Parallels

Parallels Mac Management for Microsoft SCCM

Deployment Guide

v8.6

Contents

Introduction

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

The guide does not cover topics related to user rights and other system requirements. This information can be found in the Parallels Mac Management for SCCM Administrator's Guide https://www.parallels.com/products/mac-management/support/.

In This Chapter

Glossary

SMS	System Management Server (the core component of System Center Configuration Manager)
CAS	Central Administration Site
DP, MP	SCCM Distribution Point, SCCM Management Point
Admin Console	SCCM Administrative Console
WDS	Windows Deployment Services
BITS	Background Intelligent Transfer Service
Parallels Mac Management	Parallels Mac Management for Microsoft SCCM
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 Mac Management extends Microsoft System Center Configuration Manager (SCCM) with the ability to manage Mac computers and Apple mobile devices. With Parallels Mac Management you can manage Mac and Windows computers, as well as Apple mobile devices using SCCM as your only management system.

Component Overview

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

Configuration Manager Console Extension

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

Parallels Configuration Manager Proxy (aka Parallels ConfigMgr Proxy)

This is the core Parallels Mac Management component. It is a Windows service application that acts as a proxy between SCCM and Mac computers.

Parallels IBCM/MDM Proxy

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

- **IBCM Proxy** enables Internet-Based Client Management (IBCM) of Mac computers. It serves as a transparent proxy that passes requests between Parallels Mac Client and Parallels Configuration Manager Proxy.

- **MDM Proxy** enables IT administrators to deploy and enroll in SCCM new Mac computers using Apple Device Enrollment Program (Apple DEP). It is also used to enroll Apple mobile devices in SCCM. In addition, MDM Proxy is used to distribute configuration profiles to Mac computers and mobile devices and to use the Remote Lock and Wipe functionality.

Parallels NetBoot Server

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

Parallels OS X Software Update Point

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

Parallels Mac Client

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

C H A P T E R   2

Core Components Deployment

This chapter describes deployment of core Parallels Mac Management components.

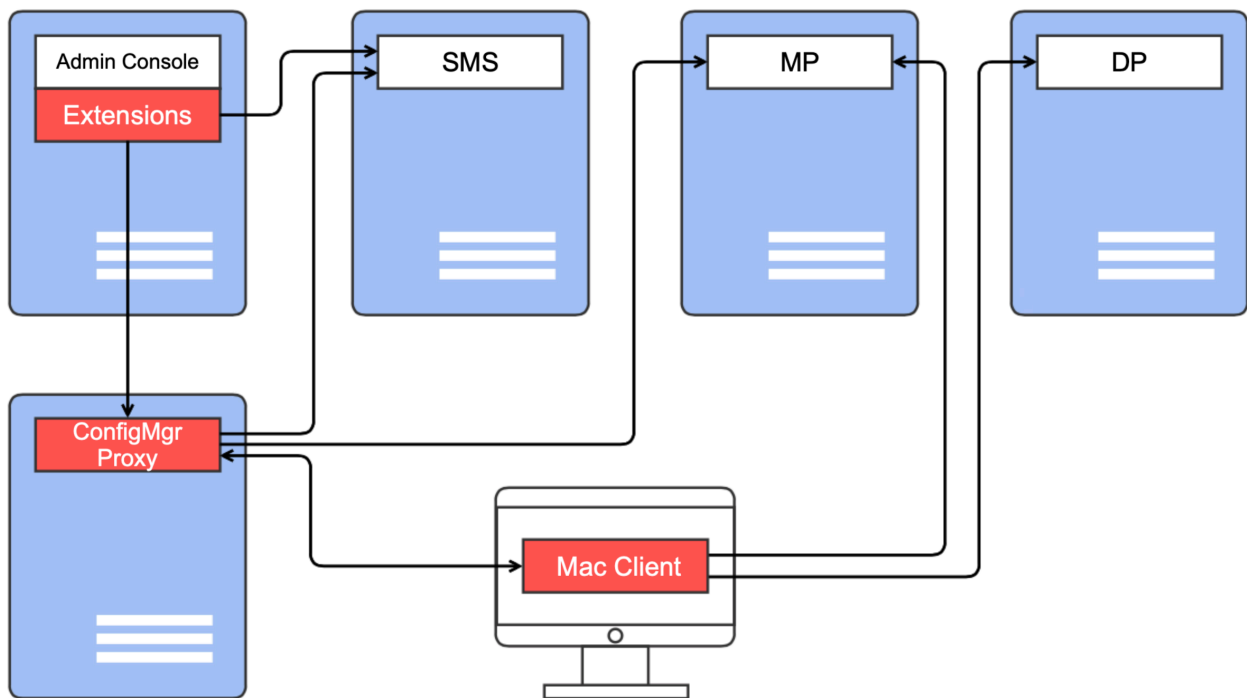**In This Chapter**

Parallels Configuration Manager Proxy

Deploying to a Standalone SCCM Site

The diagram below represents a standalone SCCM installation. The arrow lines represent communication channels between Parallels Mac Management and SCCM components.

