Parallels®

# How to Easily Integrate Mac Computers and Other Apple Devices into Windows Environments

**White Paper** | Parallels® Device Management for Microsoft Configuration Manager

# Table of Contents

## Introduction

Apple devices are growing in corporate popularity every day. The Mac penetration of US corporations increased to 23% up from 17% in 2019. It's up to IT departments to make sure these devices can properly access and utilize all necessary corporate resources and they're properly accounted for and managed.

That said, COVID-19 has presented additional challenges to IT departments. With large portions of the workforce working from home and using whatever devices are available to them, the landscape of devices accessing business networks has been further fragmented. Former hardware policies no longer apply for many companies, as they've had to allow employees to use privately owned use privately owned devices in order to remain productive.

This can be a challenge, as macOS and Windows are very different, and many Mac devices remain a minority in Windows-dominant environments. Determining how to incorporate Macs and other Apple devices, such as iPhones and iPads, into a Windows infrastructure includes several factors, such as:

- The number of devices that need support.
- The type of access these devices require.
- The tools and systems an organization already has in place.

IT departments also need to figure out how to integrate Mac computers with existing Windows and Active Directory domains.

In Windows-centric organizations, managing Mac computers is typically not the highest priority on the IT project list for a variety of reasons. Not all IT teams have expertise in managing fleets of Mac computers, given the historical dominance of Windows computers. Familiar techniques for managing PCs don't help, and the best practices for dealing with Mac computers in a complex enterprise infrastructure can require specialized training.

Having macOS devices unknowingly used in your workplace (and thus not managed by your IT team) can be a big security risk. It means that end users are accessing your network via both Windows machines and Mac computers—as well as downloading and sharing documents—making management of these devices critical. These days, hackers don't care if you're on a Mac or a PC—if your Mac isn't up to date with macOS patches, it could be vulnerable to a breach. So, how do you centrally automate these updates to make sure Mac computers are safe and protected?

IT teams typically take a combination of four main approaches when trying to accommodate Mac devices:

1. Incorporate Mac devices into the Active Directory (AD) domain using existing tools meant for Windows computers.
2. Use special third-party tools to manage Mac devices in the AD domain.
3. Manage Macs using the same approach as mobile devices.
4. Manage both Mac and PC computers in Microsoft Configuration Manager.

Enterprise IT departments can no longer prioritize other devices over Mac computers. Unmanaged Mac devices could leave corporate IT infrastructures open to potential malware downloads and attacks. IT teams have traditionally focused on managing PCs. In doing so, they have invested resources to set up, maintain and properly secure countless resources to set up, maintain and properly secure a Windows-centric infrastructure.

Microsoft Configuration Manager (formerly SCCM, now part of Microsoft Endpoint Manager) is the most widely used management system for PCs and can now natively manage your Mac environment. But it does have limitations and cannot easily manage Mac computers. This white paper will explore these limitations and offer an alternative that enables IT admins to leverage their existing Microsoft Configuration Manager deployment to control and manage Mac computers, as well as iPhones and iPads.

## Requirements for Managing Mac Computers Natively in Microsoft Configuration Manager

Microsoft Configuration Manager enables the following actions with macOS clients:

- Setting up support and enrolling devices.
- Deploying settings.
- Performing hardware inventory.
- Deploying applications.

While Configuration Manager can manage these devices, additional items need to be installed and configured to support Mac computers:

- You will need to implement a public key infrastructure (PKI) for Active Directory Certificate Services to enable Mac support. These certificates are used to communicate with Configuration Manager through SSL communications. Each Mac with a Configuration Manager client installed acts like an Internet-based client.
- Since the Mac devices are behaving like Internet-based clients, you will need to have a Configuration Manager site server with a fully qualified domain name, and a minimum of one HTTPS-enabled management point and one HTTPS-enabled distribution point.
- You will need to configure the enrollment point and enrollment proxy point features in Microsoft Configuration Manager. This will enable your macOS clients to be enrolled in the Configuration Manager environment after the client is installed.
- You will need to configure custom client settings to enable the management of these macOS clients.

Configuration Manager's built-in support for the Mac operating system does work well, but there are certain limitations to the features and functionality.

To be able to manage macOS clients, you must use PKI infrastructure and additional Configuration Manager site systems. If you don't plan on enabling HTTPS communications for your entire corporate environment, you'll need to have multiple management points and distribution points. One management point will be configured for HTTP communications, and one will be configured for HTTPS communications; the same goes for the multiple distribution points.

Other limitations of Microsoft Configuration Manager with macOS include:

- There are limited compliance settings management on macOS and these settings are only available through scripts—not through macOS profiles.
- You can't enable or manage device encryption on macOS devices.
- Configuration Manager can only push software through the new application model to macOS devices.
- There is limited ability to patch macOS devices.
- There is no support for operating system deployment on macOS devices.
- There is no support for remote control from the console for macOS devices.
- Configuration Manager cannot lock or wipe macOS devices remotely.

These limited management features and functions of Microsoft Configuration Manager with macOS clients is still something for your corporation to consider. It provides basic management of your macOS devices out of the box. But for those administrators who want or need complete Mac management and still want to leverage their existing Microsoft Configuration Manager console, there is an alternative.

## Complete Mac Management via Parallels Device Management

It is possible to control and manage Mac computers under the same corporate requirements you have for PCs using Parallels Device Management for Microsoft Configuration Manager. The solution plugs right into Microsoft's device management suite.

