hexnode

Hexnode iOS Management Solution

Securing iOS devices with a flexible and scalable management suite

Key Takeaways

- Hexnode UEM integrates with Apple Business Manager (ABM), letting you wirelessly supervise devices and deploy Apps and Books to devices in bulk.
- Offers an efficient management solution for both the Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) strategies.
- Permits you to lock down your iOS devices into kiosk mode.
- Allows you to enforce advanced security options to supervised iOS devices.
- Remotely track the location of enrolled devices in real-time.
- Configure Google Workspace to directly assign devices to respective Google workspace users once the devices are enrolled
- Track and manage mobile data usage by the managed apps on your devices
- Remotely view the screen of an iOS device directly from the Hexnode MDM console to quickly diagnose and resolve device issues
- Customize the lock screen and home screen wallpaper of user devices by setting up wallpaper configurations

The Apple device management solution from Hexnode enables you to set up, deploy and manage iOS devices in your enterprise by simply unifying all management functionalities. With Hexnode UEM, you can set up a broad range of restrictions and configurations for supervised and unsupervised iOS devices. Hexnode’s remote view enables you to view the device screen from the MDM console, making it easier to diagnose and solve device issues as and when they appear. In addition, the seamless integration of Hexnode UEM with Apple Business Manager (ABM) makes it a perfect solution for Enterprise Mobility Management.

Why Apple device management?

The soaring popularity of Apple devices in today’s business environment calls for the necessity of a Unified Endpoint Management (UEM) solution for deploying and managing the Apple devices in an organization. Manually controlling the existing fleet of devices and the influx of new devices simultaneously can place a heavy strain on organizational IT departments by making it hard to maintain and secure the entire lifecycle of the devices. With employee devices no more restricted to corporate offices, it has become vital to focus on issues like device loss which were rarely a matter of concern earlier. The focus has now shifted to features that ensure uninterrupted device usage, like remote troubleshooting while ensuring security. Therefore, it becomes necessary to integrate your organization with a UEM solution that transforms your business potential without compromising your organization's security.

Managing Apple devices with Hexnode UEM

The Apple UEM software from Hexnode lets you maintain complete control over all the iOS devices that access your organizational data. Incorporating Hexnode UEM into your mobile strategy raises employee productivity while diminishing the chances of security breaches and network vulnerabilities. Hexnode's Apple UEM suite scales to manage the iPhones or iPads employed in large enterprises, small businesses, hospitals, schools, universities and so on. Hexnode UEM supports iOS devices running iOS 4 and later versions.

Features of Hexnode iOS device management

Enrolling Apple devices seamlessly

- Offering several options to enroll devices into your organization quickly and easily over-the-air.
- Letting you enroll devices via email requests as well as allowing you to connect and enroll devices physically if your policies require it.
- No authentication enrollment to let users enroll devices with a single enrollment URL.
- Configure Google Workspace with Hexnode console to assign the device directly to the respective Google Workspace user on enrollment.
- Self-enrollment to let users enroll their devices either using their preassigned password or their directory passwords.

Integrating with Apple Business Manager (ABM)

- Automated enrollment makes the device setup rapid and easy.
- Allowing you to wirelessly supervise devices and automate the enrollment of Apple devices.
- Enabling you to install non-removable MDM profiles, restricting users from altering device configurations manually, and silently push apps.
- With Apps and Books, you can buy apps and books from the Apple Store and even custom B2B apps from third-party developers.
- Offering Managed Distribution enables administrators to instantly push apps to the required devices without the need for an Apple ID.

Supporting Corporate-Owned devices

- Providing both onsite and remote view over the corporate-owned devices.
- Controlling business applications, emails, and security right away from the central admin console.
- Letting you enroll devices in bulk thereby allowing you to assign the devices to multiple users at once.
- Enabling admins to configure and monitor security policies, update, push applications and disenroll devices for reissuing them to other users.
- Allowing businesses to separate traffic at the app level, allowing the segregation of personal and corporate data with per-app-VPN.

- Avoid security threats caused by accessing corporate data from unauthorized devices by authenticating them with certificates.
- Protect corporate data by controlling the apps that can open documents downloaded from the enterprise domain using Safari.
- Remotely monitor and diagnose device issues and resolve problems reported by users quickly.

Advanced security options for Supervised mode

- Allowing you to turn on supervised mode for the devices connected to the network with the help of Apple DEP.
- Enabling you to place advanced security measures on institutional-owned devices, such as silent app installation, single app mode, and always-on VPN.
- Permitting you to restrict the functioning of certain apps.
- Delay iOS updates to give additional time to test bugs and issues associated with the latest OS release.
- Administrators can have more control over the devices and restrict features like keyboard shortcuts, messages, Airdrop, erase and changing passcodes etc.
- Easily push proxy settings to iOS devices in bulk over the air.
- Enforcing security and compliance of the enrolled devices.

