Parallels Device Management for Configuration Manager

Deployment Guide

v9.0

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

Contents

CHAPTER 1

Introduction

The guide is for network and Microsoft Configuration Manager administrators who are planning to deploy Parallels® Device Management for Configuration Manager in their organization. This guide assumes that the reader has knowledge of Configuration Manager, its architecture and its components.

The guide begins with the information on how to prepare your computing environment for the installation of Parallels Device Management. It then describes in detail how to install and configure Parallels Device Management components.

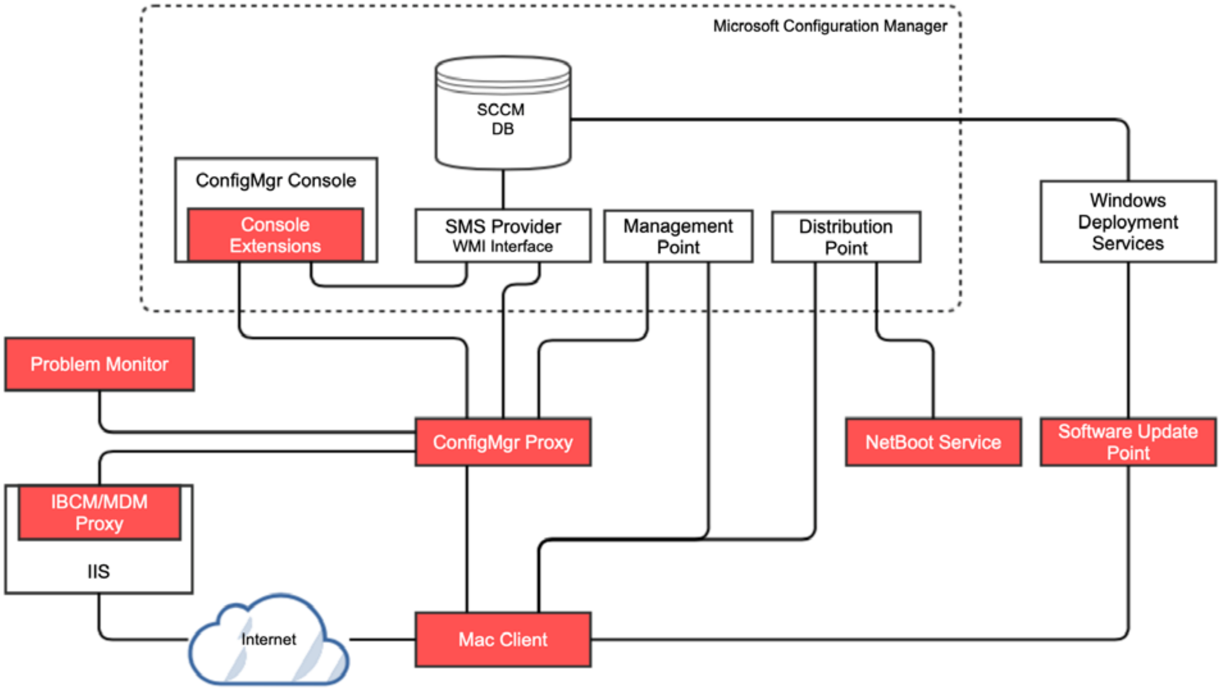
In This Chapter

Glossary

SMS	System Management Server (the core component of System Center Configuration Manager)
CAS	Central Administration Site
DP, MP	Configuration Manager Distribution Point, Management Point
Admin Console	Configuration Manager Administrative Console
WDS	Windows Deployment Services
BITS	Background Intelligent Transfer Service
Parallels Device Management	Parallels Device Management for Configuration Manager
ConfigMgr Proxy	Parallels Configuration Manager Proxy
Extensions	Parallels Configuration Manager Console Extensions
NetBoot	Parallels NetBoot Service
PSUP	Parallels OS X Software Update Point
WSUS	Windows Server Update Services
IBCM/MDM Proxy	Parallels IBCM/MDM Proxy
APNs	Apple Push Notification Service
Apple DEP	Apple Device Enrollment Program. On diagrams in this guide also refers to the Apple DEP website.
Mac Client	Parallels Mac Client

Solution overview

Parallels Device Management extends Microsoft Configuration Manager with the ability to manage Mac computers and Apple mobile devices. With Parallels Device Management you can manage Mac and Windows computers, as well as Apple mobile devices, using Configuration Manager as your only management system.



Parallels Device Management for Configuration Manager consists of the components described below.

Parallels Configuration Manager Proxy

This is the core Parallels Device Management component, which works as a mediator between Configuration Manager and managed devices.

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 Mac Client

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

Parallels IBCM/MDM Proxy

This is a dual component that consists of two parts:

- IBCM Proxy enables Mac computers to reach Configuration Manager from the Internet.
- MDM Proxy enables Apple Device Enrollment Program (Apple DEP) and MDM for managing Mac computers and Apple mobile devices.

When you install the component, you have the ability to enable either IBCM Proxy, MDM Proxy, or both on a given server.

Parallels OS X Software Update Point

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

Parallels NetBoot Server

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

General requirements

Supported Configuration Manager versions

At the time of this writing, Parallels Device Management has been tested with Microsoft System Center Configuration Manager 2012 R2 up to Configuration Manager 2011.

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

Top-level domain requirement

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

Supported Windows and Microsoft SQL Server versions

Same requirements as for the Configuration Manager version that you are using.

Supported Mac hardware platforms

Parallels Mac Client can be installed and run natively on Intel and Apple Silicon-based Mac computers.

Supported macOS versions

- To be managed in Configuration Manager, client Mac computers must be running macOS 10.10 Yosemite — macOS 11 Big Sur.
- To capture a boot image for macOS deployment, the reference Mac computer must be running macOS 10.11 El Capitan — macOS 10.15 Catalina. Please note that macOS Big Sur and newer versions will not be supported.

Supported Apple mobile devices

- iOS devices
- iPadOS devices

CHAPTER 2

Planning for Parallels Device Management Deployment

In This Chapter

Deployment process overview

Parallels Device Management consists of multiple components, which can be installed on different servers in different combinations depending on your needs and your specific infrastructure.

Some planning should be done prior to deployment in order to have answers to the following questions:

- Which components to install?
- Where to install each component?
- What are prerequisites for each component and do you meet them?
- In which order should components be installed?

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

Before running installation and configuration wizards, make sure that you have read installation requirements for each component, which are provided in this guide.

To help you preparing and configuring your infrastructure, the following utilities are available from Parallels for download:

- **Parallels Device Management Prerequisites Check Wizard**. Use the wizard to verify whether your Configuration Manager infrastructure is ready for Parallels Device Management deployment.

- **Parallels Device Management Server Tools**. A collection of PowerShell scripts that simplify and automate the most tedious tasks required to configure Parallels Device Management server components.

To download the utilities, visit https://www.parallels.com/products/mac-management/resources/ and locate the **Utilities** section.

Which Parallels Device Management components to install

You need to install the bare minimum of Parallels Device Management components in any deployment scenario. These components are:

- Configuration Manager Proxy
- Configuration Manager Console Extensions

The following table describes main Parallels Device Management features and specific components that must be installed to use these features.

Feature	Description	Components to install
Active Directory and network discovery of Mac computers	Discover Mac computers on a network and automatically enroll them in Configuration Manager.	ConfigMgr Console Extensions Configuration Manager Proxy
Inventory of Mac hardware and installed applications	Hardware and software inventory is automatically collected and can be viewed in the Configuration Manager console.	
Software metering	Monitor and collect software usage data from Mac computers. Determine actively used software titles, software that causes problems, evaluate your software license needs, etc.	
macOS software deployment	Enables you to use the Configuration Manager Software Distribution functionality to install software and updates on managed Mac computers.	
Parallels Desktop configuration management	Configure Parallels Desktop and virtual machines installed on a Mac	
Parallels Application Portal	Allows Mac users to view and install macOS applications made available to them by the IT administrator.	Parallels Mac Client
Enroll and manage Mac computers over the Internet	Support for Configuration Manager native Internet-Based Client Management (IBCM) enables Mac users and the IT to enroll and manage Mac computers over the Internet.	IBCM Proxy

Mac and Apple mobile devices configuration management via Configuration Profiles	Configure Mac computers and enforce compliance using the Configuration Manager Compliance Settings functionality.	MDM Proxy
Enroll and manage Mac computers via Apple DEP	Support for the Apple Device Enrollment Program (DEP) and unique integration with Configuration Manager enables the IT to seamlessly set up and provision new Mac computers for their employees.	
Enroll and manage Apple mobile devices via MDM	Enroll Apple mobile devices in Configuration Manager via Parallels MDM Proxy.	
Inventory of Apple mobile device hardware and installed applications	Hardware and software inventory is automatically collected and can be viewed in the Configuration Manager console.	
Apple VPP support	Deploy licensed AppStore applications and automatically track the number of consumed licenses.	
Remote lock and wipe for Mac and Apple mobile devices.	Remotely lock and wipe a Mac computer or an Apple mobile device it it's lost or stolen.	
FileVault 2 encryption management* MDM required for Big Sur only	Enforce FileVault 2 encryption on managed Mac computers.	
macOS patch management	Automates patch and update management of Mac computers.	OS X Software Update Point
Operating system deployment. **Note: Not available for Big Sur!**	Deploy macOS images to Mac computers using the Configuration Manager Task Sequence functionality.	NetBoot Server

Order of deployment

We suggest the following order to minimize the turnarounds in deployment process:

1 Parallels Configuration Manager Proxy

2 Parallels Configuration Manager Console Extensions

3 Parallels IBCM/MDM Proxy

4 Other components, in any order.

Install Parallels Mac Management

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

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

CHAPTER 3

Deploying Parallels ConfigMgr Proxy and Console Extensions

In This Chapter

Pre-installation checklist

	Task	Topic in this guide
□	Configuration Manager, Windows, and macOS versions are supported.	General requirements (p. 8)
□	Distribution Points configured.	Distribution Point Role configuration (p. 20)
□	IIS settings on the Distribution Point server are correct.	IIS Settings on the Distribution Point server (p. 20)
□	Configuration Manager Boundaries configured.	Configuration Manager Boundaries configuration (p. 20)
□	Windows firewall configured (allows in/out-bound connections to Parallels Device Management services.	Port reference (p. 70)
□	macOS firewall configured (allows in/out-bound connections to Parallels Device Management services).	Network and firewall configuration (p. 21)
□	Network environment (allows communication between Parallels Device Management components).	Network and firewall configuration (p. 21)
□	Date and time synchronization between Windows Servers and Mac computers works reliably.	Date and time synchronization (p. 21)
□	Reporting Point Role configured. Optional but needed to view reports.	Reporting functionality requirements (p. 21)
□	Report Viewer works well. Optional but needed to view reports.	Reporting functionality requirements (p. 21)

□	Ports used by Parallels Device Management are open.	Port reference (p. 70)
□	Installation locations for Parallels Configuration Manager Proxy and Console Extensions are identified.	Deployment scenarios (p. 15)
□	User account for configuring ConfigMgr Proxy is set up.	Permissions for configuring Parallels ConfigMgr Proxy (p. 22)
□	User account for running the ConfigMgr Proxy service is set up.	Permissions for running Parallels ConfigMgr Proxy service (p. 23)
□	Certificate template for ConfigMgr Proxy created (if using PKI).	PKI configuration (p. 23)
□	Certificate template for Mac Clients created (if using PKI).	PKI configuration (p. 23)

Deployment scenarios

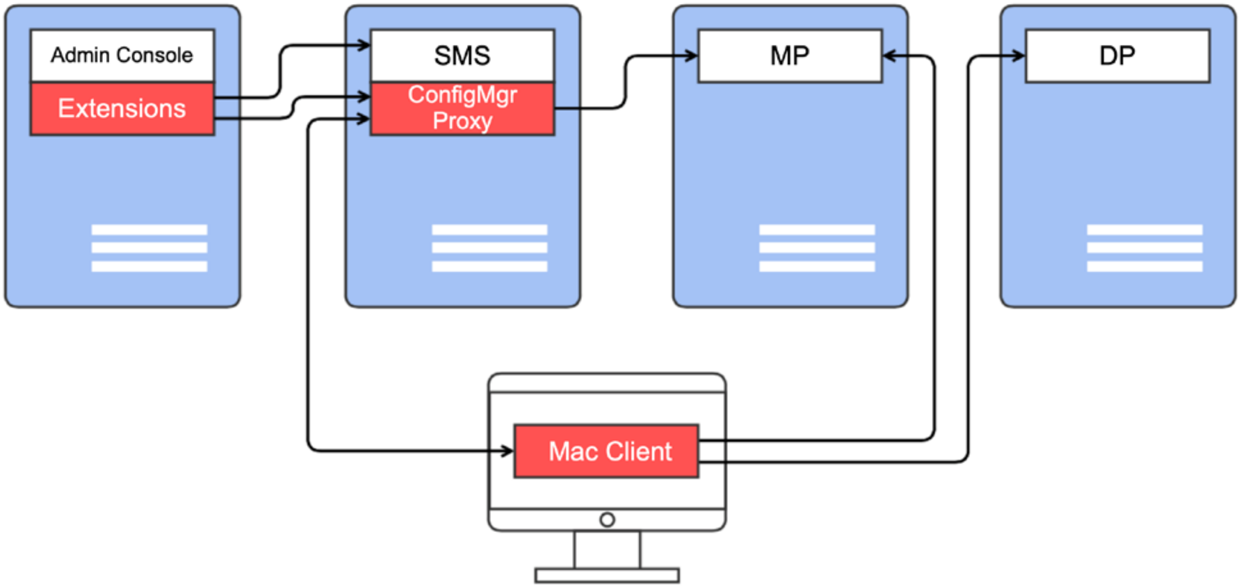
Parallels Configuration Manager Proxy must be installed on each primary Configuration Manager site. If you have secondary sites, you can choose from the following installation options:

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

Deploying to a standalone Configuration Manager site

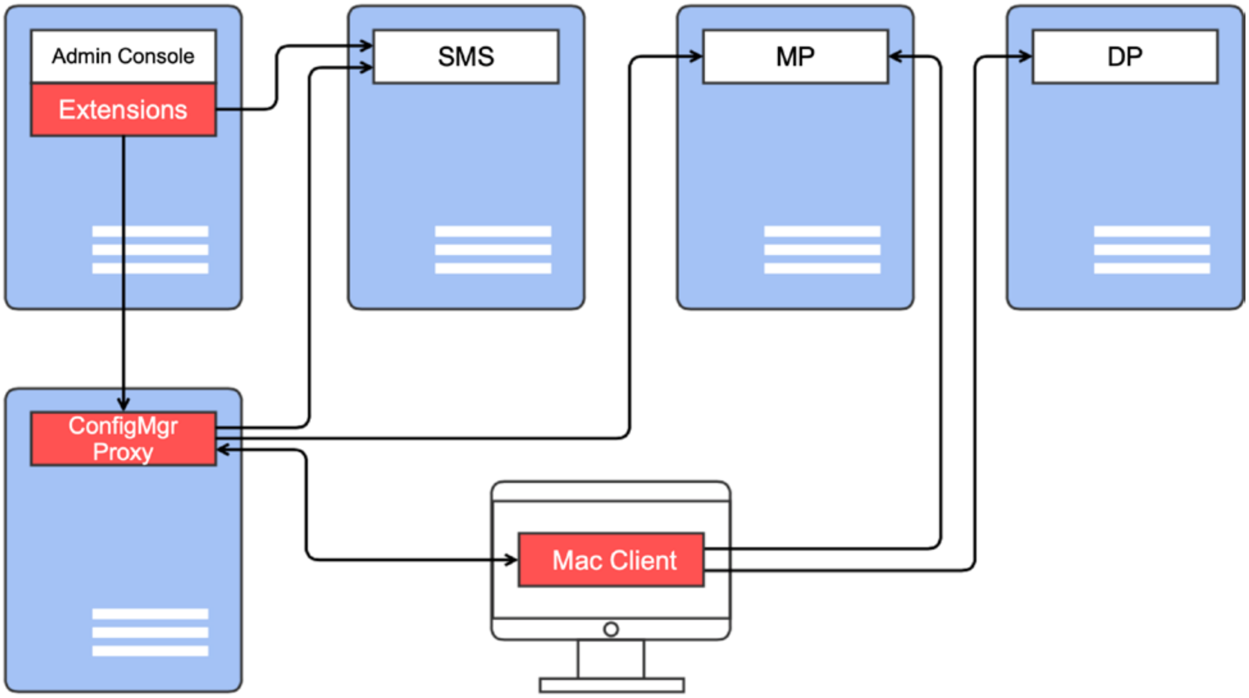
Installing Parallels Configuration Manager Proxy

Parallels Configuration Manager Proxy (ConfigMgr Proxy) can be installed on any computer that resides within Configuration Manager site boundaries and can establish a connection with the server hosting the SMS provider. In most cases, installing ConfigMgr Proxy on a server that has the SMS provider installed is recommended (see the diagram below).



The arrow lines on the diagram represent communication channels between Parallels Device Management and Configuration Manager components.

Alternatively, ConfigMgr Proxy can be installed on separate server, as shown on the following diagram:



More often than not, your Configuration Manager deployment will have several components that coexist on the same server.

Installing Parallels Device Management Console Extensions

A standalone Configuration Manager site would have at least one computer with Configuration Manager Administrative Console (Admin Console) installed. It could be installed on the same server that has the System Management Server (SMS) provider installed or on a separate computer. You must install Parallels Device Management Console Extensions on a computer that has the Admin Console installed.

Deploying to a primary site with secondary site(s)

If a primary site in your Configuration Manager installation has secondary sites, you may deploy Parallels Device Management either to the primary site only or the primary site and all secondary sites.

Deploying to a primary site

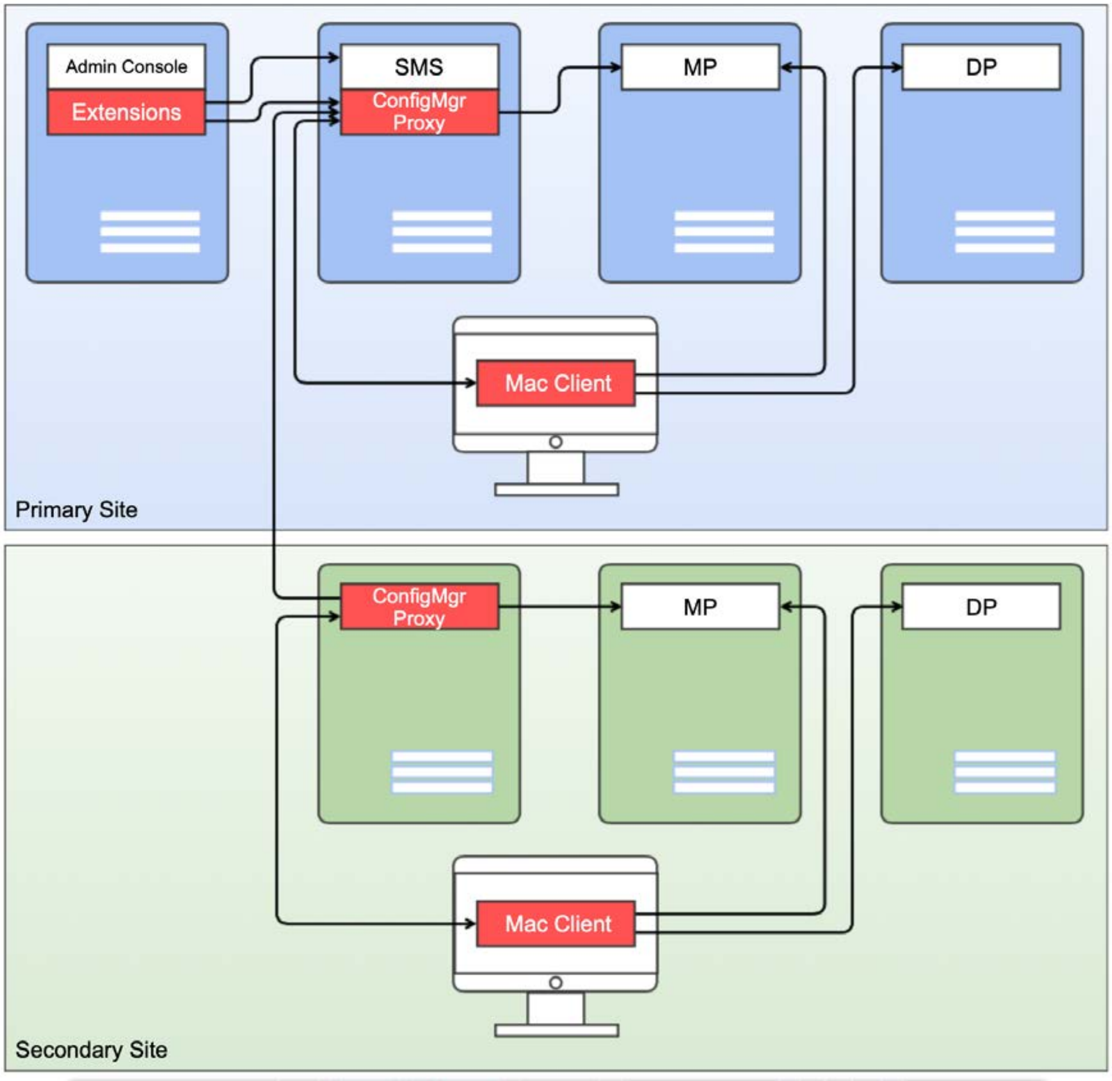
When deploying Parallels Device Management to a primary site, follow the same procedure as described in **Deploying to a standalone Configuration Manager site** (p. 16).

Deploying to a secondary site

ConfigMgr Proxy should be deployed on all secondary sites. While this is not required, it's highly recommended. The benefits of such a deployment are:

- Allows more efficient use of bandwidth. If ConfigMgr Proxy is not installed in a secondary site, Parallels Mac Clients (Mac Client) in that site will have to communicate with the ConfigMgr Proxy in the primary site.
- Simplifies manual Mac Client enrollment. If ConfigMgr Proxy is not installed in a secondary site and you try to manually enroll Mac Clients, you will have to use Active Directory (AD) credentials that have client enrollment privileges assigned in the primary site.

The following diagram illustrates a deployment where Parallels Configuration Manager Proxy is installed on secondary sites:



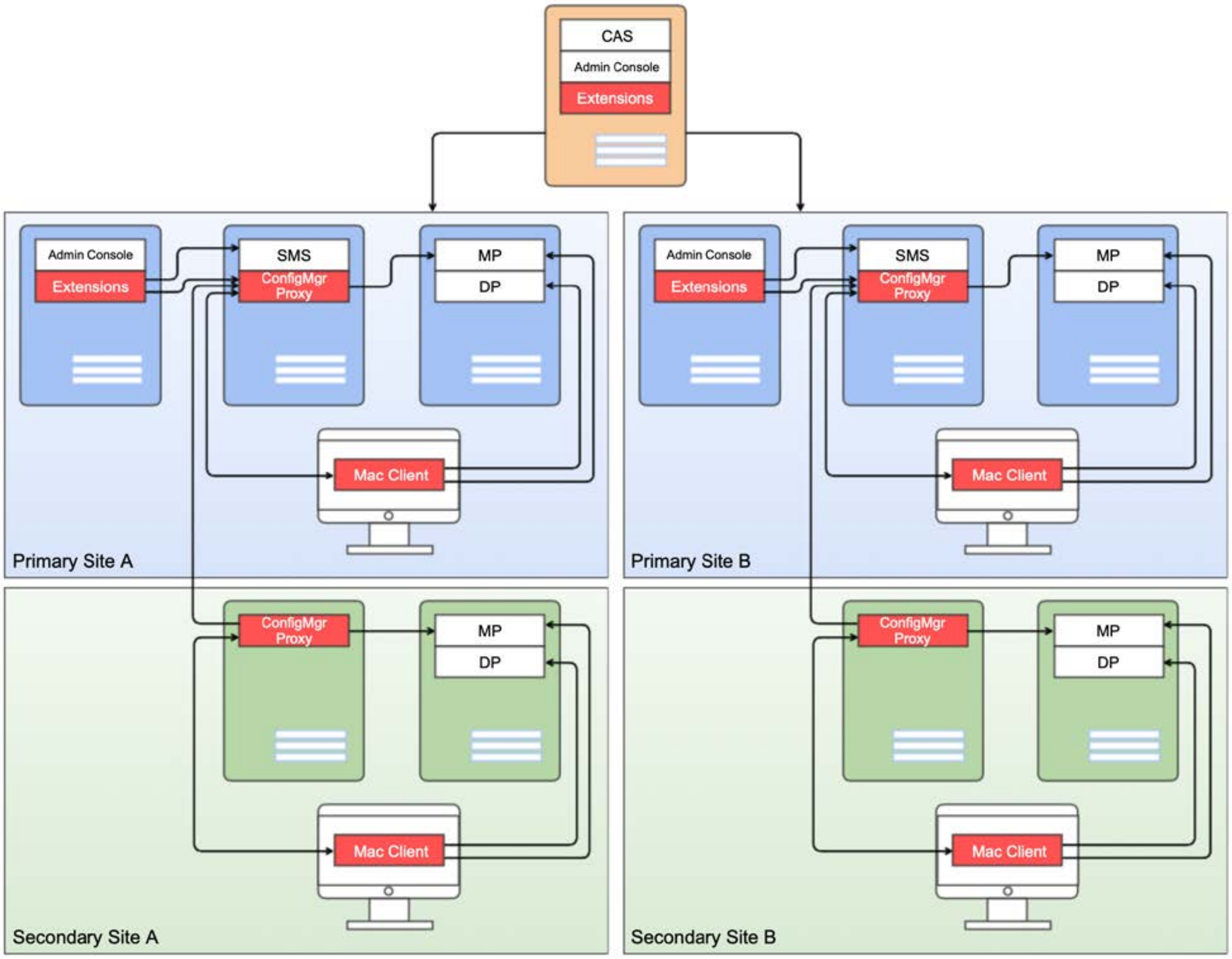
Deploying to a Central Administration Site (CAS)

The only additional step to perform when deploying Parallels Device Management in a Central Administration Site (CAS) environment is to install Parallels Console Extensions on the computer hosting the CAS Configuration Manager Console. However, this step is optional.

Note that the following features are not supported when Parallels Device Management Extensions are installed on a CAS:

- Configuration of Parallels Network Discovery
- Retrieval of escrowed FileVault 2 personal keys
- macOS image deployment functionality

The following diagram illustrates a deployment of Parallels Device Management in a CAS environment:



Parallels Configuration Manager Proxy requirements

The subsequent sections describe Parallels Configuration Manager Proxy requirements.

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 choose **Properties**.
4. In the **Distribution Point Properties** dialog set the following options:
   - On the **General** tab, select **HTTP** or **HTTPS** in the **Specify how client computers communicate with this distribution point** group. If you'll be using Public Key Infrastructure (PKI) for authentication, you need to select **HTTPS**. The PKI integration is described in **PKI configuration** (p. 23).
   - If you've selected **HTTP**, also select 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. Verify that **Windows Authentication** is enabled.
5. Click the **Default Web Site** and double-click **Authorization Rules** in the IIS section.
6. Verify that authorization is allowed for all users.

Configuration Manager Boundaries configuration

Each Mac computer should fall in an Configuration Manager boundary for enrollment to be successful. This is needed to bind a Mac to a specific ConfigMgr Proxy, especially in a multi-site Configuration Manager configuration.

Network and firewall configuration

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

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

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

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

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

Firewall should be configured in Windows and macOS to enable connectivity between the following parties:

- Console Extensions and ConfigMgr Proxy
- Console Extensions and Mac computers
- Mac computers and ConfigMgr Proxy
- Mac computers and Configuration Manager (DPs, MPs)

See also **Port reference** (p. 70)

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.

Reporting functionality requirements

The Reporting Point role and Report Viewer described below are not required in order to install Parallels Device 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. Click **Start** > **Control Panel** > **Programs and Features**.
2. Verify that **Microsoft Report Viewer Redistributable** is installed.