Figure 1: Deployment to a standalone SCCM site

The above diagram shows each SCCM and Parallels Mac Management component installed on a separate computer. More often than not, your SCCM deployment will have several components that coexist on the same computer.

Installing Parallels Console Extensions

A standalone SCCM site would have at least one computer with SCCM 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 Mac Management Extensions on a computer that has the Admin Console installed.

Installing Parallels Configuration Manager Proxy

Parallels Configuration Manager Proxy (ConfigMgr Proxy) can be installed on any computer that resides within SCCM site boundaries and can establish a connection to the server hosting the SMS provider. In Figure 1 (p. 7), ConfigMgr Proxy is installed on a separate computer. In most cases, installing ConfigMgr Proxy on a server that has the SMS provider installed (Figure 2 below) is recommended.

Figure 2: ConfigMgr Proxy is installed on the SMS server
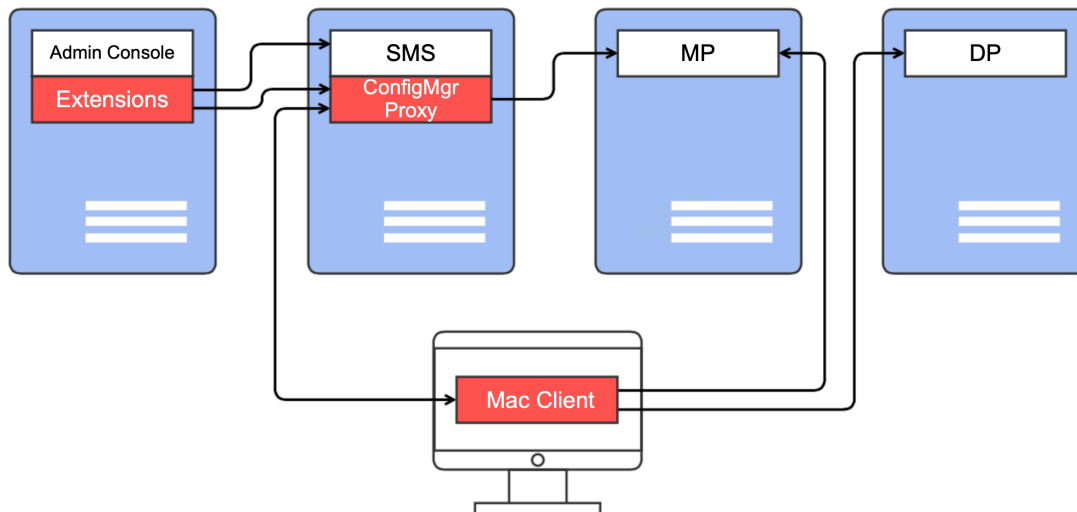
Deploying to a Primary Site with Secondary Sites

If a primary site in your SCCM installation has secondary sites, you may deploy Parallels Mac Management to the primary site or secondary sites.

Deploying to a Primary Site

When deploying Parallels Mac Management to a primary site, follow the same procedure as described in **Deploying to a Standalone SCCM Site** (p. 7).

8

Deploying to a Secondary Site

ConfigMgr Proxy should be deployed on all secondary sites. While this is not required, it is highly recommended.

Deploying ConfigMgr Proxy to all secondary sites has the following benefits:

- 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.

