



# Parallels Mac Management for Microsoft SCCM

Administrator's Guide

v5.0 Update 1

Parallels International GmbH  
Vordergasse 59  
8200 Schaffhausen  
Switzerland  
Tel: + 41 52 672 20 30  
[www.parallels.com](http://www.parallels.com)

Copyright © 1999-2016 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, Windows Vista are registered trademarks of Microsoft Corporation.  
Apple, Mac, the Mac logo, OS X, macOS, iPad, 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

<b>Introduction .....</b>	<b>8</b>
Parallels Mac Management Features Overview.....	8
About This Guide .....	9
<b>Pre-Installation Procedures .....</b>	<b>10</b>
Parallels Mac Management Component Overview.....	10
Pre-Installation Checklist .....	11
Installation Requirements.....	12
General Requirements .....	12
Parallels Configuration Manager Proxy Requirements.....	13
Parallels NetBoot Server Requirements .....	14
Parallels OS X Software Update Point Requirements.....	15
Parallels MDM Server Requirements.....	15
The Reporting Functionality Requirements .....	15
Communication Ports and Protocols .....	16
User Rights Requirements .....	17
Permissions for Running Parallels Proxy Configuration Wizard.....	17
Permissions for Running Parallels Proxy Service.....	22
Permissions for Running Parallels OS X Software Update Point.....	23
Configuring Configuration Manager Boundaries .....	24
Configuring Windows Firewall .....	25
Integrating Parallels Mac Management with PKI .....	25
PKI Integration Overview .....	26
What This Section Does Not Cover .....	26
Creating Certificate Templates for Parallels Proxy and Mac Computers.....	26
Creating a Security Group .....	28
Handling Expired Certificates.....	28

<b>Installation and Configuration .....</b>	<b>30</b>
Installation Overview .....	30
Running the Setup Wizard .....	30
Running Configuration Wizards .....	32
Configuring Parallels Configuration Manager Proxy .....	32
Configuring Parallels NetBoot Server .....	35
Configuring Parallels OS X Software Update Point .....	36
Configuring Parallels MDM Server .....	36
Maintenance and Upgrade .....	41
Viewing Proxy Service Certificate Details .....	41
Migrating Configuration Manager Proxy .....	42
Upgrading Parallels Mac Management .....	44
<b>Licensing and Activation .....</b>	<b>45</b>
Parallels Mac Management Licensing .....	45
Purchasing a Subscription .....	45
Obtaining a Trial License .....	46
Create a Parallels My Account .....	46
Register a Subscription .....	49
Creating and Managing Sublicenses .....	50
Activate Parallels Mac Management .....	52
Activate Online .....	52
Activate Offline .....	52
View and Update the License Information .....	53
Exceeding the License Limit .....	55
Deactivating Parallels Mac Management .....	56
<b>Parallels Mac Client Deployment .....</b>	<b>58</b>
Installation Options Overview .....	58
Installing Parallels Mac Client Using Discovery Methods .....	59
Enabling Remote Access on Mac Computers .....	59
Configuring Parallels Mac Client Push Installation Properties .....	60
Using Parallels Network Discovery .....	62
Using SCCM Active Directory System Discovery .....	64

Running Parallels Mac Client Installer on a Mac.....	65
Installing Parallels Mac Client Using a Script.....	66
Push Install or Update Parallels Mac Client.....	67
Configuring the Firewall .....	68
Verifying Parallels Mac Client Deployment .....	69
Updating Parallels Proxy Connection URL.....	69
Uninstalling Parallels Mac Client.....	70
Upgrading Parallels Mac Client .....	70
Automatic Upgrade of Parallels Mac Client.....	70
Upgrading Parallels Mac Client via Software Distribution .....	71
Manually Upgrading Parallels Mac Client .....	72
Using Parallels Mac Client Tools .....	72
Viewing Parallels Mac Client Properties .....	72
Initiating Policy Retrieval from a Mac.....	74
Sending Problem Reports From Parallels Mac Client.....	75
<b>Using Parallels Mac Management for Microsoft SCCM .....</b>	<b>77</b>
The Configuration Manager Admin Console .....	77
Device Collections in Parallels Mac Management .....	77
Hardware and Software Inventory.....	78
Reporting User Logon Information.....	79
Compliance Settings .....	81
Deploying OS X Configuration Profile.....	81
Enforcing FileVault 2 Encryption .....	89
Enforcing Parallels Desktop Preferences .....	104
Enforcing Parallels Desktop VM Settings .....	105
Using Discovery and Remediation Scripts .....	107
Deploying Configuration Baseline .....	111
Receiving Compliance Settings Reports .....	112
Deploying Software via SCCM Package Deployment .....	113
Creating a Software Package .....	113
Sending a Package to a Distribution Point.....	116
Deploying Software .....	117
Viewing the Package Status .....	117

Deploying Software via SCCM Application Deployment .....	118
Choose the Installation Type.....	118
Prepare a Mac Application for Configuration Manager.....	119
Create a Configuration Manager Application.....	120
Configure the Deployment Type .....	121
Deploy the Application.....	123
Installing the Application on a Mac .....	124
Using Parallels Application Portal.....	125
Operating System Deployment .....	127
Prerequisites for Deploying OS X on Mac Computers.....	127
Capturing an OS X Boot Image .....	128
Capturing an OS X System Image .....	133
Distributing the OS X System Image in SCCM.....	136
Creating a Task Sequence for Deploying OS X on Mac Computers.....	138
Deploying a Task Sequence to a Collection.....	149
Running a Task Sequence on a Mac .....	150
OS X Software Update Management .....	154
Configuration Options.....	154
Configuring Parallels OS X Software Update Point.....	162
Configuring SCCM and Deploying OS X Updates.....	163
Executing Scripts on Mac Computers.....	172
Apple Device Enrollment Program.....	173
DEP Deployment Overview.....	173
Install and Configure an MDM Server .....	174
Import a DEP Certificate to Parallels MDM Server.....	174
Configure DEP Links.....	175
Creating and Managing Enrollment Profiles .....	177
Deploying and Managing Devices.....	179
Deploying Parallels Desktop to Mac Computers .....	181
Deploying SCCM Client in Windows Running in a Virtual Machine .....	184
Providing Remote Assistance to Mac Users .....	186
Problem Reporting and Monitoring .....	187
Sending Problem Reports Using Configuration Manager Console .....	187
Sending Problem Reports Using a Standalone Reporting Utility .....	188
Sending Problem Reports from Parallels Mac Client.....	189

Using Problem Monitoring Utility .....	189
Initiating Policy Retrieval from SCCM .....	191
<b>Appendices .....</b>	<b>193</b>
Logging .....	193
Changing Log File Rotation Limits .....	197
Parallels Mac Management Database .....	198
<b>Index .....</b>	<b>200</b>

## CHAPTER 1

# Introduction

Parallels Mac Management for Microsoft SCCM extends Microsoft System Center Configuration Manager 2012 and 2012 R2 (or newer) with support for Mac computers. For companies that already have Microsoft SCCM in place, Parallels Mac Management allows administrators to use SCCM as their only system to manage both PCs and Mac.

### In This Chapter

Parallels Mac Management Features Overview .....	8
About This Guide .....	9

## Parallels Mac Management Features Overview

Parallels Mac Management adds the following Mac management features to Microsoft System Center Configuration Manager:

Feature	Description
Active Directory and Network discovery of Mac computers	Active Directory and Network discovery methods allows you to discover Mac computers on a network and enroll them in Configuration Manager.
Inventory of Mac hardware and installed applications	Mac hardware and software inventory is automatically collected and can be viewed in the Configuration Manager console.
OS X configuration management via Configuration Profiles	Enables you to configure Mac computers and enforce compliance using the Configuration Manager Compliance Settings functionality.
OS X software deployment	Enables you to use the Configuration Manager Software Distribution functionality to install software and updates on managed Mac computers.
Operating System Deployment	Enables you to deploy OS X images to Mac computers using the Configuration Manager Task Sequence functionality.
OS X Patch Management	Automates patch and update management of Mac computers.
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.
Parallels Application Portal	Allows Mac users to view and install OS X



	applications made available to them by the IT administrator.
FileVault 2 Encryption Management	Enables you to enforce FileVault 2 encryption on managed Mac computers.
Parallels Desktop and Parallels virtual machine configuration management	Enables you to configure Parallels Desktop and Parallels virtual machines installed on a Mac.

Parallels Mac Management fully integrates with the Configuration Manager console, so IT administrators can manage Mac 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 useful 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 .....	10
Pre-Installation Checklist.....	11
Installation Requirements.....	12
User Rights Requirements .....	17
Configuring Configuration Manager Boundaries.....	24
Configuring Windows Firewall .....	25
Integrating Parallels Mac Management with PKI .....	25

# Parallels Mac Management Component Overview

Parallels Mac Management for Microsoft SCCM consists of the following components:

- **Parallels Configuration Manager Proxy.** This component is a Windows service application that acts as a proxy between SCCM and Mac computers. The component must be installed on a computer running Windows Server 2008 SP2 or later.
- **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 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 OS X images to Mac computers. The component must be installed on a computer running Windows Server 2008 SP2 or later.
- **Parallels OS X Software Update Point.** Allows you to manage Apple software updates (patches) for OS X using the native SCCM functionality. The component must be installed on a server where Windows Server Update Services (WSUS) is installed.
- **Parallels MDM Server.** Enables you to deploy and enroll new Mac computers in SCCM using the Apple Device Enrollment Program. This component must be installed on a server located in DMZ.
- **Parallels Mac Client.** A client software that enables communication between a Mac computer on which it is installed and the Parallels Configuration Manager Proxy.

## Pre-Installation Checklist

You can use the following checklist to help you prepare your environment for the deployment of Parallels Mac Management for Microsoft SCCM. The **Reference** column contains links to topics describing how to accomplish a corresponding tasks. Most of these topics are located in the **Installation Requirements** (p. 12) and some other sections that follow this one.

Category	Task	Reference
<input type="checkbox"/> General requirements	Check the requirements for supported SCCM, Windows, and OS X versions.	General Requirements (p. 12)
<input type="checkbox"/> Parallels Proxy	.NET Framework 4.0 is required	.NET Framework 4.0 (p. 13)
<input type="checkbox"/> Parallels Proxy	Proper Distribution Point Role Configuration	Distribution Point Role Configuration (p. 13)
<input type="checkbox"/> Parallels Proxy	Verify the IIS settings on the Distribution Point Server	IIS Settings on the Distribution Point Server (p. 13)
<input type="checkbox"/> Parallels Proxy	Check Configuration Manager Boundaries Configuration	Configuration Manager Boundaries Configuration (p. 24)
<input type="checkbox"/> Parallels Proxy	Configure Windows Firewall	Configuring Windows Firewall (p. 25)
<input type="checkbox"/> Parallels Proxy	Configure OS X Firewall	Configuring OS X Firewall (p. 68)
<input type="checkbox"/> Parallels Proxy	Verify that your network environment is configured properly	Network Configuration (p. 14)
<input type="checkbox"/> Parallels Proxy	Date and Time Synchronization check	Date and Time Synchronization (p. 14)
<input type="checkbox"/> Parallels NetBoot Server	Optional component. Needed for the OS X Image Deployment functionality.	Parallels NetBoot Server Requirements (p. 14)
<input type="checkbox"/> Parallels OS X Software Update Point	Optional component. Needed for the OS X software update functionality.	Parallels OS X Software Update Point Requirements (p. 15)
<input type="checkbox"/> Parallels MDM Server	Optional component. Needed for the Apple DEP functionality.	Parallels MDM Server Requirements (p. 15)
<input type="checkbox"/> Other	Verify Reporting Point Role, optional, but needed to view reports	The Reporting Functionality Requirements (p. 15)
<input type="checkbox"/> Other	Verify Report Viewer, optional, but needed to view reports	The Reporting Functionality Requirements (p. 15)
<input type="checkbox"/> Other	Review the ports used by Parallels Mac Management	Communication Ports and Protocols (p. 16)
<input type="checkbox"/> User rights	Verify user rights requirements.  <b>Note:</b> This is a very important step to ensure a successful installation of Parallels Mac Management.	User Rights Requirements (p. 17)  The KB article at <a href="http://kb.parallels.com/121569">http://kb.parallels.com/121569</a> provides additional information on how to set up a service account for proper PMM installation.

<input type="checkbox"/>	PKI integration	Optional, but needed if you would like to integrate Parallels Mac Management with a Public Key Infrastructure (PKI).	Integrating Parallels Mac Management with PKI
--------------------------	-----------------	----------------------------------------------------------------------------------------------------------------------	-----------------------------------------------

## Installation Requirements

Before proceeding, please read this section to learn about system requirements for installing Parallels Mac Management for Microsoft SCCM.

The section begins with General Requirements and then describes requirements for installing individual Parallels Mac Management components. It concludes with describing communications ports and protocols used by Parallels Mac Management.

### General Requirements

#### Supported SCCM Versions

Parallels Mac Management supports Microsoft System Center Configuration Manager 2012, 2012 R2, and newer. Please make sure that you have the latest service pack and critical updates installed.

#### Supported Windows Versions

Windows components of Parallels Mac Management follow the same system requirements as the Microsoft System Center components.

#### Supported OS X Versions

The following versions of OS X operating system are supported:

- OS X 10.7 Lion
- OS X 10.8 Mountain Lion
- OS X 10.9 Mavericks
- OS X 10.10 Yosemite
- OS X 10.11 El Capitan
- macOS 10.12 Sierra

## Parallels Configuration Manager Proxy Requirements

The following subsections describe requirements for a server on which the Parallels Configuration Manager Proxy component will be installed.

### .NET Framework 4.0

The server on which Parallels Configuration Manager Proxy will be installed must have the .NET Framework 4.0 installed.

### 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 page, 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. 25).
  - 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. 24) for complete details.

## Windows and OS X Firewall Configuration

See **Configuring Windows Firewall** (p. 25) and **Configuring OS X Firewall** (p. 68).

## Network Configuration

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

In addition, verify that your Mac computers have network access to SCCM site servers. Use the `tracert` command in OS X 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 OS X network preferences on a Mac:

- 1 In OS X, 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 NetBoot Server Requirements

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.
- Must have BITS 4.0 installed.

Additionally, the user account that you'll use to configure the Parallels NetBoot Server must have sufficient privileges. See the following KB article: <http://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: <http://kb.parallels.com/118518>.

Please also see **Communication Ports and Protocols** (p. 16) for the list of ports used by NetBoot Server.

## Parallels OS X Software Update Point Requirements

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

- 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/en-us/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: <http://kb.parallels.com/en/123756>.

## Parallels MDM Server Requirements

The Parallels MDM Server component must be installed on a server that meets the following requirements:

- Must be located in DMZ.
- Must be accessible from the server where the Parallels Proxy component will be installed (p. 13).

## 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.

## Communication Ports and Protocols

Communication ports used by Parallels Mac Management should not be used by other programs. Please review the following table and make sure that the ports listed are available. Please note that the table doesn't include ports used by the standard System Center Configuration Manager services and by standard Windows services.

Program	TCP	UDP	Platform	Required	Notes
<b>Configuration Manager Proxy</b> pma_isv_proxy_service.exe	8760, 8761		Windows	Required	The default ports 8760 and 8761 can be changed if needed using the Configuration Manager Proxy configuration utility.
<b>NetBoot Server</b> pma_netboot_service.exe bootpd (DHCP)		67, 68	Windows	Optional	Required for the NetBoot Server functionality.
<b>NetBoot Server</b> pma_netboot_service.exe tftpd (TFTP)		69	Windows	Optional	Required for the NetBoot Server functionality.
<b>NetBoot Server</b> pma_netboot_service.exe HTTPD (Web)	80		Windows	Optional	Required for the NetBoot Server functionality.
SSH server	22		Mac	Optional	Required for the Network Discovery functionality.



VNC server	5900		Mac	Optional	Needed to accept VNC connections on a Mac.
Mac client	8000		Mac	Required	Required for Parallels Mac Client to accept incoming connection from Parallels Configuration Manager Proxy.

Additionally, you must enable RPC ports to allow WMI/RPC traffic to pass through. RPC ports can be opened by enabling the Group Policy firewall exception as described below:

- 1 Edit the Group Policy object (GPO), which is used to manage Windows Firewall settings in your organization. The GPO can be edited using the Group Policy Object Editor snap-in (gpedit.msc).
- 2 In the GPO Editor, navigate to **Computer Configuration / Administrative Templates / Network / Network Connections / Windows Firewall**.
- 3 Open either the **Domain Profile** or **Standard Profile**, depending on which profile you use.
- 4 Right-click the **Windows Firewall: Allow inbound remote administration exception** item and choose **Edit**.
- 5 Select the **Enabled** option and click **OK**.

## 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 Proxy Configuration Wizard

A user that will be running the Parallels Configuration Manager Proxy Configuration Wizard must have specific permissions. This section describes these permissions.

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 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 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 by clicking **Start > All Programs > Microsoft SQL Server 2008 R2**.

- 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 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 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 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 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 configuring 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. 15).

## Configuring 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.

## Configuring Windows Firewall

To enable Parallels Configuration Manager Proxy and Parallels NetBoot Server network communications, their executable files must be added to the Windows firewall exception list.

The name and path of the Configuration Manager Proxy executable is:

```
%ProgramFiles(x86)%\Parallels\Parallels Mac Management for Microsoft  
SCCM\pma_isv_proxy_service.exe
```

The name and path of the NetBoot Server executable is:

```
%ProgramFiles(x86)%\Parallels\Parallels Mac Management for Microsoft  
SCCM\pma_netboot_service.exe
```

To add the executables to the Windows firewall exception list, open the Windows Control Panel and click (or double-click) Windows Firewall. Add the .exe files to the list of programs allowed through Windows Firewall.

For the list of ports used by Parallels Mac Management for Microsoft SCCM, see **Services, Ports and Protocols** (p. 16).

## 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. 30). 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 (or newer)

**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/en-us/library/dn786443.aspx>

### Creating Certificate Templates for Parallels 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 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 Proxy can automatically handle a situation when digital certificates issued to Mac computers or the Parallels Proxy itself expire. It can also detect if a signing certificate of the certification authority (CA) has changed, thus invalidating the currently issues certificates. The following describes how Parallels Proxy handles the above events:

- When Parallels 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 (you can configure how soon), it will automatically renew the certificate.
- Parallels Proxy will also check if the signing certificate of the currently used certification authority matches the one on 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.
- Parallels Proxy validates its own digital certificate at preset intervals (the time interval can be configured). 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 v5.0 doesn't support automatic renewal of the Parallels 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 <http://kb.parallels.com/en/123836>.

You can configure digital certificate validation parameters according to your needs by making changes in Windows registry at the following location:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\pma\_cm\_proxy\Parameters

Use the following key values to modify the configuration:

#### ***PkiCertificateExpirationThresholdDays***

**Type:** DWORD

**Default:** 30

**Description:** Specifies how soon a Parallels Client certificate must be renewed. The value denotes the number of days until a certificate expiration date. For example, let's say the value of this parameter is set to 30 (which is default). During validation, if a given certificate will expire in 30 days or earlier, it will be automatically renewed. If the certificate expires in 31 or more days, then it will be validated again the next time Parallels Proxy communicates with the Parallels Mac Client.

#### ***CDWORDmProxyPkiCertificateCheckPeriodSecs***

**Type:** DWORD

**Default:** 86400 (1\*24\*60\*60 or once in 24 hours)

**Description:** Specifies the time interval, in seconds, at which Parallels Proxy validates its own certificate. The minimum allowed value is 30 seconds.

#### ***ForcePkiCertificateValidation***

**Type:** DWORD

**Default:** 0

**Description:** This parameter turns logging on or off for certificates that are not compliant with base policy. If the parameter is set to zero (default), no log entries will be created for such certificates. Any non-zero value enables logging. Please note that this parameter is not related to certificate expiration dates. It creates log entries if a chain of trust cannot be established with a given certificate.

# Installation and Configuration

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

## Installation Overview

Parallels Mac Management for Microsoft SCCM consists of several components, which are installed in Windows using the same installation wizard (except Parallels Mac Client, which is installed in OS X). If you are installing the components on different servers, run it on each server and select only the component(s) that you want installed on that particular server.

Please note that 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 sites (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.

Before running the installation wizard, please make sure that you have read **Installation Requirements** (p. 12) for each component that you are planning to install.

## Running the Setup Wizard

The **Parallels Mac Management for Microsoft SCCM Setup** wizard is used to install Parallels Mac Management. When you run the wizard, you need to select the components you wish to install on a given server. The rest of the installation is mostly automatic.

When installing Parallels Mac Management for the first time, you must install at least Parallels Configuration Manager Proxy and the Configuration Manager Console Extension (but necessarily both on the same Windows machine). Other components are optional, so you should install them only if you want to use the functionality that they provide. You should also decide in advance on which servers you want to install individual components and then run the setup wizard on each server selecting only the component(s) you want to install.

To install Parallels Mac Management:

- 1** Run the **Parallels Mac Management for Microsoft SCCM Setup Wizard**.
- 2** Read the info on the **Welcome** page and click **Next**.
- 3** On the **License Agreement** page, read the End-User License Agreement. If agreed with the terms, select **I accept the terms in the license agreement** and click **Next**.
- 4** On the **Select Components** page, select the components you wish to install from the following list:
  - **Parallels Configuration Manager Proxy**. A Windows service application that acts as a proxy between SCCM and Mac computers. This component is required for Parallels Mac Management to work.
  - **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.
  - **NetBoot Server**. Enables Mac computers to boot from a network. You need to install this component if you plan to deploy OS X images on Mac computers.
  - **OS X Software Update Point**. Allows you to manage Apple software updates (patches) for OS X using the native SCCM functionality. The component must be installed on a server where Windows Server Update Services (WSUS) is installed.
  - **MDM Server**. Select this component if you plan to deploy and enroll new Mac computers in SCCM using the Apple Device Enrollment Program (DEP).
  - Click **Next** and then click **Install** to begin the installation.
- 5** Wait for the installation to finish.
- 6** On the **Setup Completed** page, verify that the installation was successful. Make sure that the **Configure Parallels Mac Management for Microsoft SCCM** option is selected and click **Finish** to close the **Setup Wizard**.

In a second a two, a configuration wizard will open where you can configure Parallels Mac Management. Each Parallels Mac Management component has its own configuration wizard (except the Configuration Manager Console Extension, which doesn't need to be configured). For example, if you chose to install all of the components on the same server, all configuration wizards will automatically run one after another. As soon as you complete one wizard, the next one will open after a short delay.

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

## Running Configuration Wizards

Read this section to learn how to use Parallels Mac Management configuration wizards.

### Configuring Parallels Configuration Manager Proxy

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

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

#### 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.

#### 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.

#### 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's access rights for configuring the Proxy service. If the user has insufficient rights, 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. 17) 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.

## Parallels Client Certificate Management Settings

On the **Parallels Client certificate management settings** page, select the protocol (HTTP or HTTPS) that the Parallels 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. 26) section, you should see the Parallels 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.

## 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. 189) for more info.
- **FileVault Key Administrators.** This role grants read rights to the Parallels Mac Management SQL Server database (p. 198). 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.

## 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.

## 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.

## 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.

## Conclusion and Notes

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. For more information, please see **View Proxy Service Certificate Details** (p. 41).

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.

## Configuring Parallels NetBoot Server

If you chose 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**.

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 chose to install the **OS X Software Update Point** component, the **Parallels OS X Software Update Point Configuration Wizard** will automatically open. You can also run the wizard manually by going to **Apps > Parallels** and double-clicking the **OS X Update Point Configuration Utility**.

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 right 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. 15).
- 3 On the **Configuration settings summary** page, review the installation summary. If satisfied, click **Finish** to apply the settings and close the wizard.

## Configuring Parallels MDM Server

The **Parallels MDM Server Configuration Wizard** will start if you chose to install the MDM Server component.

You can also run the wizard manually by navigating to **Apps > Parallels** and double-clicking **MDM Service Configuration Utility**.

To configure the component, complete the wizard as described in the subsequent sections.

## Parallels MDM Service Account

On the **Parallels MDM Service Account** page, specify the username and password of an account that will be used to run the MDM service on this machine. The account doesn't have any specific requirements. Considering that the server is located in DMZ, a non-administrative local account should be used to run the service.

After specifying the account credentials, click **Next** to continue.

## Parallels MDM Server Location

On the **Parallels MDM Server Location** page, specify the location of the MDM server and incoming port numbers so other Parallels Mac Management components and Mac computers can communicate with it:

- **Parallels MDM server FQDN:** A fully qualified domain name of the local server. For example, `mdm.mycompany.com`.
- **Port used for incoming Mac connections:** Specify the port number on which the MDM server should listen for incoming connections from your Mac computers. You should configure the host server and the ports according your needs.
- **Port used for incoming Parallels Mac Management connections:** Specify the port number on which the MDM server should listen for connections from Parallels Mac Management (specifically, the local DEP service, which runs on the same server as Parallels Proxy).

Click **Next** to continue.