Permissions for configuring Parallels ConfigMgr Proxy

To configure ConfigMgr Proxy using the Parallels Configuration Manager Proxy Configuration Wizard, you need a domain user with the following set of permissions:

- Local Administrator rights on the computer where the Parallels Configuration Manager Proxy will be installed.
- DCOM Remote Activation permissions are required to enable communication of the CM Proxy configuration utility with SMS Provider using DCOM.
- Full Administrator rights in Configuration Manager are required to make changes in WMI objects in Configuration Manager during CM Proxy configuration. Changes include retrieving site information, registering CM Proxy certificates, and others.
- Specific permissions on the following containers in Active Directory:
  - **a** System/ParallelsServices — to create/modify/set permissions on Service Connection Point AD objects.
  - **b** ProgramData/Parallels — to create/modify/set permissions on AzMan (Authorization manager) store objects.
- Permissions to read/write Service Principal Name 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.
- Permissions in MS SQL Server are required to create and work with a database storing the Parallels Device Management data.

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

For detailed instructions about granting permissions for configuring ConfigMgr Proxy, see the following KB article: https://kb.parallels.com/125282.

You can also use PMM Server Tools to grant all necessary permissions using PowerShell script. For details, see https://kb.parallels.com/125278.

Permissions for running Parallels ConfigMgr Proxy service

To run the Parallels Configuration Manager Proxy service, you need a domain user with the following set of permissions:

- Local administrator rights on the computer where the Parallels Configuration Manager Proxy will be installed.
- DCOM Remote Activation permissions are required to enable communication of CM Proxy with SMS Provider using DCOM.
- Full Administrator rights in Configuration Manager are required for ConfigMgr Proxy to make changes in WMI objects in Configuration Manager.
- Read, Write, and Create All Child Objects permissions on the System/ParallelsServices/PmaConfigMgrProxy-<site-code> container in Active Directory, if it exists.
- Read and write permissions on Configuration Manager Network Share are required for ConfigMgr Proxy for registering new devices in Configuration Manager.

For detailed instructions about granting permissions for running ConfigMgr Proxy, see the following KB article: https://kb.parallels.com/125283.

You can also use PMM Server Tools to grant all necessary permissions using PowerShell script. For details, see https://kb.parallels.com/125278.

PKI configuration

If your Configuration Manager is configured for HTTPs (PKI) then you will need to configure the Parallels Configuration Manager Proxy to use the PKI mode as well to enable its communication with Configuration Manager. Such a configuration will enable ConfigMgr Proxy and Parallels Mac Clients to communicate with Configuration Manager securely by using mutual authentication and encrypted data transfers.

If Configuration Manager is configured for both HTTPs and HTTP, you can skip this section and continue with **Configuring Parallels Configuration Manager Proxy** (p. 27). You can perform the PKI integration at any time later by completing the steps described in subsequent sections and then reconfiguring Parallels Device Management. The reconfiguration involves running the Configuration Manager Proxy Configuration Wizard and specifying the appropriate options on the Parallels Client certificate management settings page of the wizard.

To configure ConfigMgr Proxy to use the PKI mode you need to prepare two certificate templates in your Certificate Authority (CA) trusted by Configuration Manager:

- ConfigMgr Proxy certificate template — it is used for issuing a PKI certificate for the ConfigMgr Proxy at the time of its configuration. This PKI certificate will secure the communication between the ConfigMgr Proxy and the Configuration Manager site.
- Parallels Mac Client certificate template — it will be used for issuing a PKI certificates for Parallels Mac Clients by the ConfigMgr Proxy at the time of enrolling of a Mac in Configuration Manager. This PKI certificate will secure the communication between Parallels Mac Client and the Configuration Manager site.

What this section does not cover

The material presented in this and subsequent sections does not cover any of the concepts behind PKI design and implementation. It describes what needs to be done in order to integrate Parallels Device Management with an existing PKI installation. If you would like to learn more about PKI, you can read the Securing Public Key Infrastructure (PKI) content on the Microsoft's website, which can be found at the following URL: https://technet.microsoft.com/library/dn786443.aspx.

Creating a certificate template for ConfigMgr 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.

For detailed instructions on how to manually create a certificate template, please also see https://kb.parallels.com/125276.

You can also use PMM Server Tools to grant all necessary permissions using PowerShell script. For details, see https://kb.parallels.com/125278.

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.

For detailed instructions on how to manually create a certificate template, please also see https://kb.parallels.com/125281.

You can also use PMM Server Tools to grant all necessary permissions using PowerShell script. For details, see https://kb.parallels.com/125278.

Handling expired certificates

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

- When the Proxy needs to communicate with a Mac, it first examines the digital certificate of the Parallels Mac Client running on it. If a certificate has expired or will expire soon, it will automatically renew the certificate.
- Parallels Configuration Manager Proxy will also check if the signing certificate of the currently used certification authority matches the one used by the Parallels Mac Client's certificate. If it's not, a new certificate will be issued for the Parallels Mac Client using the current CA.
- The Proxy validates its own digital certificate at preset intervals. If a certificate is not valid, a log entry is created in the `isv_proxy_service.log` file and in the Windows event log. The relevant log entries can be viewed in the `%WINDIR%\Logs\pmm\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 Device Management does not support automatic renewal of the Parallels Configuration Manager Proxy certificate. This functionality may become available in a later version of Parallels Device Management. For the instructions on how to renew the certificate manually, please see https://kb.parallels.com/123836.

Configuring Parallels Configuration Manager Proxy

The Parallels Configuration Manager Proxy Configuration Wizard starts automatically after the Parallels Device Management installation is completed. 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.

Step 1: SMS Provider location

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

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

Step 2: Configuration Manager Proxy service account

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

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

Step 3: Prerequisites check

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

- Current user access rights for configuring the ConfigMgr Proxy. See **Permissions for configuring Parallels ConfigMgr Proxy** (p. 22).

- Access rights of the user you specified in the previous step for running the ConfigMgr Proxy service. See **Permissions for running Parallels ConfigMgr Proxy service** (p. 23).

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 don't need to quit the wizard at this point. Simply make the required changes and then click the **Rerun** button. If the fixes were sufficient (all prerequisites are met), the **Next** button becomes enabled and you can continue to the next wizard page.

Step 4: Parallels Client certificate management settings

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

The options described below allow you to integrate Parallels Device 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.

The **Mac client certificate template** field is used to specify a certificate template for Mac computers. Click the **Browse** button to select a template.

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

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

Step 5: Role-based security

The **Role-based security** page allows you to configure the Configuration Manager Proxy role-based access control. The roles are created during the Parallels Device 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.

- **FileVault Key Administrators**: This role grants read rights to the Parallels Device Management database. 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 Device Management features.
- **Enrollers**: Members of this role can only enroll Mac computers in Configuration Manager.

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 Windows **Select Users, Computers, Service Accounts, or Groups** dialog to specify a user or a group.

Step 6: Configuration Manager Proxy communication ports

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

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

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

Step 7: Customer Experience Program

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

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

Step 8: Configuration settings summary

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

If you need to reconfigure 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.

Installing Console Extensions and iMazing Profile Editor

Parallels Device Management v9.0 and newer comes with iMazing Profile Editor from DigiDNA. The editor is used to create configuration profiles for Mac computers and Apple mobile devices in the Configuration Manager console. The editor is installed together with ConfigMgr Console Extensions, but the installation is carried out as a separate process where you can choose whether to install it. We highly recommend to install iMazing Profile Editor if you plan to create configuration profiles. When installed, the editor is integrated into the Configuration Manager console, so there's no need to use an external profile editor.

To install iMazing Profile Editor, select the ConfigMgr Console Extensions component in the Parallels Device Management installer. The iMazing Profile Editor installer runs as a post-install action in the full featured GUI mode (it will not run in the silent mode). During the installation, please read the iMazing Profile Editor license agreement and then follow the onscreen instructions.

Please note that iMazing Profile Editor can also be installed later directly from the Configuration Manager console. If you didn't install the editor, you will be asked if you want to install it when trying to create a configuration profile in the console. For more information, please see the **Parallels Device Management for Configuration Manager Administrator's Guide**.

Updating and removing iMazing Profile Editor

An installed iMazing Profile Editor is updated using the install/update/repair cycle of Parallels Device Management. A confirmation dialog to update iMazing Profile Editor will be presented to a user if the Parallels Device Management installation package includes a newer version of iMazing Profile Editor compared to the currently installed version.

Note that iMazing Profile Editor is not automatically uninstalled when you remove Parallels Device Management from a computer. To uninstall it, use the standard Windows software uninstallation facilities.

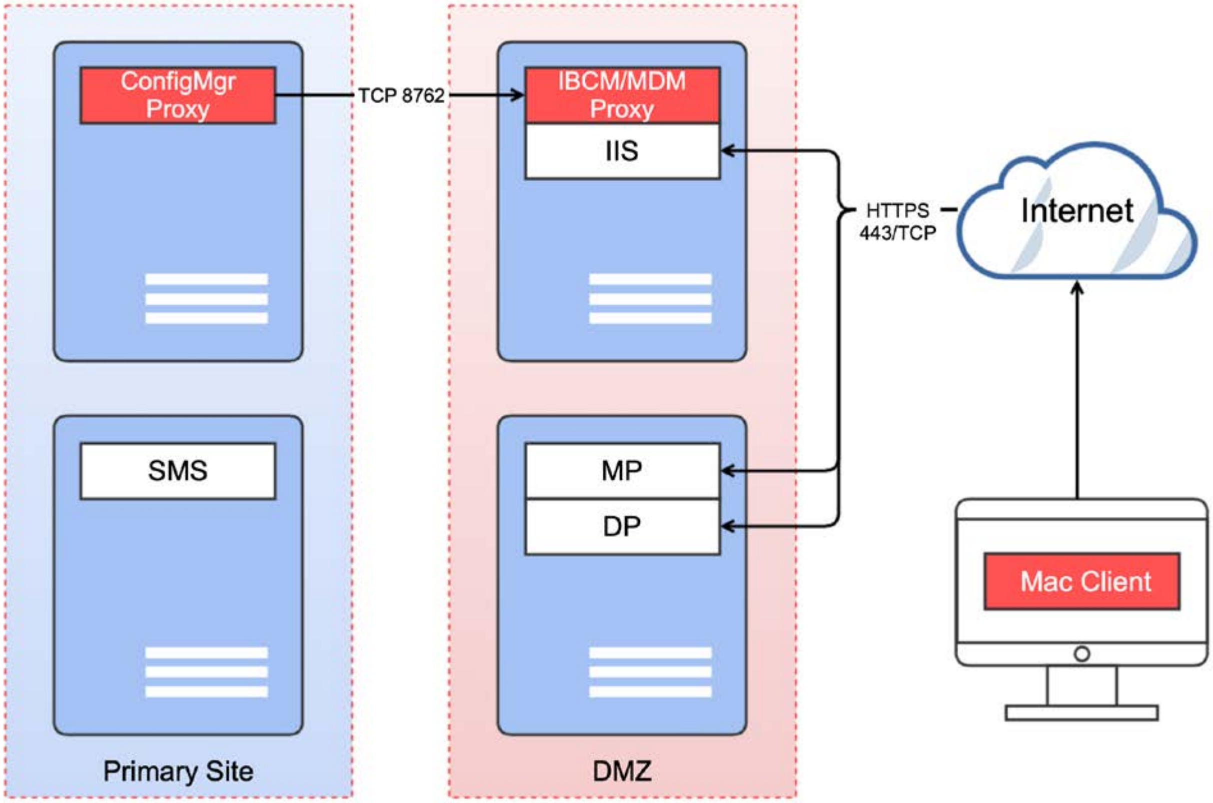
CHAPTER 4

Deploying IBCM/MDM Proxy

In This Chapter

Overview

A typical infrastructure used by Parallels IBCM/MDM Proxy is illustrated in the diagram below.



- Parallels IBCM/MDM Proxy serves as a transparent proxy that passes requests between managed devices (Mac computers and Apple mobile devices) and Parallels Configuration Manager Proxy.
- The connector is a plugin to IIS, which is also used by Configuration Manager in the IBCM setup for communications between Mac computers on the Internet and Management Points / Distribution Points.
- A single instance of Parallels IBCM/MDM Proxy serves a single primary Configuration Manager site. If you have multiple primary sites, then you will need to repeat the hierarchy shown above for each primary Configuration Manager site.

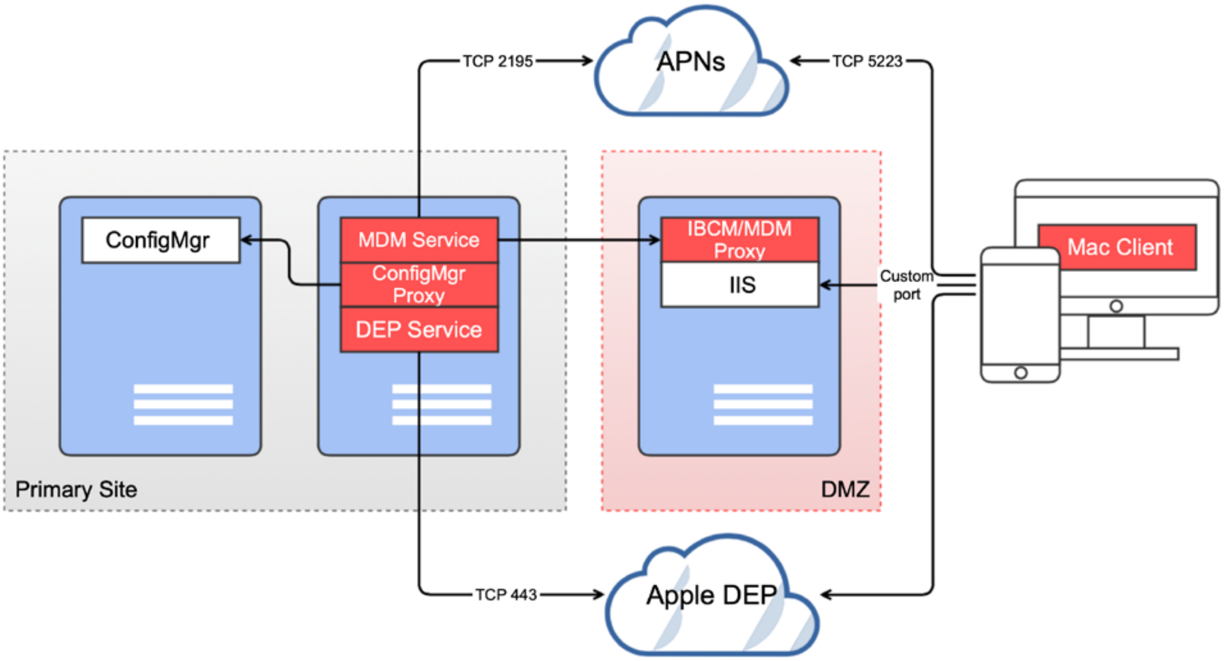
Parallels Configuration Manager Proxy establishes a permanent SSL-secured link with Parallels IBCM/MDM Proxy, which is configured after the components are installed. Trust is established using the certificate pinning mechanism, when each party is configured to stick to a specific certificate of another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

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

MDM Proxy specifics

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

The following diagram shows components that participate in a Parallels Device Management MDM configuration. It provides information on where the components are located and how they communicate with each other.