Figure 3: Secondary site with Parallels Configuration Manager Proxy installed
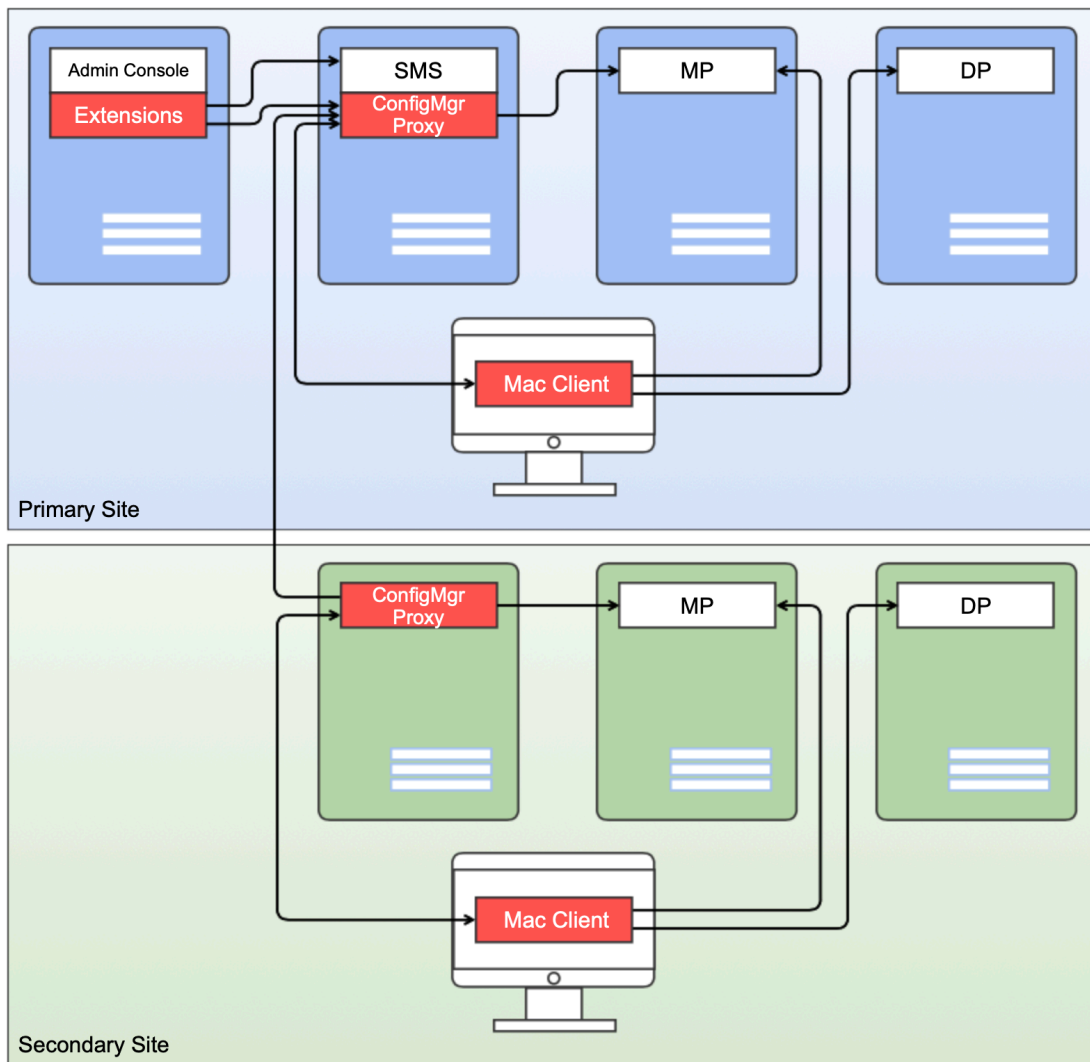
Deploying to a Central Administration Site

The only additional step to perform when deploying Parallels Mac 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.

The following features are not supported when Parallels Mac Management Extensions are installed on a CAS:

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

Figure 4: Deploying Parallels Mac Management in a CAS environment
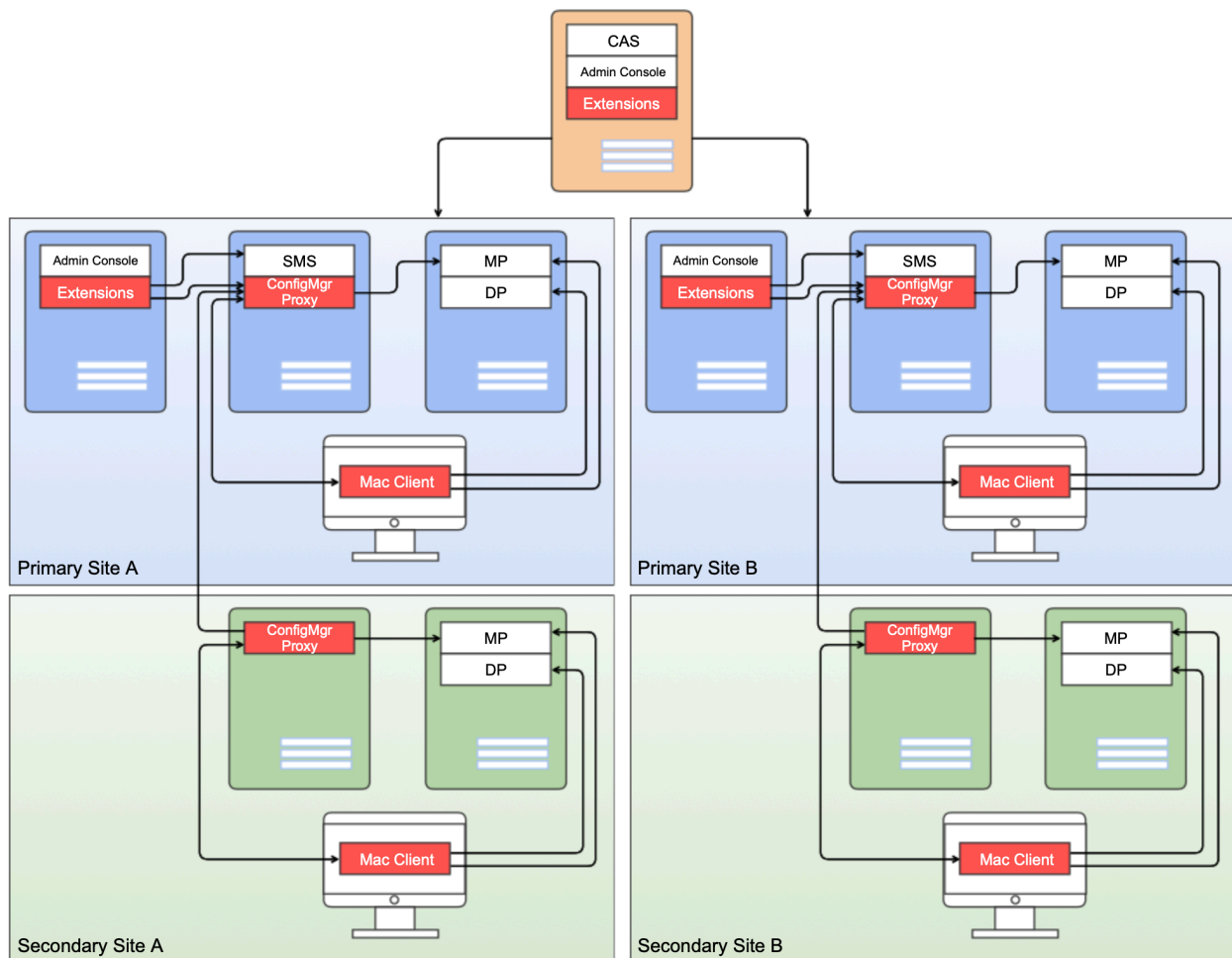
Deploying Parallels NetBoot Server

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

The server on which Parallels NetBoot Server (NetBoot) will be installed must meet the following requirements:

- The SCCM Distribution Point (DP) role is installed on this server.
- Windows Deployment Service (WDS) is installed and running. If WDS and DHCP are both installed on this server, the "Do not listen on port 67" option must be selected in the WDS service properties.
- The server is a PXE service point.
- BITS 4.0 is installed.

  Background Intelligent Transfer Service (BITS) transfers files (downloads or uploads) between a client and a server and provides progress information related to the transfers.

These requirements remain the same for any SCCM deployment configuration, whether it's a standalone, primary, or secondary site deployment.

Figure 5: Deploying NetBoot
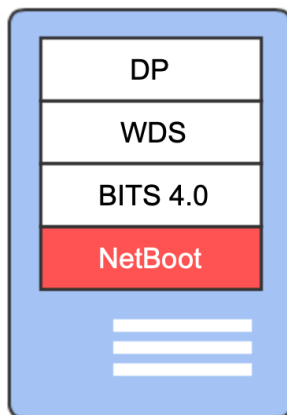
Parallels Software Update Point Deployment

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

In This Chapter

Required Components

Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) must be installed and configured for local publishing of updates. Installation instructions are available at the following location:

https://msdn.microsoft.com/en-us/library/bb902479

On the web page, refer to the "To set up the update server for locally-published content" section.