## Parallels MDM Web Server Certificate

On this page, specify a web server certificate, which will be used by Mac computers to ensure authenticity of the MDM server when establishing an SSL connection. Select from the following options:

- **Keep the current SSL certificate.** Select this option if you have configured this MDM server before and want to keep the current certificate.
- **Import SSL certificate from file.** To import a certificate from a file, select this option and then click **Browse** to select the file. If the certificate file is password-protected, specify the password in the field provided.

Click **Next** to continue.

### APNs Certificate

Parallels Mac Management uses push notifications for MDM functions, such as Parallels Mac Client push installation and some others. To enable push notifications, you need to obtain a corporate APNs push certificate and make it available to the MDM server.

The **APNs Certificate** page gives you the three options of specifying a certificate described below. Please note that depending your selection, the wizard will go to a different page when you click **Next**.

Select from one of the following options:

- **Keep the current APNs certificate.** Select this option if this MDM server has been previously configured and already have a certificate. When you click **Next**, the wizard will go to the **Prerequisites Check** page (p. 40).
- **Import an APNs certificate from a file.** Select this option if you already have an APNs certificate file. Click **Next** and then specify the file. Click **Next** again to go to the **Prerequisites Check** page (p. 40).
- **Generate a new APNs certificate.** Select this option if you don't have a certificate and need to generate one. When you click **Next**, the wizard will open several successive pages where you can generate a certificate. These pages are described in the **Generate an APNs Certificate** section (p. 38), which follows this one.

### Generate an APNs Certificate

The **Generate an APNs Certificate** wizard page opens after you select the **Generate a new APNs certificate** option on the **APNs Certificate** page (described in the previous section) and click **Next**.

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 **Generate an APNs Certificate** 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 right 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 unrestricted Internet access, you can use this option. If your Internet access is limited to certain domains, you may add pmm.parallels.com to the allowed domain list (if your security policy allows it).

**License key:** When using the automatic CSR option, you must also specify your Parallels Mac Management license key in the field provided.

- **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

When you select this option and click **Next**, the configuration wizard will do the following:

- 1 Create a CSR and an associated private key.

**Important Note:** The private key associated with this CSR will NOT become available to Parallels.

- 2 Connect to the Parallels certificate signing service over the Internet and sign the CSR with Parallels' own MDM Signing Certificate.
- 3 When the signing process is complete, the next page opens where you can specify a local folder where you want to save the signed CSR file and the private key.
- 4 Once 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:
  - a Open the Apple Push Certificates Portal in a web browser and log in using your Apple ID and password.
  - b Upload the signed CSR file.
  - c Download the created APNs certificate file named "MDM\_<VendorName>\_Certificate.pem".
- 5 Back in the wizard, click **Next** to proceed to the page where you can upload the APNs file to the MDM server. Click **Browse** to browse for a target folder.
- 6 When done, click **Next** to upload the APNs file and proceed to the **Prerequisites Check** page (p. 40).

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

When you select this option and click **Next** in the step described in the beginning of this section, the the following will happen:

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

**Important Note:** The private key associated with this CSR will NOT become available to Parallels.

- 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:
  - a Visit Parallels My Account at <https://account.parallels.com>. Sign in using your Parallels My Account email address and password (if you don't have an account, you must register for one first).

- b** Once signed in, navigate to **Parallels Mac Management > MDM Certificate Signing Request**.
  - c** Follow the instructions on the **MDM Certificate Signing Request** page and upload the CSR file that you saved in step 2 above. When instructed, download the signed CSR to your local server.
  - d** Open the Apple Push Certificates Portal in a web browser and log in using your Apple ID and password.
  - e** Upload the signed CSR that you obtained from Parallels My Account earlier.
  - f** Download the created APNs certificate file named “MDM\_<VendorName>\_Certificate.pem”.
- 4** Back in the wizard, click **Next** to proceed to the page where you can upload the APNs file to the MDM server. Click **Browse** to browse for a target folder.
- 5** When done, click **Next** to upload the APNs file and proceed to the **Prerequisites Check** page (p. 40).

### Prerequisites Check

Verify that all of MDM server requirements are met. The requirements that are checked on this page are as follows:

- Ports for incoming connections that you specified for this MDM server must not be used by any other program or service.
- The specified web server certificate must be issued to the current host and must not be expired.
- The specified APNs certificate must be valid and not expired at the time of verification.
- The MDM server must be able to connect to APNs. See the **Certificates Requirements** subsection in **Parallels MDM Server Requirements** (p. 15) for details.

If one or more of the requirements are not met, you have to resolve any issues before proceeding. If an issue can be resolved on one of the wizard pages, click **Back** to go to that page. If it's an external issue, correct it and click **Rerun** to perform the validation again.

When all requirements are met, click **Next**.

### Configuration Settings Summary

This is the final page of the **Parallels MDM Server Configuration Wizard**. Review the configuration settings summary and click **Finish** when ready.

For the complete information about enabling and using the DEP functionality in Parallels Mac Management, please read the **Apple Device Enrollment Program** section (p. 173).



# Maintenance and Upgrade

## Viewing Proxy Service Certificate Details

The account that you use to run the Parallels Configuration Manager Proxy service must have permissions to access the certificate store on the local computer and to read the Configuration Manager Proxy certificate private key. The permissions are set automatically when you run the **Configuration Manager Proxy Configuration Wizard** and specify the account for running the service.

If you experience difficulties accessing Mac computers from the Configuration Manager console, verify that certificate permissions are valid for the account that you use to run the Parallels Configuration Manager Proxy service.

### 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.

### Migrating Configuration Manager Proxy

This section describes how to migrate the Parallels Configuration Manager Proxy to another server on the same Configuration Manager site.

To migrate the Parallels Configuration Manager Proxy:

- 1 Export the 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 Proxy on the new server.

The following describes the certificate export and import procedures. The Proxy installation and uninstallation procedures are described in **Install Parallels Mac Management for Microsoft SCCM** (p. 30).

#### Exporting Certificate from Certificate Store

To export a certificate:

- 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 Certificate into Certificate Store

To import a certificate:

- 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. 69).

## Upgrading Parallels Mac Management

To upgrade Parallels Mac Management to a newer version, you need to uninstall the current version and then install a new one.

To run the uninstaller, go to **Control Panel > Programs > Uninstall a program** and uninstall the **Parallels Mac Management for Microsoft SCCM** program. If Parallels Mac Management components are installed on different servers, you need to uninstall each component individually. When done, install the new version of Parallels Mac Management for Microsoft SCCM. Please note that after upgrading Parallels Mac Management, you need to upgrade the Parallels Mac Client on each managed Mac. See **Upgrading Parallels Mac Client** (p. 70) for more information.

## CHAPTER 3

# Licensing and Activation

This chapter explains how the Parallels Mac Management licensing works and how to obtain a license and use it to activate a Parallels Mac Management installation.

You can read more about Parallels Mac Management licensing in the **Parallels Mac Management for Microsoft SCCM Licensing Guide**, which is available for reading and download on the Parallels website.

### In This Chapter

Parallels Mac Management Licensing .....	45
Activate Parallels Mac Management.....	52

## Parallels Mac Management Licensing

Parallels Mac Management for Microsoft SCCM is licensed on a per managed Mac basis. The number of individual licenses in your subscription denotes the number of Mac computers that you can manage in SCCM.

You license Parallels Mac Management with a prepaid subscription, which works as follows:

- A subscription is purchased for a predefined period of time.
- A subscription can include any number of individual licenses (the maximum number of Mac computers that you can manage).
- Support is included in the cost of the subscription.

No matter how many licenses in your subscription, you'll receive a single license key. A license key can be used to activate a single installation of Parallels Mac Management. If you need to activate several Parallels Mac Management installations to work simultaneously, you need multiple license keys.

## Purchasing a Subscription

To purchase a Parallels Mac Management subscription, please contact the Parallels Sales team or a Parallels Partner/Reseller.

## Obtaining a Trial License

If you would like to evaluate Parallels Mac Management, you need to obtain a trial license from the Parallels Sales team or a Parallels Partner/Reseller.

## Create a Parallels My Account

Parallels My Account is a web application that enables Parallels customers (consumers and organizations) to view and manage licenses for various Parallels products. The instructions below describe how to quickly get started with Parallels My Account.

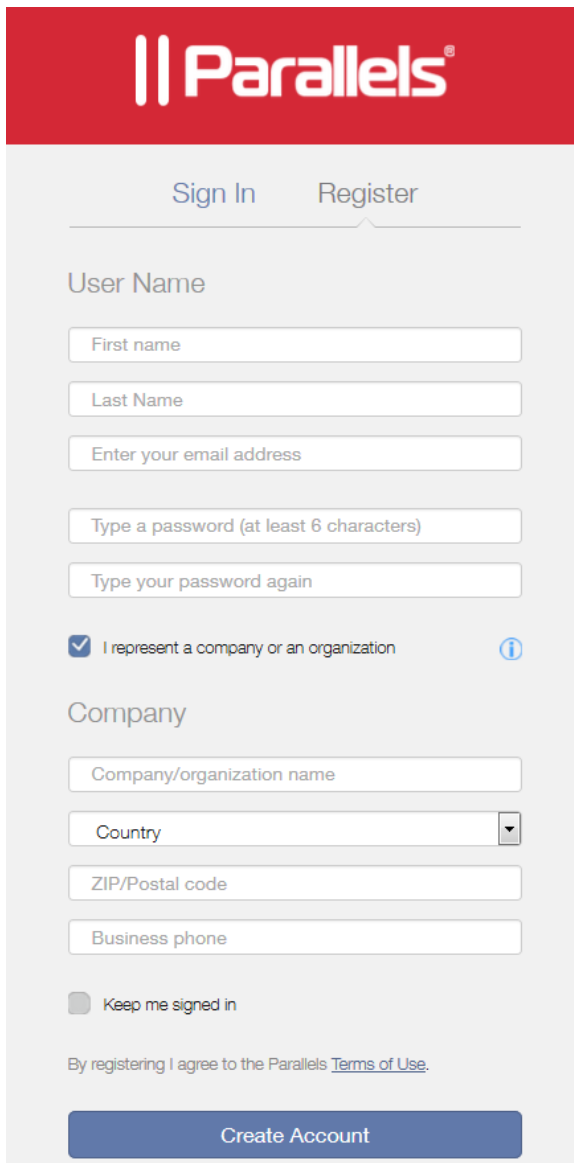
You can create an account for your company or organization when you first create a Parallels My Account, or after you already created a private account.

### Create a Parallels My Account from scratch

If you are a new customer and don't have a Parallels My Account, you can create one for yourself and for your organization as follows:

- 1 Visit Parallels My Account at <https://account.parallels.com>

- 2 Click **Register**. The registration page opens.


The image shows the Parallels registration page. At the top is a red header with the Parallels logo. Below the header, there are two tabs: "Sign In" and "Register", with "Register" being the active tab. The registration form includes fields for "User Name" (split into "First name" and "Last Name"), "Enter your email address", "Type a password (at least 6 characters)", and "Type your password again". There is a checkbox labeled "I represent a company or an organization" which is checked, and an information icon to its right. Below this is a "Company" section with fields for "Company/organization name", "Country" (a dropdown menu), "ZIP/Postal code", and "Business phone". At the bottom of the form is a checkbox labeled "Keep me signed in" and a link to the "Terms of Use". A blue "Create Account" button is at the very bottom.

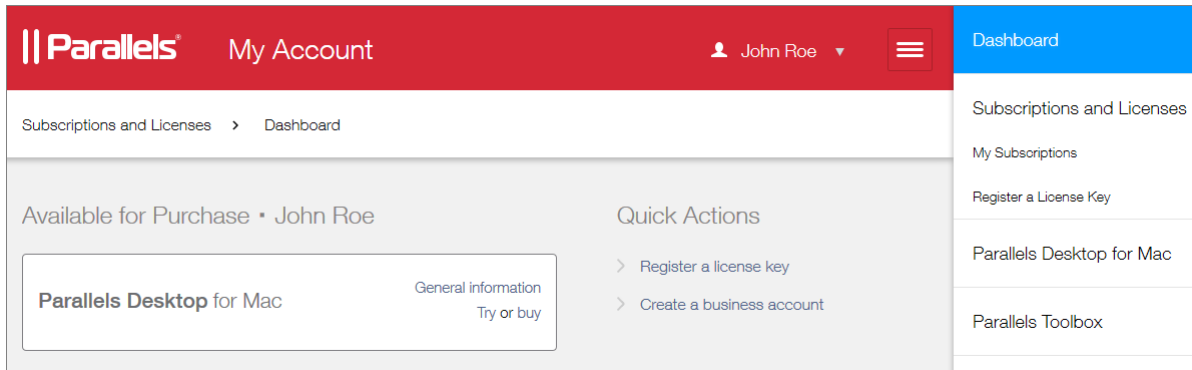
- 3 Select the **I represent a company or an organization** option. This step is required to create a business account for your organization.
- 4 Specify your personal and your company info (all fields are required) and click **Create Account**.

This creates an account for you personally and a business account for your organization to which you are assigned as the account administrator. When you log in to your account using you email address and password, you can manage personal and business products from the same account.

## Creating a Parallels business account from an existing account

If you already have a personal Parallels My Account, follow these steps to create a business account for your organization:

- 1 Log in to Parallels My Account using your email address and password.
- 2 Click  next to your user name to open a side menu. If the **Dashboard** page is not already displayed, click **Dashboard** in the side menu.
- 3 On the **Dashboard** page, click **Create a business account** in the **Quick Actions** section.



- 4 A message box opens with an explanation of what a business account is. Read it and then click **Proceed**.
- 5 In the **Registering a Business Account** dialog, type the name of your organization and then specify your country, state/city (if applicable), ZIP or postal code, and your business phone number.


- 6 When done, click **Create a Business Account**.

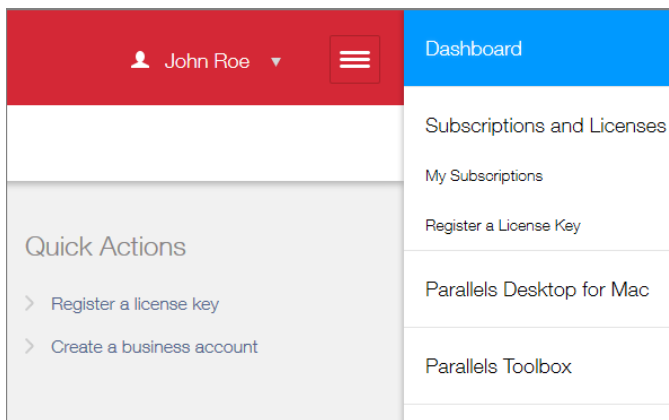


A business account is created for your organization to which you are assigned as the account administrator. When you log in to your personal account, you can manage personal and business products from the same account.

## Register a Subscription

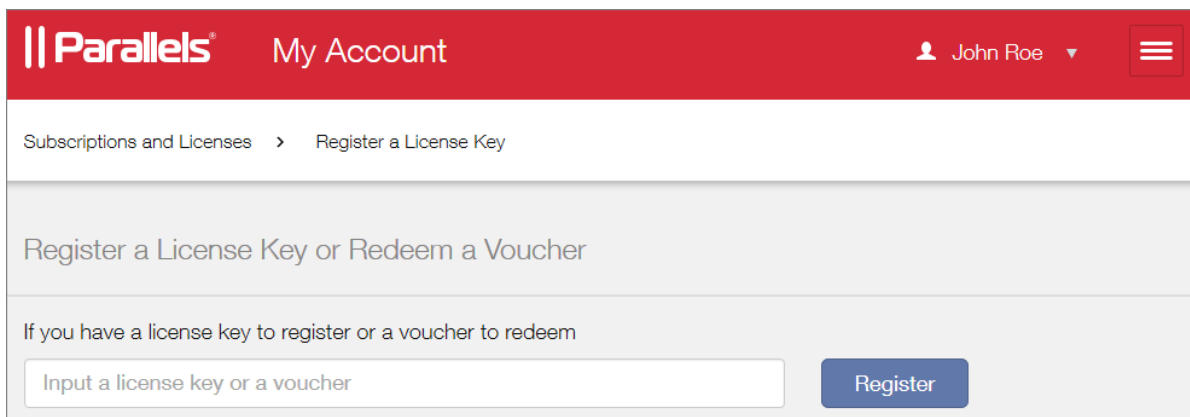
To register your subscription in Parallels My Account:

- 1 Sign in to Parallels My Account using your email address and password.
- 2 Click  next to your user name to open a side menu. If the **Dashboard** page is not already displayed, click **Dashboard** in the side menu.



- 3 Click the **Register a license key** link in the **Quick Actions** section. The **Register a License Key** page opens.

You can also open this page by expanding **Subscriptions and Licenses** section in the side menu, then clicking **Corporate Subscriptions**, and finally clicking the **Register a License Key** link.



- 4 Type the license key that you received with your subscription and click **Register**.
- 5 When your license key is registered, you will see a confirmation message.

- 6 If you would like to view your subscription information, click the **Open Corporate Subscriptions** button. This will open the **Subscription Details** page where you can view the information.

Your subscription is now registered and your license key can be used to activate the Parallels product to which it applies.

## Creating and Managing Sublicenses

A sublicense is a virtual license that is linked to the master license but has its own license key, the total number of individual licenses you allocate to it, and its own expiration date.

### Planning for sublicenses

Sublicenses are useful in these typical scenarios:

- You want to grant a division of your organization the ability to use a limited number of your available licenses. You can create a sublicense with a required number of licenses and give the sublicense key to the administrator for that division.
- You have multiple SCCM sites and you want to activate them using different license keys with different number of total licenses allocated to each key.

### Creating a sublicense

To create a sublicense:

- 1 In the side menu, expand **Subscriptions and Licenses** and click **Corporate Subscriptions**.
- 2 If you have more than one Parallels product registered, select Parallels Mac Management in the drop-down list and then click a subscription for which you want to create a sublicense.
- 3 On the **Subscription Details** page, click **Details** in the **Products** section.
- 4 On the **Product Details** page, click **Create a Sublicense**.
- 5 The **New Sublicense** dialog opens.
- 6 Type a sublicense name.
- 7 Specify the number of licenses to allocate to this sublicense.
- 8 In the **Expires** section, select one of the following:
  - **With the subscription.** The sublicense will have the same expiration date as the subscription.
  - **On date.** Specify a desired expiration date.
- 9 Click **Create** to create a sublicense.

- 10** The **New Sublicense** dialog opens where you can review the created sublicense. Note the **License Key** property. This is the key that was automatically assigned to this sublicense. You'll need it to activate a Parallels Mac Management installation. You can copy or write it down now or you can do it later.
- 11** Click **Close** to close the **New Sublicense** dialog.
- 12** The sublicense appears on the **Product Details** page in the **Sublicenses** section.

Sublicenses						6 sublicenses
Name/Key	Type	Max lic.	Used	Available	Expires on	
Primary key [Redacted]	Primary	10	0	10	November 29, 2017	
Sublicense 1 [Redacted]	Reserved	1	0	1	November 29, 2017	<a href="#">Edit</a>
Sublicense 2 [Redacted]	Reserved	1	0	1	November 29, 2017	<a href="#">Edit</a>
						<a href="#">Create a Sublicense</a>

The first row in the table always displays the primary license key. This is the same key as the one displayed in the **Product Details** section above the **Sublicenses** section. The key is included in this table for you to easily see in one place how your licenses are distributed between your primary key and sublicenses.

## Modifying a sublicense

To modify a sublicense, click the **Edit** link on the same row. This opens the **Edit Sublicense** dialog. You can modify any of the sublicense properties except the license key.

Please note that if you want to decrease the number of licenses in a sublicense, you have to make sure that no active Mac computers will be affected in the corresponding SCCM site. If the number of individual licenses in a sublicense falls below the number of active Mac computers, you will lose the ability to manage some of them.

## Deleting a sublicense

To delete a sublicense, click the **Edit** link and then click the **Delete** button. You should only delete a sublicense if you never used it to activate Parallels Mac Management or if you deactivated the corresponding Parallels Mac Management installation prior to deleting the sublicense.

## Activate Parallels Mac Management

After you registered your subscription in Parallels My Account, you can activate Parallels Mac Management using your license key.

You can use the online or the offline method to activate Parallels Mac Management. The method you choose depends on the following:

- If the server on which you have Parallels 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 method in detail.

### Activate Online

To activate Parallels Mac Management using the online activation method:

- 1 Open the Configuration Manager console.
- 2 Navigate to **Administration / Overview / Parallels Mac Management / Licenses**.
- 3 Right-click your site in the **Licenses** list and choose **Activate license**.
- 4 The **Parallels Mac Management - Activate License** dialog opens.
- 5 Input your license key and select the **Activate online** option.
- 6 Click **Next**.
- 7 Parallels Mac Management connects to the Parallels Licensing Server and verifies the key.
- 8 If the key is valid, the license information is displayed on the screen. Review the 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 activated and the activation information is added to Parallels My Account.

### Activate Offline

If the server on which you have Parallels Proxy installed has limited or no Internet access, you can 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 Right-click your site in the **Licenses** list and choose **Activate license**.
- 4 The **Parallels Mac Management - Activate License** dialog opens.
- 5 Input your license key and select the **Activate offline** option.
- 6 Click **Next**.
- 7 Click the **Save** button to save to offline activation request file. Specify a location and file name and click **Save**. Do not close the **Parallels Mac Management - Activate License** dialog.
- 8 You now need to obtain the license activation file from Parallels My Account. To do so, visit <https://account.parallels.com> and sign in using your email address and password.
- 9 Once signed in, click  next to your user name to open a side menu.
- 10 In the side menu, expand the **Parallels Mac Management** section and click **Offline Activation and Validation**.
- 11 On the **Offline Activation and Validation** page, submit the offline activation request file you saved earlier.
- 12 Follow the instructions and download the license activation file.
- 13 Go back to the Configuration Manager console. In the **Parallels Mac Management - Activate License** dialog, click **Browse** and select the license activation file you've obtained from Parallels My Account.
- 14 Click **Next**. Your license information is displayed on the screen. Review the information and click **Activate**.
- 15 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 activated and the activation information is added to your Parallels My Account.

## View and Update the 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 your site in the **Licenses** list and choose **Properties**.

**3** The **Parallels Mac Management - License Information** dialog opens where you can view the following information:

- **License key:** The license key that was used to activate this installation.
- **Start date:** The license key start date.
- **End date:** The license key end date.
- **Number of licenses:** The maximum number of Mac computers that can be managed in this installation.
- **Used licenses:** The current number of managed Mac computers.
- **Remaining licenses:** The number of licenses remaining.

The license usage information is reported back to the Parallels Licensing 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 in the following subsection.

### Refresh the license information


The **Refresh** button on the **Parallels Mac Management - License Information** dialog allows you to retrieve the current license information from the Parallels Licensing Server to reflect possible changes to your subscription. Normally, this update is done automatically every 24 hours if the server on which the Parallels Proxy is running has Internet access. By clicking the **Refresh** button, you can retrieve this information at any time. This functionality is useful when, for example, 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 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 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. Don't close this dialog (you will return to it later).
- 4 Visit <https://account.parallels.com> and sign in using your email address and password.
- 5 Once signed in, click  next to your user name to open a side menu.
- 6 In the side menu, expand the **Parallels Mac Management** section and click **Offline Activation and Validation**.
- 7 On the **Offline Activation and Validation** page, specify the offline request file you saved earlier.
- 8 Follow the instructions and download the subscription information file.
- 9 Go back to the Configuration Manager console and select this file.
- 10 Your local subscription information is 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 Mac computers managed through it. If at any time the number of computers exceeds the license limit, the following happens:

- 1 The information about the event is recorded to the Parallels Proxy log file.
- 2 If an attempt is made to manually enroll a Mac in SCCM, an error message will be shown on the Mac during the registration procedure.
- 3 All managed Mac computers 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 Parallels Desktop and Virtual Machine configuration items.
  - Creating/editing Configuration Profiles.
  - 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 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, 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

You can deactivate a Parallels Mac Management installation and release the license key, so it can be used to activate Parallels Mac Management installed in another SCCM site.

Depending on whether you activated Parallels Mac Management using the online or the offline activation method, the deactivation will be performed using the same method.

To deactivate Parallels Mac Management:

- 1 In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / Licenses**.
- 2 Right-click your site in the **Licenses** list and choose **Properties**.
- 3 The **Parallels Mac Management - 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 the Parallels Licensing Server 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 on Parallels My Account. Follow the steps below to learn how to do it.
- 5 You are asked to save the offline deactivation request file. Specify a location and file name and click **Save**.
- 6 You now need to update your license information on Parallels My Account, so the license that you just released can be used to activate a different Parallels Mac Management installation.
- 7 Visit <https://account.parallels.com> and sign in using your email address and password.
- 8 Once signed in, click  next to your user name to open a side menu.
- 9 In the side menu, expand the **Parallels Mac Management** section and click **Offline Activation and Validation**.



- 10** On the **Offline Activation and Validation** page, specify the offline deactivation request file you saved earlier.

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

## CHAPTER 4

# Parallels Mac Client Deployment

Parallels Mac Client is a software for Mac 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 Mac in Configuration Manager.