Implementing BYOD

- Enhancing productivity by allowing employees to use their own iPhones and iPads for work.

- Allowing you to enforce BYOD policies in regulation with your business goals.
- Configuring corporate policies that meet your organizational requirements.
- Reducing IT operational expenses considerably as the users bring in their own devices to the workplace.
- Strong password policies to prevent instances of unauthorized access and ensure device and data security.
- Business container and managed domains to restrict the data flow between personal and corporate spaces.
- App catalog to create a customized app store on the device.
- Configure VPN to create a safe and encrypted connection to another network by choosing between options like on-demand, always-on or per app VPN depending on your requirements.

Setting up iOS kiosks

- Enabling you to lock down your iPhones/iPads to a single application or a handful of apps.
- Restrict your devices to single or multiple web applications.
- Automatically allow or block access to specific websites selectively to users.
- Letting you effectively employ this lockdown feature for retail stores, auto- mated information booths, educational institutions, and any other type of enterprise that needs to utilize a fleet of devices in kiosk mode.

- Making it easier to update enterprise apps on devices locked in kiosk mode without exiting the kiosk directly from the Hexnode console
- Lockdown supported apps in the foreground without any interruptions and let them exit the kiosk mode independently.

Identity and Access Management

- Enforcing the enrolled devices with strong password policies reduces the possibilities of data breaches and malware attacks that ruin an entire network.
- Setting up password requirements that incorporate length, complexity, special characters, timeout periods, passcode history and retry limits.
- Ensuring that a device password meet complexity requirements based on corporate policies.

Permitting you to configure and restrict the device features

- Allowing you to configure and restrict the device features that conflict with corporate regulations directly from the admin's central console.
- Disabling device features such as the camera, microphone, Siri, and apps such as YouTube, Facebook, Twitter etc.
- Enabling you to enforce corporate policies, deploy apps, and restrict access to device features without having to connect to the devices physically.
- Restricting iCloud settings such as backup, document sync, and security and privacy settings like lock screen notification, force encrypted backups and explicit content etc.

Managing applications

- Restricting access to specific apps from users or groups of users.
- Boosting productivity by blacklisting apps that cause distractions or security issues.
- Enabling distribution and removal of apps on the enrolled devices which ensures that the users have their devices equipped with all the necessary applications.
- Enabling administrators to create a customized app store hosting a set of apps that can meet the requirements of an organization.
- Add URLs, telephone numbers or even facetime links frequently used as apps to save your time.
- Manage notification settings for each app on your iOS devices to control when and how individual apps receive notifications.

Remotely monitor and track devices

- Letting you monitor and track all your devices on the MDM network in real-time.
- Tracking the movements of devices through an unauthorized area.
- Letting administrators and users to remotely lock or wipe a device in case the device is either lost or stolen.
- Remotely monitor your device screen from the Hexnode console, making it easier to diagnose and solve device issues reported by users.

Monitoring device compliance

- Allowing you to monitor the enrolled devices in real-time and ensure that they are always in compliance with the corporate policies.
- Alerting the administrators immediately upon policy violations.
- Monitoring password policy compliance, app compliance, detecting rooted devices, disabling Wi-Fi access to targeted users are some of the robust compliance management features of Hexnode UEM.

Expense management

- Enabling organizations to control cellular or roaming data usage by the managed apps.
- Helps control unnecessary data expenses in the organization.
- Choose the required app, enterprise, VPP or store app from the list and apply the policies individually or in bulk right from the console.

Configurations

- Easily push additional features of your choice into devices to manage various device functionalities with custom configuration profiles.
- Allow iPhones and iPads to connect to AirPlay-enabled devices on the same network.
- Enable your iOS devices to print with AirPrint-compatible or shared printers wirelessly with AirPrint.

Visit/learn more

www.hexnode.com

Sign up for a free trial

www.hexnode.com/mobile-device-management/

Knowledge base

www.hexnode.com/mobile-device-management/help/

Personalization

- Customize the device font type by adding new fonts as and when required.
- Remotely set suitable lock screen messages to be displayed on devices to help finder return the device if they are lost or misplaced.
- Change the look of iOS devices by setting home screen or lock screen wallpaper as per the organization's requirements.
- Flexibility to organize apps and folders on the home screen and the dock, create new pages and more with Home Screen Layout.