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

Pre-installation checklist

	Task	Topic in this guide
□	If upgrading from a version less than 8.5 to version 8.5 or later, the older MDM setup is migrated.	—
□	Server (preferably in DMZ) for installing IBCM/MDM Proxy is identified, separate for each primary Configuration Manager site.	Parallels IBCM/MDM Proxy requirements (p. 35)
□	Server is accessible from the host where the primary ConfigMgr Proxy is installed.	Parallels IBCM/MDM Proxy requirements (p. 35)
□	A publicly available domain name is assigned to the server.	Parallels IBCM/MDM Proxy requirements (p. 35)
□	IIS 7.0 or above installed on the server.	Parallels IBCM/MDM Proxy requirements (p. 35)
□	IIS Web Server role is installed.	Parallels IBCM/MDM Proxy requirements (p. 35)
□	IIS Management script and tools are installed.	Parallels IBCM/MDM Proxy requirements (p. 35)
□	At least one internet-enabled MP exists.	—
□	At least one internet-enabled DP exists.	—
□	A Web server certificate for IBCM Proxy is obtained (it is possible to use a wildcard certificate).	Secure IBCM/MDM Proxy website with an SSL certificate (p. 36)
□	A Web server certificate for MDM Proxy is obtained (it is possible to use a wildcard certificate).	Secure IBCM/MDM Proxy website with an SSL certificate (p. 36)
□	The Parallels Configuration Manager Proxy certificate imported to the certificate store on the server where IBCM/MDM Proxy will be installed.	Enable trust between IBCM/MDM Proxy and CfgMgr Proxy (p. 36)
□	Parallels MDM certificate is imported to the certificate store on the server where IBCM/MDM Proxy will be installed.	Enable trust between IBCM/MDM Proxy and MDM service (p. 37)

Post-installation checklist

	Task	Topic in this guide
□	MDM link is configured.	Configure the MDM Link (p. 40)
□	APNs is configured.	Configure APNs certificate (p. 41)
□	Automatic MDM enrollment configured for Macs enrolled in Configuration Manager.	Configure Automatic Mac Enrollment in MDM (p. 44)
□	If upgraded from version less than 8.5 to version 8.5 and later, the older MDM setup is migrated.	—

□	A connection is established with the Apple DEP web service.	Establish a connection with the Apple DEP web service (p. 45)
□	Apple VPP support is configured (if planning to use this functionality).	Configuring Apple VPP support (p. 47)

Parallels IBCM/MDM Proxy requirements

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

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

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

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

Prerequisites

In order for Parallels IBCM/MDM Proxy to work, Parallels Device Management must be configured for Public Key Infrastructure (PKI). For details please see **PKI configuration** (p. 23).

Other requirements for installing Parallels IBCM/MDM Proxy are:

- The server on which you'll be installing Parallels IBCM/MDM Proxy must be accessible from the server where Parallels ConfigMgr Proxy is installed. Note that the Parallels ConfigMgr Proxy must be installed and configured before you install Parallels IBCM/MDM Proxy.
- The server must be accessible from the Internet. For increased security, the server should be located in DMZ.
- Ensure that a publicly available domain name is assigned to the server. Mac computers and Apple mobile devices will use this domain name to communicate with Parallels IBCM/MDM Proxy over the Internet.
- IIS 7.0 or above must be installed.

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

Secure IBCM/MDM Proxy website with an SSL certificate

Parallels IBCM/MDM Proxy uses an IIS website to receive HTTP/HTTPS requests. A Web server certificate can be one of the following:

- Self-signed or purchased.
- Issued for specific host or wildcard.

By using a wildcard SSL certificate, so you don't have to purchase a separate certificate for each Internet-facing host.

To use a wildcard certificate:

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

Enable trust between IBCM/MDM Proxy and CfgMgr Proxy

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

To enable trust:

1 Log in to the computer where Parallels Configuration Manager Proxy is installed and export the certificate named **Parallels Configuration Manager Proxy** (without the private key) from the **Local Computer** > **Personal** certificate store. To export the certificate, open the **Certificates** snap-in (run the `certlm` command), then navigate to **Local Computer** > **Personal** > **Certificates**, locate the Parallels Configuration Manager Proxy certificate, right-click it and choose **All Tasks** > **Export**. Use the DER or Base-64 encoding.

2 Now log in to the computer where Parallels IBCM/MDM Proxy is installed and import the certificate from the previous step into the **Local Computer** > **Personal** certificate store. When running the **Certificate Import Wizard**, select **Place all certificates in the following store** and choose **Personal** from the drop-down list.

Enable trust between IBCM/MDM Proxy and MDM service

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

To enable trust:

1 Log in to the computer where Parallels Configuration Manager Proxy is installed and export the certificate named **Parallels MDM Service** (without the private key) from the **Local Computer** > **Personal** store. To export the certificate, open the **Certificates** snap-in (run the `certlm` command), then navigate to **Local Computer** > **Personal**, locate the **Parallels MDM Service** certificate, right-click it and choose **All Tasks** > **Export**.

2 Now log in to the computer where Parallels IBCM/MDM Proxy is installed and import the certificate from the previous step into the **Computer** > **Trusted Root Certificates** store. When running the **Certificate Import Wizard**, select **Place all certificates in the following store** and choose **Trusted Root Certificates** from the drop-down list.

Configure Parallels IBCM/MDM Proxy

The **Parallels IBCM/MDM Proxy Configuration Wizard** starts automatically after the component is installed. You can also run the wizard manually by navigating to **Apps** > **Parallels** and double-clicking **IBCM/MDM Proxy Configuration Utility**.

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

Configuring Parallels IBCM Proxy

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

Enabling IBCM:

- Install and configure IBCM Proxy on a server accessible from Internet.
- Configure IBCM Link from the Configuration Manager Console to enable communication between ConfigMgr Proxy and IBCM Proxy.

Run the configuration wizard

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

Configure IBCM Link

in this step, you need to configure the IBCM link so that Parallels Configuration Manager Proxy can communicate with Parallels IBCM/MDM Proxy.

To configure the link:

1. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **IBCM** / **IBCM Link**.
2. Right-click the **IBCM link** item in the right pane and choose **Properties**.
3. In the **IBCM Link Properties** dialog, click the **Configure** button to open the **Parallels IBCM Proxy Link Configuration Wizard**.
4. On the first page of the wizard, enter the Parallels IBCM/MDM Proxy location information, including:
   - The hostname of the computer where Parallels IBCM/MDM Proxy is running.
   - The port number on which Parallels IBCM/MDM Proxy is listening for Parallels Configuration Manager Proxy requests. This is the port you specified when you configured Parallels IBCM/MDM Proxy.
5. Click **Next**.

6 On the next page, a test connection will be established and you will see the details of the certificate provided by the remote party. Review the details of the certificate and confirm that it is the certificate that belongs to Parallels IBCM/MDM Proxy. If it is, click **Accept** and wait for the configuration settings to be applied. After that, click **Finish** to close the wizard. When the link is configured, its settings will be displayed in the preferences dialog.

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

Conclusion

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

Configuring Parallels MDM Proxy

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

Enabling MDM:

- Install and configure MDM Proxy on a server accessible from the Internet.
- Configure MDM Link from the Configuration Manager Console to enable communication between Parallels MDM service and MDM Proxy.
- Configure APNS certificate to enable communication between Parallels MDM Service and Apple Push Notification service.

Run the Configuration Wizard

1 On the first page, specify the port for incoming Parallels Configuration Manager Proxy connections. Make sure that this port is open for incoming connections.

2 On the next page, specify the Parallels Configuration Manager Proxy certificate that you have imported earlier. Click **Browse** to select the certificate.

3 Click **Next** to go to the next page of the wizard.

4 On the **Choose Web Sites for Parallels IBCM/MDM Proxy** page, select **MDM Proxy** (this will enable MDM Proxy on this computer) and then select an IIS web site from the drop-down list.

5 On the **Prerequisites Check** page, verify that all of the requirements are met. If not, resolve the issues and click the **Rerun** button (you can also go back or you can close the wizard and run it again later).

6 Click **Next** and then click **Finish** to close the wizard.

Configure the MDM Link

In this step, you need to configure the MDM link so that Parallels MDM Service can communicate with Parallels IBCM/MDM Proxy.

To configure the link:

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

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

   a Log in to the machine where MDM Proxy is installed.

   b Open the Internet Information Services (IIS) Manager.

   c Go to server-name > **Sites** > site-name > **ParallelsMacManagement.MDM**.

   d Double click on **SSL Settings**.

   e In **Client certificates**, choose the **Accept** option and click **Apply**.
5. Click **Next**. The wizard will try to connect to Parallels IBCM/MDM Proxy using the specified parameters. If the connection fails, verify that the information on the previous page is entered correctly and that the Parallels Configuration Manager Proxy certificate has been imported to the IBCM/MDM Proxy server.

6 On successful connection, the next page of the wizard opens displaying the Parallels IBCM/MDM Proxy certificate information. You need to accept it to continue. If you do, the certificate thumbprint is stored and will be used to verify future connections to Parallels IBCM/MDM Proxy. If the certificate is changed for any reason in the future, you will need to run this wizard again.

Configure APNs certificate

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

To configure APNs:

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

2 Right-click on **MDM Service** in the right pane and choose **Configure APNs**.

3 In the **APNs Certificate Properties** dialog, click **Configure**.

4 The **APNs Certificate Configuration Wizard** opens. Complete the wizard as described below.

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

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

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

- **Obtain a CSR from Parallels automatically** (p. 42)
- **Save the CSR file locally and then sign it using the Parallels certificate signing service** (p. 42)

Obtain a CSR from Parallels automatically

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

1 A progress bar will appear indicating the CSR preparation progress. During this time, the wizard will do the following in the background

a Create a certificate signing request (CSR) and the associated private key.

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

b Connect to the Parallels certificate signing service over the Internet and sign the CSR with Parallels MDM Signing Certificate.

2 Once the signed CSR is ready, the next page opens where you need to specify a local folder where you want to save it.

3 After the CSR file is saved, another page opens with instructions to proceed to the Apple Push Certificates Portal. Do not click **Next** yet and do the following instead:

o Open the Apple Push Certificates Portal in a web browser and log in using your Apple ID and password.

o **Important:** If this is the first time you are creating a certificate, click the **Create a Certificate** button. If you are renewing an existing certificate, find it in the **Certificates for Third-Party Servers** list and click the **Renew** button. After that, follow the onscreen instructions and upload the signed CSR file when asked to do so.

o Download the created APNs certificate file named “MDM_<VendorName>_Certificate.pem” to your local computer.

4 Back in the wizard, click **Next** to proceed to the page where you need to upload the APNs certificate file to the local server. Click **Browse** and specify a target folder.

5 When done, click **Next** to upload the APNs file.

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

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

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

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

2 A page opens where you can specify a local folder for saving the CSR and the private key files. Specify the folder and click **Next**.

3 Another page opens with instructions on how to proceed with signing the CSR and obtaining an APNs certificate from Apple. Do not click **Next** yet and do the following instead:

- Visit Parallels My Account at https://my.parallels.com. Sign in using your email address and password (if you don't have a Parallels account, you must register for one; a Parallels account is required to activate Parallels Device Management and to use other services, such as certificate signing).
- Once signed in, click **MDM Certificate** inside the **Parallels Device Management** product card.
- Follow the instructions on the **MDM Certificate Signing** page and upload the CSR file that you saved in step 2 above. When instructed, download the signed CSR to your local computer.
- Open the Apple Push Certificates Portal in a web browser and log in using your Apple ID and password.
- **Important:** If this is the first time you are creating a certificate, click the **Create a Certificate** button. If you are renewing an existing certificate, find it in the **Certificates for Third-Party Servers** list and click the **Renew** button. After that, follow the onscreen instructions. When asked, upload the signed CSR file that you obtained from Parallels My Account earlier.
- Download the created APNs certificate file named “MDM_<VendorName>_Certificate.pem” to your local computer.

4. Back in the wizard, click **Next** to proceed to the page where you need to upload the APNs file to the local server. Click **Browse** and specify a target folder.
5. When done, click **Next** to upload the APNs file.

Configure MDM profile signing

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

To sign the profile:

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

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

Configure Automatic Mac Enrollment in MDM

Note: This section describes configuration steps that only need to be performed if you are not using Apple DEP or if some of your Mac computers were not enrolled in Configuration Manager through DEP.

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

To configure automatic MDM enrollment:

1. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Device Management** / **Mobile Device Management** / **MDM Service**.
2. Right-click **MDM Service** in the right pane and choose **Enrollment Properties**. The **Parallels Mac Client MDM Enrollment Properties** dialog opens.
3. Select the **Enable automatic enrollment of Macs into Parallels MDM service** option and then choose one of the following:
    - **Enroll all Mac resources**. All Mac computers that are enrolled in Configuration Manager will be automatically enrolled in MDM (computers that are already enrolled in MDM via Apple DEP are excluded).
    - **Enroll Mac resources from following collections**. Only the Mac resources from the specified collection(s) will be enrolled. Select this option and click the **[+]** icon to select a collection and add it to the list (you can add more than one collection).
4. **Prompt user to approve the MDM profile** — select this option to prompt a Mac user to approve and install the MDM profile. This must be done because of the following requirements:
    - Apple requires user-approved MDM when delivering security-sensitive payloads. If you will be delivering such payloads to Mac computers via MDM, you need to select this option.
    - User approved MDM is required when delivering configuration profiles to macOS Big Sur. If target Mac computers run macOS Big Sur, you need to select this option.

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

    - MDM approval can only be done personally by a Mac user. With this option enabled, the user will see a dialog when Parallels Mac Client receives a policy update. The dialog informs the user that their computer must be enrolled in MDM and contains instructions on how to do it. The user should follow the instructions and install the MDM profile. If the user simply closes the dialog, it will be shown again on each policy update until the MDM profile is installed. Please also see macOS Big Sur notes below.

