Apple Device Management

For the robust security of the digital workspace

WHITE PAPER

hexnode

Table of Contents

Business transformation with Apple: The enterprise adoption that ignited an IT revolution

The mobile revolution that hit the world in recent years has made a massive impact on the work culture. There was a time when BlackBerry was the most desired phones for work. However, with the advent of Apple and its cool devices, people and even companies started to roll out Apple devices for work. It is nothing but the core security features and the incredible user experience from Apple that attract businesses to Apple products.

> "A handful of Apple devices in an enterprise can be controlled using Apple's native management solutions such as Profile Manager and Apple Configurator but managing a vast influx of devices is a big deal."

An enterprise-level deployment of hundreds of thousands of devices obviously needs some form of an automated process for its configuration and management. As they say, with great device fleet, comes great responsibility. Moreover, the rapid growth of mobile devices always accompanies a series of security risks and malicious attacks. A third-party MDM solution can effectively address these corporate risks and security vulnerabilities. This white paper addresses the importance, challenges, and strategies involved in controlling Apple devices with the **Apple management solution** from **Hexnode.**

79% **21%**
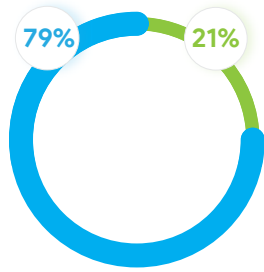
"According to the analysis of over 16 PB of data from 2017-2018, Egnyte, the data protection and file sharing company found that the most mobile collaboration happens on iOS."

It was only a matter of time before Apple came up with its own solution for device management

"The process of securing and managing Apple devices within an enterprise has never been an easy task. However, the complexity of Apple device management has considerably reduced with the advent of enterprise management tools offered by Apple."

Apple has preoccupied the world of Enterprise Mobility management, incorporating data security and device-level control. Security has always been a significant concern to enterprises as it is essential to build a reliable and robust business ecosystem. The process of securing and managing Apple devices within an enterprise has never been an easy task. However, the complexity of Apple device management has considerably reduced with the advent of enterprise management tools offered by Apple. The Mobile Device Management (MDM) service offered by Apple helps manage corporate as well as personally-owned iOS devices while securing all the corporate information assets. It simplifies bulk deployments of iOS devices and streamlines the ongoing management processes such as account configuration, app distribution, policy setup, device restriction settings, and other remote configurations. Apple extends two pivotal tools named **Profile Manager** and **Apple Configurator** for making the device management workflows more comprehensible.

	Profile Manager	Apple Configurator
Working	- Completely over-the-air.	- Requires a physical USB connection.
Use cases	- Configure and remotely manage iOS, macOS, and tvOS devices. - Assign configuration profiles to a user's email accounts, device contacts, messages, and calendar.	- Set up multiple configurations for iPhones and iPads before deployment. - Apple Configurator tool best fits for organizations like schools and enterprises with small device count.
Benefits	- Create and quickly distribute configuration profiles for different types of users. - Installing a configuration profile on a user device will push all the settings defined in the profile to that device. - Enables deployment of devices in bulk. - Allows user-based profile association. - Enables instant passcode resetting.	- Import configuration profiles from the iPhone Configuration Utility. - Enforce mobile device security policies. - Create and install configuration profiles on devices. - Modify or remove the existing profiles. - Basic MDM capabilities. - Supervise iOS devices. *Apple iOS supervised mode helps administrators gain greater control over the devices, including the ability to unlock additional restrictions on the devices.* - The integration with Apple Device Enrollment Program (DEP) helps automate the device enrollment processes. - Integration with Apple Volume Purchase Program (VPP) enables the purchase and distribution of apps.

Enter: Mobile Device Management to the world of Apple

The inrush of Apple devices into enterprises always accompanied by a set of crucial security challenges. The difficulty in mass rollouts, inability to handle multiple users on a single device, troubles in managing OS upgrades are some of the common challenges faced by IT folks while managing Apple devices without the aid of third-party software. An improper device management scheme can ruin the entire working of an enterprise.

With the advent of third-party Mobile Device Management tools, device management has become remarkably efficient and streamlined than ever before. Appropriating your enterprise with a Mobile Device Management solution comes off well when you understand what to look for in MDM systems and how to reap benefits from them.

An MDM is an end-to-end software suite comprising of several tools designed to automate device management and push various configurations to the devices wirelessly. Apart from that, it grants a robust device monitoring mechanism with automated compliance checks and periodic reporting.

MDM lets admins manage and configure devices, control user access to corporate assets, including the applications purchased from the App Store. Additionally, an MDM solution enables you to lock or wipe devices either instantaneously or remotely without even the need to touch them.

> "The native management tools from Apple suits your business environment when the requirement is to control only a handful of devices, along with some basic management capabilities."