### In This Chapter

Installation Options Overview .....	58
Installing Parallels Mac Client Using Discovery Methods .....	59
Running Parallels Mac Client Installer on a Mac .....	65
Installing Parallels Mac Client Using a Script.....	66
Push Install or Update Parallels Mac Client.....	67
Configuring the Firewall .....	68
Verifying Parallels Mac Client Deployment .....	69
Updating Parallels Proxy Connection URL.....	69
Uninstalling Parallels Mac Client .....	70
Upgrading Parallels Mac Client .....	70
Using Parallels Mac Client Tools .....	72

## Installation Options Overview

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

- **Parallels Network Discovery** (p. 59). 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. 59). 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. 65). Log into a Mac and manually install Parallels Mac Client on it by running the installation package.
- **Using an installation script** (p. 66). 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. 67). 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 Proxy needs to log into it. In order to do this, the Mac must be configured to accept SSH connections and have an administrator account set up that the Parallels Proxy can use. This can be a domain account (for domain joined Mac computers) or a local account (for either domain joined or non-domain joined 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 OS X 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

Parallels Configuration Manager Proxy will connect to Mac computers over SSH, so you need to enable SSH access on each Mac. To do so:

- 1 On a Mac, 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 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 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.

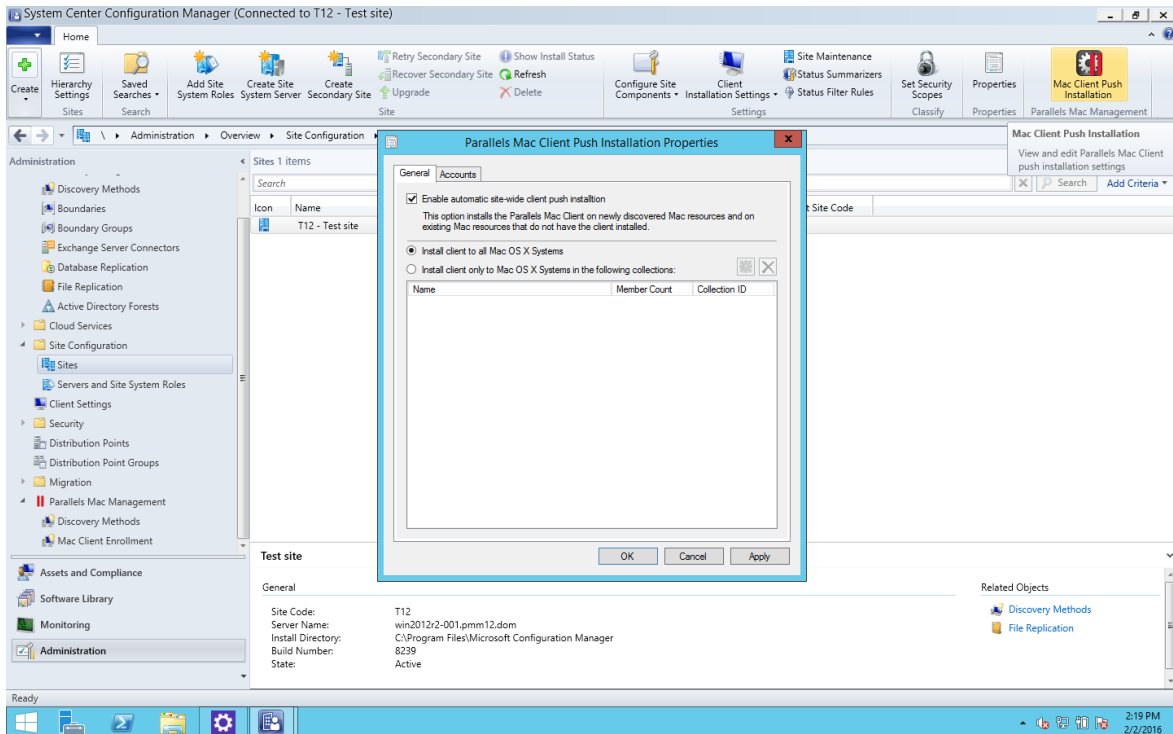
## Configuring Parallels Mac Client Push Installation Properties

Parallels Mac Client push installation properties must be configured, so that Parallels 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. 59) 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 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 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 provides 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. 60) 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. 24).

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 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. 77).

## 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. 60).



## Running Parallels Mac Client Installer on a Mac

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

First, you need to download the Parallels Mac Client installer to the Mac:

- 1 Make sure that the Parallels Configuration Manager Proxy service is installed and running.
- 2 Log into the computer running the Configuration Manager console.
- 3 In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / Mac Client Enrollment**.
- 4 In the **Mac Client Enrollment** list, right-click the **Mac Client installation package download URL** item and then click **Properties** in the context menu.
- 5 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:  
`http://myhost.local:8761/files/pma_agent.dmg`
- 6 The Mac user enters the URL into a Web browser to download the `pma_agent.dmg` image.

To install Parallels Mac Client on the Mac:

- 1 After the `pma_agent.dmg` download is complete, double-click it to open the image.
- 2 In the **Parallels Mac Management for Microsoft SCCM** window, 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 be allowed to administer this Mac.
- 4 When the installation is complete, click **Close** to exit the installation assistant.

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

- 1 Read the information provided on the **Introduction** page and then click **Continue**.
- 2 On the **Authorization** page, enter your organization's domain name (e.g. *Example.CompanyName.com*), your domain username (e.g. *UserName*) and password. Please note that the username should contain the domain logon name only. It should NOT contain the domain name separated by a slash or the "@" sign.
- 3 Click **Continue**.
- 4 If you receive an error, click the **Try Again** button 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. 70).

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

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

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

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

## 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 http://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. 60).
  - **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. 59) 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 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 answers "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. 62).

To see if a Mac has Parallels Mac Client installed and running on it, 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 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 OS X 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. 42).

## 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.

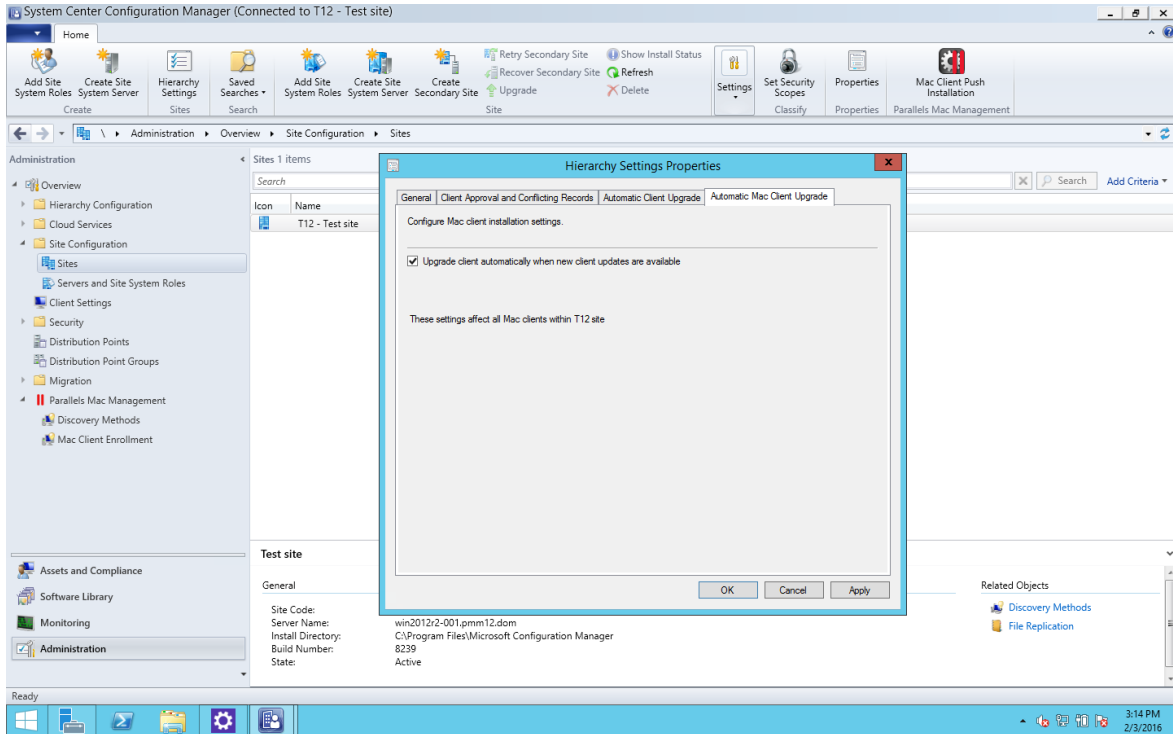
Each method is described in detail in the following subsections.

### 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. 113) 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. 70). 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

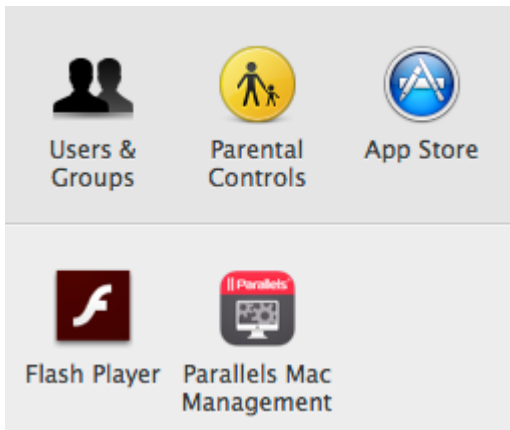
The Parallels Mac Client properties window allows you to see the Mac Client properties, send a problem report, and retrieve policies from Configuration Manager.

To open the Parallels Mac Client properties window:

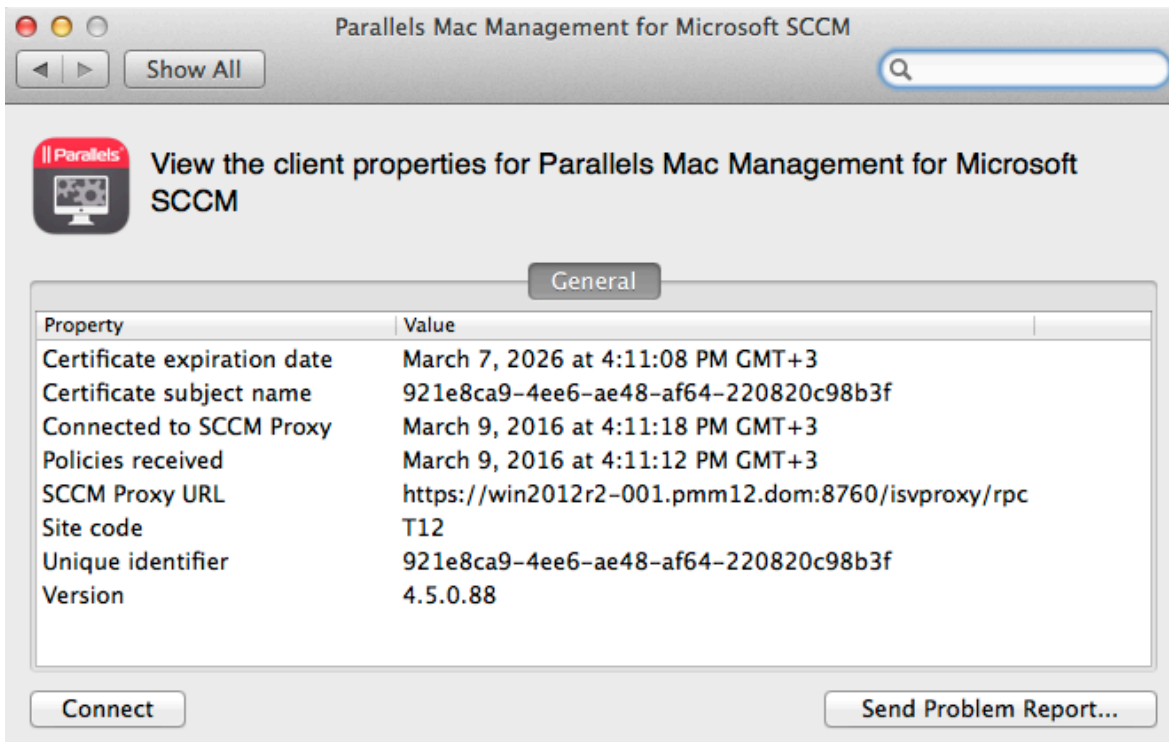
- 1 In OS X, open System Preferences.



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



- 3 The client properties window opens.



- 4 The **General** box contains the following Parallels Mac Client properties:
- **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 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 buttons at the bottom of the window are:

- **Connect.** When clicked, connects to the Parallels Configuration Manager Proxy and downloads the latest policy from Configuration Manager. For more information, please see **Initiating Policy Retrieval** below.
- **Send Problem Report.** Click this button to send a problem report to Parallels Support. For more information, please see **Sending Problem Reports from Parallels Mac Client** below.

## Initiating Policy Retrieval from a Mac

Parallels Mac Client downloads its policy from Configuration Manager on a schedule. There may be a need to download the latest policy before the scheduled download occurs. Parallels Mac Client provides you with this ability.

### Using the Client Properties Dialog to Initiate Policy Retrieval

To initiate policy retrieval:

- 1 In System Preferences, click the **Parallels Mac Management** icon (or click **View > Parallels Mac Management for Microsoft SCCM**).
- 2 Click the **Connect** button to initiate policy retrieval. A text will appear next to the button informing you of the progress.
- 3 If the connection to Configuration Manager was successful, the text will say "Connected" and will specify how many policy updates have been received.
- 4 The **Policies received** property in the **General** list box will be updated if at least one update has been received. The property will remain unchanged if no updates are available.