- As an IT administrator, you have the ability to determine whether the user has approved and installed the MDM profile. For details, see the **Reporting UAMDM Status** section.

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

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

macOS 11 Big Sur notes

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

1 In the notification dialog, click the **Open System Preferences** button.

2 The **System Preferences** dialog opens with the **Profiles** pane selected.

3 Clicks **Install** and follow the onscreen instructions to install the profile.

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

Post-installation steps

After deploying IBCM/MDM Proxy, you need to perform some post-installation steps in order to use some of the functionality.

Establish a connection with the Apple DEP web service

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

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

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

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

2 Right-click a DEP link in the right pane and choose **Properties**. The **DEP Link Properties** dialog opens.

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

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

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

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

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

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

Assign devices to the virtual MDM server

Assign your devices to the virtual MDM server on the Apple DEP website. For more information, please see the Apple Business Manager Getting Started Guide: https://www.apple.com/business/docs/site/Apple_Business_Manager_Getting_Started_Guide.pdf

View devices assigned to DEP

In the Configuration Manager console, navigate to **Administration** / **Parallels Device Management** / **Device Enrollment Program** / **Devices**. The list of devices assigned to the virtual MDM server will now be retrieved from your Apple DEP account and displayed in the **Devices** pane.

View DEP link properties

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

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

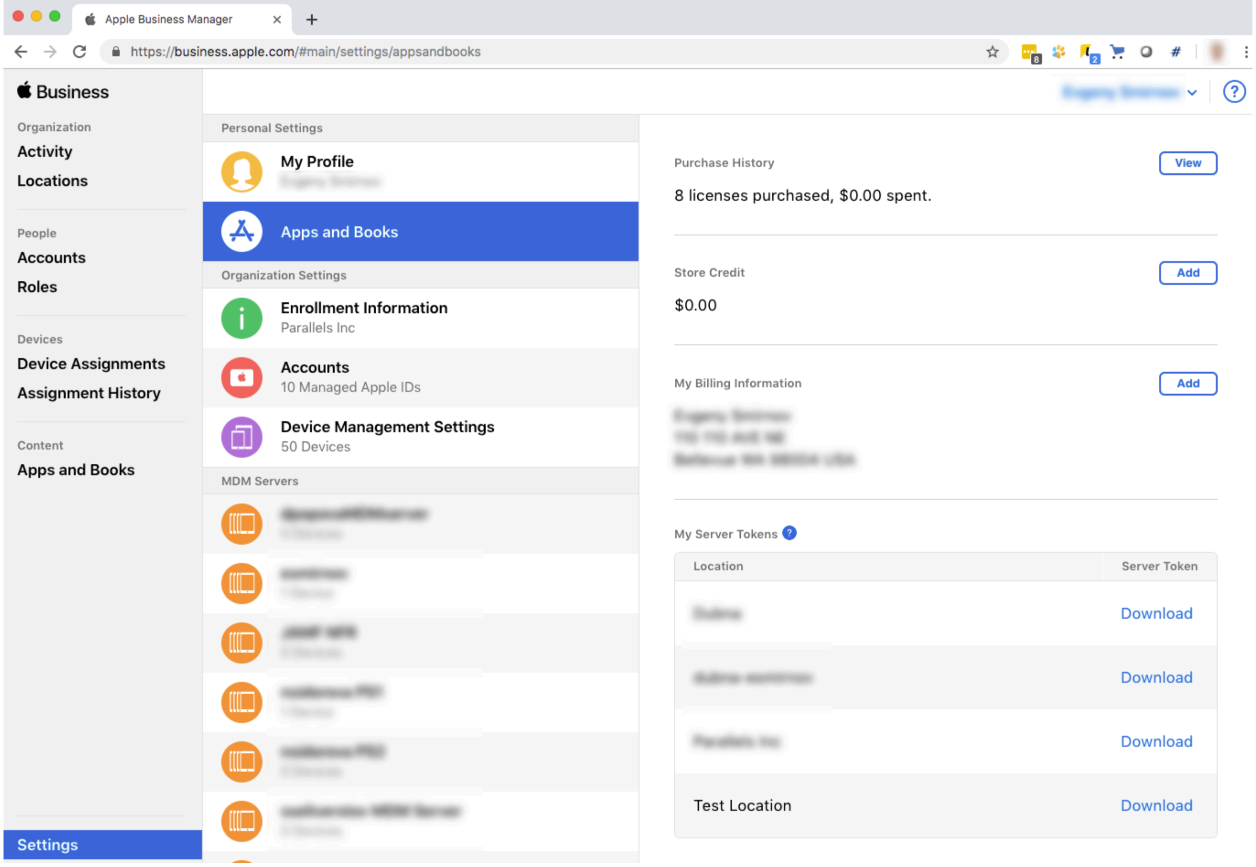
Configuring Apple VPP support

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

To add a VPP token:

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

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



Apple Business Manager

https://business.apple.com/#main/settings/appsandbooks

Business

[redacted]

Organization
- Activity
- Locations

People
- Accounts
- Roles

Devices
- Device Assignments
- Assignment History

Content
- Apps and Books

Settings

Personal Settings

My Profile
[redacted]

Apps and Books

Organization Settings

Enrollment Information
Parallels Inc

Accounts
10 Managed Apple IDs

Device Management Settings
50 Devices

MDM Servers

[redacted]

Purchase History — View

8 licenses purchased, $0.00 spent.

Store Credit — Add

$0.00

My Billing Information — Add

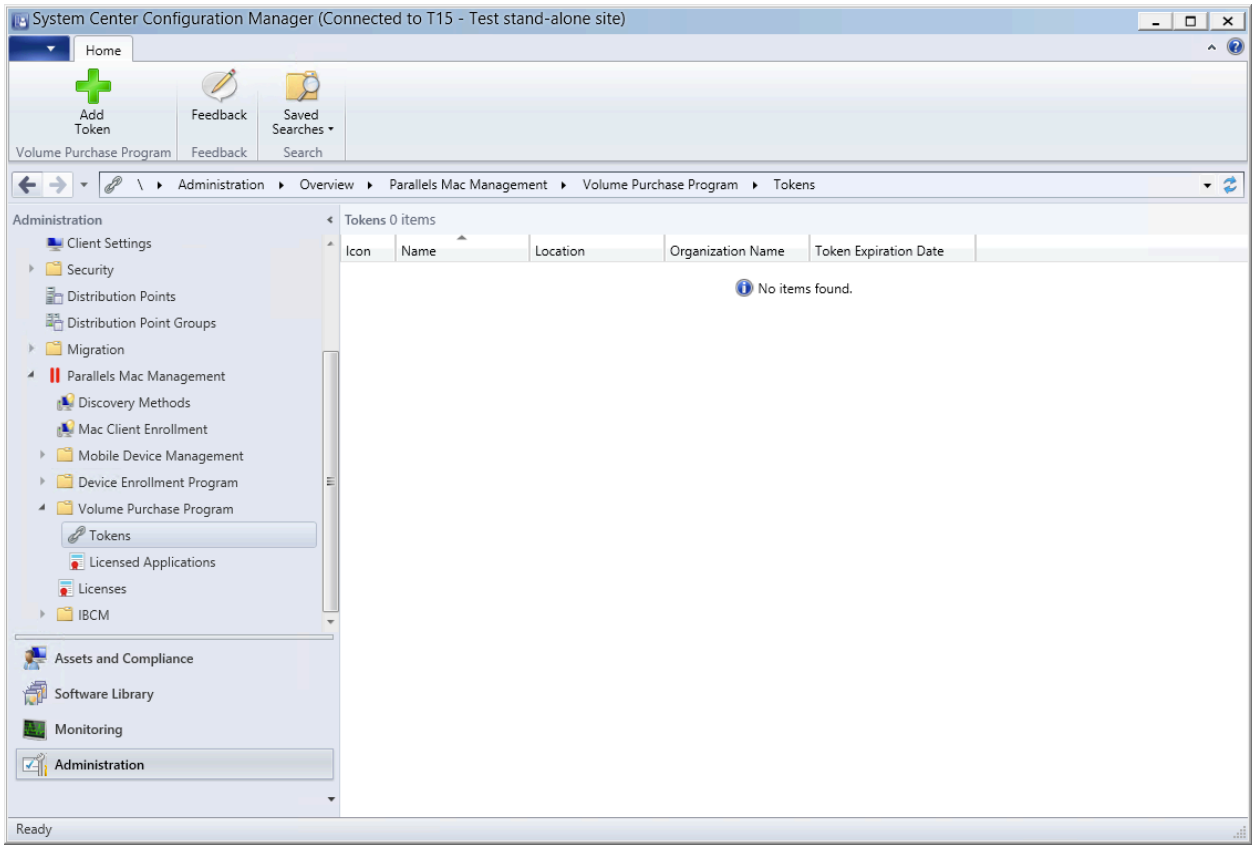
[redacted]

My Server Tokens

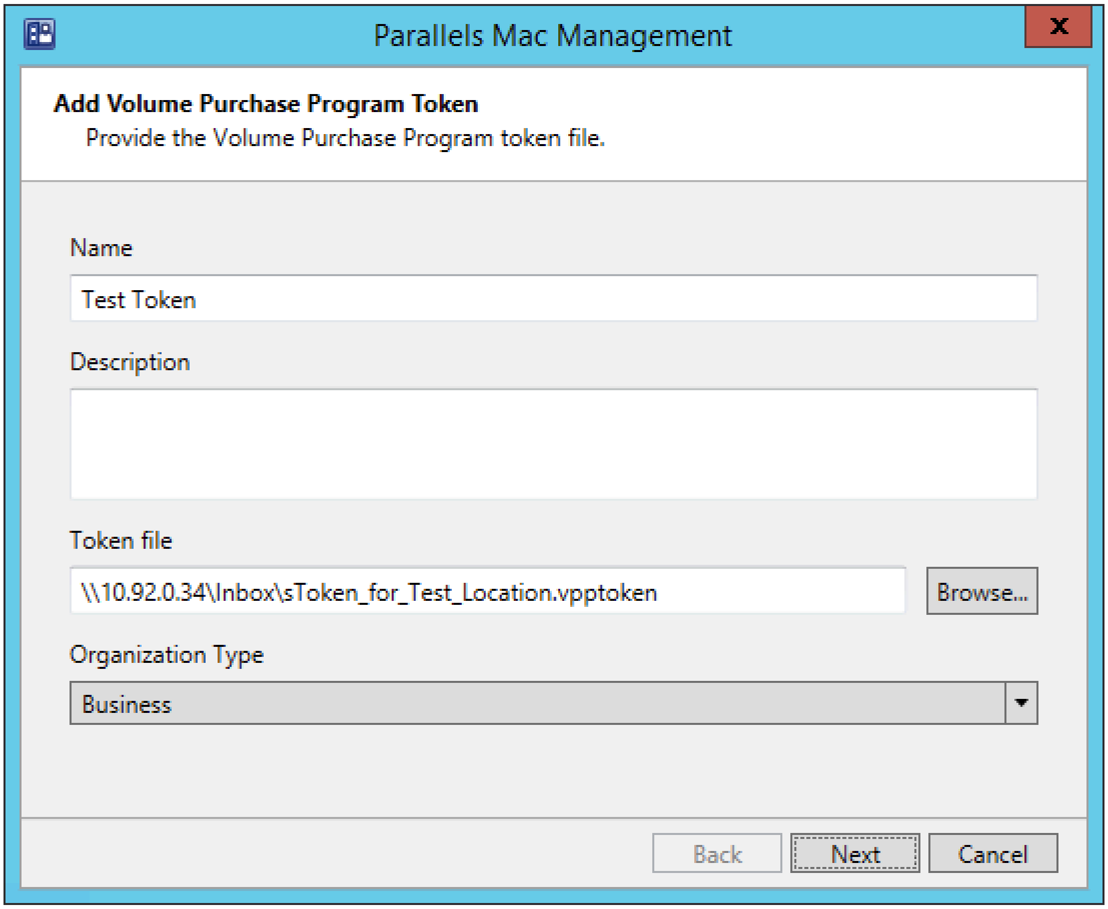
Location	Server Token
[redacted]	Download
[redacted]	Download
[redacted]	Download
Test Location	Download

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

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



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



Add Volume Purchase Program Token

Provide the Volume Purchase Program token file.

