becomes available for installation on managed Mac computers. If you deployed an application as **Available**, it will appear on a Mac computer in Parallels Application Portal according to a schedule:

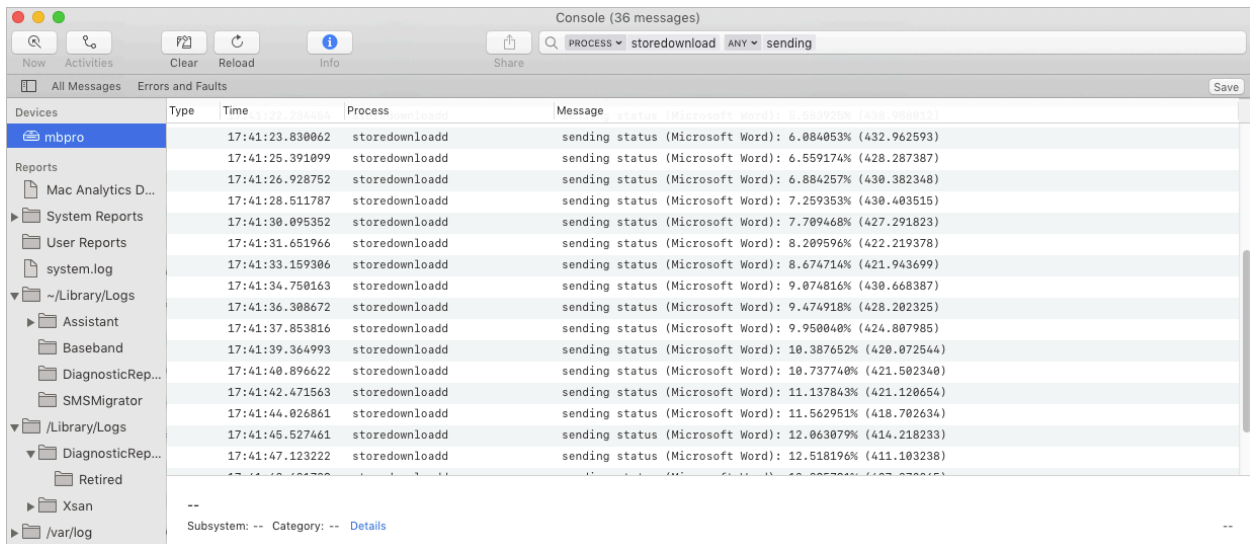


To begin the installation, click the **Install** button. Please note that downloading and installing a large application may take some time. During that time the installation status is displayed in the area below the **Cancel** button, which is what the **Install** button is changed to once you click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



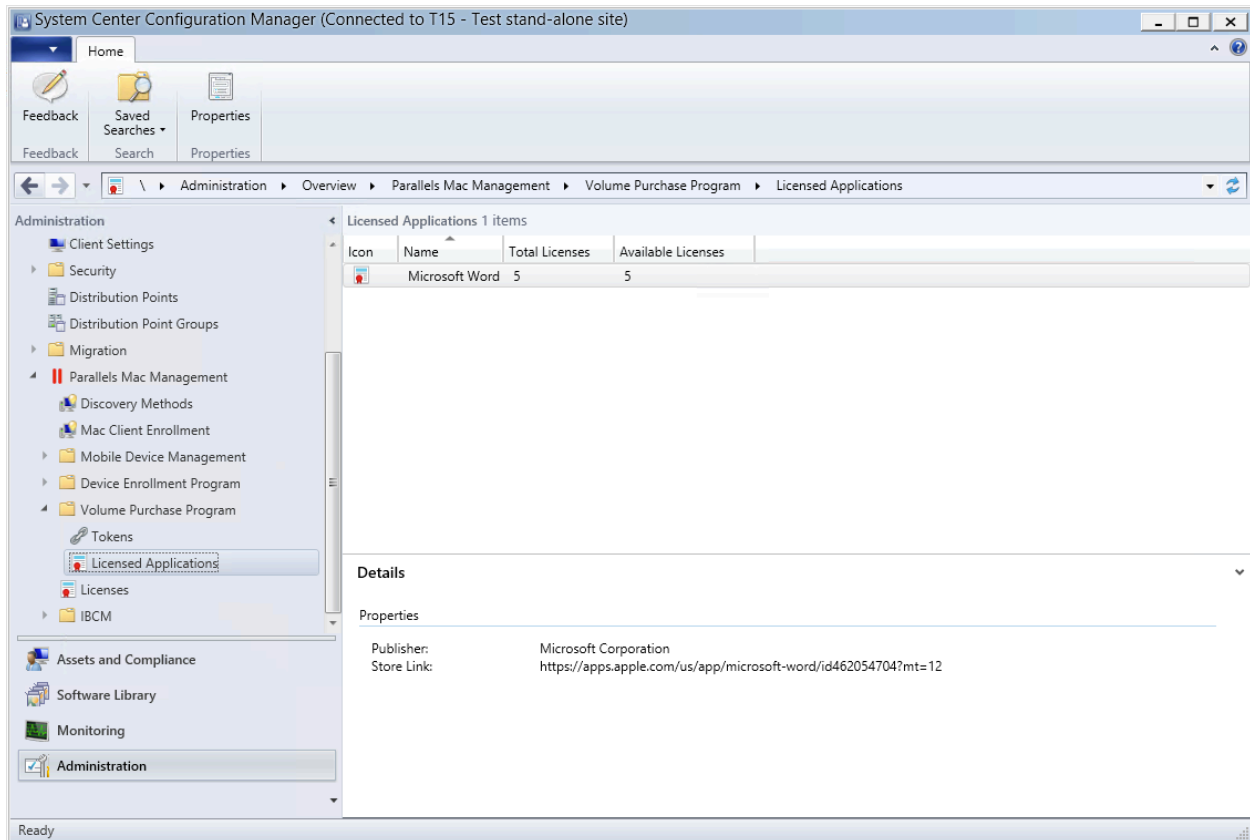
Troubleshooting

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 Search 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 SCCM, the total number of licenses and the number of available licenses are displayed in the Configuration Manager console:



License assignment

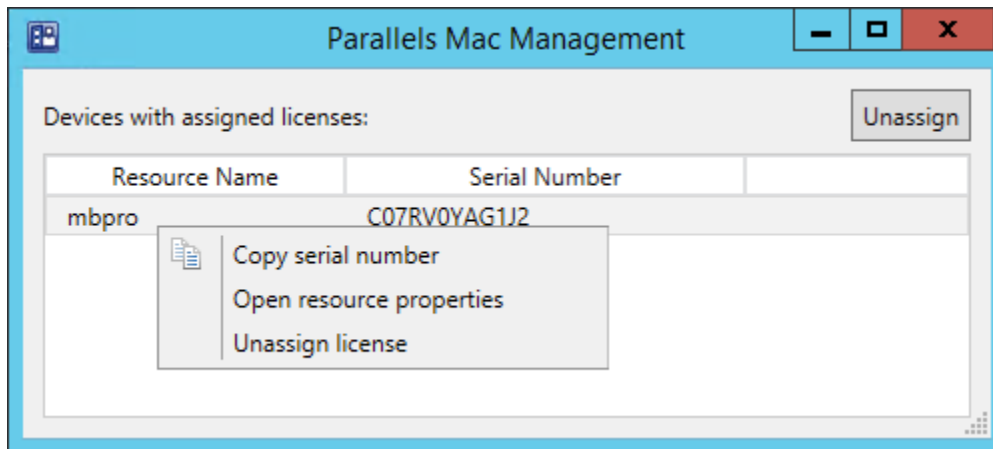
A license is assigned to a particular installation (Mac computer) when you deploy the application and a user initiates the installation. If the deployment was configured as "required" (i.e. silent installation), the license is assigned when the installation begins in the background.

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 Mac computers on which the application is currently installed. Find a computer 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 computers and corresponding resources

As was said above, you can see the list of Mac computers on which a given application is installed by right-clicking the application and choosing **Properties**. If you need to locate an SCCM resource corresponding to a Mac computer, do the same and then right-click a Mac computer and choose **Open resource properties**.



Uninstalling VPP Applications

To uninstall an application that was installed earlier, use the same SCCM 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 SCCM the same way as described earlier in this section (p. 217).
- 2 Deploy the application using the **Deploy Software Wizard (p. 223)**. 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.

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 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)

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 Mac Management provides you with the ability to remotely lock and wipe a device if it's lost or stolen.

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. The following topics describe the installation and configuration procedures:

- **Parallels IBCM/MDM Proxy Requirements** (p. 18)
- **Install Parallels Mac Management** (p. 38)

- **Configuring Parallels IBCM/MDM Proxy** (p. 43)

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 SCCM outside of Apple DEP, you need to enroll them in MDM before you can wipe and lock them. For more information, see **Configure Automatic Mac Enrollment in MDM** (p. 51).

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 SCCM. See **Enrolling Apple Mobile Devices in SCCM** (p. 84).

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 Mac 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 Mac 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 SCCM, 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 Mac 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.

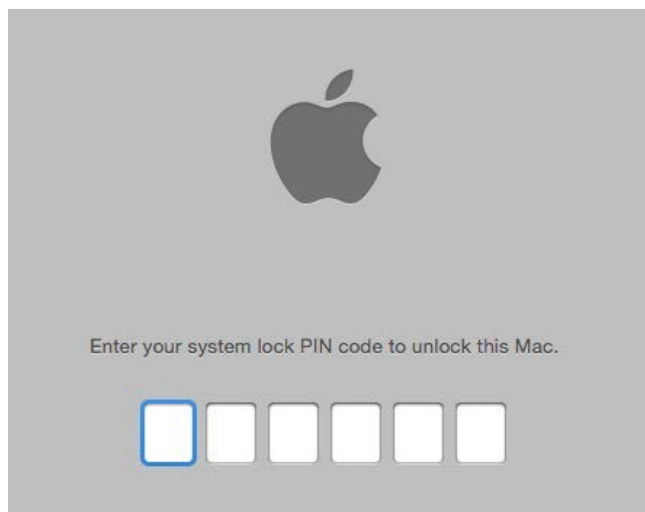
After you cancel the wipe operation, the status in the Mac properties dialog is changed to **Wipe Canceled**.

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 SCCM 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 SCCM 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 Mac Management database (p. 257). Unlock keys are never deleted even for Mac computers that are no longer assigned to an SCCM site.

To retrieve the unlock key:

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

Internet-Based Client Management

Beginning with Parallels Mac Management v7.0, you have the ability to enroll and manage Mac computers that are not connected to the corporate network. It extends the SCCM native Internet-based client management functionality (IBCM) to Mac computers managed with Parallels Mac Management.

To use this functionality, you need Parallels IBCM/MDM Proxy installed and configured for IBCM. For details, please see the following sections:

- **Parallels Mac Management Components Overview** (p. 11)
- **Parallels IBCM/MDM Proxy Requirements** (p. 18)
- **Configuring Parallels IBCM/MDM Proxy** (p. 43)

Enrolling Mac Computers

Internet-based client management (IBCM) allows you to enroll and manage Mac computers in SCCM 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 SCCM and for you to manage them.

To be managed via the Internet, a Mac computer must be enrolled in SCCM 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 SCCM. The differences between the two scenarios are 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 SCCM, 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. For more information, see **Running Parallels Mac Client Installer on a Mac** (p. 71).

Mac computers enrolled in SCCM with Parallels Mac 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 Mac 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 Mac 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 SCCM 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 Mac 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. 188).