### 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 failed:

```
<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 Problem Reports From Parallels Mac Client

If you are experiencing a problem with Parallels Mac Client, you can obtain a problem report and then send it to Parallels Support. To obtain a report:

- 1 In System Preferences, click the **Parallels Mac Management** icon (or click **View > Parallels Mac Management for Microsoft SCCM**).
- 2 Click the **Send Problem Report** button to obtain a 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.

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.
- 4 The **Send Problem Report** dialog opens. This is the same dialog as the one that opens when you click the **Send Problem Report** button described above.

## CHAPTER 5

# Using Parallels Mac Management for Microsoft SCCM

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

### In This Chapter

The Configuration Manager Admin Console .....	77
Device Collections in Parallels Mac Management .....	77
Hardware and Software Inventory .....	78
Compliance Settings .....	81
Deploying Software via SCCM Package Deployment.....	113
Deploying Software via SCCM Application Deployment .....	118
Operating System Deployment .....	127
OS X Software Update Management .....	154
Executing Scripts on Mac Computers .....	172
Apple Device Enrollment Program.....	173
Deploying Parallels Desktop to Mac Computers .....	181
Deploying SCCM Client in Windows Running in a Virtual Machine.....	184
Providing Remote Assistance to Mac Users .....	186
Problem Reporting and Monitoring .....	187
Initiating Policy Retrieval from SCCM.....	191

## The Configuration Manager Admin Console

Parallels Mac Management for Microsoft SCCM extends the Configuration Manager console with support for Mac computers. The Configuration Manager console is the primary interface to manage Mac computers in your enterprise. After you install Parallels Mac Management, the Mac-specific GUI elements are integrated into the console allowing you to accomplish Mac management tasks.

## 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. 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 OS X 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.

**Unknown Mac OS X Systems** is a special collection to which you deploy task sequences as part of OS X deployment. The collection is not supposed to contain any devices. For more information, see **Operating System Deployment** (p. 127).

## Hardware and Software Inventory

Hardware and software inventory information is collected from enrolled Mac computers on a schedule and is saved in the Configuration Manager database. In addition to scheduled inventory gathering, you can request an inventory update manually.

To view the collected hardware and software inventory:

- 1 Open the collection containing Mac resources (e.g. **All Mac OS X Systems**).
- 2 Right-click a Mac of interest 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.

To request an unscheduled inventory update:

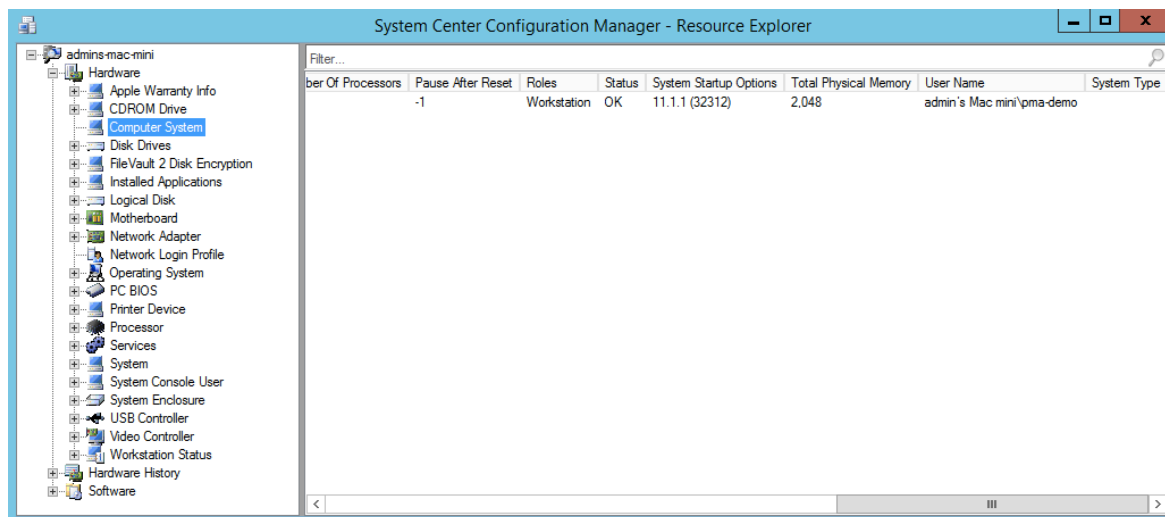
- 1 In the Configuration Manager console, open the device collection containing your Mac computers.
- 2 Select one or more Mac computers (or the entire collection), then right-click on a selection and choose **Request Inventory Update**.
- 3 A dialog opens displaying the progress (number of processed 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.

## Reporting User Logon Information

Mac user logon details are reported by the 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

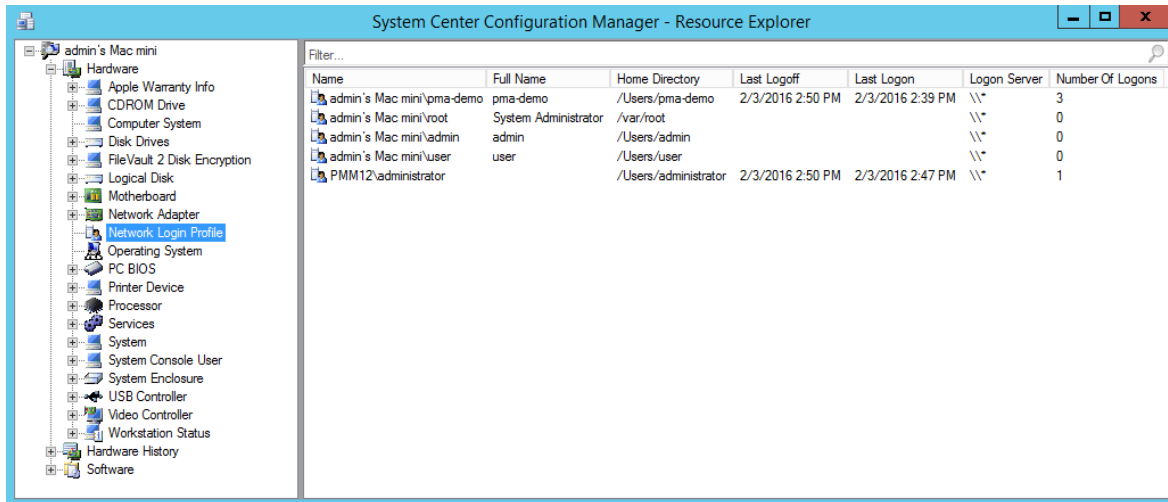
This node reports general computer information along with names of currently logged on users. The **User Name** column contains the user name in the `qualifier\account` format, where qualifier is the computer's NetBIOS name or a domain name. If there's no currently logged on user, the column will contain `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. On the left is a tree view of system resources, with 'Network Login Profile' selected. The main pane displays 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

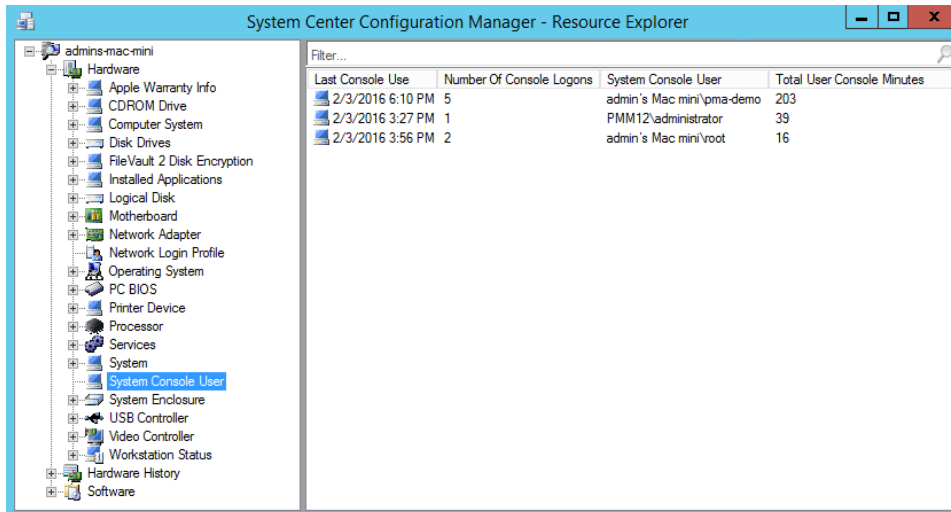
### System Console User

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 OS X 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. On the left, a tree view shows the hierarchy of system resources, with 'System Console User' selected. The main pane displays 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

## Compliance Settings

Compliance settings is a set of tools that allow you to assess the compliance of Mac computers in your organization with regard to whether OS X is configured correctly, volumes on Mac computers are encrypted, and whether Parallels Desktop (if installed) is configured properly. Compliance is evaluated by creating a configuration baseline that contains configuration items that you want to evaluate.

This section contains information about how to create configuration items, set up a configuration baseline, and then deploy the baseline to a device collection.

## Deploying OS X Configuration Profile

Parallels Mac Management for Microsoft SCCM provides you with the functionality to monitor and enforce OS X configuration settings on Mac computers.

First, you need to create an OS X configuration profile using one of the following options:

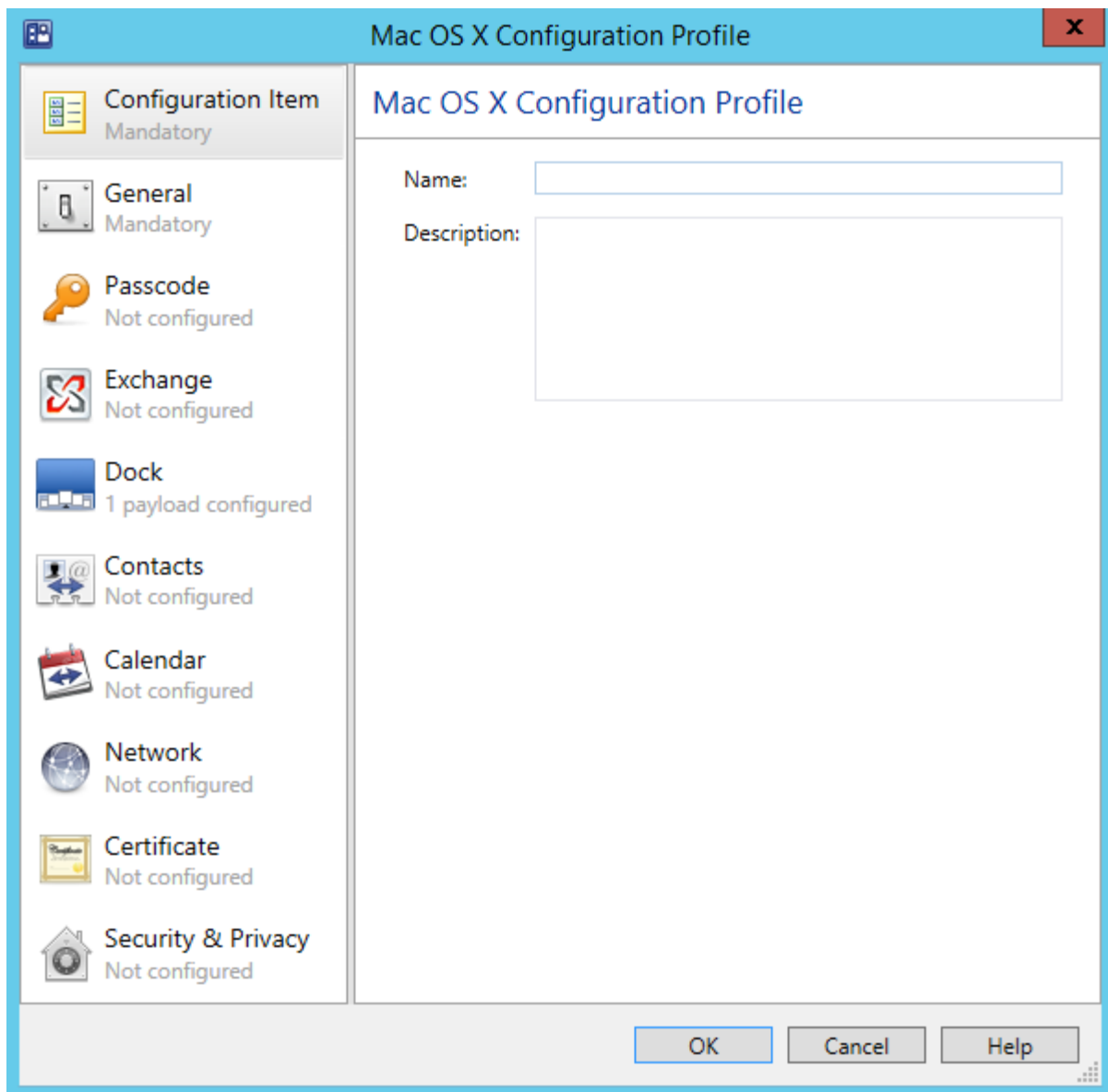
- Using a custom OS X profile editor. The editor is provided by Parallels Mac Management and is integrated into the Configuration Manager console.
- Creating a profile from a `.mobileconfig` file that can be created using the OS X Server's Profile Manager.

Read on to learn how use the options above.

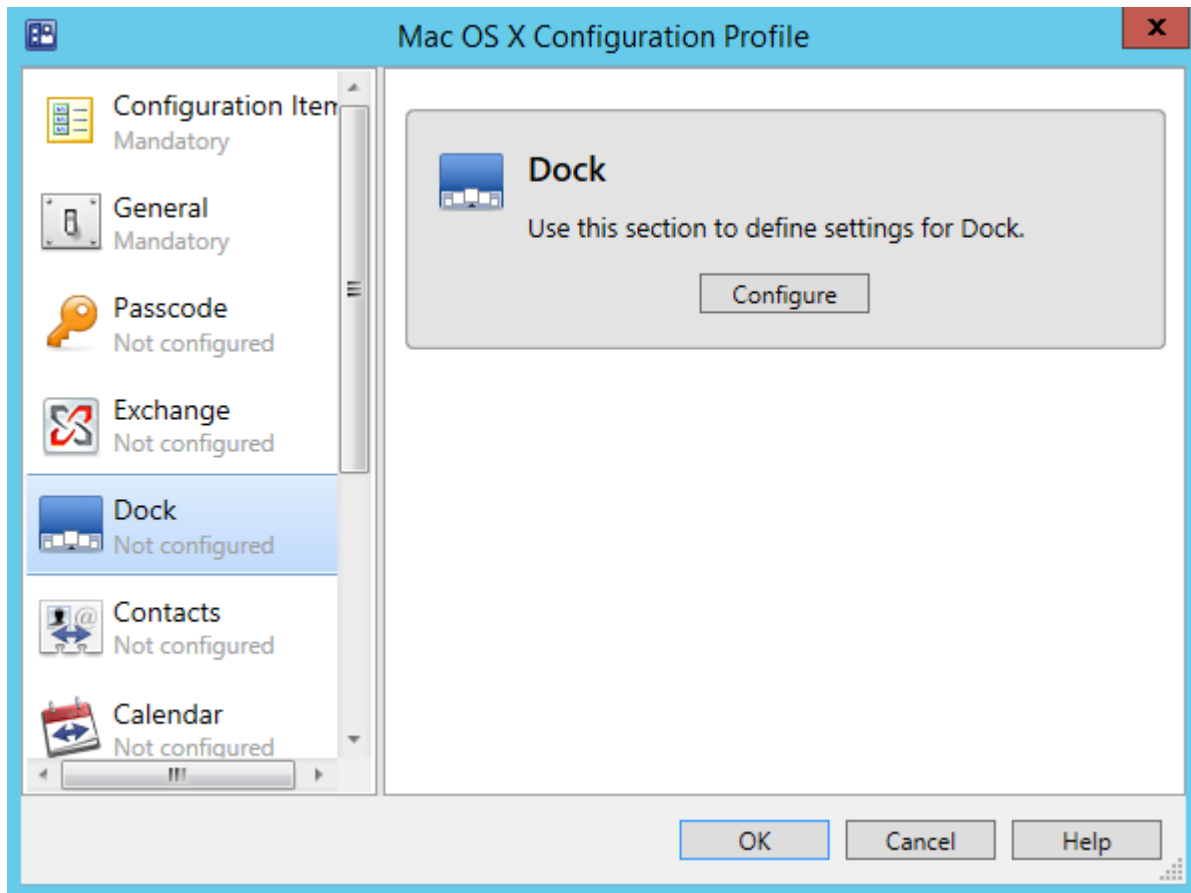
## Creating OS X Configuration Profile Using the Profile Editor

To create an OS X configuration profile using the built-in profile editor:

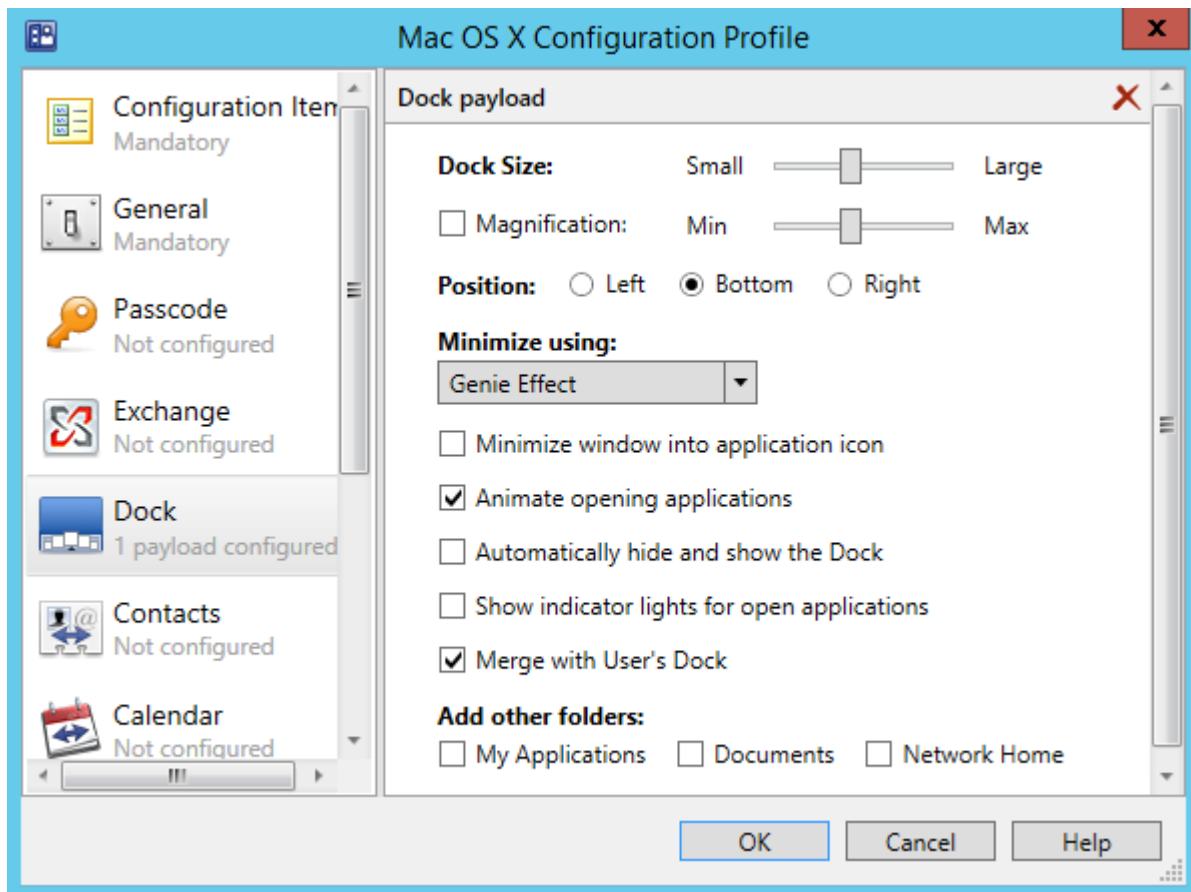
- 1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings / Configuration Items**.
- 2 Right-click **Configuration Items**, point to **Create Parallels Configuration Item**, and then click **Mac OS X Configuration Profile**.
- 3 The **Mac OS X Configuration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



The left pane of the dialog contains the list of payloads. The right pane contains the 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 Mac OS X Profile Settings

When setting up an OS X 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 OS X 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 OS X 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 OS X 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 an OS X configuration profile using the Profile Manager, you 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.

## Payload 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 OS X system preferences. The following list provides a general description of each payload. For the complete information about creating an OS X 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.

### 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. 111) for more information.

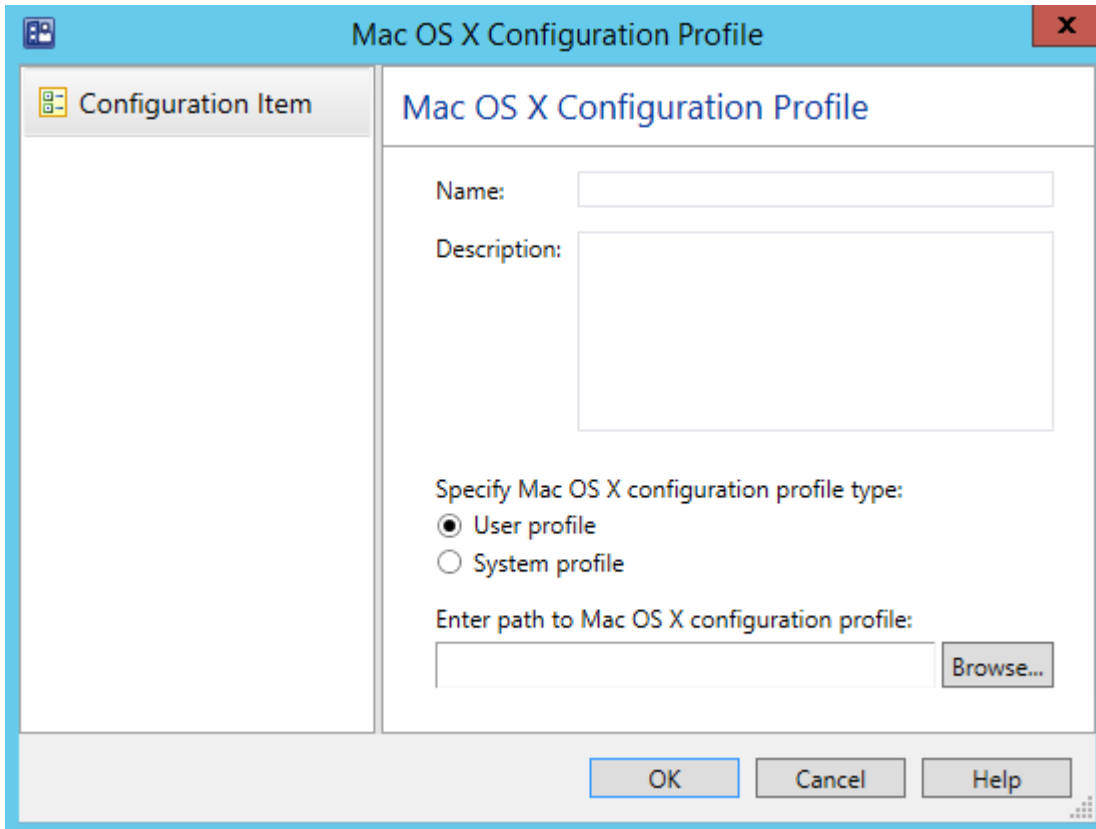
### Creating OS X Configuration Profile from .mobileconfig File

Alternately, you can create an OS X configuration profile from a `.mobileconfig` file that was created using OS X Server Profile Manager. You can use this approach if you already have this file or if you prefer to use Profile Manager for any reason. For supplementary information, see **Using Profile Manager** at the end of this section.

To create a Mac OS X Configuration Profile configuration item from a `.mobileconfig` file:

- 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 **Mac OS X Configuration Profile from File**.

- 3 The **Mac OS X Configuration Profile** dialog opens.



- 4 Enter a configuration item name and description.
- 5 Select the profile type from the following options:
- **User profile.** Select this 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 this option when you want to install the configuration profile as `root`.
- 6 Click the **Browse** button, select a `.mobileconfig` file, and click **Open**.
- 7 Click **OK** to save the configuration item. 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.
- 8 To edit the profile, right-click it and select **Edit Parallels Configuration Item** from the context menu. 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 into a file, edit it in an external application (e.g. Profile Manager) and then import it back into the configuration item.

The import operation will perform 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. 111) for more information.

### Using Profile Manager

Profile Manager is a tool provided by Apple that allows you to create an OS X configuration profile (an XML file) containing the configuration settings that your organization requires. The configuration profile can then be deployed to Mac computers to configure them using the specified settings.

**Note:** You need a Mac with an OS X Server installed to use the Profile Manager.

To create a configuration profile using Profile Manager:

- 1 Log into your OS X Server.
- 2 Open Services and find "Profile Manager" in the service list.
- 3 Click the **On** button to start the service.
- 4 In a Web browser, enter the URL for Profile Manager (e.g. `http://my_server.com/profilemanager/`).
- 5 Log into Profile Manager using an administrator account.
- 6 In the Library, select the profile and click the **Edit** button to edit it. For a complete information about individual profile settings, see the documentation that comes with Profile Manager.

When setting up a 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. 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 the actual value. If a payload contains this tag in at least one field, the 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 OS X side. You can enter the `%user_interaction_required%` tag into any field that you want a user to set manually.



- 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 required settings are missing), the interactive mode will be used and the user will have to specify them manually.

In the interactive mode, a standard System Preferences dialog will be opened in OS X 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 are invalid, 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 an appropriate report is sent to the administrator.

When you save the configuration profile, Profile Manager creates a file with the ".mobileconfig" extension. The file is an XML document containing the OS X configuration settings that you specified. Copy the file to a location where the Configuration Manager console can access it (e.g. a directory on the server running the Configuration Manager console).

## 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. 198). 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. 90)
- **FileVault 2 Encryption with Personal Recovery Key** (p. 97)

## 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 (the command is available in OS X 10.7.2 or later):

```
$ 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:

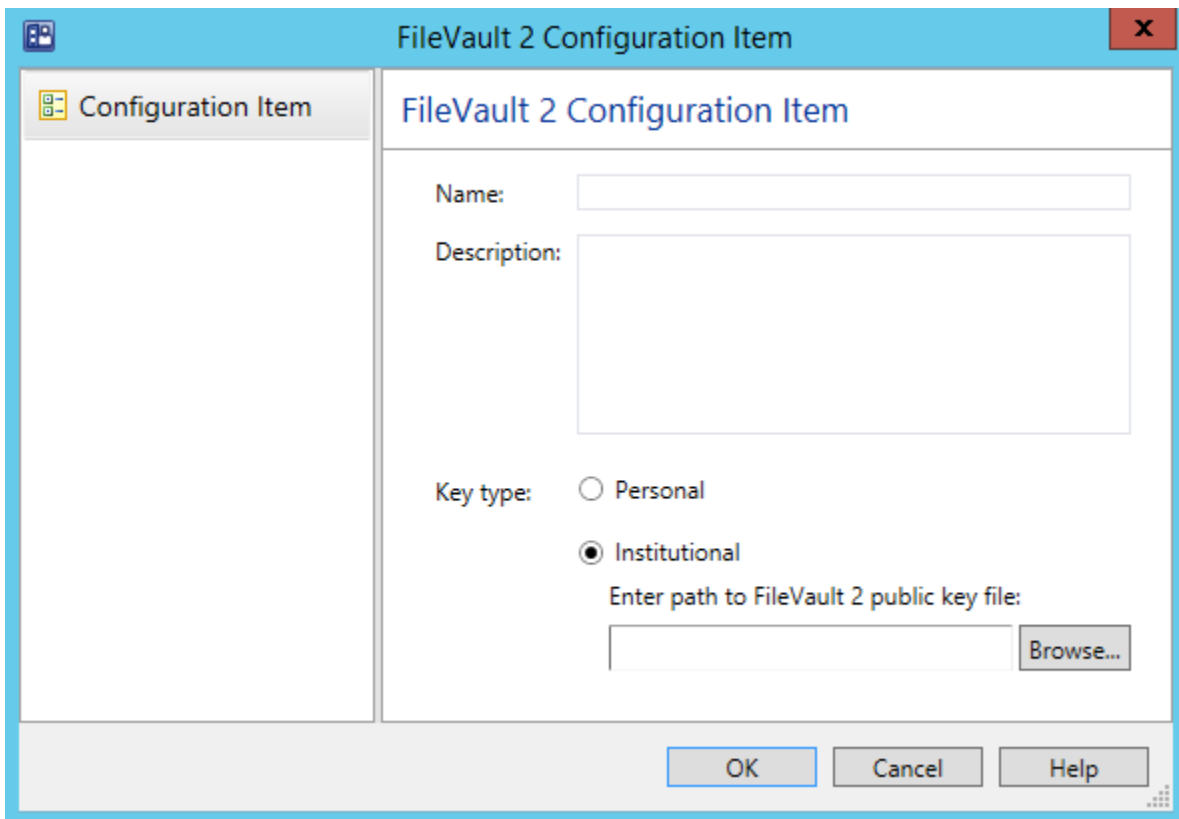
- 1 Run the Keychain Access application (Applications/Utilities).
- 2 In the **Keychain Access** window, select "FileVaultMaster" keychain in the **Keychains** panel.
- 3 In the right pane, right-click the "FileVault Recovery Key" certificate and then click **Export** in the context menu.
- 4 Choose 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

o 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. 97).

- 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**.

The screenshot shows a Windows-style dialog box titled "FileVault 2 Configuration Item". On the left is a sidebar with a "Configuration Item" icon and label. The main area is titled "FileVault 2 Configuration Item" and contains the following fields: "Name:" with a text input box, "Description:" with a larger text area, "Key type:" with two radio buttons labeled "Personal" and "Institutional" (the latter is selected), and "Enter path to FileVault 2 public key file:" with a text input box and a "Browse..." button. At the bottom are "OK", "Cancel", and "Help" buttons.

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

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a device collection. See **Deploying Configuration Baseline** (p. 111) 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 message box 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 OS X 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 OS X 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 an OS X 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 OS X 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. 198). 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).
  - **LVGUID**. 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. 198). 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 / 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 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.

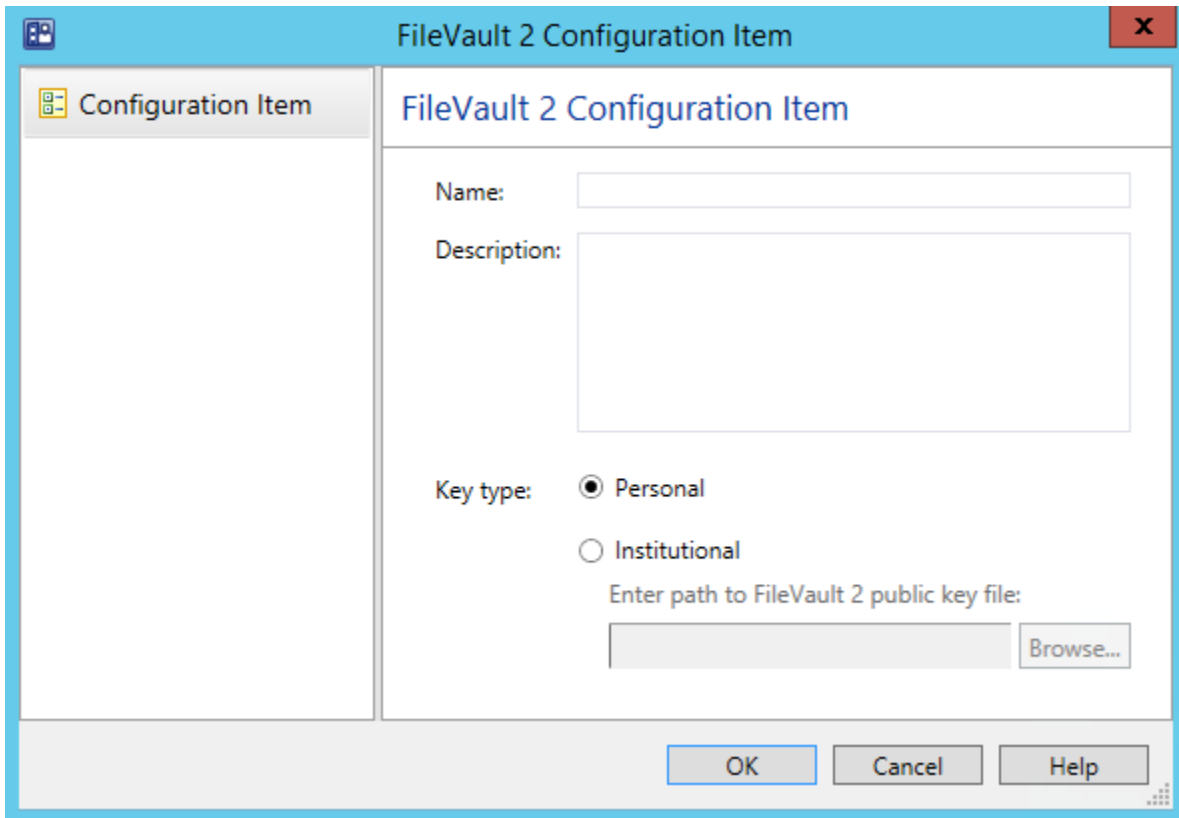
### Creating FileVault 2 Configuration Item

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. 90).

- 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**.

The image shows a Windows-style dialog box titled "FileVault 2 Configuration Item". On the left is a sidebar with a "Configuration Item" icon and label. The main area is titled "FileVault 2 Configuration Item" and contains the following fields: a "Name:" text box, a "Description:" text area, a "Key type:" section with two radio buttons ("Personal" which is selected, and "Institutional"), and an "Enter path to FileVault 2 public key file:" section with a text box and a "Browse..." button. At the bottom are "OK", "Cancel", and "Help" buttons.

- 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. 111) 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 message box 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 OS X 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 OS X 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 an OS X 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 OS X 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. 198) 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).
  - **LVGUID.** 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. 95).

### *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. 198). 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:

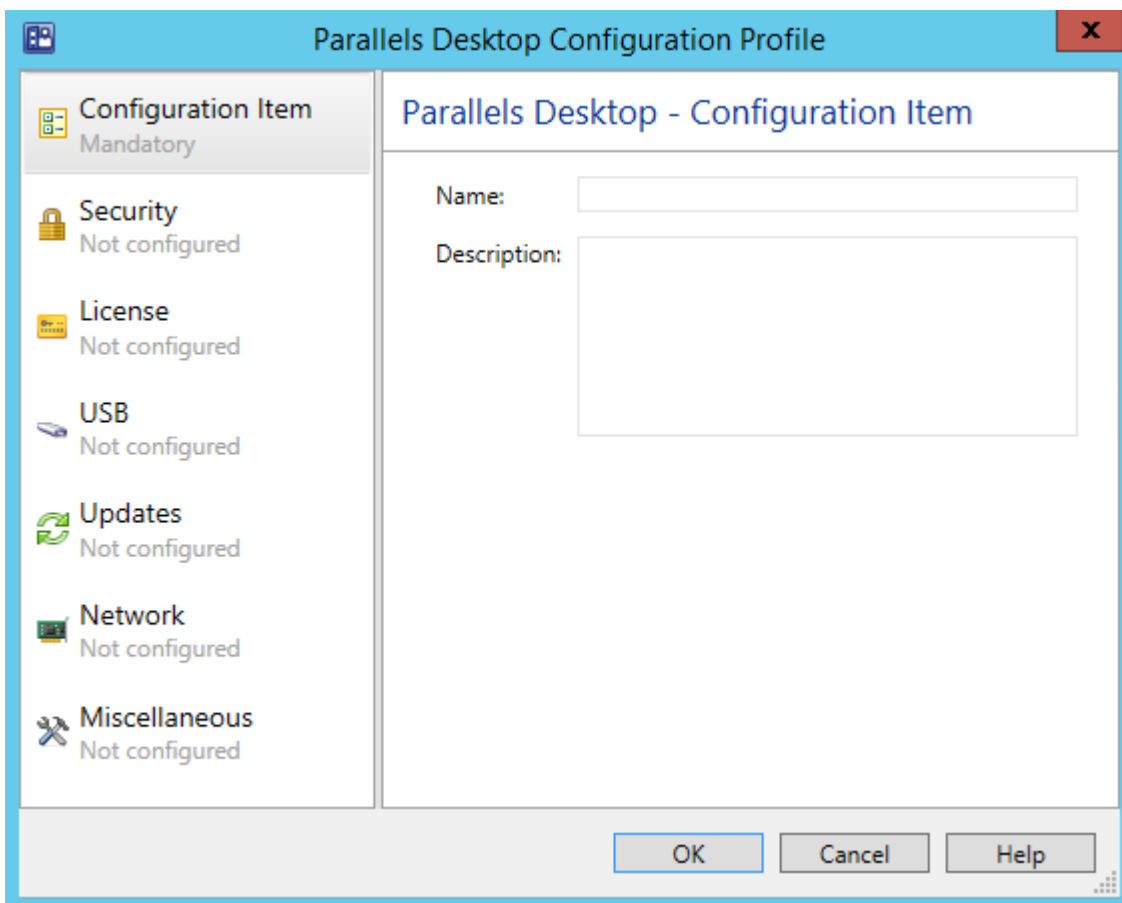
```
$ diskutil cs decryptVolume UUID -passphrase recoverykey
```

## 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 then click **Edit Parallels Configuration Item** in 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. 111) for more information.