Apple Configurator	Third-party MDM
- Not for personal BYOD device management	- For both personal and company-owned devices
- No over-the-air process.	- Can do everything over-the-air.
- Need to physically connect the device to a Mac every time.	- Has features and functionalities far superior to Apple Configurator.

Now, don't you think it is a great idea to integrate enterprises with a third-party MDM solution?

Giving wings to Apple device management

Hexnode, with its user-centric design, makes the configuration and management of devices fast, easy, and efficient. Hexnode MDM provides intuitive ways to refurbish an organization with the level of control they need to secure the devices, applications, data, and network. The diverse set of features and a hands-off approach from Hexnode makes it proficient at protecting sensitive corporate content from getting into wicked hands. Furthermore, Hexnode empowers an enterprise to build a comprehensive and secure device management strategy to the workforce in its BYOD environment.

Key benefits of Apple device management with Hexnode

- ✓ Remotely view and monitor devices in real-time
- ✓ Manage multiple devices from a central console
- ✓ Enforce device configurations and restrictions
- ✓ Manage, monitor and secure apps and data
- ✓ Set up corporate WiFi, email, VPN, and other network settings
- ✓ Initiate lock or wipe action upon device thefts
- ✓ Remotely track device locations in real-time
- ✓ Maintain compliance with corporate policies
- ✓ Lockdown devices into kiosk mode

iOS management

The iOS management solution keeps corporate data safe by enforcing comprehensive IT security policies over every iOS devices entering an enterprise. The Hexnode Apple MDM solution scales to manage the iOS devices employed in large enterprises, small businesses, hospitals, schools, and universities.

Hexnode offers different ways for enrolling iOS devices based on the considerations such as the size of the company, number of devices, and security aspects. The enrollment methods include *Enrollment without authentication, Email/SMS enrollment, Self enrollment, Apple Configurator enrollment, DEP enrollment*. Here're some of the capabilities that Hexnode iOS management offers enterprises.

– Remote view

Can remotely view the screen of an enrolled iOS device directly from the MDM portal and monitor the activities in real-time.

– Containerization

The **Containerization** helps to isolate work apps and data from personal apps and data, thereby protecting the corporate assets from data security breaches.

– Device wipe

When the devices containing sensitive corporate content are either misplaced or stolen, you can remotely wipe the device containers to prevent the corporate data from being exploited.

– Location tracking

Allows the administrators to monitor and track the location of every device on their MDM network in real-time. The movements of devices through an unauthorized area can be tracked and can also remotely initiate the lock or wipe action upon device loss or theft.

– iOS kiosk lockdown

Enables you to restrict your iPhones/iPads to a single application or a handful of apps. Setting up iOS kiosks benefits retail stores, automated information booths, educational institutions, and any other type of enterprise that needs to utilize devices with restricted user access.

— Integration with Apple Business Manager (ABM)/ Apple School Manager (ASM)

The integration of Hexnode with ABM/ ASM *enables wireless supervision of iOS devices, automated device enrollment, silent app installation,* and more. Working with ABM, Hexnode offers Managed Distribution, that allows IT admins to push apps instantly to the concerned devices without the need for an Apple ID.

Mac management

Hexnode offers a Mac management solution that develops a specific management strategy for Mac computers along with appropriate IT security controls in place. The solution makes the deployment and configuration of Mac devices quick and rapid while ensuring device security and compliance with corporate security policies. Here's an overview of some of the capabilities of Hexnode Mac management.

— Over-the-air enrollment

The Mac devices are enrolled in Hexnode seamlessly over-the-air so that the admin need not have physical access to each device.

Support for BYOD and COPE

Delivers a robust Mac management solution for both Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) business models.

Web content filtering

Enable or disable the use of specific websites. Blacklisting a website prevent users from accessing any page on that website whereas whitelisting block the users from accessing any of the websites except the whitelisted ones.

Integration with Apple Business Manager (ABM)/ Apple School Manager (ASM)

The seamless integration of Hexnode with Apple Business Manager/ Apple School Manager enables you to automatically deploy and configure your Macs in bulk with maximum ease. Moreover, the purchase and distribution of in-house applications as well as apps and books purchased through Apple Volume Purchase Program (VPP) can be implemented without the need for an Apple ID or an invitation request to the end-users.

The Mac management from Hexnode becomes flexible and more comprehensive with the capabilities including restricted access to App Store, automatic configuration of system update settings, and many more. The solution helps administrators to ensure that the right apps and business policies are deployed on the right devices.

Hexnode secures the entire fleet of Mac devices in an enterprise by configuring, deploying, and managing personal devices and corporate

devices independently with a different set of security policies. Hexnode Mac management solution provides complete control over your Mac devices by enforcing strong password policies, disk encryptions, firewall configurations, screensaver settings, certificate management, and much more.