Deploying Parallels Desktop on Mac Computers

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 Mac Management for Microsoft SCCM 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 SCCM Package Deployment** (p. 172)). Parallels Desktop deployment adds a few extra steps, which are described below.

Note: The instructions below describe the Mass Deployment feature, which is only supported by Parallels Desktop for Mac Business Edition. Other Parallels Desktop editions do not support it.

Preparing a 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 as described in the **Configuring a Distribution Point** section.

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 Status of a Package** (p. 176) for the information on how to see the package distribution results.

Deploying SCCM Client in Windows Running in a Virtual Machine

If you are using Parallels Desktop for Mac Business Edition in your organization to run Windows on Mac computers, you can manage Windows running in a virtual machine using the native SCCM functionality. In order to do so, you need to install the Configuration Manager client software in a Windows virtual machine as described below.

The native Configuration Manager client software can be deployed to Windows virtual machines using the Parallels Mac Management software distribution feature. The steps are as follows:

- 1** Configure a distribution point.
- 2** Create a software distribution package.
- 3** Create a program.
- 4** Send the package to the distribution point.
- 5** Deploy the software.

The rest of this section describes how to create a software distribution package (step 2 in the list above) and a program containing instructions to install the client software in Windows (step 3). The rest of the steps have no specific requirements and are performed normally.

Prerequisites

Before creating a package, verify that the following requirements are met:

- Windows running in a Parallels virtual machine is a member of the same domain as the Configuration Management site.
- Windows has Parallels Tools installed.

Creating a Software Distribution Package

A software distribution package is a container for an application, file, or information that need to be applied to client computers. In this instance, the package will contain the Configuration Manager client software and a special file containing command-line instructions that you have to create prior to creating a package.

To create a command line file, on the computer running the Configuration Manager console, navigate to the `C:\Program Files (x86)\Microsoft Configuration Manager\Client` directory. The directory should contain the Configuration Manager client software. Create a text file in the directory and name it `install_agent_for_vm.cmd`. Copy and paste the following instructions into the file:

```
ccmsetup /noservice SMSSITECODE=<sitecode> CCMDEBUGLOGGING=1  
CCMENABLELOGGING=TRUE CCMLOGLEVEL=0 SMSDIRECTORYLOOKUP=NOWINS SMSMP=<mp  
hostname>
```

The command line above uses two variables: `<sitecode>` and `<mp hostname>`. Substitute the variables as follows:

- `<sitecode>` — substitute with the Configuration Manager site code.
- `<mp hostname>` — substitute with the management point hostname.

Create a distribution package and a program as described in the **Software Distribution** section. When creating a package, specify the Configuration Manager client agent directory as the source. When specifying the command line for a program, use the following line:

```
:::osname=^Windows.*$!vmname=^.*$!checkversion=%SYSTEMROOT%\CCM\LSInter  
face.dll|4.0.6487.2177!cmdline= install_agent_for_vm.cmd
```

When the package is created, send it to a distribution point and specify the deployment settings. See **Deploying Software via SCCM Package Deployment** (p. 172) for details.

Managing Windows Virtual Machine

After you install the Configuration Manager client agent in a Windows virtual machine, the machine can be managed from the Configuration Manager console. Please note that depending on the networking mode used by the virtual machine, some of the standard SCCM management functions may not work. Please read the explanation below.

A Parallels virtual machine can be configured to operate in one of the following networking modes:

- **Host-only.** This networking mode completely hides the virtual machine from the outside world, so it cannot be managed by the Configuration Manager.
- **Bridged.** This mode makes the virtual machine appear on your local network and the Internet as a standalone computer, so it can be fully managed by the Configuration Manager just like a physical Windows machine.

- **Shared.** A machine that operates in this mode has full network access, but cannot be accessed by other computers on your network. This means that the Configuration Manager features that need to connect to the virtual machine will not work. For example, the Remote Tools feature will not work. However, the SCCM client agent running in a virtual machine can communicate with the Configuration Manager, so features like software distribution, compliance settings, hardware and software inventory will work. In general, if a management task is initiated and performed by the client agent, it will work. If a task is initiated on the Configuration Manager site and then tries to connect to the client agent running in a virtual machine, it will not work.

To set the networking mode for a Parallels virtual machine, open the virtual machine in Parallels Desktop, select **Virtual Machine** in the Parallels Desktop menu, and click **Configure**. In the virtual machine configuration dialog, click the **Hardware** tab and then select **Network 1** (or the network adapter of interest) in the list. Use the **Type** drop-down list box to set the network type.

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 Mac 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 Mac Management for SCCM 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.

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 Mac Management problem reporting tools and utilities.

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 Mac Management for Microsoft SCCM** 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 Mac 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. 243). 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

A reporting utility is installed on a Mac computer during the Parallels Mac Client installation. To run the utility, open **System Preferences** and then click **Parallels Management** (if your **System Preferences** are organized by categories, it is located in the **Other** category). For more information about using the utility, see **Sending Parallels Mac Client Problem Report** (p. 82).

Using Problem Monitoring Utility

Parallels Mac Management for Microsoft SCCM provides a utility that allows you to monitor the system in real time for possible problems. The utility is installed together with Parallels Mac 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 Mac 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 Mac 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 close 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 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.

Initiating Policy Retrieval from SCCM

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 done from an individual Mac computer as described in the **Initiating Policy Retrieval from a Mac** section (p. 81). The functionality described here allows you to initiate policy retrieval for multiple Mac computers from the Configuration Manager console.

To initiate policy retrieval from the Configuration Manager console:

- 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.

Appendices

In This Chapter

Port Reference	248
Logging	251
Changing Log File Rotation Limits	254
Enforcing TLS 1.2.....	256
Parallels Mac Management Database.....	257

Port Reference

This section describes communication ports used by Parallels Mac Management for Microsoft SCCM. Please note that these ports should not be used by other programs. Please also note that the tables don't include ports used by the standard System Center Configuration Manager services and standard Windows services.