Parallels OS X Software Update Point

This is a component of Parallels Mac Management that enables macOS patch management in SCCM. It must be installed on a computer where WSUS is installed.

Download Updates from Apple Servers

This is the default configuration. It is the simplest scenario in which macOS update catalogs and packages are downloaded from Apple servers over the Internet.
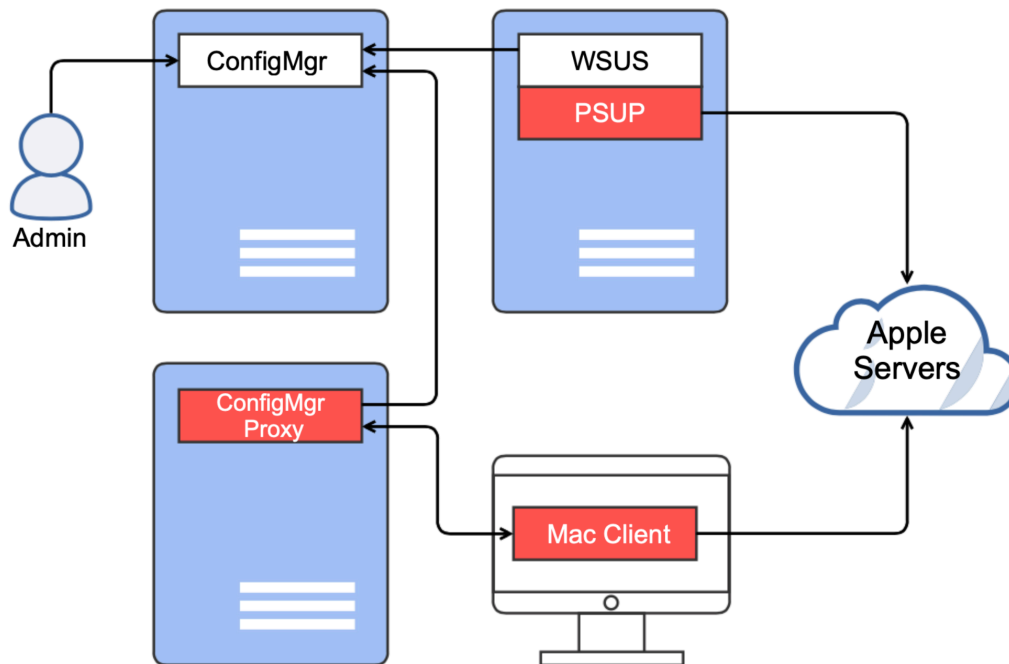
When this scenario is used, macOS updates are installed on Macs as follows:

1 Parallels OS X Software Update Point (SUP) downloads macOS update catalogs from Apple and imports them into WSUS.

2 WSUS is synchronized with SCCM.

3 The SCCM administrator deploys updates to Macs.

4 Macs download deployed updates from Apple's servers, after which the updates are silently installed on them.

5 A Mac user can check for updates using the standard macOS functionality and install any of the available updates.

13

Download Updates from a Local Update Server

This configuration allows you to use a local update server to host macOS update catalogs and update packages.
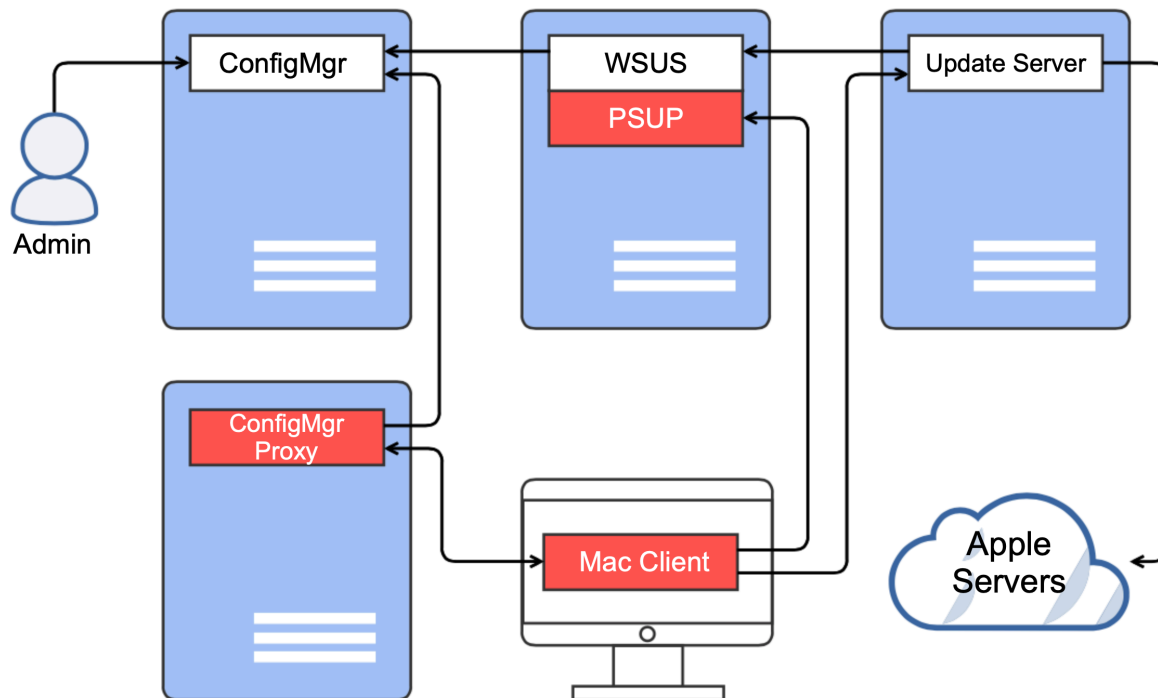