Name: Test Token

Description:

Token file: \\10.92.0.34\Inbox\sToken_for_Test_Location.vpptoken

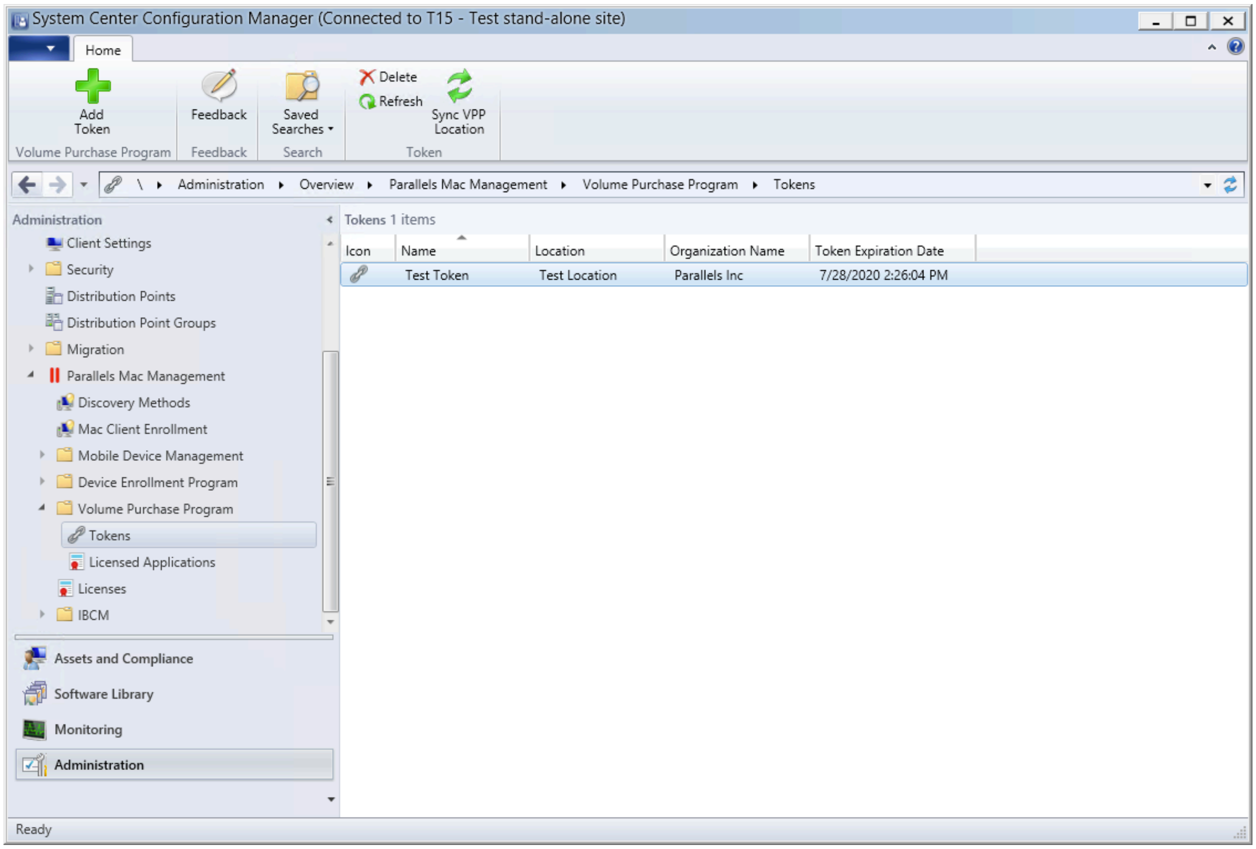
Organization Type: Business

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

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

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

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



Icon	Name	Location	Organization Name	Token Expiration Date
🔗	Test Token	Test Location	Parallels Inc	7/28/2020 2:26:04 PM

CHAPTER 5

Deploying Parallels OS X Software Update Point

In This Chapter

Pre-installation checklist

	Task
□	.Net Framework v4.0 or later installed
□	Windows Server Update Services (WSUS) is installed and configured for local publishing of updates
□	The WSUS signing certificate deployed
□	User account for running SUP service configured

Parallels OS X Software Update Point requirements

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

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

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

- Windows Server Update Services (WSUS) must be installed and configured for local publishing of updates. Please see the following page on the Microsoft's website for more info: https://msdn.microsoft.com/library/bb902479

  On the web page, refer to the "To set up the update server for locally-published content" section for instructions.
- A user account must be configured for running the Parallels OS X Software Update Point service. The account must have administrative rights on the local sever and must be a member of the WSUS Administrators group.
- The WSUS signing certificate must be deployed and accessible by the user account that will be running the Parallels OS X Software Update Point service. Please see the following KB article for more information: https://kb.parallels.com/123756.

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.

Configuring Parallels OS X Software Update Point

The Parallels OS X Software Update Point Configuration Wizard starts automatically after the component is installed. 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 rights on the local server and must be a member of the WSUS Administrators group.
2. On the **Prerequisites Check** page, verify that all of the requirements are met. If one or more of the requirements are not met, you need to resolve them before proceeding.
3. On the **Configuration settings summary** page, review the installation summary. If satisfied, click **Finish** to apply the settings and close the wizard.

Post-installation steps

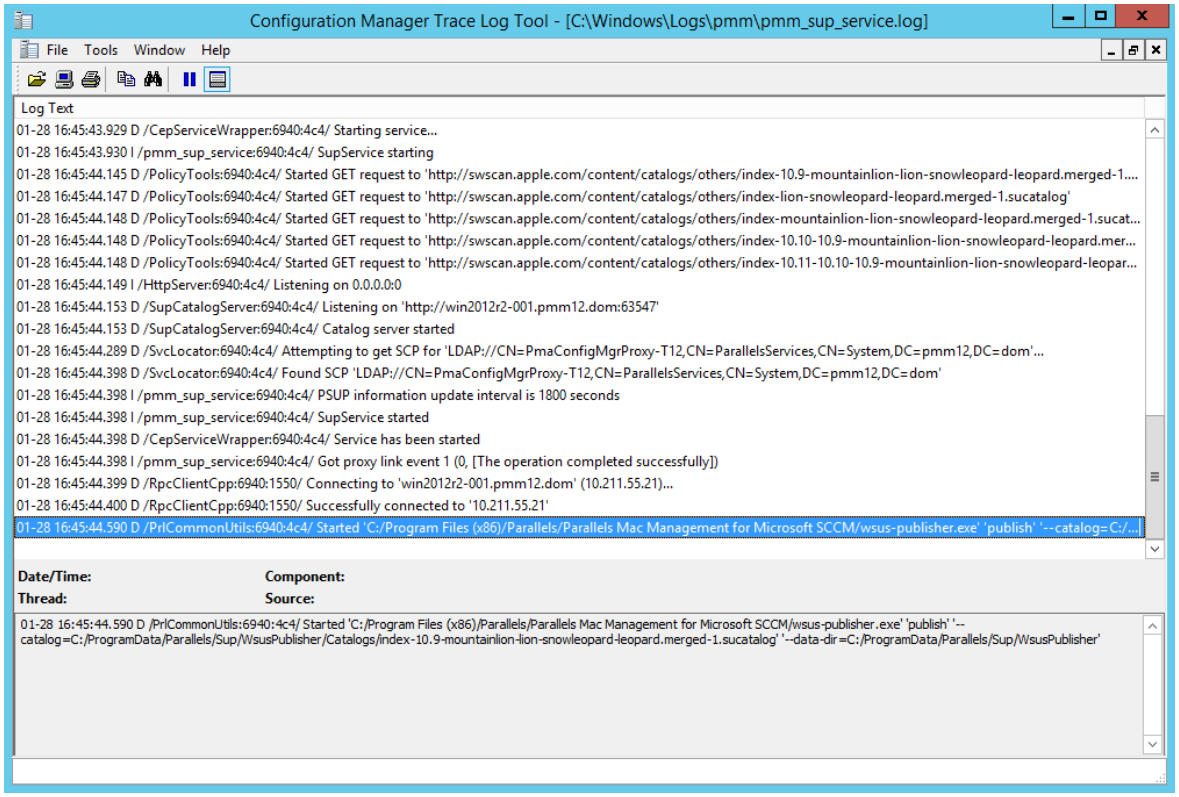
After you've deployed Parallels OS X Software Update Point, you need to import the information about available macOS updates into Configuration Manager, so they can be later deployed on Mac computers. The subsequent sections describe how to do it.

Import macOS software updates

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

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

   `%Windir%\Logs\pmm\pmm_sup_service.log` file.



Configuration Manager Trace Log Tool - [C:\Windows\Logs\pmm\pmm_sup_service.log]
File
Tools
Window
Help
Log Text
Date/Time:
Component:
Thread:
Source:

```
01-28 16:45:43.929 D /CepServiceWrapper:6940:4c4/ Starting service...
01-28 16:45:43.930 I /pmm_sup_service:6940:4c4/ SupService starting
01-28 16:45:44.145 D /PolicyTools:6940:4c4/ Started GET request to 'http://swscan.apple.com/content/catalogs/others/index-10.9-mountainlion-lion-snowleopard-leopard.merged-1....
01-28 16:45:44.147 D /PolicyTools:6940:4c4/ Started GET request to 'http://swscan.apple.com/content/catalogs/others/index-lion-snowleopard-leopard.merged-1.sucatalog'
01-28 16:45:44.148 D /PolicyTools:6940:4c4/ Started GET request to 'http://swscan.apple.com/content/catalogs/others/index-mountainlion-lion-snowleopard-leopard.merged-1.sucat...
01-28 16:45:44.148 D /PolicyTools:6940:4c4/ Started GET request to 'http://swscan.apple.com/content/catalogs/others/index-10.10-10.9-mountainlion-lion-snowleopard-leopard.mer...
01-28 16:45:44.148 D /PolicyTools:6940:4c4/ Started GET request to 'http://swscan.apple.com/content/catalogs/others/index-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopar...
01-28 16:45:44.149 I /HttpServer:6940:4c4/ Listening on 0.0.0.0:0
01-28 16:45:44.153 D /SupCatalogServer:6940:4c4/ Listening on 'http://win2012r2-001.pmm12.dom:63547'
01-28 16:45:44.153 D /SupCatalogServer:6940:4c4/ Catalog server started
01-28 16:45:44.289 D /SvcLocator:6940:4c4/ Attempting to get SCP for 'LDAP://CN=PmaConfigMgrProxy-T12,CN=ParallelsServices,CN=System,DC=pmm12,DC=dom'...
01-28 16:45:44.398 D /SvcLocator:6940:4c4/ Found SCP 'LDAP://CN=PmaConfigMgrProxy-T12,CN=ParallelsServices,CN=System,DC=pmm12,DC=dom'
01-28 16:45:44.398 I /pmm_sup_service:6940:4c4/ PSUP information update interval is 1800 seconds
01-28 16:45:44.398 I /pmm_sup_service:6940:4c4/ SupService started
01-28 16:45:44.398 D /CepServiceWrapper:6940:4c4/ Service has been started
01-28 16:45:44.398 I /pmm_sup_service:6940:4c4/ Got proxy link event 1 (0, [The operation completed successfully])
01-28 16:45:44.399 D /RpcClientCpp:6940:1550/ Connecting to 'win2012r2-001.pmm12.dom' (10.211.55.21)...
01-28 16:45:44.400 D /RpcClientCpp:6940:1550/ Successfully connected to '10.211.55.21'
01-28 16:45:44.590 D /PrlCommonUtils:6940:4c4/ Started 'C:/Program Files (x86)/Parallels/Parallels Mac Management for Microsoft SCCM/wsus-publisher.exe' 'publish' '--catalog=C:/...
```

```
01-28 16:45:44.590 D /PrlCommonUtils:6940:4c4/ Started 'C:/Program Files (x86)/Parallels/Parallels Mac Management for Microsoft SCCM/wsus-publisher.exe' 'publish' '--
catalog=C:/ProgramData/Parallels/Sup/WsusPublisher/Catalogs/index-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog' '--data-dir=C:/ProgramData/Parallels/Sup/WsusPublisher'
```

Configure synchronization of Configuration Manager with WSUS

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

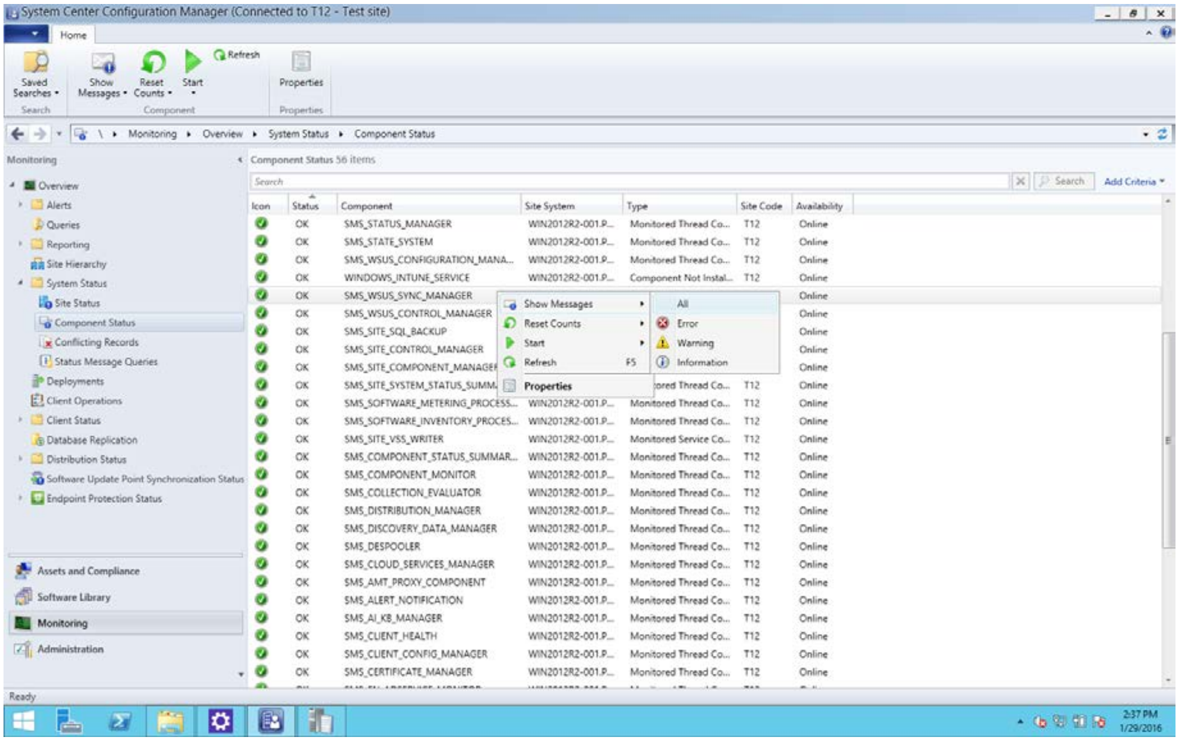
If you already have a synchronization scheduled, you can either wait for it to complete or you can start it manually. This is necessary for the **Apple** option to appear in the **Software Update Point Component Properties** dialog, as you will see later in this topic.