Note: *TCP Dynamic* or *UDP Dynamic* means that every time a service starts, it identifies an available port and uses that port number.

Parallels Configuration Manager Proxy (inbound ports)

Process Name	Port	Description
pma_isv_proxy_service.exe	TCP 8760	HTTPS connections from Managed Mac computers and ConfigMgr Console Extensions. NOTE: Can be customized using the Configuration Manager Proxy configuration utility.
	TCP 8761	HTTP requests to download client packages. NOTE: Can be customized using the Configuration Manager Proxy configuration utility.
pmm_dep_service.exe	TCP Dynamic	HTTPS connections from the Parallels ConfigMgr Console Extensions.
pmm_mdm_service.exe	TCP Dynamic	HTTPS connections from the Parallels ConfigMgr Console Extensions.
pmm_vpp_service.exe	TCP Dynamic	HTTPS connections from the Parallels ConfigMgr Console Extensions.

Parallels Configuration Manager Proxy (outbound ports)

Process Name	Port	Description
pma_isv_proxy_service.exe	TCP 443	HTTPS connections to the Parallels License Server.
	TCP 1433	Connections to the SQL Server database.
pmm_dep_service.exe	TCP 443	HTTPS connections to the Apple DEP service.
	TCP 1433	Connections to the SQL Server database.
pmm_mdm_service.exe	TCP 443 or 2197	TLS connections to the Apple Push Notification service. For details about changing the default port 443 to 2197, please see: - PMM Admin Guide: MDM Proxy Specifics (p. 21) - PMM Deployment Guide: Deploying MDM Proxy
	TCP 1433	Connections to the SQL Server database.
pmm_vpp_service.exe	TCP 443	HTTPS connections to the Apple VPP service.
	TCP 1433	Connections to the SQL Server database.
pmm_mdm_policy_service.exe	TCP 1433	Connections to the SQL Server database.

Note: Port used to communicate with the SQL Server can be configured by the administrator.

Parallels NetBoot Server (inbound ports)

Process Name	Port	Description
IIS Service	TCP 80	HTTP communication.
DHCP/WDS Service	UDP 67	DHCP communication.
WDS Service	UDP 69	TFTP communication.

Parallels NetBoot Server (outbound ports)

Process Name	Port	Description
pma_netboot_service.exe	UDP 68	Boot Service Discovery Protocol (BSDP) communication.
	UDP Dynamic	BSDP communication. Port is selected by the BSDP client.

Parallels OS X Software Update Server (inbound ports)

Process Name	Port	Description
pmm_sup_service.exe	TCP Dynamic	HTTPS connections from Managed Mac computers

Parallels OS X Software Update Server (outbound ports)

Process Name	Port	Description
pmm_sup_service.exe	TCP 8760	Communication with the Parallels Configuration Manager Proxy service.

Parallels IBCM/MDM Proxy (inbound ports)

Process Name	Port	Description
w3wp.exe (IIS Worker Process)	TCP 8762	TLS connections from the Parallels Configuration Manager Proxy service and Parallels MDM service. NOTE: Can be customized using the IBCM/MDM Proxy configuration utility.

Managed Mac computer (inbound ports)

Process Name	Port	Description
pma_agent	TCP 8000	HTTPS connections from the Parallels Configuration Manager Proxy service.
SSH server	TCP 22	Used by Network Discovery and Execute Script.
VNC server	TCP 5900	Needed to accept VNC connections on a Mac computer.

Managed Mac computer (outbound ports)

Process Name	Port	Description
pma_agent	TCP 8760	Communication with the Parallels Configuration Manager Proxy service.
	TCP 5223	5223 Communication with the Apple Push Notification service.
pma_agent_ui	TCP 8760	Communication with the Parallels Configuration Manager Proxy service.

Parallels ConfigMgr Console Extensions (outbound ports)

Process Name	Port	Description
Microsoft.ConfigurationManagement.exe	8760	Communication with the Parallels Configuration Manager Proxy service.
	TCP Dynamic	Communication with the Parallels DEP service, Parallels MDM service, Parallels VPP service.

Logging

Parallels Mac Management maintains its own log files which capture information about its processes. The log files are created and maintained for each component including Parallels Configuration Manager Proxy, Configuration Manager Console Extension, and clients running on individual Mac computers. Some information about Parallels Mac Management processes is also recorded in the System Center Configuration Manager log files. You can use the information contained in the log files to help you troubleshoot issues that might occur in the Parallels Mac Management for Microsoft SCCM.

Parallels Mac Management for Microsoft SCCM Log Files

The Parallels Mac Management log files are located in the following directories:

- Windows computer running Parallels Configuration Manager Proxy: %windir%\Logs ; %windir%\Logs\pmm
- Windows computer running Parallels OS X Software Update Point: %windir%\Logs\pmm
- Windows computer running Configuration Manager console: %windir%\Logs
- macOS (Parallels Mac Client): /Library/Logs/

The following table describes the Parallels Mac Management for Microsoft SCCM log files:

Component	Log File Name	Log File Description
Parallels Configuration Manager Proxy	pma_setup.log	This log file is created during the SCCM Proxy installation. It contains information about the installation procedures and the changes they make to the system. Please note that when the SCCM Proxy and the SCCM Console Extension components are installed on the same computer, the pma_setup.log is shared between them.
	pma_isv_proxy_config.log	This log file is created and updated every time the SCCM Proxy configuration utility is run. It contains information about the configuration parameters selected by the user (SMS Provider, service account name, etc.) and the results of the configuration operations.
	pma_isv_proxy_service.log	This is the main SCCM Proxy log file. It is updated as needed while the SCCM Proxy service is running. It contains information related to the SCCM Proxy operations such as starting/stopping the service, reading various system properties, starting or stopping Mac management utilities and others.