1. Configure and operate an in-house administration structure for Mac computers.
2. Support Mac computers using the existing PC administration (to the best of its ability).
3. Use one unified device management tool to fully manage both types of computers.

### Parallels Device Management Feature Overview

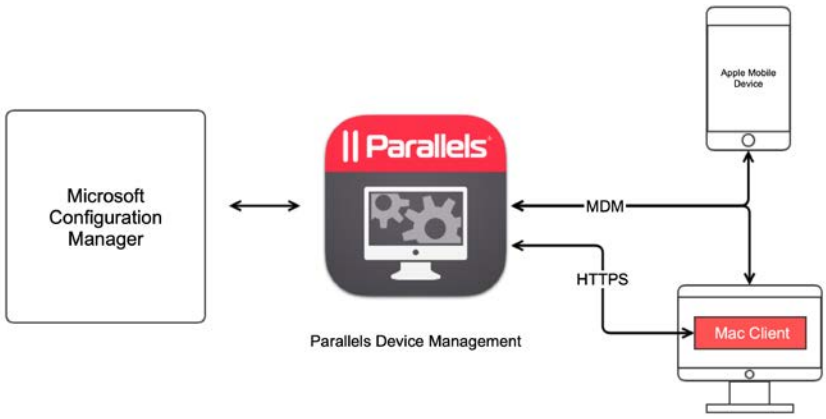
| Feature | Description |
|---|---|
| Discovery and enrollment | • Discover your Mac fleet by scanning the network and using AD system discovery.<br>• Enroll Mac computers in the Configuration Manager and install Parallels clients automatically.<br>• Enroll users manually through the administrator or permit Mac users to enroll themselves.<br>• Benefit from zero-touch enrollment and configuration with Apple Device Enrollment Program (DEP). |
| Asset inventory | • Take hardware and software inventory of your Mac computers.<br>• Perform custom inventory reporting through scripts.<br>• Leverage native Microsoft Configuration Manager reports for details on Mac computers.<br>• Report information about user logons. |
| Security | • Automate the management of macOS software updates via Configuration Manager to thousands of Mac computers.<br>• Secure your valuable information using FileVault 2 full-disc encryption with key escrow.<br>• Keep your corporate data safe with ability to lock or wipe a Mac if it is lost or stolen. |
| Compliance | • Configure macOS by deploying configuration profiles and running scripts.<br>• Enable FileVault 2 full-disk encryption to secure corporate data.<br>• Gain visibility into patch compliance with flexible, real-time monitoring and reporting via Configuration Manager's reporting dashboard.<br>• Support provided for reporting applications usage stats to Configuration Manager Software Metering. |
| Software and image deployment | • Support provided for package and application deployment models.<br>• Leverage a self-service application portal.<br>• Support provided for silent deployment and deployment with user interaction.<br>• Deploy macOS images to Mac via Configuration Manager using task sequences. |

Parallels Device Management not only helps with managing Mac computers just like Windows machines in Microsoft Configuration Manager, it also manages iOS devices seamlessly. You can add all iPhones and iPads within your organization into your existing endpoint management without an additional dedicated solution for Mobile Device Management.

Windows clients, Mac clients and iOS devices—they can all be managed through a single pane of glass. The result? Less security risks and devices to manage, and greater compliance.

## With Parallels Device Management, You Can Leverage What You Know

With Parallels Device Management, you can manage Mac and Windows computers using Configuration Manager as your only management system. This is important, as according to IDC, 70% of successful breaches originate on the endpoint. New features of Parallels Device Management include Remote Lock and Wipe, a data-security compliance feature that enables IT managers to lock a Mac or erase all data in the event it is lost or stolen.




*Parallels Device Management for Configuration Manager*

Parallels Device Management consists of the following components:

- Parallels Configuration Manager Proxy: A Windows service that acts as a mediator between Microsoft Configuration Manager and managed Mac computers and Apple mobile devices.
- Parallels Configuration Manager Console Extensions: A set of dynamic libraries that extends the Configuration Manager console to provide a graphical user interface, enabling you to manage Mac computers, iPhones and iPads. This component must be installed on the computer where the Configuration Manager console is installed.
- Parallels Mac Client: A client application that performs all the system management tasks on behalf of Microsoft Configuration Manager. The client gathers hardware and software inventory information, enables the automated installation of software titles and security patches and is used to apply compliance policies.
- Other components: Enables you to manage Apple software updates and Internet-based client management and MDM for Mac computers and Apple mobile devices.

Parallels Device Management can be deployed in a matter of minutes, and because it integrates into Configuration Manager, it requires no special training. You can simply manage Mac computers alongside PCs via the same console.

IT admins need solutions to manage the increasing number of Mac computers and Apple devices that are entering Windows-based enterprises, either through dedicated purchase programs or due to the increase in remote work, where any practical device available is becoming a “work device.”

Parallels Device Management ensures that IT teams can easily discover and manage these devices. It's a solution that leverages existing processes for PCs and supports the extension of compliance requirements to Mac—all from Configuration Manager's console.

## Conclusion

As corporations keep adding macOS and iOS devices to their official purchasing programs, the number of Apple devices in businesses will only continue to rise. Additionally, BYOD and remote work are becoming the norm rather than the exception, which can potentially add many more Mac machines and Apple devices to a company's network.

Parallels Device Management helps businesses support, control and manage how employees use their favorite devices and preferred technology while helping IT teams leverage existing Microsoft Configuration Manager setups to manage Mac computers, iPhones and iPads.

Learn how your organization can successfully integrate and manage Apple devices using Parallels Device Management.