## Enforcing Parallels Desktop VM Settings

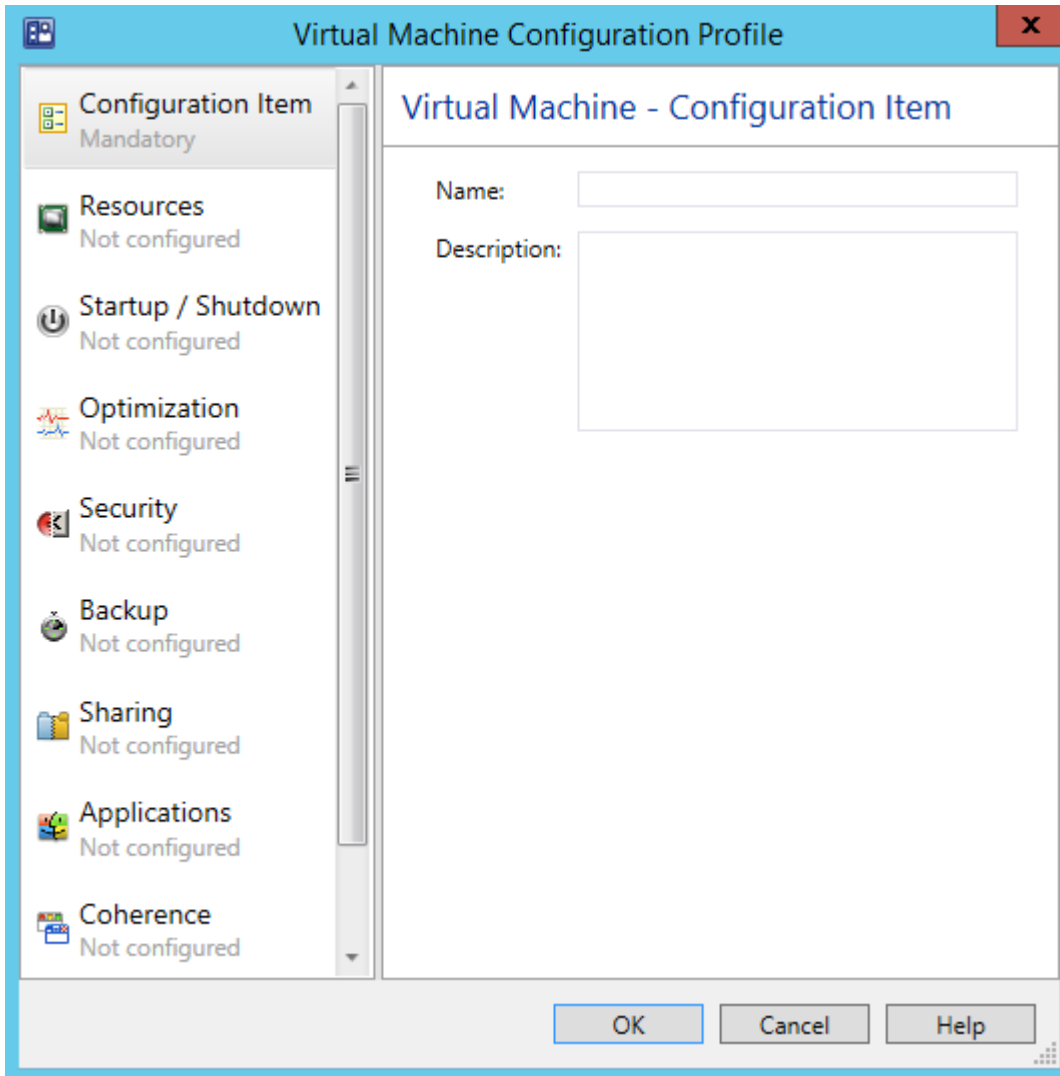
A Parallels Desktop virtual machine has numerous configuration options that can be customized according to your organization requirements. To monitor Mac computers for virtual machine configuration compliance you need to create a virtual machine configuration item specifying the desired configuration 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 then click **Edit Parallels Configuration Item** in 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. 111) 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 OS X.

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. 107)
- Create a discovery script (p. 109)
- Create a remediation script (p. 109)
- Specify the script interpreter to be used (p. 110)
- Define Compliance Rules (p. 111)

## 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 the OS X 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 OS X version, you can create multiple Mac collections based on the OS X 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. 109) 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. 109) 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. 111) 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. 111) 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. 107).

The script can be written in any scripting language supported by OS X, such as Bash, Python, Apple Script, etc. See **Specifying Script Interpreter** (p. 110) 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. 109), 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 OS X with root privileges. Please also note that you cannot access OS X 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. 107).

The script can be written in any scripting language supported by OS X, such as Bash, Python, Apple Script, etc. See **Specifying Script Interpreter** (p. 110) 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 OS X with root privileges. Please also note that you cannot access OS X 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. 107).

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 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 in the list. Click **OK**.
- 4 When 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. To delete a baseline, right-click it and then click **Delete**.

## Receiving Compliance Settings Reports

Corporate policies can be enforced on Mac computers using the Compliance Settings functionality. Parallels Mac Management for Microsoft SCCM provides a reporting functionality that allows you to evaluate the results of enforcing corporate policies on individual Mac computers.

To enforce a policy, the IT administrator creates a configuration item, adds it to a baseline, and then deploys the baseline to a Mac collection. When the baseline runs, each configuration item is applied to a Mac and modifies a corresponding configuration according to the rules that it contains.

After the configuration changes are made to the Mac, the following reports are generated on the Mac side:

- A report for each configuration item applied to a Mac (a configuration baseline can contain more than one configuration item, so a report is generated for each individual item).
- A summary report for the baseline after all configuration items are applied to a Mac.

As soon as a report is generated, the Parallels Mac Client sends it to the Configuration Manager Proxy, which 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 cannot establish a connection with the Configuration Manager Proxy, the reports are saved locally on the Mac 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 and the configuration item (or configuration baseline) together with the following items describing the results of the Mac compliance evaluation:

- **Compliance State** — describes whether the Mac 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 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. 118).

## 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.

## 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**.

## The Program Type Page

Select the **Standard program** option and click **Next**.

## 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 OS X shell command and is executed as-is. For example, to run the OS X 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 (OS X 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 OS X 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**.

## 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 OS X 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 a 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 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 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 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 software will be advertised to Mac computers in the specified collection and will be distributed to them according to the schedule that you specified.

## Viewing the Package Status

While software distribution is in progress, the Parallels Mac Client running on target Mac computers 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. 113), 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.

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. 118)
- 2 Prepare a Mac application for Configuration Manager (p. 119)
- 3 Create a Configuration Manager application (p. 119)
- 4 Configure the Deployment Type (p. 121)
- 5 Deploy the application (p. 123)

The remaining 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. 124)
- Using Parallels Application Portal (p. 125)

### 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 an OS X 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. 125).

## Prepare a Mac Application for Configuration Manager

Before you can deploy a native OS X software package (.app, .dmg etc.) in SCCM, you must use the **CMAAppUtil** tool to convert it to the **.cmmac** format that Configuration Manager understands.

The **CMAAppUtil** tool is provided by Microsoft:

- 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=47719>
- 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 an OS X application package to the **.cmmac** format:

- 1 Copy the OS X 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** If the application that you are creating is an upgrade or a replacement for an existing application in the Parallels Application Portal, then you can specify a supersedence relationship on the **Supersedence** tab page. Select the **Allow users to see deployments for this an all applications that it supersedes...** option if you want to display all versions of the application in the Application Portal. If the option is cleared, only the top application will be shown.
- 4** 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 following instructions 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. You have to find out what the actual uninstallation command line for a given application is yourself.

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 OS X 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 OS X version.

To specify the OS X 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 OS X tree, select one or more OS X versions. If you check **Select all**, all existing and all future OS X 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'll 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** — This option is similar to the **Display in Software Center and show all notifications** option (above) with one exception: the installer will run in the background, so the user will have no control over the installation process. The user will still be given a choice to install the application or to postpone the installation, and to restart or postpone restarting the Mac if it is required.
- **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

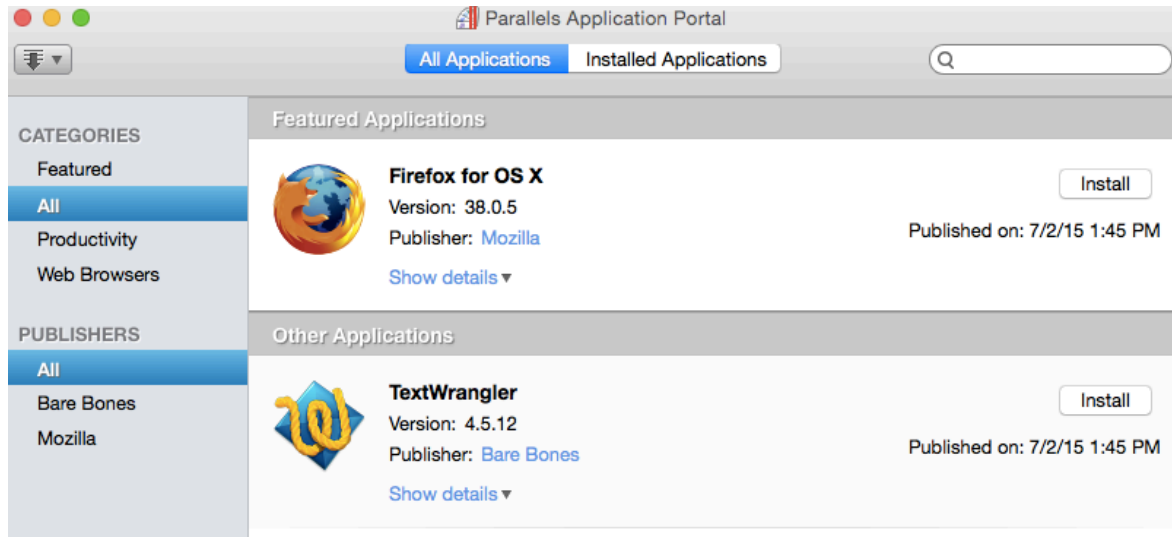
If the installation type was specified as silent (the **Deploy Software Wizard** | **User Experience** page | **Hide in Software Center and all notifications** option was selected), no message asking the user to install the application will be displayed, and the installation will be performed silently 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 an OS X 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. 118).

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. 120). 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. 121).

## Operating System Deployment

Parallels Mac Management provides you with the ability to deploy OS X on Mac computers. To deploy OS X on Mac computers, you need to do the following:

- 1 Capture an OS X boot image by using the image builder utility included with Parallels Mac Management.
- 2 Capture an OS X system image using a task sequence or the image builder utility.
- 3 Distribute the boot image and the system image to a distribution point.
- 4 Create a task sequence that will deploy the OS X system image and optionally execute other steps, which include:
  - Join Domain — adds a Mac to a domain after an OS X image has been deployed on it.
  - Install Package — allows you to install a software package on a Mac.
  - Set Hostname — sets a Mac's hostname.
  - Apply Configuration Profile — allows you to apply an OS X configuration profile to a Mac.
  - Execute Script — allows you to execute a script of your choice on a Mac.
- 5 Deploy the task sequence to a collection of Mac computers.
- 6 Boot a Mac from the network and execute the task sequence on it.
- 7 When you deploy OS X on a Mac, the task sequence will also automatically install Parallels Mac Client on it and will enroll the Mac in SCCM.

## Prerequisites for Deploying OS X on Mac Computers

Before using the OS X 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. 14).

- 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: <http://kb.parallels.com/118518>.
- The reference Mac computers that will be used to capture OS X images must have a Recovery HD partition.

## Capturing an OS X Boot Image

An OS X 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.

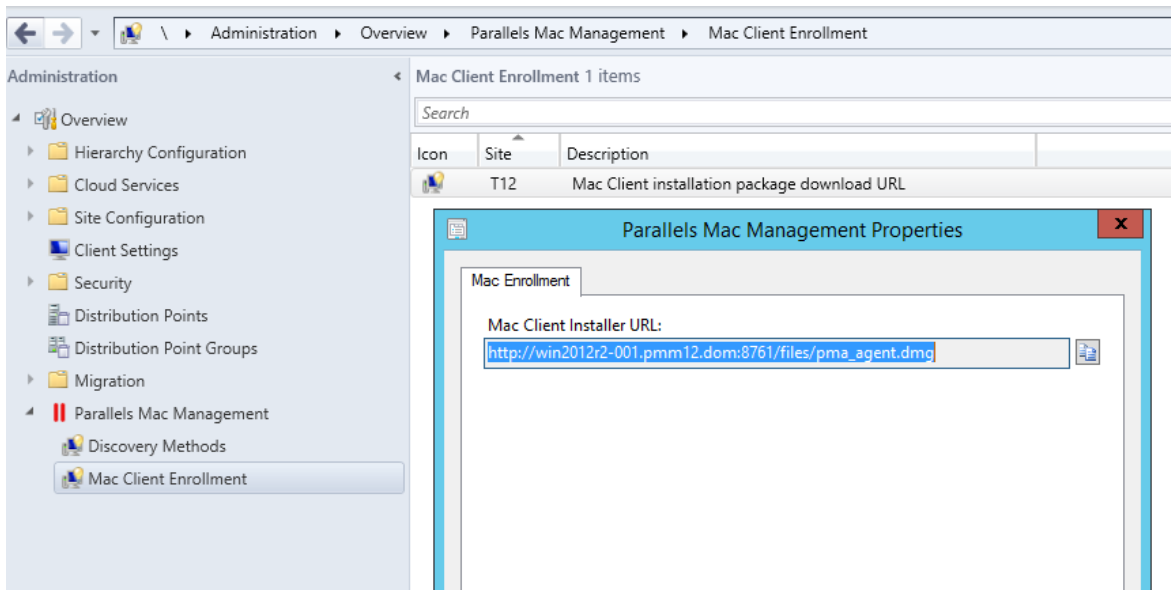
### OS X Version Support

The reference Mac must be running OS X 10.9 or later. Older versions of OS X are not supported.

### Capture an OS X Boot Image

To capture an OS X 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 OS X.

## Using the Image Builder Utility

To use `PmmOsdImageBuilder.dmg` utility to capture a NetBoot image, do the following:

- 1 Open Terminal and change directory to the `PmmOsdImageBuilder.dmg` image mount point (e.g. `/Volumes/Parallels OSD Image Builder 5.0.xxxx.yyyyyy`).
- 2 Execute the following command in Terminal:

```
sudo ./pmm_osd_image_builder netboot -n [output-dir] --ntp-servers  
[ntp_servers] --ssh-authkeys [ssh_keys_file] --ignore-version-  
mismatch
```

The parameters in the command above are:

`-n [output-dir]` — The name of a directory where you want the boot image to be created.

`--ntp-servers [ntp_servers]` — (optional) Comma-separated NTP (Network Time Protocol) server hostnames or IP addresses. The time on a Mac will be synchronized with your domain controller using the specified server(s). If the parameter is omitted, no time synchronization will be performed, in which case you need to use other means to make sure that the time is in sync.

`--ssh-authkeys [ssh_keys_file]` — (optional) A path to a file with an SSH public key in the `authorized_keys` format. The key will be installed in the NetBoot image to allow root SSH access to a Mac when it's booted from the network. If this parameter is omitted, no SSH access to a Mac will be available. For more info, see <http://kb.parallels.com/123466>.

`--ignore-version-mismatch` — (optional) A flag to ignore OS X version mismatch between the active boot partition and the recovery partition. The OS X version must be the same on both partitions. If there's a version mismatch and this parameter is not included, you will receive an error. In such a case you'll have to either upgrade OS X on the recovery partition or use a different Mac. If you include this parameter, the error will be ignored and the image will be created, but doing so may result in a malfunction of the resulting boot image. If you don't know whether the OS X versions match on the two partitions, run the utility first without including the parameter. If you receive the error, you'll know that they don't, so you can take appropriate actions.

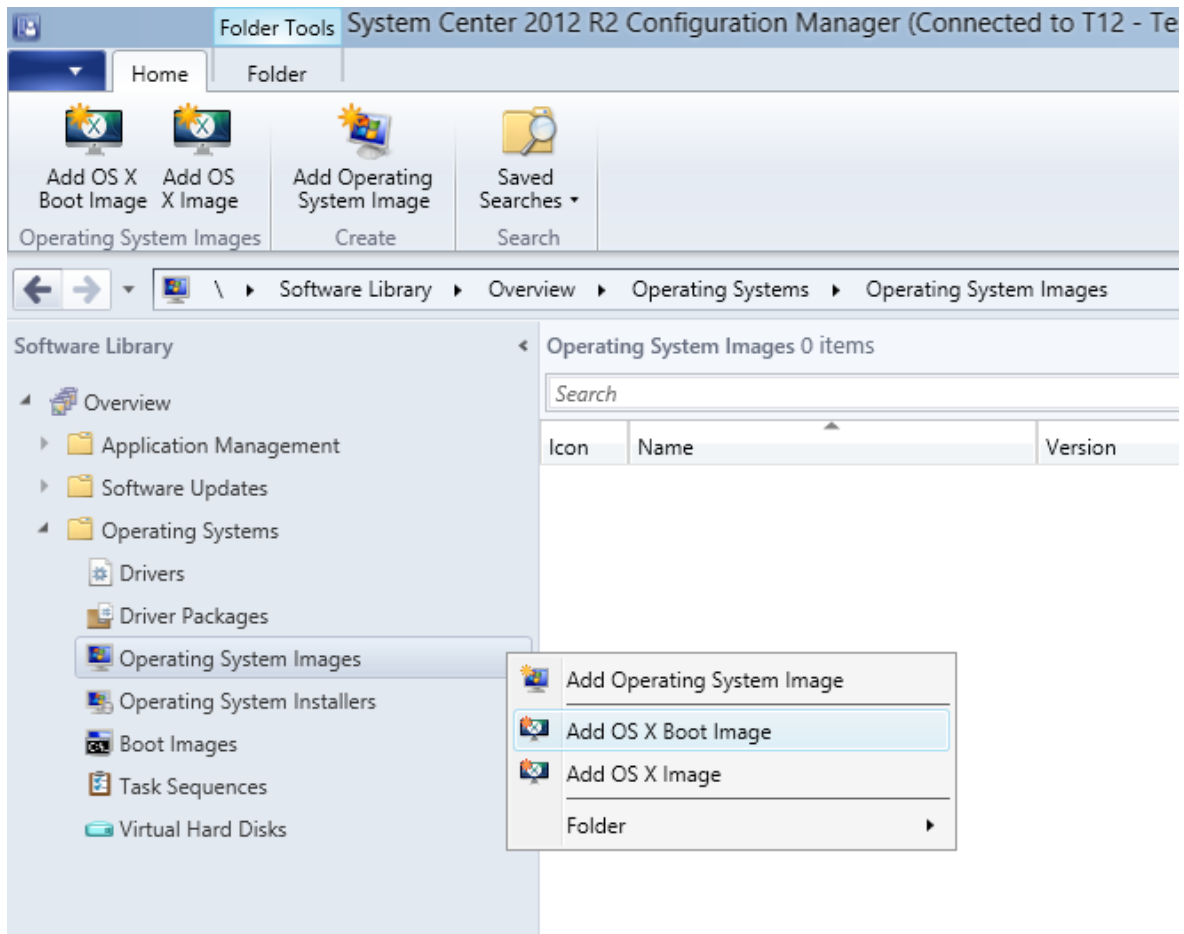
- 3 Copy the entire resulting `[output-dir]` directory to a location on the computer running the Configuration Manager console, so you can add it later to SCCM.

## Add the OS X Boot Image to Configuration Manager

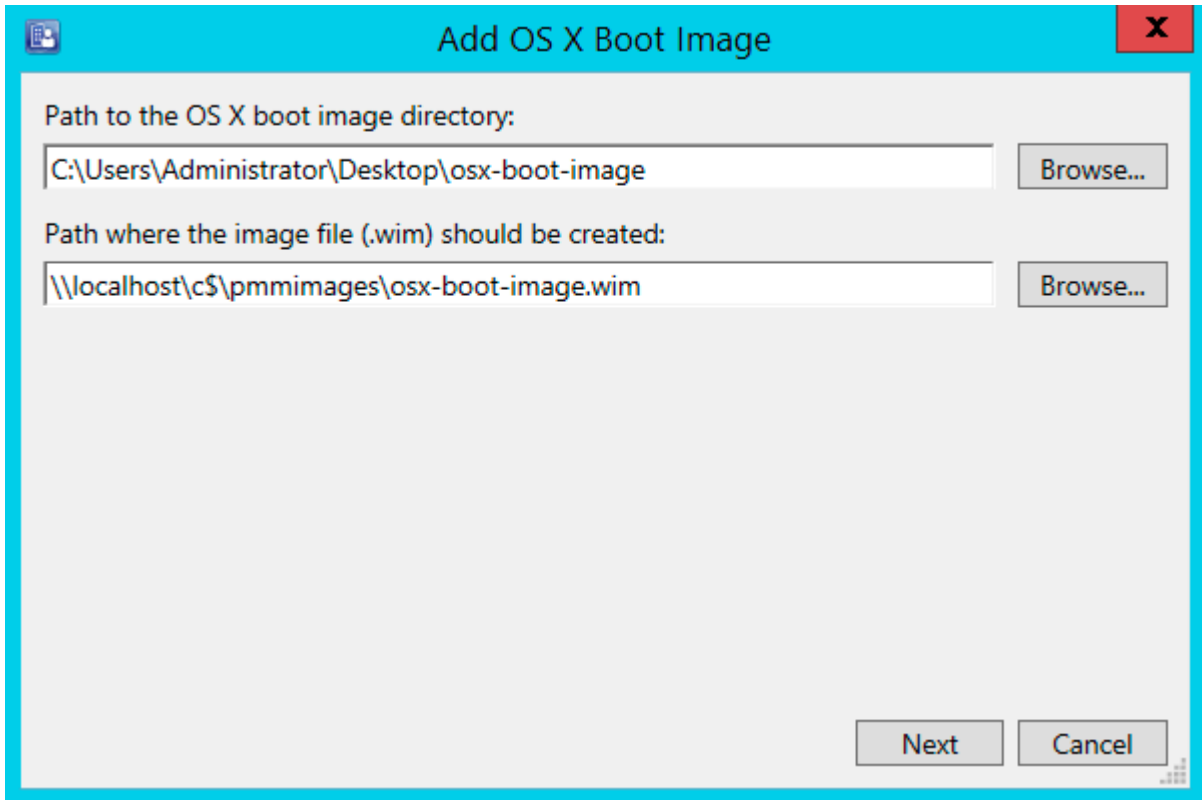
To add the OS X boot image to Configuration Manager, do the following:

- 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.



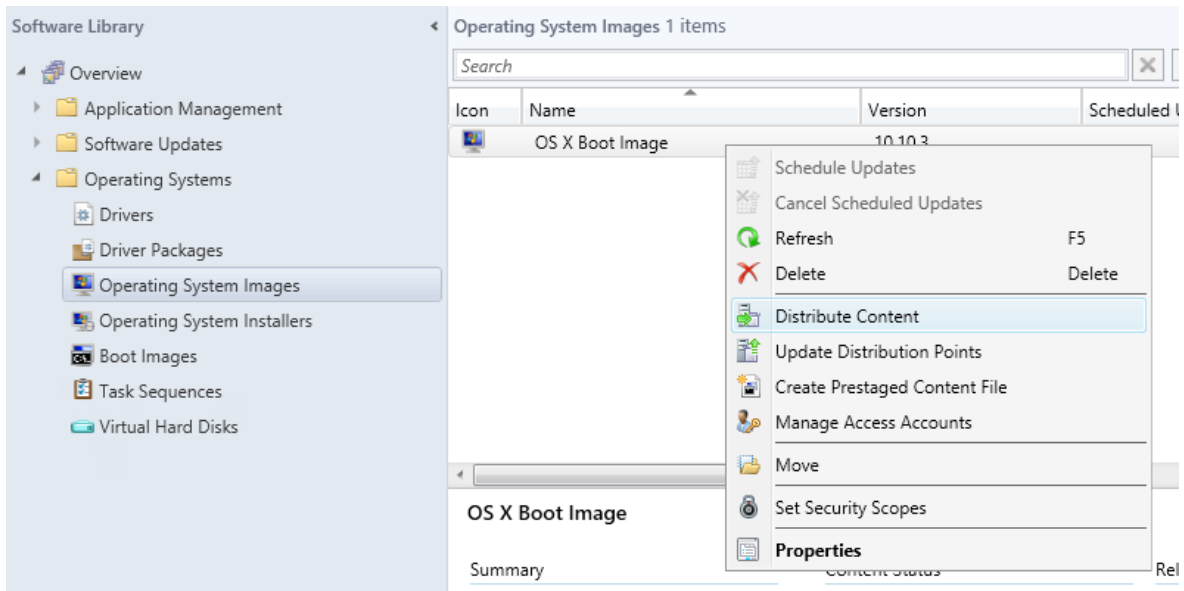
- 4 In the **Path to the OS X boot image directory** field, specify the path to the OS X boot image folder. The other field should contain name and path where you want the image file (.wim) to be created.
- 5 Click **Next**.
- 6 Specify an OS X image name and version and click **Next**.
- 7 Wait for the image to be converted to the .wim format.
- 8 Click **Finish**.