When this scenario is used, macOS updates are installed on Macs as follows:

1 Parallels OS X Software Update Point (SUP) downloads macOS update catalogs from the local update server (Update Server) and imports them into WSUS.

2 WSUS is synchronized with SCCM.

3 The SCCM administrator deploys updates to Macs.

4 Macs download update catalogs from Parallels OS X Software Update Point and then download update packages from the local update server.

5 The deployed updates are silently installed on a Mac.

6 A Mac user can check for updates using the standard macOS functionality and install any of the available updates. Please note that the OS X Software Update service will use the update catalogs that were downloaded from Parallels OS X Software Update Point, not the Apple's servers. Update packages will also be downloaded from the local update server.

Note: To use this configuration, you need a local update server (Update Server). Parallels Mac Management does NOT include this functionality. You will have to use the Apple's macOS Server or a third-party software to act as a local update server.

Restrict Which Updates a Mac User Can Install

This configuration allows you to restrict which updates a Mac user can see and install. Note that this configuration can use Apple's servers or a local update server.

When this scenario is used, macOS updates are installed on Macs as follows:

1 Parallels OS X Software Update Point downloads macOS update catalogs from Apple's servers or the local update server (depending on the configuration) and imports them into WSUS.

2 WSUS is synchronized with SCCM.

3 The SCCM administrator deploys updates to Macs.

4 Macs download full update catalogs from Apple's servers or the Parallels OS X Software Update Point (depending on the configuration). The catalogs are then filtered to include only the updates that were deployed in SCCM. If a Mac user now checks for available updates using the standard macOS functionality, they will not be able to see and install hidden updates.

5 Macs download update packages from the location specified in a catalog (Apple's servers or a local update server).

6 The deployed updates are silently installed on a Mac.

7 If a Mac user checks for updates using the standard macOS functionality, they will see only the updates that were deployed (or none at all if the updates have already been installed on this Mac).

Parallels IBCM Proxy Deployment

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. The MDM Proxy part is described in **Parallels Components for MDM and Apple DEP Support** (p. 18). This section focuses on deploying the component with IBCM Proxy enabled.

