IT’s New Best Friend? Transforming Mac Computers and Devices into Trusted Business Partners

White Paper | Parallels® Device Management

Table of Contents

©2021 Parallels International GmbH

Introduction

The COVID-19 pandemic saw a dramatic increase in remote working. This sudden shift meant that many businesses were not prepared to support a fully remote workforce. Many companies were either lacking laptop computers, device management solutions, tools to support remote working or some combination of all three.

Investments in tools for remote working have increased, mainly in conferencing, collaboration and remote desktop tools. The pandemic has also increased bring your own device (BYOD) adoption as employees working from home are using any device available to them and/or whatever is most convenient.

The above developments have created a major shift in how IT can monitor and manage devices. As IT's physical access to work devices fell by the wayside, and many companies had to adapt their policies to allow such device usage in order to keep operations running, the device landscape across many businesses has changed.

New, user-owned devices have begun to enter the network, among them Mac computers and other Apple devices. For a long time, Mac was seen as an exotic species in a world dominated by Windows. But the growth of Apple global market share seems unstoppable, and Mac computers have already become a common sight in many organizations, with a survey conducted by Parallels finding that more than 50% of companies now allow Macs to enter the network, either as a BYOD or official company device.

However, it's still not uncommon for this transition to be somewhat improvised from an IT perspective. As so-called "shadow Mac computers" have started to emerge—i.e., those not officially approved by IT/management—IT departments must now make sure these devices operate just as reliably and securely within a mixed IT landscape that contains Windows-only PCs.

Fortunately, there is an elegant solution: Parallels® Device Management for Configuration Manager (formerly known as Parallels Mac Management for Microsoft SCCM). This plug-in seamlessly integrates Apple computers into the administration of Windows IT landscapes.

Why Apple Device Use Is Increasing

Using Mac computers alongside Windows machines has become common in many offices. This is primarily for two reasons: employees are taking their personal MacBook to the office, or they can choose to have a Mac at work instead of a PC. As working from home has seen a huge increase during the pandemic, many privately owned Mac computers have entered business networks around the world. Some companies have even made Mac the standard. There are four good reasons to use Mac computers in business:

Lower support costs

Companies that use Mac and Windows computers regularly refer to the significantly reduced support costs associated with Apple computers, which typically results in fewer calls made to an internal help desk. As a result, Mac users often require fewer staff resources than Windows users do.

Improved data security

Data security and integrity is an important issue for every IT administration. These days there isn't an organization out there that can fully function without a strategy to protect against external and internal threats, as well as one that minimizes damage and speeds recovery in the event of loss. While Mac computers have become more susceptible to attacks in recent years, viruses, Trojans and ransomware primarily target Windows systems. This means that Mac computers are less affected from the outset. macOS also features more integrated security, such as FileVault 2 for data encryption, and Gatekeeper, which protects against the loading of harmful software.

Increased reliability

Apple is the only computer manufacturer that offers synchronized hardware and software. This is a massive benefit in terms of the reliability of Mac systems. In contrast, Microsoft must go to enormous lengths to make Windows run smoothly on the numerous different PCs available on the market.

Easier to use

Many users have become familiar with the intuitive, imaginative and particularly user-friendly operation of Mac systems and want to use them for work. Apple has attributed particular importance to its user interface—and for many Mac lovers, Windows just doesn't compare.

Apple Market Share Keeps Growing

Windows continues to dominate the world of desktop computers and laptops across the globe. However, the number of Mac computers in companies is growing. According to analyst estimates, Apple's Mac share in businesses reached 23% in the US in 2020, up from 17% in 2019. This is strengthened by cases where Mac computers find their way into large companies on a broad scale. Take the following examples:

- IBM has been letting employees decide whether they want to work with PCs or Apple computers since mid-2015. There are now more than 200,000 Apple devices installed at IBM. The IT group surprised everyone with the announcement that Mac clients cost the company significantly less overall than PCs.
- Others have since followed IBM's example, including software company SAP, financial service provider Capital One and retail giant Walmart, and many confirm the lower overall cost of Mac devices when directly compared with Windows.

These days, many IT managers in Windows-based companies cannot afford to dictate that their users only use PCs. It's hard to avoid a certain number of macOS systems in a world that was previously Windows-only. There are a couple reasons for this:

- Employees who use Mac computers at home may ask for a Mac at work because it's the device they're most familiar with, and so management fulfils this request to keep them happy and productive.
- For employees in certain departments (e.g., marketing, which often uses graphics applications that work best on Mac), Mac computers have become the system of choice. In this case, IT is forced to permit exceptions to the Windows standard, even if they can only provide minimal device support.

Incidentally, the trend of Mac computers appearing in businesses is outpacing the increased global market share of Apple computers. It seems that Mac computers are simply finding their way into companies another way, such as employees bringing their own computer into work or using them while working from home.

Because of this, Mac computers are generally present in offices already, regardless of whether IT supports them as an official PC alternative. These "shadow devices" are unregistered, unmanaged, unsupported and above all, not subject to company security policies. This means that these computers not only complicate the administration and operation of an organization's IT landscape, but they also represent a security risk—both to the internal network operation and to external threats.

Regardless of whether Mac computers are officially permitted or have spread through BYOD, the complex task of integrating them into the IT landscape falls to the IT department. IT is confronted with a landscape that—while often mostly Windows-centric—is nonetheless mixed, with both PCs and Mac computers requiring the same level of support, functionality and security.

Options for Mac Computers in the Windows Landscape

IT departments basically have three options when it comes to integrating Mac computers into an existing Windows administration:

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.

