Security Challenges: Integrating Apple Computers into Windows Environments

White Paper | Parallels Mac Management for Microsoft SCCM | 2018

Presented By:

Parallels®

WME

Windows Management Experts Inc.

Table of Contents

Security Challenges: Integrating Mac into Windows Environments

Apple® Mac devices are growing in corporate popularity by the day. It's up to IT departments to make sure that these devices utilize all resources in the environment, as well as ensure they're visible and managed. This can be a challenge, as Mac® and Windows are very different, and Mac devices remain a minority in Windows-dominant environments. Determining how to incorporate Mac into a Windows infrastructure includes a number of factors, such as: the number of devices that need support; what type of access they require; and what tools and systems an organization already has. IT departments also need to figure out how to integrate

Mac with existing Windows and Active Directory domains.
In Windows-centric organizations, managing Mac is not the highest priority on the IT project list for a variety of reasons. Few IT teams have expertise in managing Mac. Familiar techniques for managing PCs don't help, and the best practices for dealing with Mac in a complex enterprise infrastructure can be convoluted and are not widely known.

Having unmanaged devices with macOS® in your environment is a big security risk. 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, the "bad guys" don't care if you're on a Mac or a PC. The Intel central processing unit (CPU) in Mac computers is similar to those in PCs, and as such both are vulnerable to many common attacks. If your Mac isn't up to date with macOS patches, it could be vulnerable. How do you centrally automate these updates to make sure Mac computers are safe and protected?

IT teams take 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 Mac like mobile devices.
4. Manage both Mac and PC computers in Microsoft SCCM.

Enterprise IT departments can no longer treat Mac computers as an afterthought. Unmanaged Mac devices leave corporate IT infrastructures open to malware downloads and attacks, as hackers target OS vulnerabilities beyond Windows. Traditionally focused exclusively on managing PCs, IT has spent countless resources to set up, maintain, and properly secure a Windows-centric infrastructure. Microsoft® System Center Configuration Manager (SCCM) 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 paper will explore these limitations and offer an alternative that allows IT admins to leverage their existing Microsoft SCCM deployment to control and manage Mac computers.

Requirements for Managing Mac Natively in Microsoft SCCM

Microsoft SCCM allows for the following:

- Setting up support and enrolling macOS clients
- Deploying settings to your macOS clients
- Performing hardware inventory of your macOS clients
- Deploying applications to your macOS clients

While SCCM is capable of managing these devices, additional items need to be installed and configured to support Mac:

- 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 SCCM through SSL communications. Each Mac with an SCCM client installed acts like an Internet-based client.
- Since the Mac devices are acting like Internet-based clients, you will need to have an SCCM 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 SCCM. This will allow your macOS clients to be enrolled in the SCCM environment after the client is installed.
- You will need to configure custom client settings to enable the management of these macOS clients.

SCCM's built-in support for the Mac operating system does work great, but there are certain limitations to the features and functionality of this support.

To be able to manage Max OS X® clients, you must have PKI infrastructure and additional SCCM site systems. If you are not planning on enabling HTTPS communications for your entire corporate environment, you will 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, as is the same for the multiple distribution points.

- With SCCM support for macOS clients, there is no automatic enrollment of devices. With Microsoft Windows devices, you can discover them in Active Directory and automatically install the client on them. With macOS clients, you will need to manually install the client and manually enroll them in the environment. This is a time-consuming task for corporations that have a large number of macOS devices.
- While SCCM offers compliance settings management on macOS, those settings are limited and available only through scripts, not through OS X profiles.
- SCCM can't enable or manage device encryption on macOS devices.
- SCCM can only push software through the new application model to macOS devices.
- SCCM has limited ability to patch macOS devices.
- It does not support operating system deployment on macOS devices.
- SCCM does not support remote control from the console for macOS devices.
- It cannot lock or wipe macOS devices remotely

The extra required items and the limited management features and functions of macOS clients notwithstanding, managing macOS clients with Microsoft SCCM is still something for your corporation to consider. It provides basic management of your macOS devices out of the box. For administrators who want or need complete Mac management and still want to leverage their existing Microsoft SCCM console, there is an alternative.

Complete Mac Management via Parallels Mac Management

Control and manage Mac computers under the same corporate requirements you have for PCs. Parallels® Mac Management for Microsoft® SCCM plugs right into Microsoft SCCM and offers these key management features:

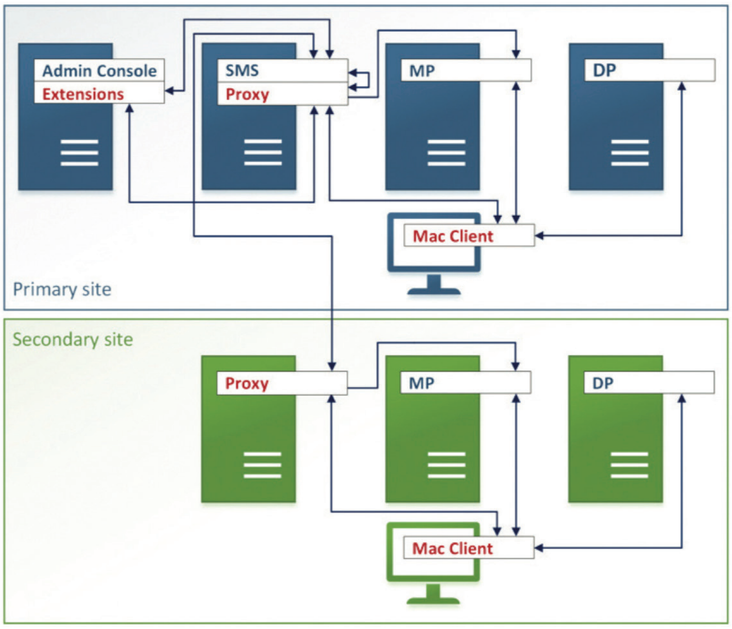
Discovery and Enrollment	Enrollment via network and SCCM AD system discoveries Automatic client installation and enrollment Manual client installation and enrollment Zero-touch enrollment via Apple Device Enrollment Program (DEP)
Asset Inventory	Gather hardware and software inventory of your Mac computers Leverage native Microsoft SCCM reports for details on Mac computers Report information about user log-ons
Security	Automated macOS patch management: Provides automated OS X patch management via SCCM to thousands of Mac computers Secure your corporate data by enforcing FileVault® 2 full- disk encryption using a personal or institutional key Lock or wipe a Mac remotely

Compliance	macOS configuration profiles and shell scripts Administer FileVault 2 full-disk encryption to secure corporate data Gain visibility into patch compliance with flexible, real-time monitoring and reporting via SCCM reporting dashboard Support for reporting applications usage stats to SCCM Software Metering
Software and Image Deployment	Support for deployment of a wide range of software packages: .dmg, .pkg, .iso, .app, scripts, and stand-alone files Support for package and application deployment models Self-service application portal Support for silent deployment and deployment with user interaction Deploy macOS images to Mac via SCCM using task sequences

Solution Overview: Leverage What You Know

Managing Mac is not the highest priority on the IT project list for various reasons. One of the real problems is that few IT teams have expertise in managing Mac. Familiar techniques for managing PCs don't help, and the best practices for dealing with Mac in a complex enterprise infrastructure can be convoluted and are not widely known.

Parallels® Mac Management for Microsoft® SCCM is a software plug-in that extends SCCM 2012 and 2012 R2 with the ability to fully manage macOS systems. With Parallels Mac Management, you can manage Mac and Windows computers, using SCCM as your only management system. In fact, according to a Windows IT Pro survey[1], 66% of IT pros said that using a single management system would streamline their operations, and 58% determined they would also benefit through cost savings for their organization.
New features of Parallels Mac Management include Remote Lock and Wipe, a data-security compliance feature that allows IT managers to lock a Mac or erase all data in the event it is lost or stolen.



[1] Slide 20, MacTrendsSummary May2016.pdf

Parallels Mac Management consists of the following components:

- Parallels Configuration Manager Proxy: A Windows service application that acts as a proxy between SCCM and Mac computers. The application must be installed on a computer running Windows Server® 2008 SP2 or later.
- 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 OS X computers. This component must be installed on the computer where the Configuration Manager console is installed.
- 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 OS X images on Mac computers.
- Parallels OS X Software Update Point: Allows you to manage Apple software updates (patches) for macOS using the native SCCM functionality. The component requires Windows Server Update Services (WSUS) and must be installed on the same server as WSUS.
- Parallels Mac Client: A client application that enables communication between a Mac computer on which it is installed and Parallels Configuration Manager Proxy. The client inventories hardware and software installation information, enables the automated installation of software packages and security patches, and is used to apply compliance policies.

Parallels Mac Management can be deployed in a matter of minutes, and because it integrates into SCCM, it requires no special training. Just manage Mac computers alongside PCs via the same console. Michele Bleser, the managing director of technology at consultancy Slalom, Inc, said, “Parallels Mac Management is an awesome and unique tool for helping primarily PC-based organizations like Slalom cost-effectively support their ever-growing Mac user base.”

With more and more Mac computers entering the Windows-based enterprise, Parallels Mac Management ensures that IT discovers and manages them easily, leverages existing processes for PCs, and allows for extension of compliance requirements to Mac, all from the SCCM console.

About Parallels

Parallels software helps businesses support, control, and manage how employees use their favorite devices and preferred technology. IT teams can benefit from solutions created for cross-platform environments, including: seamless delivery of virtual desktops and applications to any device; enterprise deployments of Windows on Mac; leveraging existing Microsoft SCCM to manage Mac; and remote access from any device. More information is available at parallels.com, or speak to one of our team members by calling +1 425 282-6448.

About Windows Management Experts, Inc.

Windows Management Experts, Inc. (WME) is a leading system integrator for Microsoft Infrastructure and Cloud solutions. A Microsoft Certified Partner with gold competency in datacenter, device, and deployment, WME has over 30 years of combined experience and passion for transforming IT operations through the development of solutions and products that make the job of their customers easier. WME’s Strategic Services division concentrates on strategic talent strategies, partnerships, and acquisitions, partnering with organizations to assess and solve information technology challenges leveraging digital technologies—cloud, mobile, security, infrastructure, and data. Schedule a free consultation by visiting windowsmanagementexperts.com or by calling +1 888 307-0133.