	pma_discovery.log	This log file is updated every time the Parallels Network Discovery runs. It contains information about the discovery itself (processes started, subnets searched, etc) and the information about discovered Mac computers, including IP address, hostname, MAC address, whether the Client installation was initiated on a Mac, and other info.
	pmm_cep_master_service.log	This log file belongs to the Parallels Customer Experience Program module. The log is updated when the corresponding service collects information and generates reports about the system.
Parallels OS X Software Update Point	pmm_sup_service.log	This log file belong to the Parallels OS X Software Update Point component. it is updated when the corresponding service performs any of its operations.
SCCM Console Extension	pma_setup.log	The SCCM Console Extension component has just one log file: pma_setup.log. The file contains information about the component installation procedure. Please note that when the SCCM Proxy and the SCCM Console Extension components are installed on the same computer, the pma_setup.log is shared between them.
Parallels Mac Client	pma_agent.log	This is the main client software log file, which contains information about the client operations. The file is updated when the Mac Client communicates with SCCM Proxy and/or performs actions on the Mac computer on which it is running.
	pma_agent_ui.log	This log file is updated when the client installation and registration utilities are run on the Mac by a user. The file also records information when an operation is performed on the Mac that is user-specific. An example of such an operation is applying a Mac configuration profile (a profile is applied for each individual Mac user if more than one user exists). Please note that if a Mac user doesn't have privileges to write to the /Library/Logs directory, the log file will be created in the /Users/<user_name>/Library/Logs directory.
	pma_agent_uninstaller.log	This log file is created when the client is uninstalled from the Mac computer.

System Center Configuration Manager Log Files

Some of the Parallels Mac Management process information is recorded in the SCCM log files. You may examine these files in addition to the log files described above. Please note that SCCM creates these files on the fly and not all of them may actually exist.

The following table describes the Site Server log files which are located in the <SCCM_InstallationPath>\LOGS folder. The files may contain information about the SCCM Proxy component.

Log file	Log file description
Colleval.log	Records activities when collections are created, changed, and deleted by the Collection Evaluator.
Datadr.log	Processes Management Information Format (MIF) files and hardware inventory in the Configuration Manager database.
Ddm.log	Saves DDR information to the Configuration Manager database by the Discovery Data Manager.
Distmgr.log	Records package creation, compression, delta replication, and information updates.
Offermgr.log	Records advertisement updates.
Offersum.log	Records summarization of advertisement status messages.
Polycpv.log	Records updates to the client policies to reflect changes to client settings or advertisements.
Smsprov.log	Records WMI provider access to the site database.
statesys.log	Records the processing of state system messages.

The following table describes the Management Point log files, which are located in the %ProgramFiles%\SMS_CCM\LogS folder. The files may contain information about the SCCM Proxy component.

Log file	Log file description
MP_CliReg.log	Records the client registration activity processed by the management point.
MP_Ddr.log	Records the conversion of XML.ddr records from clients, and copies them to the site server.
MP_Framework.log	Records the activities of the core management point and client framework components.
MP_GetAuth.log	Records the status of the site management points.
MP_GetPolicy.log	Records policy information.
MP_Hinv.log	Converts XML hardware inventory records from clients and copies the files to the site server.
MP_Location.log	Records location manager tasks.
MP_OOBMgr.log	Records the management point activities related to receiving OTP form a client.
MP_Policy.log	Records policy communication.

MP_Relay.log	Copies files that are collected from the client.
MP_Retry.log	Records the hardware inventory retry processes.
MP_Sinv.log	Converts XML software inventory records from clients and copies them to the site server.
MP_SinvCollFile.log	Records details about file collection.
MP_Status.log	Converts XML.svf status message files from clients and copies them to the site server.

The following table describes the Admin UI log files, which are located in the <SCCM_InstallationPath>\AdminUI\AdminUILog directory. The files may contain information about the Configuration Manager Console Extension component.

Log file	Log file description
ResourceExplorer.log	Records errors, warnings, and information about running the Resource Explorer.
SMSAdminUI.log	Records the local Configuration Manager console tasks when you connect to the Configuration Manager site.

Parallels Mac Management for Microsoft SCCM Crash Dumps

In addition to log files, crash dumps may be generated if a Parallels Mac Management component terminates abnormally. The crash dumps are generated for the Configuration Manager Proxy component and for Parallels Mac Clients running on individual Macs. Please note that crash dumps may not be created every time a component crashes. If a dump doesn't exist in the directories specified below, it can be found in the problem report, which will be generated instead.

The crash dump file locations are:

- Parallels Configuration Manager Proxy:
%ALLUSERSPROFILE%\Microsoft\Windows\WER\ReportQueue\AppCrash_pma_isv_proxy_*, where AppCrash_pma_isv_proxy_* is the name of a directory containing the crash dump files (the name is appended with a unique suffix for each dump).
- Parallels Mac Client: /Library/Logs/CrashReporter/pma_agent*.crash, where pma_agent*.crash is the name of the directory containing the files (the asterisk character is substituted with a unique dump identifier).

Changing Log File Rotation Limits

About Log File Rotation

Parallels Mac Management for Microsoft SCCM implements log file rotation that ensures that the log files don't grow in size indefinitely. The amount of data contained in an individual log file and the total size of all logs are kept at a reasonable limit. Log file rotation is enabled by default.