Configure synchronization settings

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

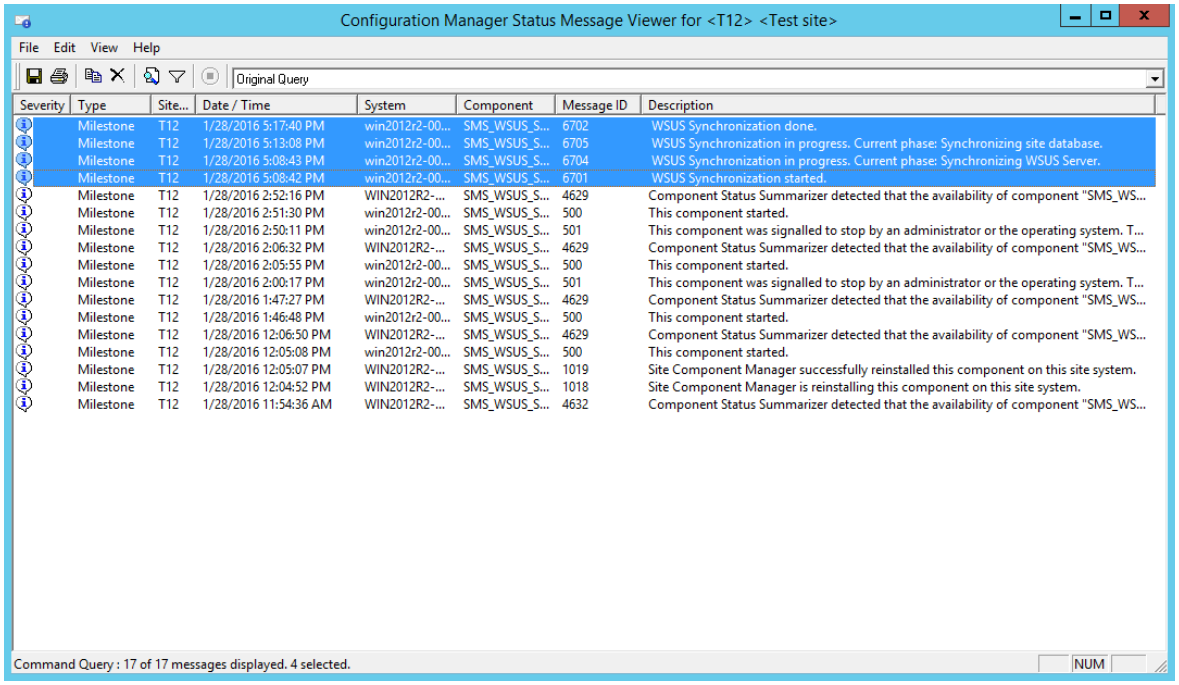
2 Right-click **All Software Updates** and choose **Synchronize Software Updates**.

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



Icon	Status	Component	Site System	Type	Site Code	Availability
✓	OK	SMS_STATUS_MANAGER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_STATE_SYSTEM	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_WSUS_CONFIGURATION_MANA...	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	WINDOWS_INTUNE_SERVICE	WIN2012R2-001.P...	Component Not Instal...	T12	Online
✓	OK	SMS_WSUS_SYNC_MANAGER				Online
✓	OK	SMS_WSUS_CONTROL_MANAGER				Online
✓	OK	SMS_SITE_SQL_BACKUP				Online
✓	OK	SMS_SITE_CONTROL_MANAGER				Online
✓	OK	SMS_SITE_COMPONENT_MANAGEF				Online
✓	OK	SMS_SITE_SYSTEM_STATUS_SUMM		ored Thread Co...	T12	Online
✓	OK	SMS_SOFTWARE_METERING_PROCESS...	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_SOFTWARE_INVENTORY_PROCES...	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_SITE_VSS_WRITER	WIN2012R2-001.P...	Monitored Service Co...	T12	Online
✓	OK	SMS_COMPONENT_STATUS_SUMMAR...	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_COMPONENT_MONITOR	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_COLLECTION_EVALUATOR	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_DISTRIBUTION_MANAGER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_DISCOVERY_DATA_MANAGER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_DESPOOLER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_CLOUD_SERVICES_MANAGER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_AMT_PROXY_COMPONENT	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_ALERT_NOTIFICATION	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_AI_KB_MANAGER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_CLIENT_HEALTH	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_CLIENT_CONFIG_MANAGER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online
✓	OK	SMS_CERTIFICATE_MANAGER	WIN2012R2-001.P...	Monitored Thread Co...	T12	Online

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


Configuration Manager Status Message Viewer for <T12> <Test site>
File
Edit
View
Help
Original Query
NUM

Severity	Type	Site...	Date / Time	System	Component	Message ID	Description
ⓘ	Milestone	T12	1/28/2016 5:17:40 PM	win2012r2-00...	SMS_WSUS_S...	6702	WSUS Synchronization done.
ⓘ	Milestone	T12	1/28/2016 5:13:08 PM	win2012r2-00...	SMS_WSUS_S...	6705	WSUS Synchronization in progress. Current phase: Synchronizing site database.
ⓘ	Milestone	T12	1/28/2016 5:08:43 PM	win2012r2-00...	SMS_WSUS_S...	6704	WSUS Synchronization in progress. Current phase: Synchronizing WSUS Server.
ⓘ	Milestone	T12	1/28/2016 5:08:42 PM	win2012r2-00...	SMS_WSUS_S...	6701	WSUS Synchronization started.
ⓘ	Milestone	T12	1/28/2016 2:52:16 PM	WIN2012R2-...	SMS_WSUS_S...	4629	Component Status Summarizer detected that the availability of component "SMS_WS...
ⓘ	Milestone	T12	1/28/2016 2:51:30 PM	win2012r2-00...	SMS_WSUS_S...	500	This component started.
ⓘ	Milestone	T12	1/28/2016 2:50:11 PM	win2012r2-00...	SMS_WSUS_S...	501	This component was signalled to stop by an administrator or the operating system. T...
ⓘ	Milestone	T12	1/28/2016 2:06:32 PM	WIN2012R2-...	SMS_WSUS_S...	4629	Component Status Summarizer detected that the availability of component "SMS_WS...
ⓘ	Milestone	T12	1/28/2016 2:05:55 PM	win2012r2-00...	SMS_WSUS_S...	500	This component started.
ⓘ	Milestone	T12	1/28/2016 2:00:17 PM	win2012r2-00...	SMS_WSUS_S...	501	This component was signalled to stop by an administrator or the operating system. T...
ⓘ	Milestone	T12	1/28/2016 1:47:27 PM	WIN2012R2-...	SMS_WSUS_S...	4629	Component Status Summarizer detected that the availability of component "SMS_WS...
ⓘ	Milestone	T12	1/28/2016 1:46:48 PM	win2012r2-00...	SMS_WSUS_S...	500	This component started.
ⓘ	Milestone	T12	1/28/2016 12:06:50 PM	WIN2012R2-...	SMS_WSUS_S...	4629	Component Status Summarizer detected that the availability of component "SMS_WS...
ⓘ	Milestone	T12	1/28/2016 12:05:08 PM	win2012r2-00...	SMS_WSUS_S...	500	This component started.
ⓘ	Milestone	T12	1/28/2016 12:05:07 PM	WIN2012R2-...	SMS_WSUS_S...	1019	Site Component Manager successfully reinstalled this component on this site system.
ⓘ	Milestone	T12	1/28/2016 12:04:52 PM	WIN2012R2-...	SMS_WSUS_S...	1018	Site Component Manager is reinstalling this component on this site system.
ⓘ	Milestone	T12	1/28/2016 11:54:36 AM	WIN2012R2-...	SMS_WSUS_S...	4632	Component Status Summarizer detected that the availability of component "SMS_WS...

Command Query : 17 of 17 messages displayed. 4 selected.

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**.

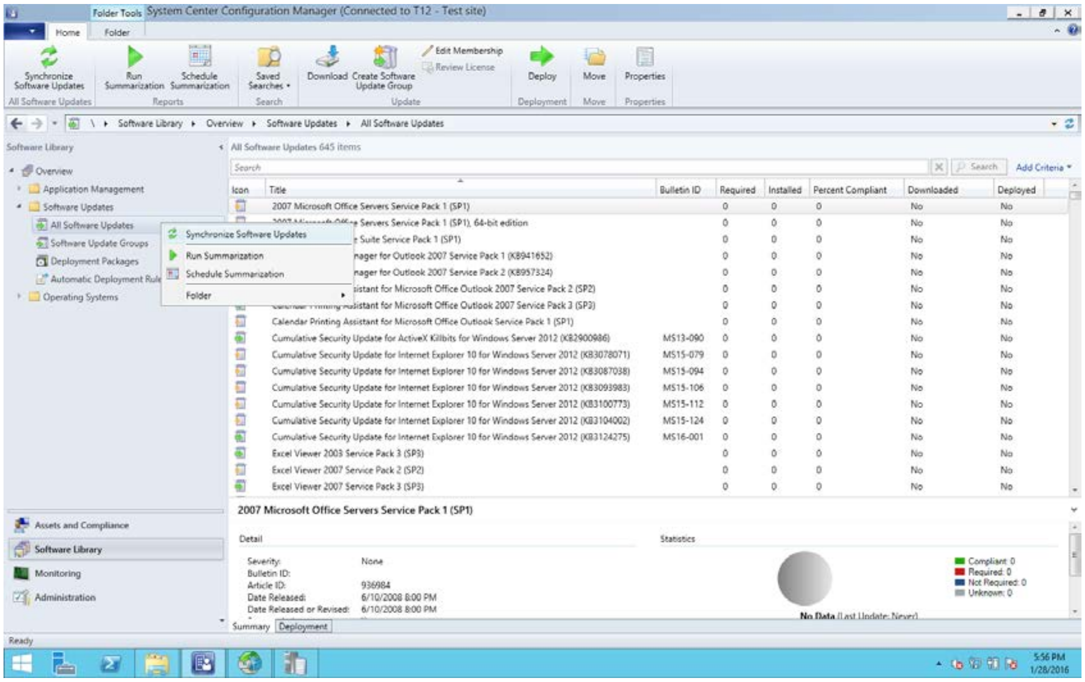
Note: If the **Apple** product is not present on the **Products** tab page it's because the software update point did not synchronize with WSUS after the Apple software updates were imported. In such a case try repeating the steps described in this topic from the beginning.

Synchronize Configuration Manager 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 Configuration Manager documentation.

To synchronize Configuration Manager with WSUS manually:

1 Run the WSUS synchronization again.



All Software Updates 645 items

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed
	2007 Microsoft Office Servers Service Pack 1 (SP1)		0	0	0	No	No
	2007 Microsoft Office Servers Service Pack 1 (SP1), 64-bit edition		0	0	0	No	No
	Suite Service Pack 1 (SP1)		0	0	0	No	No
	nager for Outlook 2007 Service Pack 1 (KB941652)		0	0	0	No	No
	nager for Outlook 2007 Service Pack 2 (KB957324)		0	0	0	No	No
	sistant for Microsoft Office Outlook 2007 Service Pack 2 (SP2)		0	0	0	No	No
	Calendar Printing Assistant for Microsoft Office Outlook 2007 Service Pack 3 (SP3)		0	0	0	No	No
	Calendar Printing Assistant for Microsoft Office Outlook Service Pack 1 (SP1)		0	0	0	No	No
	Cumulative Security Update for ActiveX Killbits for Windows Server 2012 (KB2900986)	MS13-090	0	0	0	No	No
	Cumulative Security Update for Internet Explorer 10 for Windows Server 2012 (KB3078071)	MS15-079	0	0	0	No	No
	Cumulative Security Update for Internet Explorer 10 for Windows Server 2012 (KB3087038)	MS15-094	0	0	0	No	No
	Cumulative Security Update for Internet Explorer 10 for Windows Server 2012 (KB3093983)	MS15-106	0	0	0	No	No
	Cumulative Security Update for Internet Explorer 10 for Windows Server 2012 (KB3100773)	MS15-112	0	0	0	No	No
	Cumulative Security Update for Internet Explorer 10 for Windows Server 2012 (KB3104002)	MS15-124	0	0	0	No	No
	Cumulative Security Update for Internet Explorer 10 for Windows Server 2012 (KB3124275)	MS16-001	0	0	0	No	No
	Excel Viewer 2003 Service Pack 3 (SP3)		0	0	0	No	No
	Excel Viewer 2007 Service Pack 2 (SP2)		0	0	0	No	No
	Excel Viewer 2007 Service Pack 3 (SP3)		0	0	0	No	No

2007 Microsoft Office Servers Service Pack 1 (SP1)

Detail

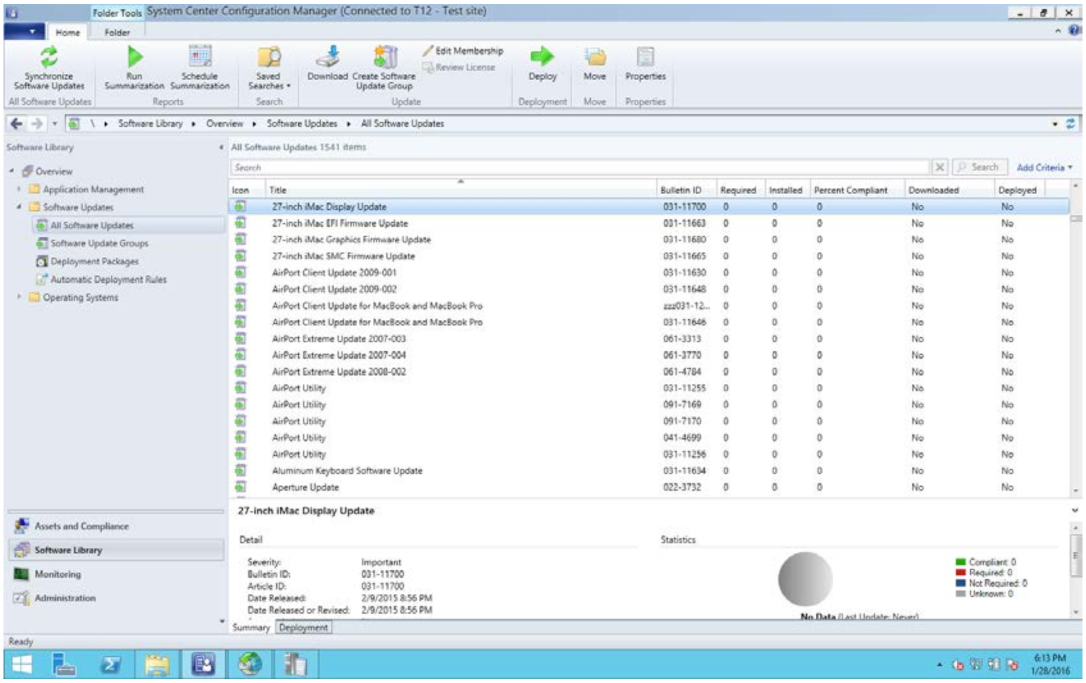
Severity: None
Bulletin ID:
Article ID: 936984
Date Released: 6/10/2008 8:00 PM
Date Released or Revised: 6/10/2008 8:00 PM

Statistics

🟩 Compliant: 0
🟥 Required: 0
🟦 Not Required: 0
▨ Unknown: 0

No Data (Last Update: Never)

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



All Software Updates 1541 items

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed
	27-inch iMac Display Update	031-11700	0	0	0	No	No
	27-inch iMac EFI Firmware Update	031-11663	0	0	0	No	No
	27-inch iMac Graphics Firmware Update	031-11680	0	0	0	No	No
	27-inch iMac SMC Firmware Update	031-11665	0	0	0	No	No
	AirPort Client Update 2009-001	031-11630	0	0	0	No	No
	AirPort Client Update 2009-002	031-11648	0	0	0	No	No
	AirPort Client Update for MacBook and MacBook Pro	zzz031-12...	0	0	0	No	No
	AirPort Client Update for MacBook and MacBook Pro	031-11646	0	0	0	No	No
	AirPort Extreme Update 2007-003	061-3313	0	0	0	No	No
	AirPort Extreme Update 2007-004	061-3770	0	0	0	No	No
	AirPort Extreme Update 2008-002	061-4784	0	0	0	No	No
	AirPort Utility	031-11255	0	0	0	No	No
	AirPort Utility	091-7169	0	0	0	No	No
	AirPort Utility	091-7170	0	0	0	No	No
	AirPort Utility	041-4699	0	0	0	No	No
	AirPort Utility	031-11256	0	0	0	No	No
	Aluminum Keyboard Software Update	031-11634	0	0	0	No	No
	Aperture Update	022-3732	0	0	0	No	No

27-inch iMac Display Update

Detail

Severity: Important
Bulletin ID: 031-11700
Article ID: 031-11700
Date Released: 2/9/2015 8:56 PM
Date Released or Revised: 2/9/2015 8:56 PM

Statistics

🟩 Compliant: 0
🟥 Required: 0
🟦 Not Required: 0
▨ Unknown: 0

No Data (Last Update: Never)

CHAPTER 6

Deploying Parallels NetBoot Server

In This Chapter

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.
- Background Intelligent Transfer Service (BITS) must be installed and enabled. Parallels Device Management has been tested with BITS 4.0 and 5.0.