Apple TV management
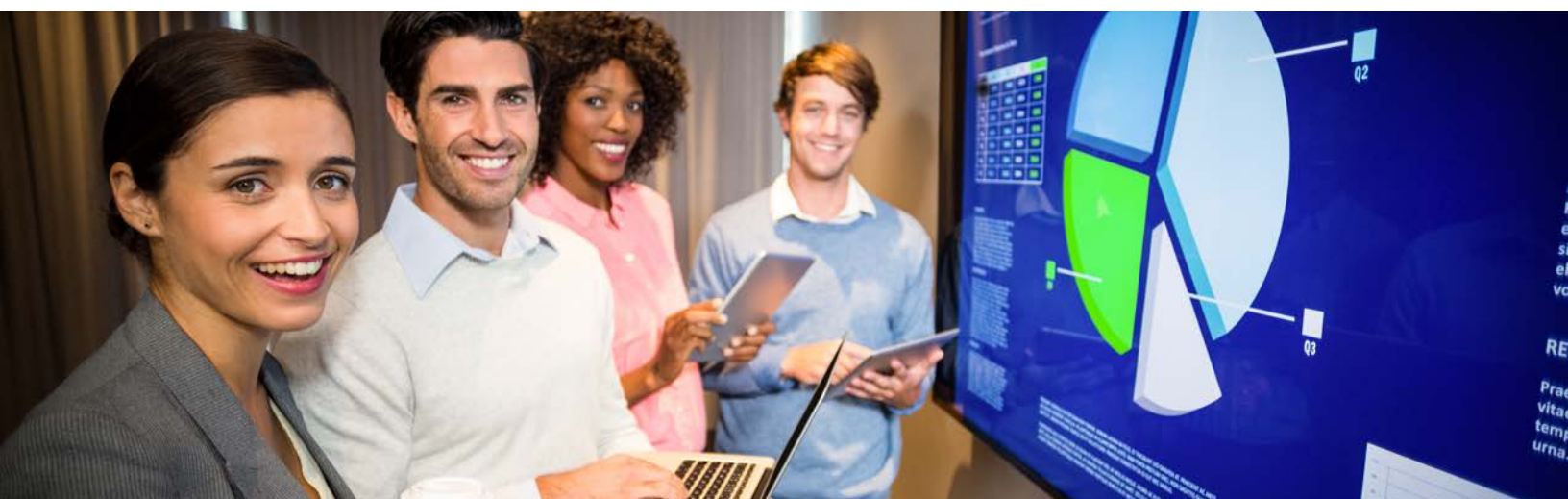
With Apple TV management solution, device administrators can instantly set up and deploy Apple TVs in an enterprise. With Hexnode, admins can remotely manage, monitor and secure apps, devices, data, and network from a centralized admin console.

The tvOS devices enroll in Hexnode either via Apple Configurator or Apple Business Manager (ABM). The solution helps admins configure various policies to apply MDM configurations automatically to the enrolled devices. Listed below are some of the capabilities of Hexnode Apple TV management.

– Secure tvOS devices

Secures the tvOS devices by preventing untrusted devices from accessing the networks as well as ensuring secure access to services such as Wi-Fi, Email, VPN through digital certificates.

– Over-the-air app installation

Enables wireless installation of in-house apps in bulk.

– iOS kiosk lockdown

Allows admins to lock down supervised tvOS devices to a single enterprise application. This makes the application launch automatically upon turning the device screen On. The Apple TV kiosk solution from Hexnode can also block the end-users from exiting the kiosk mode on their own.

– Integration with Apple Business Manager (ABM)/ Apple School Manager (ASM)

The integration helps you deploy all the settings, configuration, and apps automatically upon device startup.

The solution lets admins restrict the tvOS device settings such as VoiceOver, Invert Colors, Zoom adjustments, touch, Auto-Lock, and more. The admins can block the users from downloading explicit media from Apple Books, iTunes Store. Furthermore, they can configure Global HTTP Proxy to protect the devices from security threats and external attacks. On configuring Wi-Fi profiles with Hexnode, the devices can automatically establish a connection with the specified Wi-Fi network without even prompting for a password.

Conclusion

> "In a nutshell, the absence of a third-party Mobile Device Management solution significantly decreases workplace productivity and can lead to the failure of an entire organization."

The native management frameworks from Apple allows organizations to control a few devices in a small business environment. However, these solutions are inadequate to keep a wide range of Apple devices under control and to manage an inrush of new devices into the enterprise.

A third-party Mobile Device Management solution benefits an enterprise workforce and networks by implementing a seamless workflow of mobile devices on the corporate infrastructure. A robust MDM suite enables IT admins to configure, and control devices while managing the security of corporate data flowing through them. The MDM tool from Hexnode offers an excellent solution for controlling the employees and their overall mobility operations. Moreover, Hexnode Apple management solution works equally well for all the small, medium, and large business environments.

> "With tons of security restrictions and other configurations, the Mobile Device Management solution from Hexnode takes the sting out of managing the Apple devices flowing across enterprise networks, thereby helping businesses achieve its strategic goals and objectives."

hexnode