Whatever option is used, it should be able to fulfil all common tasks, regardless of computer type, including:

- Registration of hardware and software equipment in the system administration (if not provided by the user).
- Automatic configuration for first-time rollout, and if the device is replaced.
- Integration into the company-wide data backup system.
- Monitoring for undesired or suspicious activities.
- Monitoring for compliance with security regulations.
- Remote maintenance.
- Central patch and update distribution.
- User support.
- License monitoring.
- Reporting.

Option 1: Two Administration Systems, Double the Effort

An obvious solution to managing Mac computers in a Windows network is configuring and operating a separate management tool for Apple computers. The market offers well-suited solutions for this. However, this means the effort needed to support devices doubles. Not only do two whole IT administration systems need to be configured and operated, but many administration tasks—from configuring and monitoring devices to data backup—need to be performed twice. Even if everything goes according to plan, something may be missed during integration, such as system administration or reporting.

Option 2: One Administration System with Many Limitations

The second option is using the existing endpoint management for Windows to also administer Mac computers. As it happens, Microsoft Configuration Manager (formerly known as SCCM)—the most-used system for PC administration—can also administer a Mac environment. But the system has its limits.

For example, Mac computers are not automatically registered when administered with Configuration Manager. Windows computers are located in Active Directory, and the client program is then automatically installed onto it. You must install the client on Mac computers manually, and then also register the devices in the environment manually. If there are many Mac computers, this becomes a time-consuming task.

Other limitations of Microsoft Configuration Manager include:

- Although it offers administration for compliance settings on Mac, these settings are limited and only available via scripts, not macOS Configuration Profiles.
- It cannot activate and administer encryption of Mac computers.
- It can only transfer software to macOS systems via the new application model.
- It's limited in its capacity to install patches on Mac computers.
- It does not support deployment of Apple's operating system.
- It does not support remote operation of Mac from the console.
- Mac computers cannot be remotely locked or wiped.

The restricted administration of Mac with Microsoft Configuration Manager also requires additional tools to be installed and configured:

- The IT department needs to configure a public key infrastructure for the Active Directory Certificate Services to enable Mac support. The certificates issued serve to communicate with the Microsoft Configuration Manager system via SSL (Secure Sockets Layer). This means every Mac with a Configuration Manager client installed operates like an Internet-based client.
- As Mac computers therefore behave like Internet-based clients, you need a site server with a qualified domain name and at least one management point and distribution point for HTTPS on the Configuration Manager side.
- You must configure the Enrollment Point and Enrollment Proxy Point functions in Configuration Manager. This then enables the Mac computers to enroll into Microsoft's Configuration Manager environment once the client has been installed on them.
- You need to configure certain settings to enable the administration of Mac computers.

You also require more than one management point and one distribution point if you do not want to install HTTPS communication across your entire IT landscape. One of these points is then configured for HTTP communication and the other for HTTPS, in each case.

Enable Full, Unified Functionality with Parallels Device Management

The basic functions for Mac administration can be implemented using Microsoft Configuration Manager alone, albeit with extra effort. However, there is an alternative for fully integrated management of Mac computers in a Windows environment: Parallels Device Management for Configuration Manager.

Parallels Device Management is a plug-in that fully integrates itself into the functionality and operation of Configuration Manager. Parallels Device Management can be configured in minutes and does not require special training, as it is a plug-in for Configuration Manager. A company that wants to seamlessly administer and support Mac in its Windows environment without extra work is well-advised to implement this solution.

©2021 Parallels International GmbH

Parallels Device Management provides IT administrators with full control of all Mac computers, as well as iPhones and iPads, in their network landscape. Key features include:

Mac detection and registration

Like Configuration Manager, Parallels Device Management registers Mac computers via network scan and Active Directory system discovery. The Apple Device Enrollment Program (DEP) is also supported; new Mac devices can be automatically registered and configured from any location, eliminating the need for time-consuming imaging or manual configuration. IT can also let Mac users auto-enroll in Parallels Device Management via an email invitation. This is ideal in a remote scenario, where IT doesn't have physical access to machines.

Inventory and report creation

Mac computers report comprehensive hardware and software information, which can be used for generating various reports in Microsoft Configuration Manager. This also includes more detailed information, such as logged-in users and session duration. The Software Metering Usage Report Cycle is also supported in order to calculate the active usage of software—and therefore the need for software licenses—on Mac computers.

Software application deployment

Flexible options enable software applications to be deployed. Applications and package deployment models from Configuration Manager are supported. Available macOS applications can be presented in the Parallels Application Portal and installed by users at their convenience.

Security compliance

Compliance with security regulations can be ensured using various configuration items, such as macOS configuration profiles, activation of FileVault hard disk encryption and Python/shell scripts.

Conclusion

ideal add-on for all admins in Windows-centric environments. It enables IT to add Apple devices into an organization's existing device management suite. This enables seamless device management across Windows, macOS and even iOS devices with one single unified tool: Microsoft Configuration Manager.: Microsoft Configuration Manager.

There's no need for Apple-specific management tools, or to manage Mac computers with a "mobile device management" tool. Instead, Parallels Device Management lets you keep working without Mac-specific training or tools. Your policies, metering and software distribution will simply apply for all Mac and iOS devices across the network.

Learn how Parallels Device Management can boost your company's device management abilities.

©2021 Parallels International GmbH. All rights reserved. Parallels, and the Parallels Logo are trademarks or registered trademarks of Parallels International GmbH in Canada, the United States and/or elsewhere. Apple, iPad, iPhone, Mac, and macOS are trademarks of Apple Inc. All other company, product and service names, logos, brands and any registered or unregistered trademarks mentioned are used for identification purposes only and remain the exclusive property of their respective owners. Use of any brands, names, logos or any other information, imagery or materials pertaining to a third party does not imply endorsement. We disclaim any proprietary interest in such third-party information, imagery, materials, marks and names of others. For all notices and information about patents please visit https://www.parallels.com/about/legal/