Parallels Mac Management for Microsoft SCCM consists of a number of executables including services, graphical user interface, and utilities. Each executable creates its own log file named <exec_name.log>, where "exec_name" is the executable file name. The following table lists Parallels Mac Management executables and their corresponding log file names and locations:

Executable Name	Operating System	Log File Name and Path
pma_isv_proxy_service	Windows	%Windir%\Logs\pma_isv_proxy_service.log
pma_isv_proxy_config	Windows	%Windir%\Logs\pma_isv_proxy_config.log
pma_discovery	Windows	%Windir%\Logs\pma_discovery.log
pmm_cep_master_service	Windows	%Windir%\Logs\pmm\pmm_cep_master_service.log
pmm_sup_service	Windows	%Windir%\Logs\pmm\pmm_sup_service.log
pma_problem_monitor	Windows	%Windir%\Logs\pma_problem_monitor.log
pma_report_tool	Windows	%Windir%\Logs\pma_report_tool.log
	macOS	/Users/<user_name>/Library/Logs
pma_agent	macOS	/Library/Logs/pma_agent.log
pma_agent_ui	macOS	/Library/Logs/pma_agent_ui.log

A log file is populated with data when an executable is running and performing its tasks. When the size of a log file exceeds a predefined limit, the file is archived and a new empty log file is created in its place. This creates a log file rotation set consisting of the current log file and archived files. A log file rotation set is managed using the following rules:

- Log files are archived using the zlib compression library.
- The archived files in the set are named as follows:
<exec_name.1.log.gz>, <exec_name.2.log.gz>, <exec_name.3.log.gz>, etc.

The <exec_name.1.log.gz> file is the most recently archived log segment. The file with the largest sequential number in its name is the oldest. When the current log file is archived, it is named <exec_name.1.log.gz>. The existing archives are renamed by incrementing the sequential number in their names by 1. The maximum number of files in a rotation set can be configured (see **Changing Log File Rotation Limits** below). When the number of files exceeds the predefined limit, the oldest file is deleted.

- Rotation of each log is performed independently from other logs.

Changing Log File Rotation Limits

Log file rotation limits are configured similarly on both Windows and macOS computers. The following rules apply when specifying the limits:

- **Log file size limit.** The default value is 1 MB (specified in bytes). The minimum allowed value is 200 KB. The maximum allowed value is 4 MB. If a value is not set, the default value is used. If the specified value falls outside the min/max interval, the minimum or the maximum value is used respectively.

- **Maximum number of files in a rotation set.** The default value is 10. The minimum value is 1. The maximum value is 20. If a value is not set, the default value is used. If the specified value falls outside the min/max interval, the minimum or the maximum value is used respectively.

On Windows computers the log rotation limits are stored in the system registry. To modify the limits:

- Run "regedit" and search for HKEY_LOCAL_MACHINE\SOFTWARE\Parallels\Parallels Management Suite for Microsoft SCCM\Preferences.
- To set the log file size limit, modify the value of the "LogFileSizeLimit" parameter. The size is specified in bytes.
- To set the maximum number of files in a rotation set, modify the value of the "MaxNumberOfSavedLogs" parameter.

On macOS computers, the log rotation limits are stored in the `/Library/Preferences/com.parallels.pma.agent.plist` file. To modify the limits:

- Open the `com.parallels.pma.agent.plist` file in a text editor.
- To set the log file size limit, modify the value of the "LogFileSizeLimit" parameter. The size is specified in bytes.
- To set the maximum number of files in a rotation set, modify the value of the "MaxNumberOfSavedLogs" parameter.

Enforcing TLS 1.2

Parallels Mac Management uses the TLS 1.2 protocol by default for incoming connections in Parallels Mac Client. An IT administrator has the ability to change the minimum allowed TLS version by setting a registry key on a host where the following services are running:

- IBCM/MDM Proxy
- PMM Proxy

The registry key used to set the TLS version is defined as follows:

- **Path:** HKLM\SOFTWARE\WOW6432Node\Parallels\Parallels Mac Management for Microsoft SCCM\Common\SSL
- **Key:** ProtocolVersion, type: REG_SZ
- **Possible key values** (adopted QSsl::SslProtocol enumeration) are as follows:

Key value	TLS version(s)
TlsV1_0	TLS v1.0
TlsV1_0OrLater (Used by default)	TLS v1.0 and later versions
TlsV1_1	TLS v1.1
TlsV1_1OrLater	TLS v1.1 and later versions

TlsV1_2	TLS v1.2
TlsV1_2OrLater	TLS v1.2 and later versions

Notes

To test a server endpoint for a specific protocol version support, the OpenSSL for Windows tool can be used. The command line is as follows:

```
openssl s_client -<protocol-version> <host-name>:<port-number>
```

Example:

```
openssl s_client -tls1_2 win2016-001.pmm16.dom:8760
```

If the server supports the specified protocol version, then the output will include a fragment similar to the following:

```
SSL handshake has read 1246 bytes and written 362 bytes
New, TLSv1.2, Cypher is ECDHE-RSA-AES256-GCM-SHA384
Secure Renegotiation IS supported
...
```

If the server doesn't support the specified protocol version, the output look similar to this:

```
SSL handshake has read 0 bytes and written 134 bytes
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
...
```

Parallels Mac Management Database

When Parallels Mac Management for Microsoft SCCM is installed, it creates its own SQL Server database on the primary SCCM site to store security data such as recovery keys, certificates, and other.

The database name is constructed using the following syntax:

```
PMM_<site_name>
```

Where, PMM_ is used as-is and <site_name> is the name of the primary SCCM site.

At the time of this writing, the database is used to store the FileVault 2 disk encryption information, recovery keys, and Mac unlock keys. Other security related data may be stored in the database in the future.

The system administrator should backup the database regularly in order to ensure data safety.