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. The connector is a plugin to IIS, which is also used by SCCM in the IBCM setup for communications between Mac computers on the Internet and Management Points / Distribution Points.
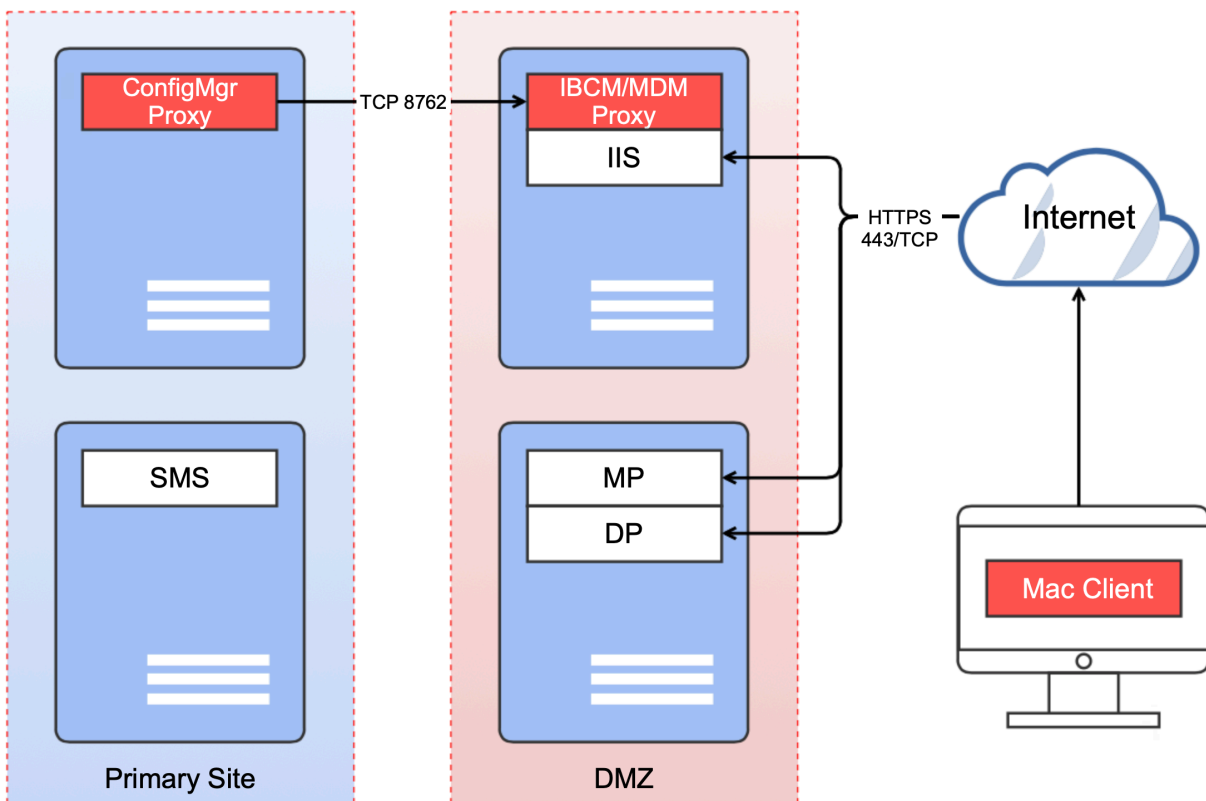
In order for Parallels IBCM/MDM Proxy to work, Parallels Mac Management must be configured for Public Key Infrastructure (PKI).

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.

- 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 will use this domain name to communicate with Parallels IBCM/MDM Proxy over the Internet.

- IIS 7.0 or above must be installed.

- IIS Web Server role must be installed.

- IIS Management script and tools must be installed.

- Placing Internet-enabled SCCM roles in DMZ is highly recommended (but not required).

- If you have multiple primary SCCM sites, a separate instance of Parallels IBCM/MDM Proxy must be deployed for each site.

- IBCM must be configured in SCCM with at least one Internet-enabled Management Point role and Distribution Point role.

Parallels Configuration Manager Proxy establishes a permanent SSL-secured link with Parallels IBCM/MDM Proxy, which is configured after the components are installed. The link is shown on the diagram above as an arrow with TCP port 8762. Trust is established using the certificate pinning mechanism, when each party is configured to stick to a specific certificate of another party.

Parallels Components for MDM and Apple DEP Support

Parallels Mac Management supports MDM enrollment and Apple DEP. To enable this functionality, you need to install the Parallels IBCM/MDM Proxy component. Other required components, including Parallels MDM service and Parallels DEP service are installed automatically when you install Parallels Configuration Manager Proxy.

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. The IBCM Proxy part is described in **Parallels IBCM Proxy Deployment** (p. 16). This section focuses on deploying Parallels IBCM/MDM Proxy with MDM Proxy enabled.

MDM Proxy enables IT administrators to perform the following tasks:

- Deploy and enroll in SCCM new Mac computers using Apple Device Enrollment Program (Apple DEP).
- Enroll Apple mobile devices in SCCM.
- Distribute configuration profiles to Mac computers and Apple mobile devices.
- Remotely lock and wipe Mac computers and Apple mobile devices.