## Distribute Content of the OS X Boot Image

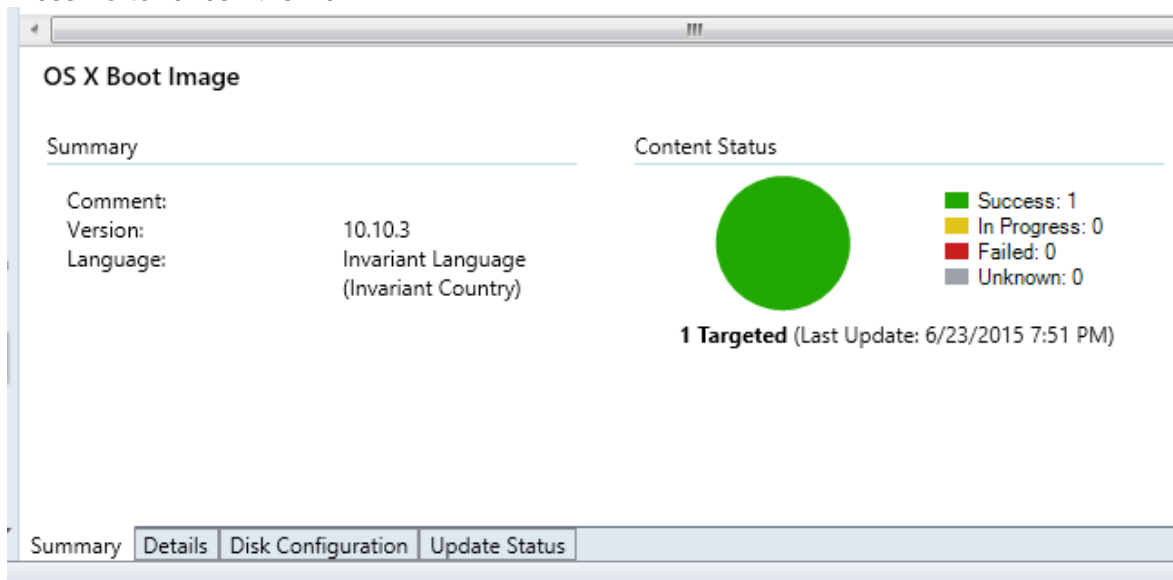
The OS X boot image must now be distributed to the computer running the Parallels NetBoot server.

To distribute the image:

- 1 In the Configuration Manager console, right-click the OS X 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 OS X Boot Image Deployment

To verify that the OS X boot image has been deployed successfully, log into a Mac connected to your network and open **System Preferences > Startup Disk**. The OS X boot image should be included in the **Select the system you want to use to start up your computer** list.

## Capturing an OS X System Image

Parallels Mac Management provides you with two methods that can be used to capture an OS X system image:

- Using a task sequence. (p. 133) 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. 135). 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 an OS X Image Using a Task Sequence

An OS X 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 an OS X system image, you need a Mac computer with OS X 10.8 or later 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 an OS X boot image that you created with Parallels Mac Management v4.0 or earlier, you MUST 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 an OS X System Image

To create a task sequence for capturing an OS X 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 OS X 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 OS X 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 OS X installed.	/dev/disk0s2	INTERNAL

## Capture an OS X Image

To capture an OS X 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 OS X 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. 149) and **Running a Task Sequence on a Mac** (p. 150).

## Capturing an OS X Image Using the Image Builder Utility

An OS X 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.

## OS X Version Support

The source partition on a reference Mac must have OS X 10.8 or a later version installed. Older versions of OS X are not supported.

## Boot a Reference Mac From a Different Partition

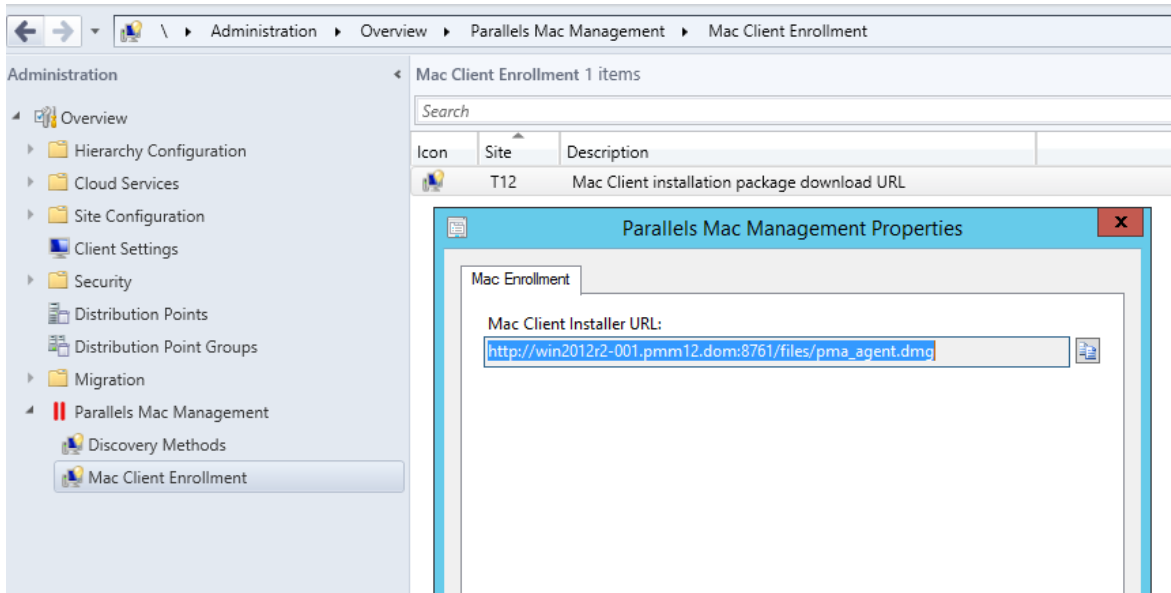
Before using the Image Builder utility, you must create an additional bootable partition on your Mac's hard drive and install OS X on it. The partition must have OS X 10.9 or a later version installed. The inactive partition from which you'll capture the image can have OS X 10.8 or a later version installed.

## Capture an OS X System Image

To capture an OS X 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 OS X.
- 5 Open Terminal and change directory to the PmmOsdImageBuilder.dmg image mount point (e.g. /Volumes/Parallels OSD Image Builder 5.0.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 OS X System Image in SCCM

### Add the Image to Configuration Manager

After you captured the OS X 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**.

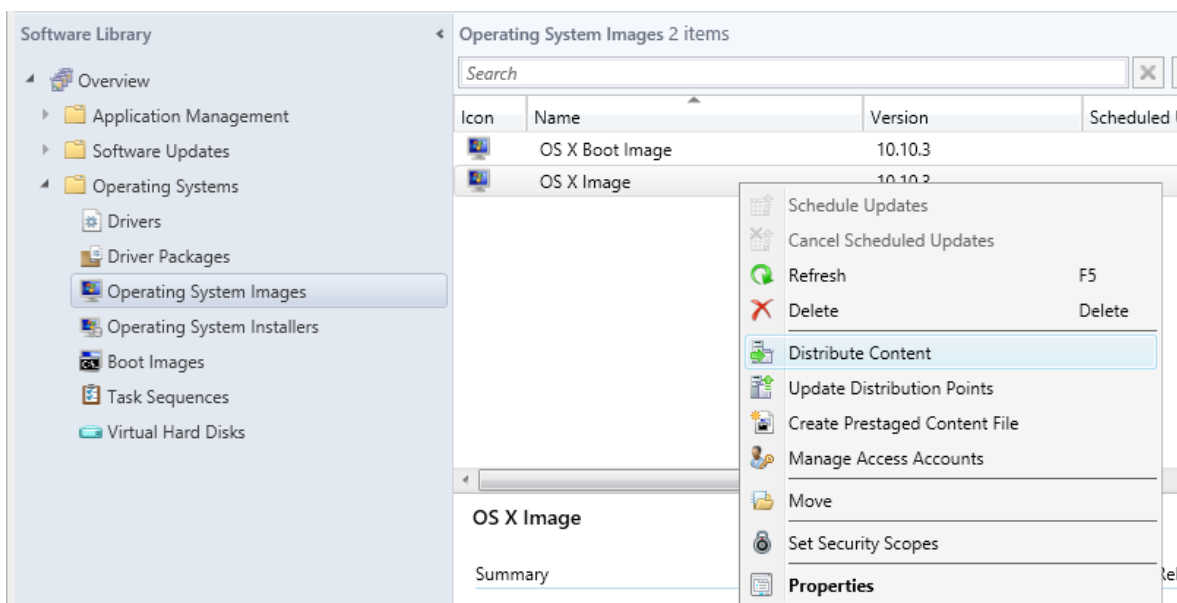


- 3 The **Add OS X Image** dialog opens.
- 4 In the **Path to the OS X image directory** field, specify the folder containing the OS X system image. The other field should contain name and path where you want the image file (.wim) to be created.
- 5 Click **Next**.
- 6 Specify an OS X image name and 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

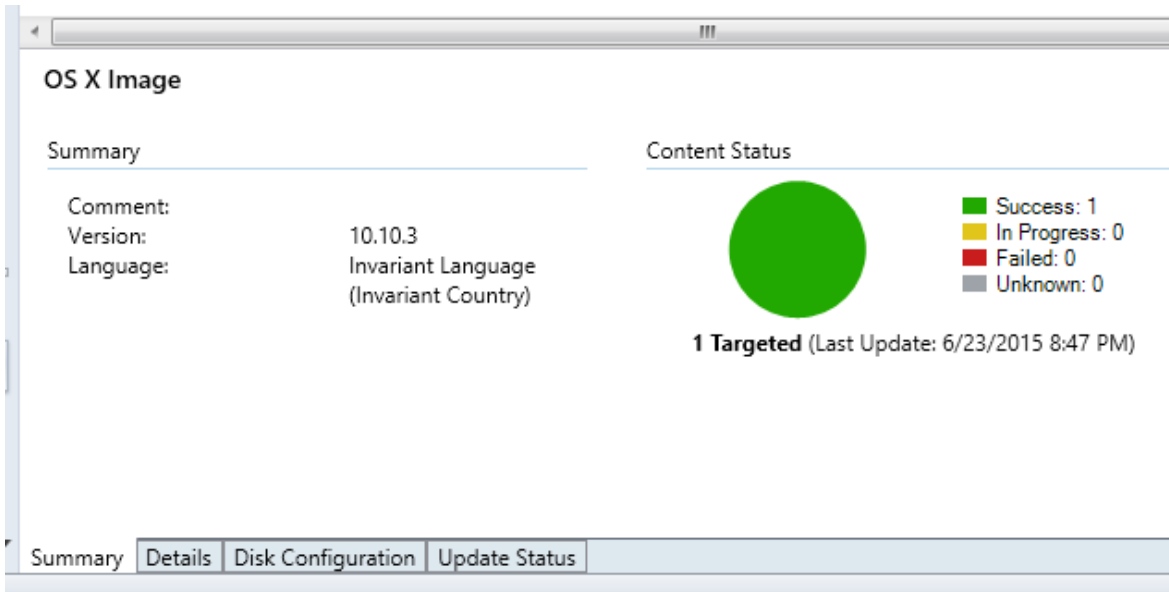
You now need to distribute the OS X image to a distribution point:

- 1 In the Configuration Manager console, right-click the OS X 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 OS X 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 an OS X 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 OS X image on Mac computers. Read on to learn how to do it.

## Creating a Task Sequence for Deploying OS X on Mac Computers

After you have distributed an OS X 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 **Task Sequences** 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 Click the **Steps** tab and then click **Add > Apply OS X Image**.
- 5 Click the **Browse** button and select the OS X system image that you distributed earlier.
- 6 Click **OK** to close the dialog. The new task sequence will appear in the task sequence list (press F5 to refresh the view).

If you need to modify the task sequence, right-click it and choose **Edit Task Sequence for Macs** in the context menu.

You can add other steps to the task sequence that will perform additional actions. These steps are described in the sub-sections that follow this one.

You can also use task sequence variables to configure settings for task sequence steps and to define conditions that must be evaluated before running a task sequence. Task sequence variables are described in the **Using Task Sequence Variables** section (p. 144).

## Join Domain

The **Join Domain** task sequence step allows you to add a Mac to a domain after an OS X 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.
- 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. 144).

## Install Package

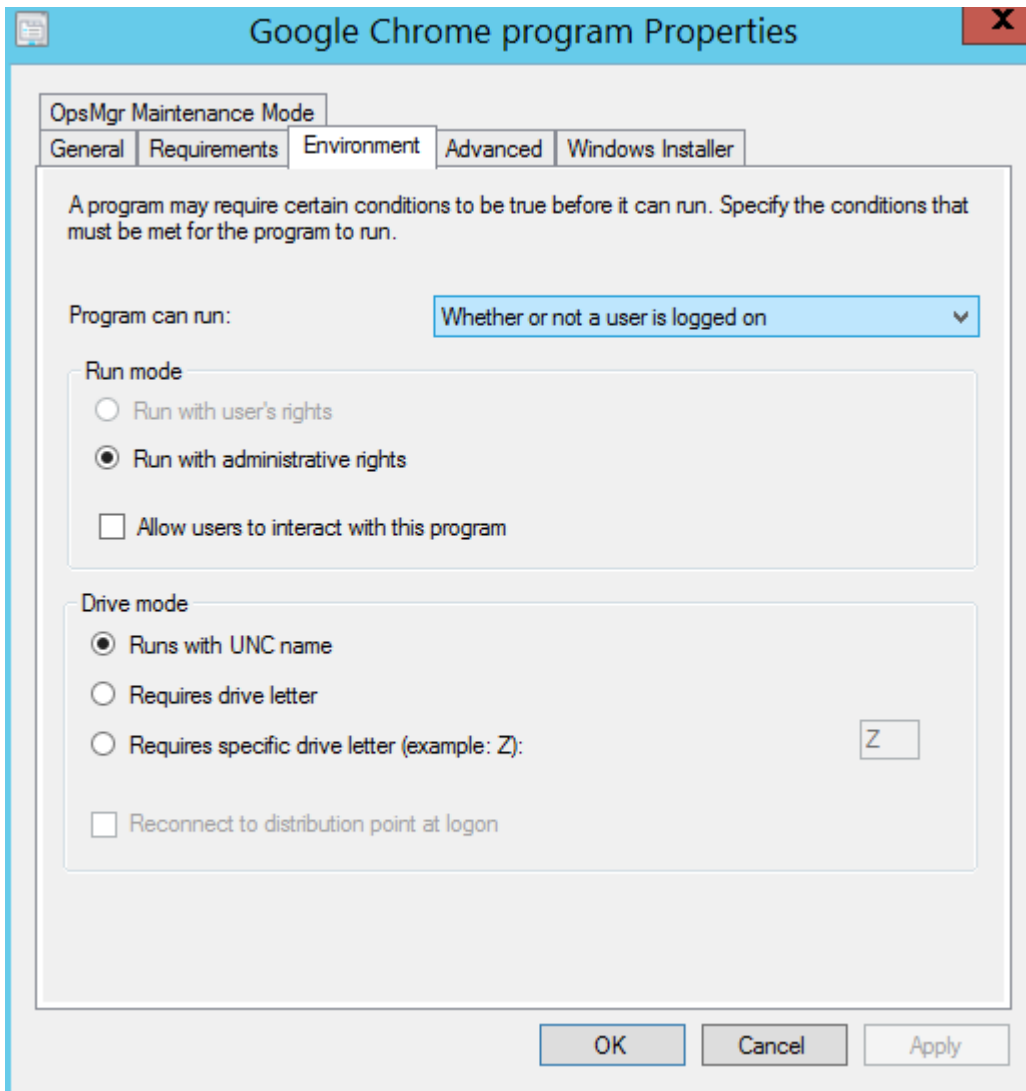
The **Install Package** task sequence step is used to install software packages on a Mac as part of a task sequence execution.

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. 113). 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. 144).

## 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. 144).

## 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 the OS X Server's Profile Manager. It is an XML file with the ".mobileconfig" extension that contains the OS X 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 the information at the end of this section).
- 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. 144).

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 setting stored in the profile. Once you export the profile, you can open the resulting .mobileconfig file in the OS X Server's Profile Manager.

## 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. 144).

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. 144).

## Using 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 Variable** 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. 113) containing the script.
- 3 Add the software package as the **Install Package** task sequence step (p. 140).

### 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
```

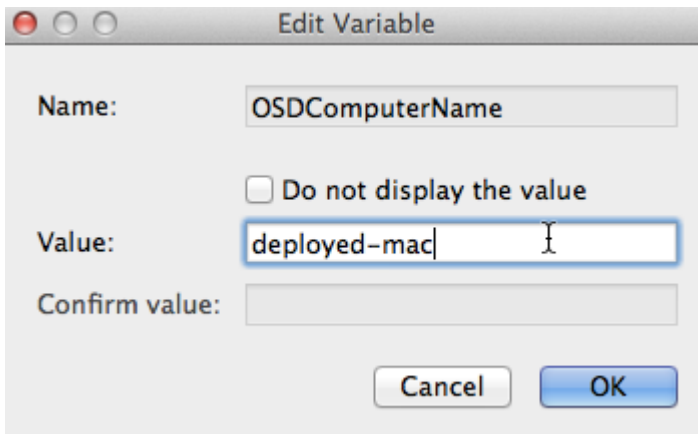
### Prompting Users to Set Empty Variables During Task Sequence Execution

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.



The screenshot shows a standard macOS-style dialog box titled "Edit Variable". It has three main input sections: "Name:" with a text field containing "OSDComputerName"; "Value:" with a text field containing "deployed-mac" which is currently selected with a blue highlight and a text cursor; and "Confirm value:" with an empty text field. Between the "Name" and "Value" fields is an unchecked checkbox labeled "Do not display the value". At the bottom right of the dialog are two buttons: "Cancel" and "OK".

- 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 finished 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 OS X on Mac computers that are not enrolled in Configuration Manager, select the **Unknown Mac OS X Systems** collection.

Deploy Software Wizard

General

Specify general information for this deployment

Task sequence: Parallels OS X Image Deployment Browse...

Collection: Unknown Mac OS X Systems Browse...

☐ Use default distribution point groups associated to this collection

☐ Automatically distribute content for dependencies

Comments (optional):

< Previous Next > Summary Cancel

- 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

To run a task sequence on a Mac computer, you need to do the following:

- 1 Start up a Mac from the network using the OS X boot image.
- 2 Select a task sequence to run.
- 3 Follow the **Parallels Task Sequence Wizards** instructions and deploy OS X 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.

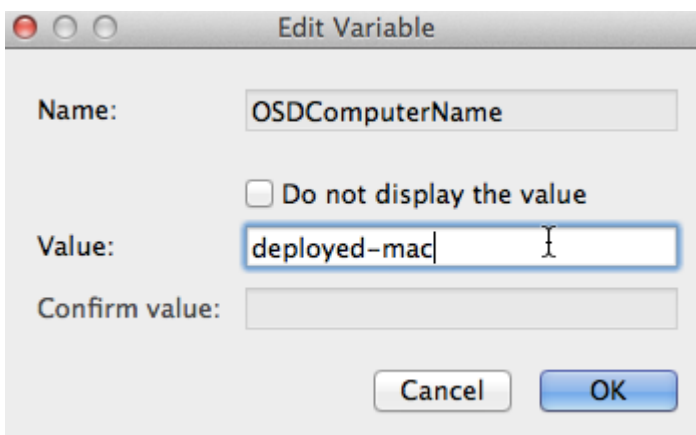
- 5 As the last step, the Mac will be enrolled in Configuration Manager and you'll be prompted to log into OS X.

The following topics describe each step in detail.

## Start Up a Mac From Network and Execute a Task Sequence

To start up a Mac from the network using the OS X boot image:

- 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 added more than one OS X boot image to SCCM, you'll be prompted to choose the one to boot from.
- 3 Upon successful boot, the **Parallels Task Sequence Wizard** will start (some delay is possible while the Mac establishes a network connection).
- 4 On the **Log In** page, enter an AD domain name and your login credentials.
- 5 Click **Continue**.
- 6 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.
- 7 Click **Continue**.
- 8 The **Edit Task Sequence Variables** pages will only show up if one or more task sequence variables used in a task sequence step have empty values (see **Set Hostname** (p. 142) for an example).
- 9 Double click the variable to assign a value to it.



The screenshot shows a standard macOS-style dialog box titled "Edit Variable". It has three main input sections: "Name:" with a text field containing "OSDComputerName"; "Value:" with a text field containing "deployed-mac" which is currently selected with a blue highlight and a cursor; and "Confirm value:" with an empty text field. Between the "Name" and "Value" fields is an unchecked checkbox labeled "Do not display the value". At the bottom of the dialog are two buttons: "Cancel" and "OK".

- 10 Click **OK** and then click **Continue** to advance to the next wizard page.
- 11 On the **Select a Destination** page, select a destination volume for the OS X image deployment.

**Warning:** Clicking **Continue** on this page will start OS X deployment immediately. You cannot go back.

- 12 The task sequence will first deploy the OS X system image to the selected volume.

- 13 Once the OS X is deployed, the Mac will be automatically rebooted from the volume to which the OS X image was applied. Once it boots back up, the task sequence execution will continue with the rest of the task sequence steps.

## Executing Task Sequence Steps

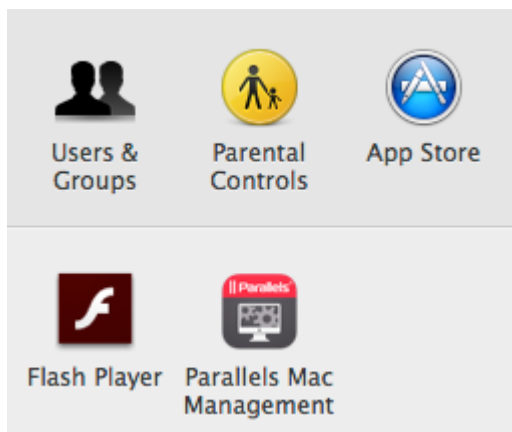
After the Mac reboots, it may take a few seconds for it to configure network access. You may see the **Starting Task Sequence** screen with the "Please wait..." message in it.

Once network is configured, you will see the **Parallels Task Sequence Wizard** once again.

If you've added one of each of the available task sequence steps, they'll be executed as follows (the actual order will depend on how you configured it in the task sequence editor):

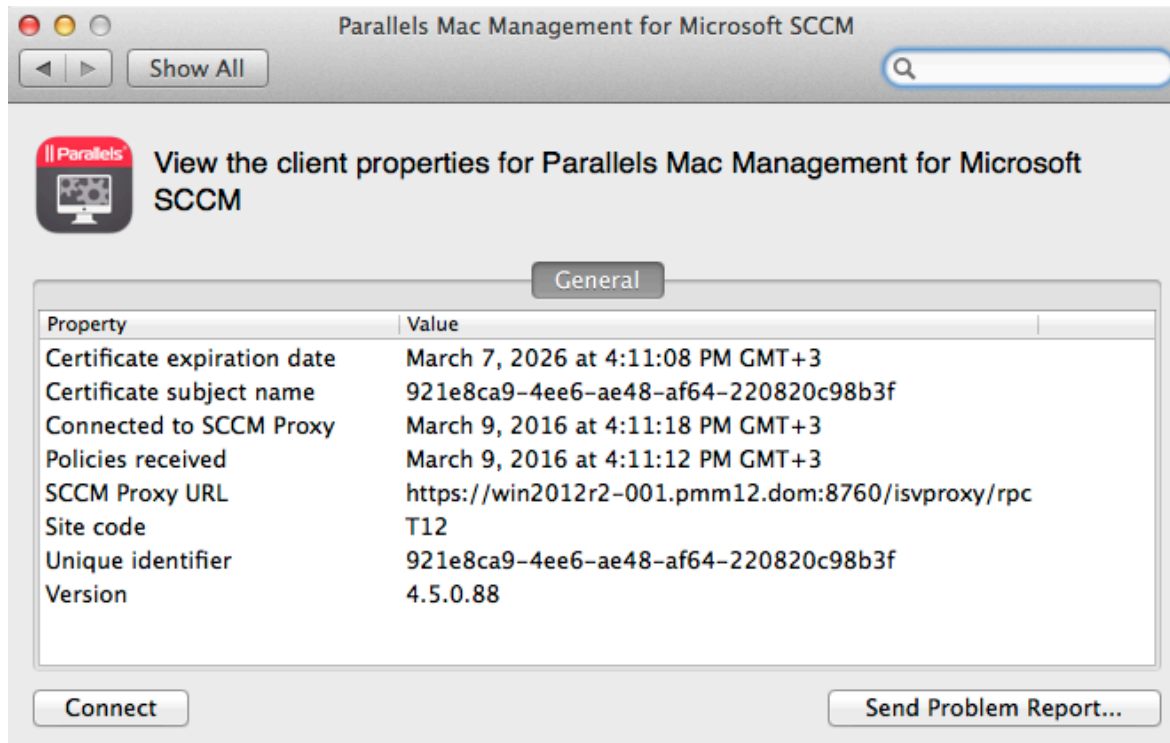
- 1 **Join Domain.** The step will add the Mac to the specified domain and (if specified) to an organizational unit.
- 2 **Install Package.** This step will silently install the software that you configured it to install.
- 3 **Set Hostname.** This step will set the Mac's hostname.
- 4 **Install Parallels Mac Client.** This step is added to a task sequence automatically. It installs Parallels Mac Client on a Mac and enrolls the Mac in Configuration Manager.

Once the task sequence run is complete, you'll be prompted to log into OS X. Once logged in, you can verify that the Mac has been enrolled in Configuration Manager as part of OS X 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 you see properties and values similar to what is shown in the picture below, the enrollment was successful.



## 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 OS X 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 OS X 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.

## OS X Software Update Management

Parallels Mac Management for Microsoft SCCM allows you to manage OS X software updates (patches) using the native SCCM functionality. Using this functionality you can import the information about available OS X updates into SCCM and then deploy the updates to Mac computers in your organization.

To use the OS X 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. 15) 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 OS X updates from Apple's servers. If you want to minimize the Internet traffic, you may prefer to host OS X updates on a local server. Please note that Parallels Mac Management does NOT include functionality for hosting OS X updates. You will have to use the Apple's OS X 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 OS X 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 OS X software update catalogs and packages is <http://swscan.apple.com/content/catalogs/others/>.

When this configuration is used, OS X 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 OS X 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 OS X functionality and install any of them.

For the information on how to configure SCCM and deploy OS X updates to Mac computers, please see **Configuring SCCM and Deploying OS X Updates** (p. 163).

## Download Updates From a Local Server

This configuration allows you to download OS X 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, OS X updates are installed on Mac computers as follows:

- 1 OS X software update catalogs and packages are hosted by a local web server (see **Hosting OS X 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 OS X 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 OS X functionality and install any of them. Please note that in this scenario the OS X 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 OS X 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 OS 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 OS X Server (a physical Apple computer with OS X 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  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pmm_sup_service\Parameters`
- 3 Add a String value to the **Parameters** 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 from the **Parameters** subkey.

### 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. 107)). 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 OS X updates to Mac, please see **Configuring SCCM and Deploying OS X Updates** (p. 163).

## 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, OS X updates are installed on Mac computers as follows:

- 1 Parallels OS X Software Update Point downloads OS X 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 OS X 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 OS X 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 OS X 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. 107)). 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):

**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 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 OS X updates to Mac, please see **Configuring SCCM and Deploying OS X Updates** (p. 163).

## Hosting OS X 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 OS X 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 OS X Server (a physical Apple computer with OS X 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 OS X 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.dom/repo/custom-catalog/
```

Once you have the updates hosted locally and know the download URL, do the following:

- 1 Open the Windows registry editor (regedit.exe) on the computer where Parallels OS X Software Update Point is installed.
- 2 Navigate to  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\pmm\_sup\_service\Parameters
- 3 Add a String value to the **Parameters** subkey 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 from the **Parameters** subkey.