Index

A

A Note about Software Updates - 235
About This Guide - 10
Add the macOS Boot Image to Configuration Manager - 142
Adding an Application to Apple Business Manager - 214
Adding or Removing Parallels Mac Management Components - 56
Administrative Rights in Authorization Manager - 28
Administrative Rights in SCCM - 25
Appendices - 248
Apple Mobile Device Collection - 96
Apply Configuration Profile - 157
Assign an Enrollment Profile to Mac Computers - 209
Automatic Upgrade of Parallels Mac Client - 78

B

Boot a Reference Mac From a Different Partition - 147

C

Capture a macOS Boot Image - 141
Capture a macOS Image - 147
Capture a macOS System Image - 147
Capturing a macOS Boot Image - 141
Capturing a macOS Image Using a Task Sequence - 145
Capturing a macOS Image Using the Image Builder Utility - 147
Capturing a macOS System Image - 145
Changing Log File Rotation Limits - 254
Choose the Installation Type - 177
Compliance Settings - 105
Conclusion - 45, 54
Configuration Manager Admin Console - 94
Configuration Manager Boundaries - 32

Configuration Manager Boundaries Configuration - 17
Configuration Options - 188
Configure Automatic Mac Enrollment in MDM - 51
Configure Synchronization of SCCM with WSUS - 198
Configure the Deployment Type - 180
Configuring Apple VPP Support - 210
Configuring Maintenance Windows - 202
Configuring Parallels Configuration Manager Proxy - 39
Configuring Parallels IBCM Proxy - 44
Configuring Parallels IBCM/MDM Proxy - 43
Configuring Parallels Mac Client Push Installation Properties - 67
Configuring Parallels MDM Proxy - 45
Configuring Parallels NetBoot Server - 54
Configuring Parallels Network Discovery - 68
Configuring Parallels OS X Software Update Point - 55, 196
Configuring SCCM and Deploying macOS Updates - 197
Configuring the macOS Firewall - 76
Create a Configuration Manager Application - 179
Create a Device Enrollment Profile - 206
Create a Domain User - 24, 30
Create a Task Sequence for Capturing a macOS System Image - 145
Creating a Bootable USB Drive - 144
Creating a Configuration Item - 134
Creating a Discovery Script - 136
Creating a macOS Configuration Profile - 106
Creating a Non-OSD Task Sequence - 170
Creating a Remediation Script - 136
Creating a Security Group - 36
Creating a Software Package - 172
Creating a Task Sequence - 150
Creating an Apple Mobile Device Configuration Profile - 114

Creating an Application - 217
Creating Certificate Templates for Parallels
 ConfigMgr Proxy and Mac Computers - 34
Creating Compliance Rules - 137
Creating FileVault 2 Configuration Item - 116,
 123
Creating FileVaultMaster Keychain - 116

D

Date and Time Synchronization - 17
DCOM Remote Activation Permission - 24,
 31
Deactivating Parallels Mac Management - 63
De-enroll an Apple Mobile Device - 87
Deploy Mac Computers - 208, 209
Deploy the Application - 182
Deploy Updates to Mac Computers - 201
Deploying a Non-OSD Task Sequence - 171
Deploying a Task Sequence to a Collection -
 166
Deploying Configuration Baseline - 138
Deploying macOS and Executing Task
 Sequences - 140
Deploying Parallels Desktop on Mac
 Computers - 235
Deploying SCCM Client in Windows Running
 in a Virtual Machine - 238
Deploying Software via SCCM Application
 Deployment - 177
Deploying Software via SCCM Package
 Deployment - 172
Deploying the Application - 223
Deploying the Software - 176
Device Collections in Parallels Mac
 Management - 95
Distribute Content of the macOS Boot Image
 - 143
Distributing the macOS System Image in
 SCCM - 148
Distribution Point Role Configuration - 16
Download Updates From a Local Server -
 189
Download Updates From Apple's Servers -
 188

E

Enable Parallels MDM - 204

Enabling Remote Access on Mac Computers
 - 66
Encrypting a Mac with FileVault 2 - 119, 127
Enforcing FileVault 2 Encryption - 115
Enforcing Parallels Desktop Preferences -
 130
Enforcing Parallels Desktop VM Settings -
 132
Enforcing TLS 1.2 - 256
Enrolling Apple Mobile Devices in SCCM - 84
Enrolling Mac Computers - 234
Enrolling Mac Computers via Apple DEP -
 204
Establish a Connection to the Apple DEP
 Web Service - 204
Exceeding the License Limit - 62
Execute Script - 160
Executing Scripts on Mac Computers - 203
Executing Task Sequence Steps - 168
Extending Hardware Inventory for Mac
 Computers - 97

F

FileVault 2 Encryption with Institutional
 Recovery Key - 115
FileVault 2 Encryption with Personal Recovery
 Key - 123
Format and Partition Disk - 152

G

General Requirements - 15

H

Handling Expired Certificates - 36
Hardware and Software Inventory - 96

I

IBCM/MDM Proxy Architecture - 19
IIS Settings on the Distribution Point Server -
 16
Import macOS Software Updates - 197
Importing a Profile from a File - 112
Initiating Policy Retrieval - 81
Initiating Policy Retrieval from SCCM - 246
Initiating Task Sequence Execution by a User
 - 172
Install Application - 154
Install Package - 156

- Install Parallels Mac Management - 38
- Installation and Configuration - 38
- Installation Location - 16
- Installation Options Overview - 65
- Installation Overview - 38
- Installation Requirements - 15
- Installing Parallels Mac Client Using a Script - 73
- Installing Parallels Mac Client Using Discovery Methods - 66
- Installing the Application on a Mac - 183
- Installing the VPP Application - 225
- Integrating Parallels Mac Management with PKI - 33
- Internet-Based Client Management - 233
- Introduction - 9

J

- Join Domain - 153

K

- Kernel Extensions - 159

L

- License Activation - 58
- License Activation Overview - 58
- Limitations and Known Issues - 201
- Local Administrator Rights - 24, 30
- Lock an Apple Mobile Device - 232
- Logging - 251

M

- Mac Computer Collections - 95
- macOS Software Update Management - 188
- Managing Apple Mobile Devices - 88
- Managing Assigned Licenses - 227
- Manually Upgrading Parallels Mac Client - 79
- MDM Management Scope - 86
- MDM Proxy Specifics - 21
- Microsoft SQL Server Permissions - 27
- Migrating Mac Computers to a New Site - 91
- Migrating Parallels ConfigMgr Proxy to a New Server - 89
- Mobile Device License Management - 87
- Mobile Device Resources in SCCM - 86
- Modifying a Task Sequence - 151