In This Chapter

Deploying MDM Proxy

Parallels IBCM/MDM Proxy serves a single primary SCCM site. It acts 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. The basic configuration is the same as the one described in **Parallels IBCM Proxy Deployment** (p. 16). The MDM specifics (including Apple DEP support) are describes below.
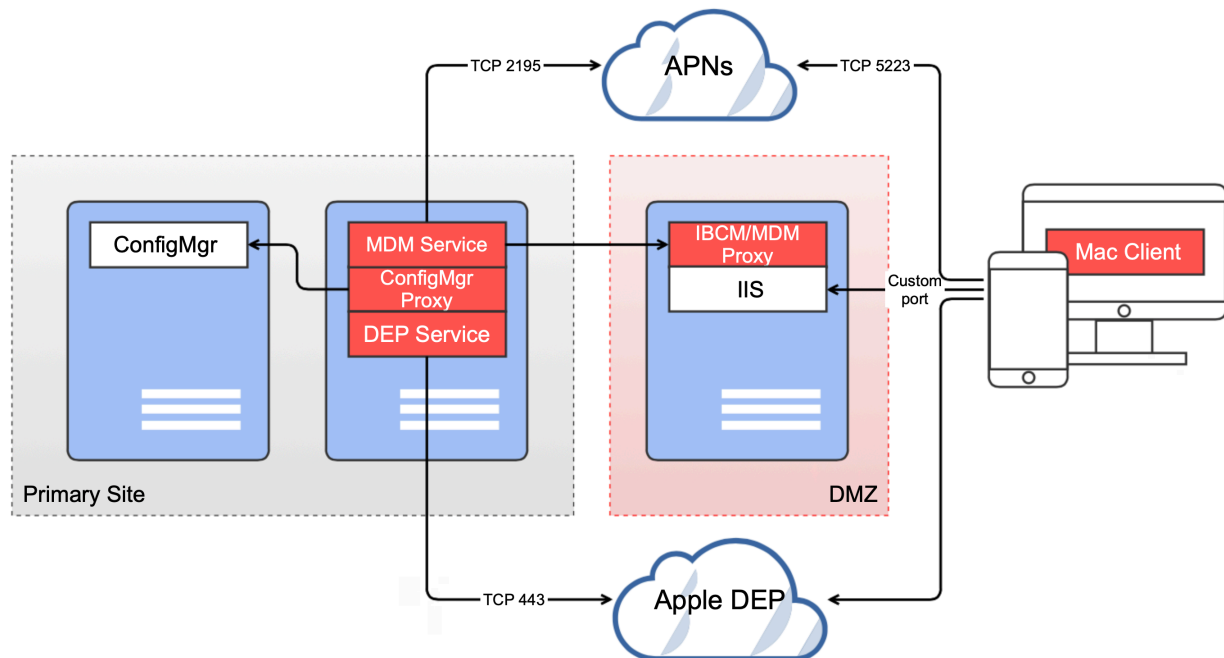
On the diagram above:

- The local Parallels DEP service is linked to the Parallels MDM service. The MDM service is linked to IBCM/MDM Proxy. The link is configured in the SCCM console.

- The local Parallels DEP service is also linked to your organization's account on the Apple DEP website. This essentially links the SCCM site to Apple DEP. The link is configured in the SCCM console and the Apple DEP website. The process involves obtaining an X.509 certificate from the local server, uploading it to the Apple DEP website and then using it to create a virtual MDM server. Finally, a token is obtained from the Apple DEP website and added to the local server, thus linking the local DEP service and the virtual MDM server.

- The Parallels MDM service uses Apple Push Notification Service (APNs) to send push notifications for MDM functions, such as Parallels Mac Client push installation and others. Establishing this communication is one of the steps you have to complete when you run the Parallels MDM Server Configuration Wizard. The process involves obtaining a certificate signing request from Parallels My Account, then uploading it to the Apple Push Certificates Portal and obtaining an APNs certificate file from it. Finally, the certificate file is added to the Parallels MDM Server, thus enabling APNs functions on it.

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. For detailed port information, please see **Port Reference** (p. 21).

C H A P T E R 7

Appendix

In This Chapter

Port Reference

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

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

Parallels Configuration Manager Proxy (inbound ports)

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

Parallels Configuration Manager Proxy (outbound ports)

Process Name	Port	Description
pma_isv_proxy_service.exe	TCP 443	HTTPS connections to the Parallels License Server.
	TCP 1433	Connections to the SQL Server database.
pmm_dep_service.exe	TCP 443	HTTPS connections to the Apple DEP service.
	TCP 1433	Connections to the SQL Server database.
pmm_mdm_service.exe	TCP 2195	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.

Index