## 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:

- 1 Log into the computer where Parallels OS X Software Update Point is installed.
- 2 Open the Registry Editor (regedit.exe) and navigate to the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pmm_sup_service\Parameters
```

By default, the **Parameters** subkey doesn't contain any values. To modify the Parallels OS X Software Update Point configuration, you need to add the appropriate values to the **Parameters** subkey 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 **Parameters** subkey:

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 OS X 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 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 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 **Parameters** subkey 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 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 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 **Parameters** subkey and name it **InfoUpdateIntervalSeconds**.
- 2 Assign the desired time interval (in seconds) as the value data.

## Set the Interval to Check for OS X Catalog Updates

When an OS X 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 **Parameters** subkey 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 OS X Updates

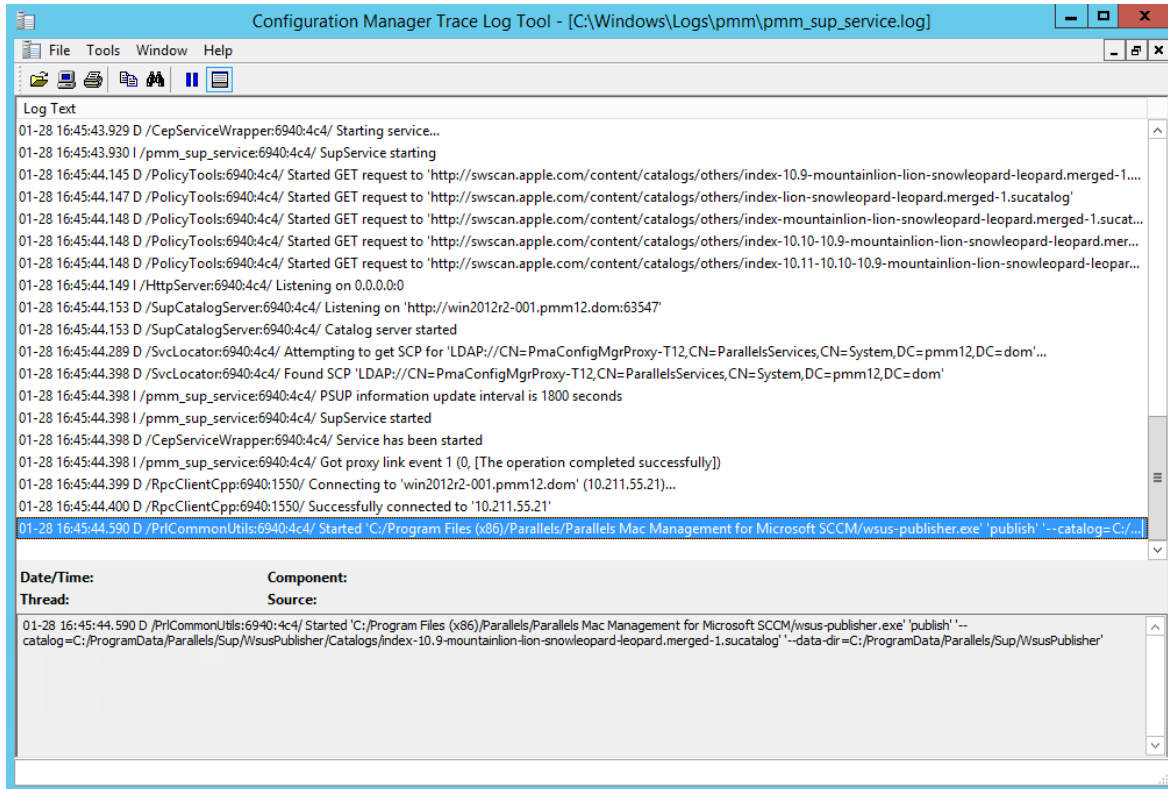
This section describes how to import the information about available OS X updates into SCCM and how to deploy updates to Mac computers.

### Import OS X Software Updates

OS X 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 OS X 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

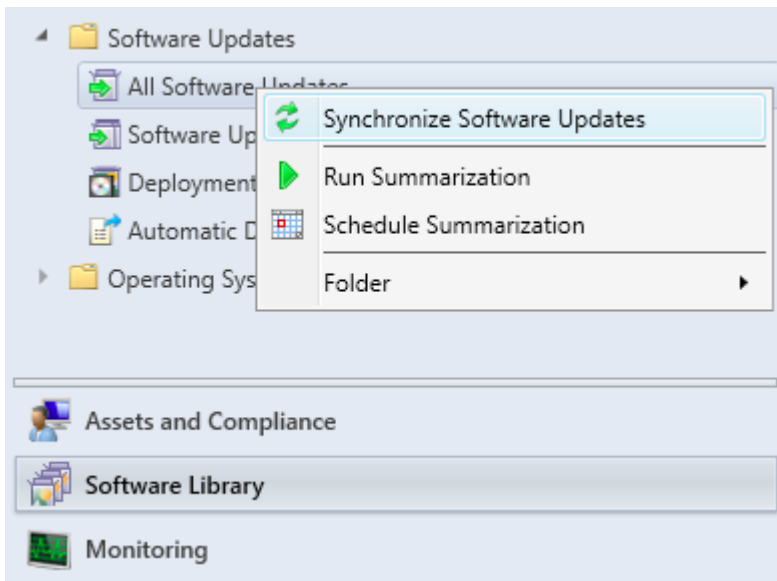
In order for the information about available OS X updates to become available in SCCM, you need to synchronize SCCM with WSUS. The steps described here must be performed only once. The synchronization itself is done by the SCCM Software Update Point role.

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.

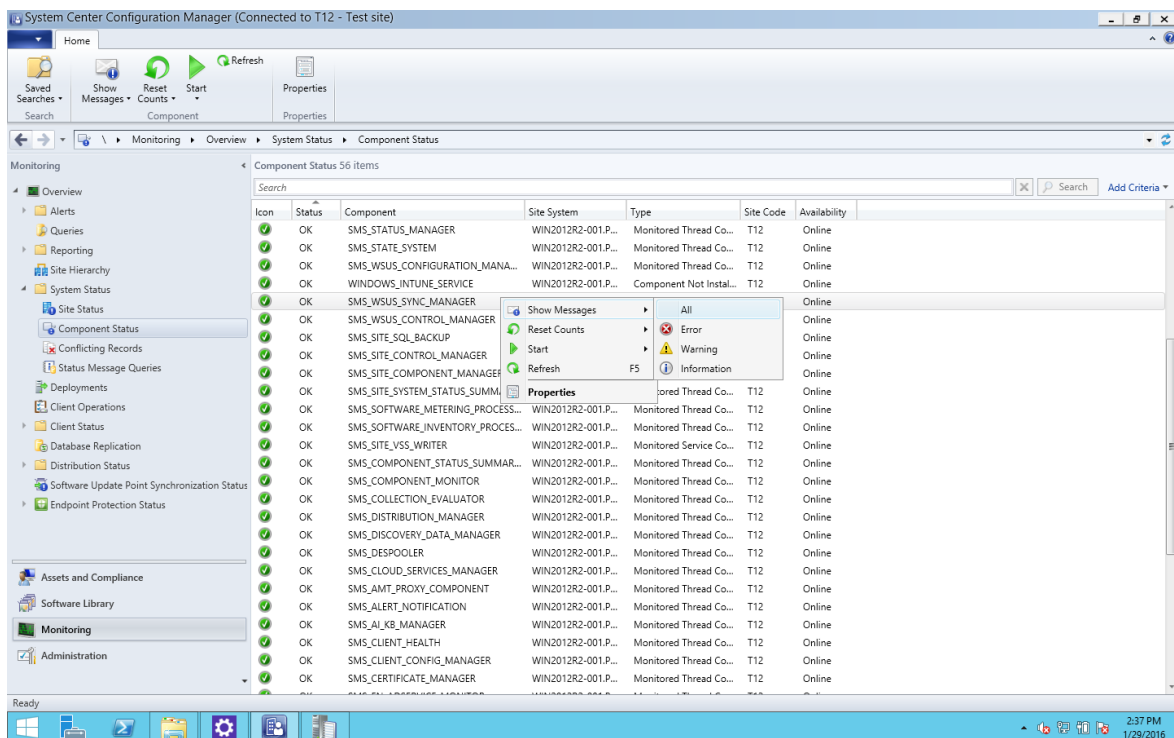
## Configure Synchronization Settings

- 1 In the Configuration Manager console, navigate to **Software Library / Software Updates**.

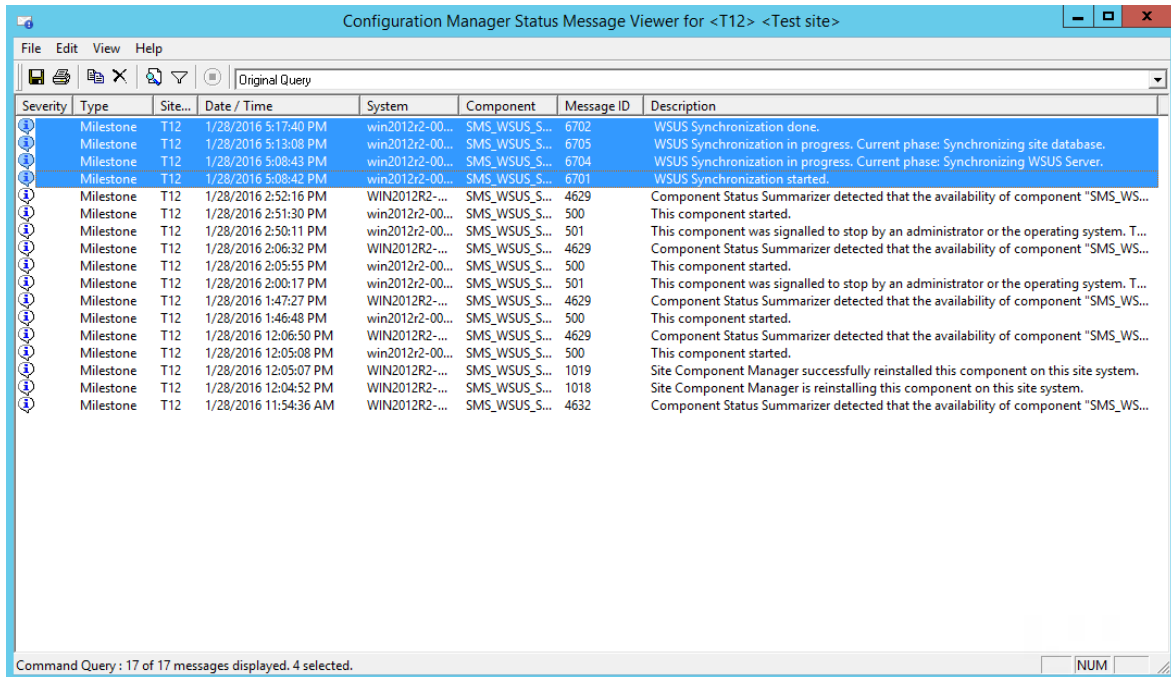
- 2 Right-click **All Software Updates** and choose **Synchronize Software Updates**.



- 3 Wait for the synchronization to complete. You can monitor the process in the **Monitoring / Overview / System Status / Component Status / SMS\_WSUS\_SYNC\_MANAGER**.



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

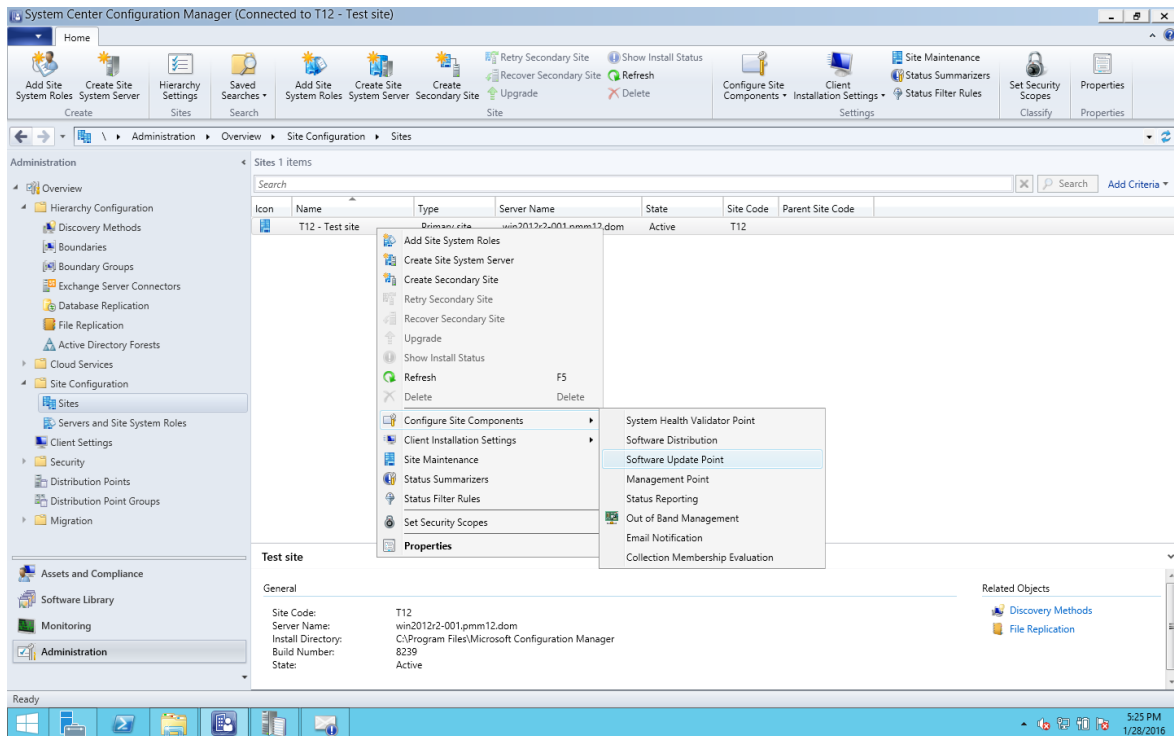


### Configure the Software Update Point Role

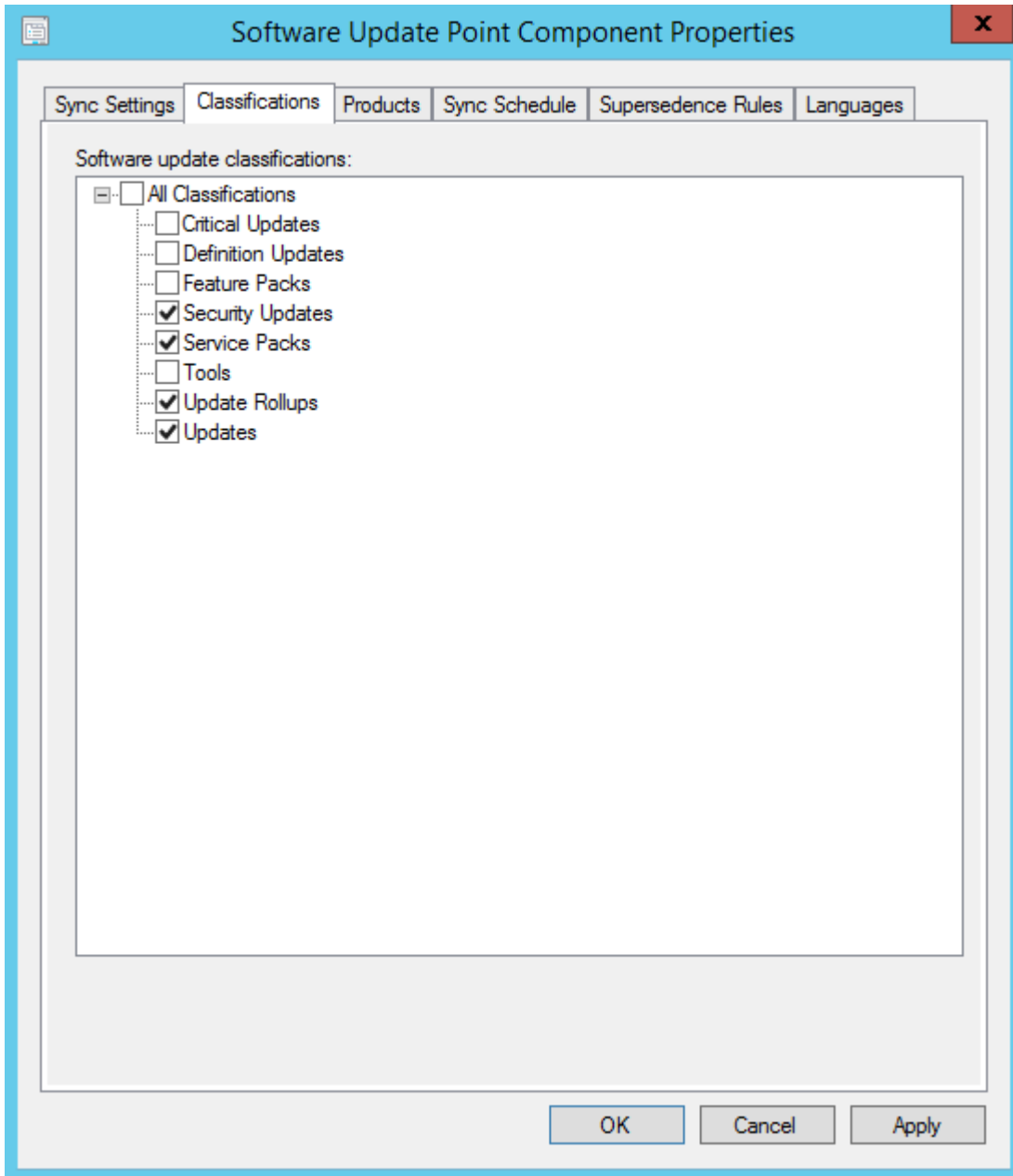
You now need to configure the Software Update Point role to synchronize Apple software updates. To do so, follow these steps:

1 Navigate to **Administration / Overview / Site Configuration / Sites**.

## 2 Right-click your site and choose **Configure Site Component > Software Update Point**.



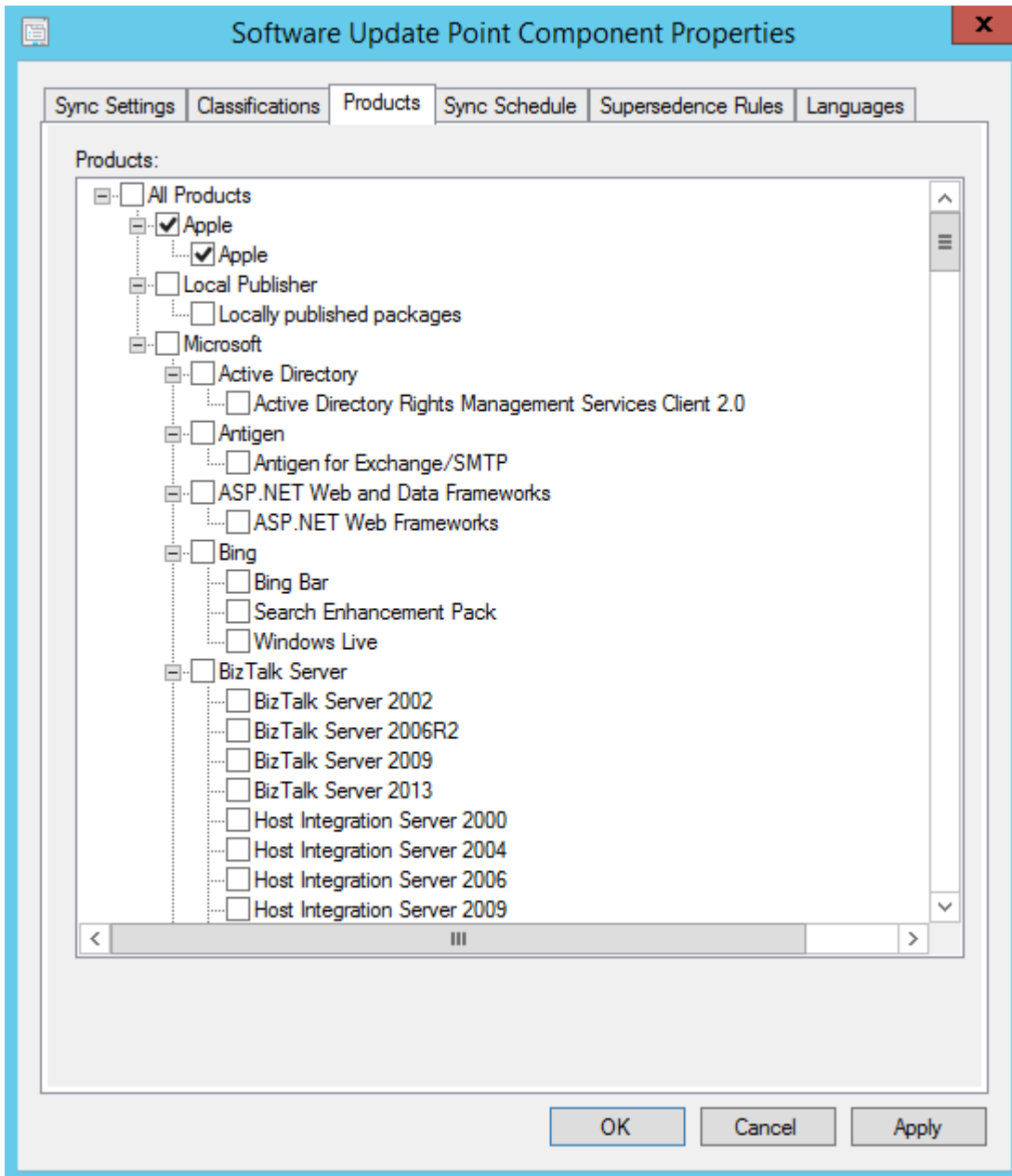
- 3 On the **Classifications** tab page, select the **Updates** option.



- 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.

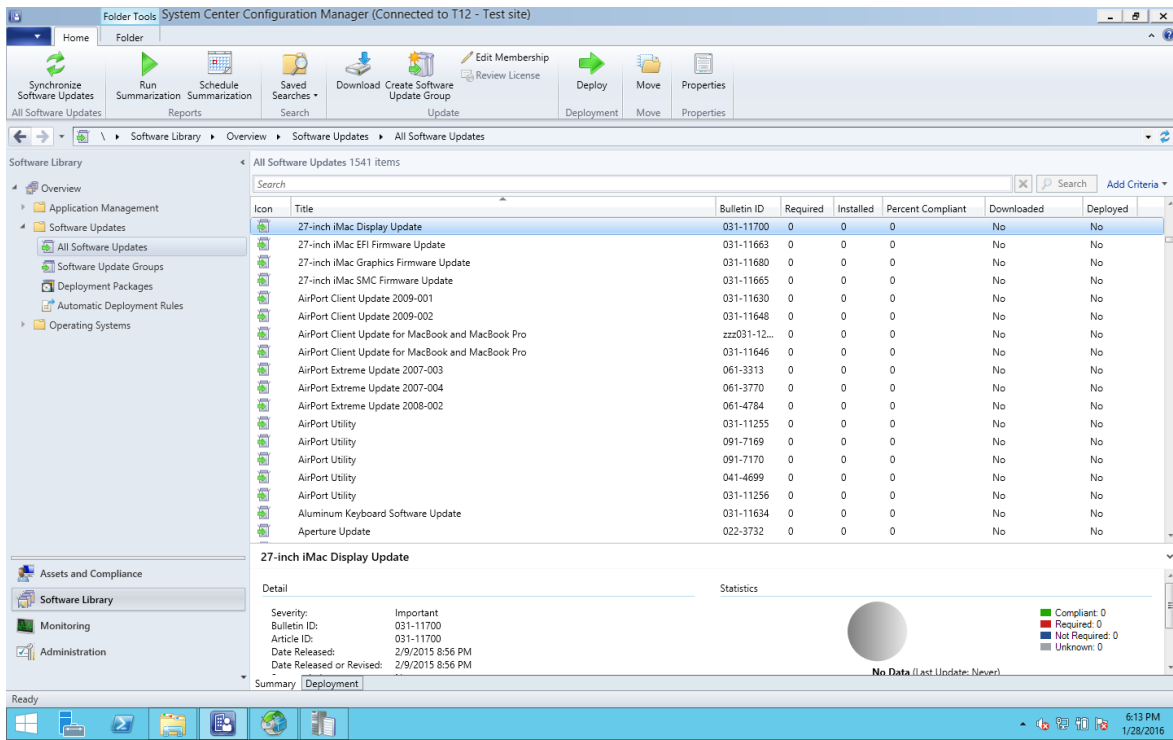


## Synchronize SCCM with WSUS

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.



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



## Deploy Updates to Mac Computers

When OS X 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.

## 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. 60).
  - **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**.

# Apple Device Enrollment Program

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 device setup procedure.

## DEP Deployment Overview

To integrate the DEP functionality into SCCM, you need to configure Parallels Mac Management by performing a number of installation and configuration steps. The following list provides you with an overview of what these steps are:

- 1** Plan for MDM server(s):
  - Decide how many local MDM servers will serve the SCCM hierarchy. One MDM server can serve multiple sites, but you can install multiple MDM servers if needed.
  - Ensure that publicly available domain name is reserved for each local MDM server you are planning to install and run.
- 2** Configure the DEP on the Apple Device Enrollment Program website:
  - Create a virtual MDM server for each primary SCCM site in which you are planning to enroll Mac computers.
  - Assign purchased Macs to these virtual MDM servers accordingly.
- 3** Install and configuring the following local components:
  - Local MDM server(s) — one or many instances (see step 1 above).
  - Local DEP server(s) — a DEP server is automatically installed when you install the Parallels Proxy component on each primary site.
- 4** Configure a local DEP service for each primary SCCM site, so it can communicate with the Apple DEP. This includes:
  - Uploading server tokens for each primary SCCM site from the corresponding virtual MDM servers on the Apple DEP website.
  - Selecting which MDM server will serve the hierarchy of this primary site.
- 5** After the DEP is configured, Mac computers associated with Parallels Mac Management become visible in the SCCM console of each SCCM site.
  - Parallels Mac Management will periodically (daily by default) update the information about the existing and new devices.
  - You can assign Mac computers to secondary sites (if they exist) and if you want them to be enrolled on these sites instead of the primary site.

**6** To specify enrollment details, you need to create one or more enrollment profiles and assigning them to selected Mac computers.

**7** When a newly purchased Mac is started for the first time, it will be configured according to the enrollment profile assigned to it, and will then be enrolled in SCCM automatically.

If at the time of the initial setup a Mac is not connected to your organization's network, Parallels Mac Client will be installed on it, but the Mac will not be enrolled in SCCM. As soon as the Mac is connected to the network, Parallels Mac Client will connect to Parallels Proxy and will enroll the Mac in SCCM.

Read on to learn how to configure Parallels Mac Management for Microsoft SCCM to enable the DEP functionality and how to use it.

## Install and Configure an MDM Server

If you haven't done so already, install and configure one or more Parallels MDM servers. For the complete instructions, please see the following topics:

- **Parallels MDM Server Requirements** (p. 15)
- **Running the Setup Wizard** (p. 30)
- **Configuring Parallels MDM Server** (p. 36)

As was mentioned earlier, you can set up as many MDM servers as you require. One MDM server can serve multiple SCCM sites, but you can set up multiple MDM servers if needed.

## Import a DEP Certificate to Parallels MDM Server

After installing and configuring a Parallels MDM Server, you need to export a certificate from the local DEP server and then import it to the MDM server.

### Export a certificate

To export a certificate:

- 1** Log in to the server where you have the Parallels Proxy installed (that's where the local DEP server is automatically installed).
- 2** Run the Microsoft Management Console (mmc.exe).
- 3** In the console, click **File > Add/Remove Snap-in** in the main menu.
- 4** In the **Add or Remove Snap-ins** dialog, select **Certificates** in the **Available snap-ins** list.
- 5** Click the **Add** button.
- 6** On the **Certificates snap-in** wizard page, select **Computer account** and click **Next**.
- 7** On the **Select Computer** page, select **Local computer** and click **Finish**.
- 8** Click **OK** to close the **Add or Remote Snap-ins** dialog.

- 9 In the console, navigate to **Certificates (Local Computer) > Personal > Certificates**.
- 10 Right-click a certificate where the **Issued To** column says "Parallels DEP Service" and choose **All Tasks > Export** in the context menu.
- 11 In the **Certificate Export Wizard**, click **Next**.
- 12 On the **Export Private Key** page, select **No, do not export the private key** and click **Next**.
- 13 On the **Export File Format** page, select **DER encoded binary X.509 (.CER)** and click **Next**.
- 14 Specify a file name and click **Next**.
- 15 Click **Finish**.

### Import the certificate

After you've exported the certificate, you need to import it to the MDM Server. To do so:

- 1 Log in to the computer where you have Parallels MDM Server installed and copy the exported certificate file to it.
- 2 Open the Microsoft Management Console (mmc.exe).
- 3 In the console, click **File > Add/Remove Snap-in** in main menu.
- 4 In the **Add or Remove Snap-ins** dialog, select **Certificates** in the **Available snap-ins** list.
- 5 Click the **Add** button.
- 6 On the **Certificates snap-in** wizard page, select **Computer account** and click **Next**.
- 7 On the **Select Computer** page, select **Local computer** and click **Finish**.
- 8 Click **OK** to close the **Add or Remote Snap-ins** dialog.
- 9 In the console, navigate to **Certificates (Local Computer) > Personal > Certificates**.
- 10 Right-click on **Certificates** and click **All Tasks > Import** in the context menu.
- 11 In the **Certificate Import Wizard**, click **Next**.
- 12 On the **File to Import** page, click **Browse** and select the certificate file.
- 13 Click **Next**.
- 14 On the **Certificate Store** page, make sure the **Place all certificates in the following store** option is set to **Personal** and click **Next**.
- 15 Click **Finish**.

## Configure DEP Links

The DEP link information is used by Parallels Mac Management to communicate with the Apple DEP and perform the following management tasks:

- Getting a list of assigned Mac computers and their properties.
- Assigning profiles to Mac computers.

- Removing profiles from Mac computers.

To configure a DEP link:

- 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 list 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 web service side. The public/private key pair is generated and stored securely on a server when you configure the local MDM server.
- 5** Visit the Apple DEP website and log in using your Apple ID and password. Once logged in, do the following:
  - a** Create a virtual MDM server for this local Parallels MDM server.
  - b** Upload the PEM-encoded X.509 certificate that you saved in previous steps.
  - c** Download the S/MIME encrypted token file generated by the Apple DEP.
- 6** Return to the **DEP Link Configuration Wizard** in the Configuration Manager console. Click **Browse** and select the server token file that you downloaded in the previous step.
- 7** Click **Next**.
- 8** On the next page, specify the FQDN of the server where the local MDM server is running (e.g. `mdm.mycompany.com`) and the port number used for incoming connections from Parallels Mac Management. You specified this info when you configured the Parallels MDM server.
- 9** Click **Next** and wait for the configuration settings to be applied. A progress bar is displayed while the settings are applied.
- 10** At this time, the S/MIME encrypted Server Token is decrypted by the Parallels DEP service and stored to be used for communication between Parallels Mac Management and the Apple DEP.
- 11** When the settings are applied, Parallels Mac Management will try to connect to the local Parallels MDM server and the Apple DEP.
  - If a connection cannot be established, a message box is displayed describing the problem. You will have to resolve any issues before continuing.
  - If both connections are successful, the local DEP service is attached to the Apple DEP and the **Finish** button on the wizard page becomes enabled.
- 12** Click the **Finish** button to close the wizard.
- 13** The **DEP Link Properties** dialog is refreshed with the new information retrieved from the Apple DEP. Review the information and close the dialog.



- 14** The list of Mac computers assigned to DEP will now be retrieved from the DEP account. You can view these Mac computers in the Configuration Manager console at the following location: **Administration / Parallels Mac Management / Device Enrollment Program / Devices**. We'll talk more about managing devices in **Deploying and Managing Devices** (p. 179).

## Viewing and reconfiguring DEP link properties

To view the 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 or with another Parallels 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 Mac computers. Read on to learn how to do it.

## Creating and Managing Enrollment Profiles

A device enrollment profile specifies the settings which will be applied to a Mac computer when it is enrolled using the Device Enrollment Program. Every Mac must have an enrollment profile assigned to it before it can be enrolled.

Parallels Mac Management provides you with the functionality to create enrollment profiles right in the Configuration Manager console. This section describes how to use this functionality.

### Create an Enrollment Profile

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.
- 3** Complete the wizard as described in the subsequent sections.

### General Information

On the **General Information** page:

- 1** Specify the profile name, so it can be easily identified in the Configuration Manager console and on the DEP website.
- 2** Specify the support phone number, email address, and department name if needed (these properties are optional).
- 3** **Supervise devices**. If selected, the device supervision during the enrollment process will be allowed.

- 4 Allow profile removal.** If cleared, a user will not be able to remove the profile from a Mac. Note that this option can be cleared only if the **Supervise devices** option (above) is selected. By default, this option is selected (i.e. users will be able to remove the profile).
- 5 This profile is mandatory.** If selected, a user will be required to apply the profile on a Mac.
- 6** When done, click **Next** to continue.

## User Experience

On this 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 an OS X Configuration Profile to use as an MDM profile. Do the following:

- 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 containing specific settings.

- 3** Click **Next** to create an enrollment profile and push it to the Apple DEP. 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.

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

## View an Enrollment Profile

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.

- 5 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 device enrollment profiles.

To delete a profile, right-click it and choose **Delete**. If a profile was already used in the past, a warning message will be displayed to prevent an accidental removal of a valid and potentially useful enrollment profile.

## Deploying and Managing Devices

To deploy Mac computers and enroll them in SCCM, you need to perform the following tasks:

- 1 Assign Mac computers to an SCCM site.
- 2 Assign an enrollment profile to Mac computers.
- 3 Deploy a Mac computer using the Device Enrollment Program, which will automatically enroll the device in SCCM.