N

- Network Configuration - 17
- Non-Operating System Deployments - 170

O

- Obtain a CSR from Parallels automatically - 48
- Offline Activation - 59
- Online Activation - 59

P

- Parallels ConfigMgr Proxy and Site Migration - 89
- Parallels Configuration Manager Proxy Requirements - 16
- Parallels IBCM/MDM Proxy Requirements - 18
- Parallels Mac Client Deployment - 65
- Parallels Mac Management Component Overview - 11
- Parallels Mac Management Database - 257
- Parallels Mac Management Features Overview - 9
- Parallels NetBoot Server Requirements - 22
- Parallels OS X Software Update Point Requirements - 22
- Permissions for Running Parallels ConfigMgr Proxy Configuration Wizard - 24
- Permissions for Running Parallels ConfigMgr Proxy Service - 28
- Permissions for Running Parallels Netboot Service - 30
- Permissions for Running Parallels OS X Software Update Point - 30
- Permissions in Active Directory - 25
- Permissions to Read/Write Service Principle Name - 26
- PKI Integration Overview - 33
- Port Reference - 248
- Post-Configuration Steps - 51
- Pre-Installation Checklist - 12
- Pre-Installation Procedures - 11
- Prepare a Mac Application for Configuration Manager - 178
- Prerequisites - 18, 84, 210, 229
- Prerequisites for Deploying macOS - 141
- Problem Reporting and Monitoring - 242

Prompting Users to Set Empty Variables
During Task Sequence Execution - 165
Push Install or Update Parallels Mac Client -
74

R

Read Rights in SCCM - 31
Receiving Compliance Settings Reports - 139
Recovering Encrypted Disk Using a Password
- 120, 128
Recovering Encrypted Disk Using Institutional
Key - 121
Recovering Encrypted Disk Using Personal
Key - 128
Remote Lock and Wipe - 229
Remote Support for Mac Computers - 240
Reporting Mac User Logon Information - 101
Reporting UAMDM Status - 53
Restrict Which Updates a Mac User Can
Install - 192
Running a Task Sequence on a Mac
Computer - 166
Running Parallels Mac Client Installer on a
Mac Computer - 71
Running Parallels Network Discovery - 70
Running Shell Scripts as Part of a Task
Sequence Step - 164

S

Save the CSR file locally and then sign it
using the Parallels certificate signing service
- 49
Secure IBCM/MDM Proxy Website with
Wildcard SSL Certificate - 54
Sending an Inventory Update to Configuration
Manager - 82
Sending Problem Reports - 82
Sending Problem Reports from Parallels Mac
Client - 243
Sending Problem Reports Using a
Standalone Reporting Utility - 243
Sending Problem Reports Using
Configuration Manager Console - 242
Sending the Package to a Distribution Point -
175
Set Hostname - 157
Set the HTTP Server Port Number - 197

Set the Interval to Check for macOS Catalog
Updates - 197
Set the Interval to Notify Parallels ConfigMgr
Proxy of Software Update Configuration
Changes - 197
Set Variables Task Sequence Step - 164
Software Metering - 104
Specify the Web Proxy Server Settings - 196
Specifying a Script Interpreter - 137
Specifying Step Properties Using Task
Sequence Variables - 162
Start Up a Mac and Execute a Task
Sequence - 167
Step 1
Prepare to Enable Trust - 46
Prepare to Enable Trust Between Proxies -
44
SMS Provider Location - 39
Step 2
Configuration Manager Proxy Service
Account - 39
Run the Configuration Wizard - 44, 46
Step 3
Configure IBCM Link - 45
Configure the MDM Link - 46
Prerequisites Check - 40
Step 4
Configure APNs Certificate - 48
Parallels Client Certificate Management
Settings - 40
Step 5
Configure MDM Profile Signing - 50
Role-Based Security - 41
Step 6
Configuration Manager Proxy
Communication Ports - 41
Step 7
Customer Experience Program - 42
Step 8
Configuration Settings Summary - 42
Synchronize SCCM with WSUS - 200

T

Task Sequence Steps - 152
Task Sequence Variables - 161
Testing Internet-Based Client Management -
234

The Reporting Functionality Requirements - 23
Troubleshooting - 169

U

Uninstalling Applications - 186
Uninstalling Parallels Mac Client - 77
Uninstalling VPP Applications - 228
Unlock a Mac - 231
Updating Legacy Task Sequences - 152
Updating Parallels ConfigMgr Proxy Connection URL - 77
Upgrading Parallels Mac Client - 78
Upgrading Parallels Mac Client via Software Distribution - 79
Upgrading Parallels Mac Management to a Newer Version - 56
User Initiated Enrollment - 84
User Rights Requirements - 23
Using Apple VPP - 210
Using Conditions in Task Sequence Steps - 163
Using Discovery and Remediation Scripts - 134
Using Groups in a Task Sequence - 161
Using Parallels Application Portal - 185
Using Parallels Mac Client Tools - 79
Using Parallels Mac Management for Microsoft SCCM - 94
Using Parallels Network Discovery - 68
Using Problem Monitoring Utility - 243
Using SCCM Active Directory System Discovery - 71
Using the Custom Settings Payload - 111
Using the macOS Profile Editor - 107

V

Verify the macOS Boot Image Deployment - 143
Verifying Parallels Mac Client Deployment - 76
Verifying the Parallels ConfigMgr Proxy Service Certificate - 42
View and Update License Information - 61
View Mac Computers Assigned to a Site - 208
Viewing and Monitoring FileVault 2 Encryption Status - 117, 125

Viewing Parallels Mac Client Properties - 79
Viewing the Package Status - 176

W

What This Section Does Not Cover - 34
Windows and macOS Firewall Configuration - 17
Wipe a Mac Computer - 230
Wipe an Apple Mobile Device - 233