Additionally, the user account that will be used to configure the Parallels NetBoot Server must have sufficient privileges. See the following KB article for details: https://kb.parallels.com/117937

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

See also **Port reference** (p. 70)

Permissions for running Parallels NetBoot Service

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

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

Create a domain user

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

To create a domain user:

1 On a server running Active Directory, open Server Manager by clicking **Start** > **Administrative Tools** > **Server Manager**.

2 Expand **Server Manager** > **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers** > <domain-name>.

3 Right-click **Users** and choose **New** > **User**.

4 In the **New Object – User** dialog, specify **Full name**, **User logon name**, and then click **Next**.

5 Type and confirm a password and click **Next**.

6 Click **Finish**.

Local administrator rights

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

To grant the administrative privileges to a user:

1 Log in to the computer that will run the NetBoot server.

2 Open Server Manager and navigate to **Configuration** > **Local Users and Groups** > **Groups**.

3 Right-click the **Administrators** group and choose **Properties**.

4 In the **Select Users** dialog, click **Add** and add the domain user you've created earlier.

5 Click **OK** and click **OK** again.

DCOM Remote Activation permission

Both users must have the DCOM Remote Activation permission:

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

2 In the **Component Services** window, navigate to **Console Root** > **Component Services** > **Computers** > **My Computer** > **DCOM Config**. Scroll down to **Windows Management and Instrumentation**, right-click it and choose **Properties**.

3 Click the **Security tab**. The **Launch and Activation Permissions** section will have either the **Customize** or **Use Default** option selected depending on your server configuration. Depending on the option selected, set the DCOM Remote Activation permission for the user as described in one of the following subsections.

Customize

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

Use Default

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

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

Read rights in Configuration Manager

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

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

Configuring Parallels NetBoot Server

The Parallels NetBoot Configuration Wizard will start automatically after the component is installed. 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 displays 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.

CHAPTER 7

Parallels Device Management Maintenance

In This Chapter

Adding or removing Parallels Device Management components

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

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

Upgrading Parallels Device Management to a newer version

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

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

To upgrade Parallels Device Management to a newer version:

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

Please note that after upgrading Parallels Device Management, you need to upgrade Parallels Mac Client on each managed Mac in your organization. See **Upgrading Parallels Mac Client** (p. 63) for more information.

Upgrading Parallels Mac Client

When you upgrade Parallels Device Management for Configuration Manager, 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 Configuration Manager 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 Device 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 Device 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 one hour (or more) for Mac computers to upgrade after Parallels Device 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 Download the Parallels Mac Client installation image file.

2 Distribute the client installation image to Mac computers.

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 are 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 the Mac. 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 installer.

CHAPTER 8

Parallels ConfigMgr Proxy and site migration

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

In This Chapter

Migrating Parallels ConfigMgr Proxy to a new host

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

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

1. Exporting the Parallels Configuration Manager Proxy certificate from the Windows certificate store on the current server.
2. Uninstalling the Proxy from the current server.
3. Importing the certificate into the Windows certificate store on the new server.
4. Installing the Parallels Configuration Manager Proxy on the new server.

The rest of this section describes how to export and import the certificate. The installation procedures are described in the **Deploying Parallels ConfigMgr Proxy and Console Extensions** (p. 14).

Exporting the certificate from the Windows certificate store

To export the certificate from the current server:

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

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**.

6 In the Microsoft Management console, navigate to **Console Root** / **Certificates(Local computer)** / **Personal** / **Certificates**.

7 Right-click the **Parallels Configuration Manager Proxy** certificate and choose **All Tasks** > **Export**. 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, do the following:

- Select **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**.

15 Copy the certificate file to the server where you want to migrate the Configuration Manager Proxy.

Importing the certificate into the Windows certificate store

To import the certificate on the new server:

1 Open the Microsoft Management Console (mmc.exe).

2 In the console, click **File** > **Add/Remove Snap-in**.

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 choose **All Tasks** > **Import**. 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 specified 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 Device Management for Configuration Manager installer.

17 Mac computers will automatically discover the new Parallels Configuration Manager Proxy and will update their own local Proxy connection records. For an explanation of how Parallels Mac Client does that, see **Updating Configuration Manager Proxy URL on a Mac** below.

Updating Configuration Manager Proxy URL on a Mac

This subsection explains how Parallels Mac Client updates the Configuration Manager Proxy connection URL when the Proxy is migrated to a new host.

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

1 First, it will try to access DNS records for the location of the Configuration Manager Proxy. If it finds the new connection URL in DNS, it will use it to connect to the Configuration Manager Proxy.

2 If the location cannot be found in DNS at this time, the client will keep trying to connect to the Proxy and to find the new location in DNS for a period of one week.

3 If after a week the connection still cannot be establish, a dialog box will be displayed in macOS asking the Mac user to enter the Active Directory credentials. The client will then connect to the Active Directory and try to retrieve the Configuration Manager Proxy connection URL from it. If succeeded, the client will use the URL to connect to the Configuration Manager Proxy. If it fails again, it will display an error message to the Mac user advising them to contact the system administrator.

Migrating Mac Computers to a new site

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

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

First, you need to prepare the migration script as follows:

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

   C:\Program Files (x86)\Parallels\Parallels Device Management for Configuration Manager\sitemigration\pkgsrc

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

2 Open the `migrate_pmm_to_new_site.sh` file in a text editor that supports Unix-style line endings (e.g. Notepad++). This is the script that will migrate Parallels Mac Client to a new Configuration Manager site when you run it on a Mac computer.

3 In the script, modify the values of the following variables:

   - TARGET_SITE_CODE must contain the side code of the new Parallels Configuration Manager Proxy.

     Example: TARGET_SITE_CODE = "T16"

   - CM_PROXY_URL must contain the URL of the new Parallels Configuration Manager Proxy.

     Example: CM_PROXY_URL = "https://win2012r2.pmm12.dom:8760/isvproxy/rpc"

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

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

1 Make sure your new Configuration Manager site has boundaries configured the same way they are configured in the old site.

2 Import all Parallels Configuration Manager Proxy certificates from the server running the old Proxy into the server running the new Proxy. For instructions, please see KB article https://kb.parallels.com/117220.

3 Log in to the server running the new Parallels Configuration Manager Proxy and open the Windows registry editor. Depending on the Windows version, find the following key:

   - 64-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Parallels Mac Management for Microsoft SCCM\CmProxy

   - 32-bit Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Parallels\Parallels Mac Management for Microsoft SCCM\CmProxy

   Add parameter `TrustedPmmSites` (type REG_MULTI_SZ). The parameter should contain the list of site codes from which you are migrating Mac computers.

4 Save the register changes and restart the Parallels Configuration Manager Proxy service for the changes to take effect.

Now open the Configuration Manager console in the old site and create a software package as follows:

- Source should be the path to the folder containing the modified `migrate_pmm_to_new_site.sh` file together with the rest of the files. If needed, copy the entire folder to a location where it can be accessed from the Configuration Manager console in the old site.
- Command line should be `chmod u+x ./install.sh && ./install.sh`

Deploy the package to the collection of Mac computers that you want to migrate to the new site.

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

CHAPTER 9

Appendices

In This Chapter

Port reference

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

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

Parallels Configuration Manager Proxy (inbound ports)

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

Parallels Configuration Manager Proxy (outbound ports)

Process Name	Port	Description
pma_isv_proxy_service.exe	TCP 443	HTTPS connections to the Parallels License Server.
	TCP 1433	Connections to the SQL Server database.
pmm_dep_service.exe	TCP 443	HTTPS connections to the Apple DEP service.
	TCP 1433	Connections to the SQL Server database.
pmm_mdm_service.exe	TCP 443 or 2197	TLS connections to the Apple Push Notification service.
	TCP 1433	Connections to the SQL Server database.
pmm_vpp_service.exe	TCP 443	HTTPS connections to the Apple VPP service.
	TCP 1433	Connections to the SQL Server database.
pmm_mdm_policy_service.exe	TCP 1433	Connections to the SQL Server database.

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

Parallels NetBoot Server (inbound ports)

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

Parallels NetBoot Server (outbound ports)

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

Parallels OS X Software Update Server (inbound ports)

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

Parallels OS X Software Update Server (outbound ports)

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

Parallels IBCM/MDM Proxy (inbound ports)

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

Managed Mac computer (inbound ports)

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

Managed Mac computer (outbound ports)

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

Parallels ConfigMgr Console Extensions (outbound ports)

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

Logging

Parallels Device 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 Device 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 Device Management for Configuration Manager.

Parallels Device Management for Configuration Manager log files

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

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

The following table describes the Parallels Device Management for Configuration Manager log files:

Component	**Log File Name**	**Log File Description**
Parallels Configuration Manager Proxy	pma_setup.log	This log file is created during the Configuration Manager Proxy installation. It contains information about the installation procedures and the changes they make to the system. Please note that when the Configuration Manager Proxy and the Configuration Manager Console Extension components are installed on the same computer, the pma_setup.log is shared between them.
	pma_isv_proxy_config.log	This log file is created and updated every time the Configuration Manager 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 Configuration Manager Proxy log file. It is updated as needed while the Configuration Manager Proxy service is running. It contains information related to the Configuration Manager 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.
Configuration Manager Console Extension	pma_setup.log	The Configuration Manager Console Extension component has just one log file: pma_setup.log. The file contains information about the component installation procedure. Please note that when the Configuration Manager Proxy and the Configuration Manager Console Extension components are installed on the same computer, the pma_setup.log is shared between them.
Parallels Mac Client	pma_agent.log	This is the main client software log file, which contains information about the client operations. The file is updated when the Mac Client communicates with Configuration Manager Proxy and/or performs actions on the Mac computer on which it is running.

	pma_agent_ui.log	This log file is updated when the client installation and registration utilities are run on the Mac by a user. The file also records information when an operation is performed on the Mac that is user-specific. An example of such an operation is applying a Mac configuration profile (a profile is applied for each individual Mac user if more than one user exists). Please note that if a Mac user doesn't have privileges to write to the /Library/Logs directory, the log file will be created in the /Users/<*user_name*>/Library/Logs directory.
	pma_agent_uninstaller.log	This log file is created when the client is uninstalled from the Mac computer.

Configuration Manager log files

Some of the Parallels Device Management process information is recorded in the Configuration Manager log files. You may examine these files in addition to the log files described above. Please note that Configuration Manager 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 Configuration Manager Proxy component.

Log file	**Log file description**
Colleval.log	Records activities when collections are created, changed, and deleted by the Collection Evaluator.
Dataldr.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.
Policypv.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 Configuration Manager 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 Device Management for Configuration Manager crash dumps

In addition to log files, crash dumps may be generated if a Parallels Device 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 Device Management for Configuration Manager 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 Device Management for Configuration Manager 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 Device 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\pmm\pma_isv_proxy_service.log
pma_isv_proxy_config	Windows	%Windir%\Logs\pmm\pma_isv_proxy_config.log
pma_discovery	Windows	%Windir%\Logs\pmm\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\pmm\pma_problem_monitor.log
pma_report_tool	Windows macOS	%Windir%\Logs\pmm\pma_report_tool.log /Users/<user_name>/Library/Logs
pma_agent	macOS	/Library/Logs/pma_agent.log
pma_agent_ui	macOS	/Library/Logs/pma_agent_ui.log

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

- Log files are archived using the zlib compression library.
- The archived files in the set are named as follows:

  `<exec_name.1.log.gz>`, `<exec_name.2.log.gz>`, `<exec_name.3.log.gz>`, etc.

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

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

Changing log file rotation limits

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

- **Log file size limit**. The default value is 1 MB (specified in bytes). The minimum allowed value is 200 KB. The maximum allowed value is 4 MB. If a value is not set, the default value is used. If the specified value falls outside the min/max interval, the minimum or the maximum value is used respectively.
- **Maximum number of files in a rotation set**. The default value is 10. The minimum value is 1. The maximum value is 20. If a value is not set, the default value is used. If the specified value falls outside the min/max interval, the minimum or the maximum value is used respectively.

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

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

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

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

Enforcing TLS 1.2

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

- IBCM/MDM Proxy
- PMM Proxy

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

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

Key value	TLS version(s)
TlsV1_0	TLS v1.0
TlsV1_0OrLater (Used by default)	TLS v1.0 and later versions
TlsV1_1	TLS v1.1
TlsV1_1OrLater	TLS v1.1 and later versions
TlsV1_2	TLS v1.2
TlsV1_2OrLater	TLS v1.2 and later versions

Notes

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

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

Example:

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

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

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

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

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

```
...
```

Parallels Device Management database

When Parallels Device Management for Configuration Manager is installed, it creates its own SQL Server database on the primary Configuration Manager 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 Configuration Manager site.

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

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

Index