Read on to learn how to perform the above tasks.

### View Mac Computers Assigned to MDM Servers

To view Mac computers assigned to MDM servers:

- 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 MDM servers. 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. If you have one or more secondary sites, you can assign Mac computers to them if you wish. To do so:

- 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 following properties:

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

- **OS:** The device's operating system: "iOS" or "OSX". 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 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 MDM server.
- **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 each Mac computer 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 / 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 Device Enrollment Program, a profile that you assign here will be used to configure the Mac.

## Enrolling Mac Computers in SCCM

After you finish configuring the Device Enrollment Program functionality (as described earlier), your Mac computers are 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 and obtains the enrollment profile assigned to it.
- 2 The Mac then connects to the Parallels MDM server (which faces the Internet and is accessible through it) as instructed by the enrollment profile settings.
- 3 The Parallels MDM server registers the Mac in SCCM as a resource.
- 4 If an MDM profile was specified in the enrollment profile, then this profile is pushed to the registered Mac.
- 5 Parallels Mac Client is then installed on the Mac. If the Mac is not connected to your organization's network, it will not be enrolled in SCCM at this time. As soon as the Mac is connected to the network, Parallels Mac Client will connect to Parallels Proxy and will enroll the Mac in SCCM.

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

## Deploying Parallels Desktop to 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 OS X.

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. 113)). 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:

<http://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. 117) 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. 113) 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.

## Providing Remote Assistance to Mac Users

The Remote Assistance feature allows a system administrator to temporarily connect to a remote Mac computer and correct any problems on it if necessary. 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 OS X 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 OS X.

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 OS X and are installed on a Mac by default. The following describes how to set up and use each connection option.

### Connect via VNC

Before using this feature, the OS X Remote Management service must be enabled on each individual Mac.

To enable OS X 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 OS X desktop.

## Connect via SSH

Before using this feature, the SSH service must be enabled on each individual Mac.

To enable SSH in OS X:

- 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 OS X.

# 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. 189). 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. 75).

## 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 the 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 a read-only information provided as a reference. If a report operation included sending it to Parallels Support, the entry will include the report ID, which can be used when following up on the report with Parallels Support.

## 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. 74). 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.



## CHAPTER 6

# Appendices

### In This Chapter

Logging.....	193
Changing Log File Rotation Limits.....	197
Parallels Mac Management Database .....	198

## 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
- OS X (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	<p>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.</p> <p>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.</p>

	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	<p>The SCCM Console Extension component has just one log file: pma_setup.log. The file contains information about the component installation procedure.</p> <p>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.</p>
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	<p>This log file is updated when the client installation and registration utilities are run on the Mac by a user.</p> <p>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).</p> <p>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/&lt;user_name&gt;/Library/Logs directory.</p>
	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
Colleva.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
	OS X	/Users/<user_name>/Library/Logs
pma_agent	OS X	/Library/Logs/pma_agent.log
pma_agent_ui	OS X	/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 OS X 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 OS X 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.

## 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 and recovery 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 the data safety.

# Index

.

.NET Framework 4.0 - 13

## A

About This Guide - 9

Activate Offline - 52

Activate Online - 52

Activate Parallels Mac Management - 52

Add the OS X Boot Image to Configuration Manager - 129

Administrative Rights in Authorization Manager - 21

Administrative Rights in SCCM - 18

APNs Certificate - 38

Appendices - 193

Apple Device Enrollment Program - 173

Apply Configuration Profile - 142

Assign an Enrollment Profile to Mac Computers - 180

Automatic Upgrade of Parallels Mac Client - 70

## B

Boot a Reference Mac From a Different Partition - 135

## C

Capture an OS X Boot Image - 128

Capture an OS X Image - 135

Capture an OS X System Image - 135

Capturing an OS X Boot Image - 128

Capturing an OS X Image Using a Task Sequence - 133

Capturing an OS X Image Using the Image Builder Utility - 135

Capturing an OS X System Image - 133

Changing Log File Rotation Limits - 197

Choose the Installation Type - 118

Communication Ports and Protocols - 16

Compliance Settings - 81

Conclusion and Notes - 35

Configuration Manager Boundaries

Configuration - 13

Configuration Manager Proxy Communication Ports - 34

Configuration Manager Proxy Service

Account - 32

Configuration Options - 154

Configuration Settings Summary - 35, 40

Configure DEP Links - 175

Configure Synchronization of SCCM with WSUS - 164

Configure the Deployment Type - 121

Configuring Configuration Manager Boundaries - 24

Configuring Parallels Configuration Manager Proxy - 32

Configuring Parallels Mac Client Push Installation Properties - 60

Configuring Parallels MDM Server - 36

Configuring Parallels NetBoot Server - 35

Configuring Parallels Network Discovery - 62

Configuring Parallels OS X Software Update Point - 36, 162

Configuring SCCM and Deploying OS X Updates - 163

Configuring the Firewall - 68

Configuring Windows Firewall - 25

Create a Configuration Manager Application - 120

Create a Domain User - 18

Create a Parallels My Account - 46

Create a Task Sequence for Capturing an OS X System Image - 133

Create an Enrollment Profile - 177

Creating a Configuration Item - 107

Creating a Discovery Script - 109

Creating a Remediation Script - 109

Creating a Security Group - 28

Creating a Software Package - 113



Creating a Task Sequence for Deploying OS X on Mac Computers - 138  
Creating and Managing Enrollment Profiles - 177  
Creating and Managing Sublicenses - 50  
Creating Certificate Templates for Parallels Proxy and Mac Computers - 26  
Creating Compliance Rules - 111  
Creating FileVault 2 Configuration Item - 90, 97  
Creating FileVaultMaster Keychain - 90  
Creating OS X Configuration Profile from .mobileconfig File - 86  
Creating OS X Configuration Profile Using the Profile Editor - 82  
Customer Experience Program - 34

## D

Date and Time Synchronization - 14  
DCOM Remote Activation Permission - 18  
Deactivating Parallels Mac Management - 56  
DEP Deployment Overview - 173  
Deploy the Application - 123  
Deploy Updates to Mac Computers - 171  
Deploying a Task Sequence to a Collection - 149  
Deploying and Managing Devices - 179  
Deploying Configuration Baseline - 111  
Deploying OS X Configuration Profile - 81  
Deploying Parallels Desktop to Mac Computers - 181  
Deploying SCCM Client in Windows Running in a Virtual Machine - 184  
Deploying Software - 117  
Deploying Software via SCCM Application Deployment - 118  
Deploying Software via SCCM Package Deployment - 113  
Device Collections in Parallels Mac Management - 77  
Distribute Content of the OS X Boot Image - 131  
Distributing the OS X System Image in SCCM - 136  
Distribution Point Role Configuration - 13  
Download Updates From a Local Server - 155

Download Updates From Apple's Servers - 154

## E

Enabling Remote Access on Mac Computers - 59  
Encrypting a Mac with FileVault 2 - 94, 101  
Enforcing FileVault 2 Encryption - 89  
Enforcing Parallels Desktop Preferences - 104  
Enforcing Parallels Desktop VM Settings - 105  
Enrolling Mac Computers in SCCM - 181  
Exceeding the License Limit - 55  
Execute Script - 143  
Executing Scripts on Mac Computers - 172  
Executing Task Sequence Steps - 152

## F

FileVault 2 Encryption with Institutional Recovery Key - 90  
FileVault 2 Encryption with Personal Recovery Key - 97

## G

General Requirements - 12  
Generate an APNs Certificate - 38

## H

Handling Expired Certificates - 28  
Hardware and Software Inventory - 78

## I

IIS Settings on the Distribution Point Server - 13  
Import a DEP Certificate to Parallels MDM Server - 174  
Import OS X Software Updates - 163  
Initiating Policy Retrieval from a Mac - 74  
Initiating Policy Retrieval from SCCM - 191  
Install and Configure an MDM Server - 174  
Install Package - 140  
Installation and Configuration - 30  
Installation Options Overview - 58  
Installation Overview - 30  
Installation Requirements - 12  
Installing Parallels Mac Client Using a Script - 66

Installing Parallels Mac Client Using Discovery Methods - 59  
Installing the Application on a Mac - 124  
Integrating Parallels Mac Management with PKI - 25  
Introduction - 8

## J

Join Domain - 139

## L

Licensing and Activation - 45  
Limitations and Known Issues - 171  
Local Administrator Rights - 18  
Logging - 193

## M

Maintenance and Upgrade - 41  
Manually Upgrading Parallels Mac Client - 72  
Microsoft SQL Server Permissions - 20  
Migrating Configuration Manager Proxy - 42

## N

Network Configuration - 14

## O

Obtaining a Trial License - 46  
Operating System Deployment - 127  
OS X Software Update Management - 154

## P

Parallels Client Certificate Management Settings - 33  
Parallels Configuration Manager Proxy Requirements - 13  
Parallels Mac Client Deployment - 58  
Parallels Mac Management Component Overview - 10  
Parallels Mac Management Database - 198  
Parallels Mac Management Features Overview - 8  
Parallels Mac Management Licensing - 45  
Parallels MDM Server Location - 37  
Parallels MDM Server Requirements - 15  
Parallels MDM Service Account - 37  
Parallels MDM Web Server Certificate - 37  
Parallels NetBoot Server Requirements - 14

Parallels OS X Software Update Point Requirements - 15  
Permissions for Running Parallels OS X Software Update Point - 23  
Permissions for Running Parallels Proxy Configuration Wizard - 17  
Permissions for Running Parallels Proxy Service - 22  
Permissions in Active Directory - 19  
Permissions to Read/Write Service Principle Name - 20  
PKI Integration Overview - 26  
Pre-Installation Checklist - 11  
Pre-Installation Procedures - 10  
Prepare a Mac Application for Configuration Manager - 119  
Prerequisites Check - 32, 40  
Prerequisites for Deploying OS X on Mac Computers - 127  
Problem Reporting and Monitoring - 187  
Prompting Users to Set Empty Variables During Task Sequence Execution - 148  
Providing Remote Assistance to Mac Users - 186  
Purchasing a Subscription - 45  
Push Install or Update Parallels Mac Client - 67

## R

Receiving Compliance Settings Reports - 112  
Recovering Encrypted Disk Using a Password - 94, 101  
Recovering Encrypted Disk Using Institutional Key - 95  
Recovering Encrypted Disk Using Personal Key - 102  
Register a Subscription - 49  
Reporting User Logon Information - 79  
Restrict Which Updates a Mac User Can Install - 158  
Role-Based Security - 33  
Running a Task Sequence on a Mac - 150  
Running Configuration Wizards - 32  
Running Parallels Mac Client Installer on a Mac - 65  
Running Parallels Network Discovery - 64  
Running Shell Scripts as Part of a Task Sequence Step - 147

Running the Setup Wizard - 30

## S

Sending a Package to a Distribution Point - 116

Sending Problem Reports from Parallels Mac Client - 189

Sending Problem Reports From Parallels Mac Client - 75

Sending Problem Reports Using a Standalone Reporting Utility - 188

Sending Problem Reports Using Configuration Manager Console - 187

Set Hostname - 142

Set the HTTP Server Port Number - 162

Set the Interval to Check for OS X Catalog Updates - 163

Set the Interval to Notify Parallels Proxy of Software Update Configuration Changes - 163

Set Variables Task Sequence Step - 147

SMS Provider Location - 32

Specify the Web Proxy Server Settings - 162

Specifying a Script Interpreter - 110

Specifying Step Properties Using Task Sequence Variables - 145

Start Up a Mac From Network and Execute a Task Sequence - 151

Synchronize SCCM with WSUS - 169

## T

The Configuration Manager Admin Console - 77

The Reporting Functionality Requirements - 15

Troubleshooting - 153

## U

Uninstalling Parallels Mac Client - 70

Updating Parallels Proxy Connection URL - 69

Upgrading Parallels Mac Client - 70

Upgrading Parallels Mac Client via Software Distribution - 71

Upgrading Parallels Mac Management - 44

User Rights Requirements - 17

Using Conditions in Task Sequence Steps - 146

Using Discovery and Remediation Scripts - 107

Using Groups in a Task Sequence - 144

Using Parallels Application Portal - 125

Using Parallels Mac Client Tools - 72

Using Parallels Mac Management for Microsoft SCCM - 77

Using Parallels Network Discovery - 62

Using Problem Monitoring Utility - 189

Using SCCM Active Directory System Discovery - 64

Using Task Sequence Variables - 144

## V

Verify the OS X Boot Image Deployment - 132

Verifying Parallels Mac Client Deployment - 69

View an Enrollment Profile - 178

View and Update the License Information - 53

View Mac Computers Assigned to MDM Servers - 179

Viewing and Monitoring FileVault 2 Encryption Status - 92, 99

Viewing Parallels Mac Client Properties - 72

Viewing Proxy Service Certificate Details - 41

Viewing the Package Status - 117

## W

What This Section Does Not Cover - 26

Windows and OS X Firewall Configuration - 14