

# Hexnode Mac Management

Adorned with simplicity and flexibility

## Key Takeaways

- Flexible and simplified deployment of Mac devices in bulk with Apple Business Manager (ABM) integration
- Remotely set up device configurations and restrictions
- Configure, deploy and manage Personal devices and Corporate devices independently with a different set of security policies.
- Enroll the Mac devices seamlessly over-the-air so that the admin need not have physical access to each device.
- Effectively manage all your applications and set restrictions on their installation from a single console
- Multiple authentication measures to ensure corporate data security
- Remotely view your end user device to monitor and diagnose device issues for real-time troubleshooting
- Schedule updates to your end user devices remotely
- Personalize your endpoints to enhance user experience
- Set up compliance criteria for your end-user devices

Apple Mac devices have fortunately seized a notable place in the prevailing business and school environments. The rapid growth of Mac computers in enterprises makes it troublesome to manage various devices and users striving to access sensitive corporate information as well as customer data. An enter-prise will certainly get into trouble when an appropriate Mac management tool is not at hand.

## Why Mac management?

Manually managing Mac computers sorely demands a lot of time, effort, and proper preparation. Thus, enterprises started learning that the best way to cope with this issue is to utilize an appropriate Mac management tool that offers killer ways to reduce your IT operational costs and time invested in managing your Macs.

## How to manage Macs in an enterprise with Hexnode MDM?

The Mac management of Hexnode MDM operates in such a way that the right management strategy is executed while promising proper IT security controls in place. Hexnode MDM lets you deploy and configure your Mac computers ensuring that the particularities of Mac management never get compromised.

Here's how Hexnode MDM simplifies Mac management,

- Provides greater flexibility and a higher level of control over your Mac deployments.

- Automating app installation and distribution on the target devices.
- Ensuring that the devices comply with corporate security policies.
- Help you secure your enterprise's fleet of Macs by enforcing strong password policies, disk encryption techniques, firewall configuration, screensaver settings, certificate management and much more.
- Monitoring and controlling app installations, managing device configurations, tracking locations and more.

## Features of Hexnode Mac management

### Simplified Mac enrollment

- Multiple enrolment options to help you choose the one best suited for your organization.
- Enroll devices in a click with enrollment URL.
- Credential-based enrollment methods to let users enroll using the credentials sent via email or SMS.
- Google Workspace enrollment to get your Mac devices assigned directly to respective Google Workspace users.
- Allow users to directly enroll devices with Active Directory, Azure Active Directory, Google or Okta credentials.

### Automated Mac enrollment and deployment

- The seamless integration of Hexnode UEM with Apple Business Manager/Apple School Manager enables you to enroll and configure your Macs automatically.

- The Hexnode UEM Application Programming Interface (API) enhances your business productivity by facilitating effective and safe communication with your existing software solution
- Enable users to log in to a Mac using their AD credentials and employ cloud-based services registered with Azure Active Directory.
- Enforce group-based policy settings on target devices.

### **Flexible and comprehensive app management solution**

- Streamline the purchase and distribution of enterprise apps as well as Apps and Books purchased through Apple Business Manager (ABM) without requiring the configuration of Apple ID or an invitation request to users.
- Set selected apps as mandatory whereby you can make sure that all the necessary apps get compulsorily installed on the Macs without any user interruption.
- Secure and manage application deployments with the use of unified app catalogs.
- Restrict the access to App Store and app installations on your Mac devices.
- Automatically configure system update settings for your Mac devices.
- Remotely configure specific settings within applications to suit the needs of your organizations to ensure that the apps are pre-configured before they are distributed to the managed devices.
- Seamlessly distribute and update in-house apps over-the-air to the devices.

- Silently install apps on the end user device without a need for user action.
- Extend the natively available capabilities on the operating system by extensions and load them without user approval.
- Set up advanced restrictions to set restrictions on app installation from the App store.

### Secure network configuration management

- Set up your Exchange ActiveSync account over the air so that you can sync Emails, Contacts, Calendars, Tasks, Reminders, and Notes with your Mac devices.
- Block users from communicating with untrusted external networks.
- Easily set up email configurations on your Mac devices with safe access to your corporate inbox.
- The location history and live location fetching features of Hexnode help you track your stolen or misplaced Mac from anywhere around the world.
- Monitor and actively diagnose device issues, detect device incidents and provide troubleshooting instructions in real-time to simplify IT operations.
- Remotely configure VPN to provide users secure access to corporate resources even when the employees are working remotely.
- Ensure protection of files or application data by giving the users the approval rights of apps or processes that need access to protected data.

- Schedule macOS updates remotely, allowing administrators to restrict or reschedule them as per the requirements.

### **Sustain the security culture in the organization**

- Implement strong password policies to protect corporate data residing on your Macs.
- Execute smart-card features on your Macs to protect privacy by implementing an extra tier of authentication.
- Manage FileVault encryption settings thereby preventing unauthorized access to your Macs.
- Configure Firewall to secure your Mac devices by sustaining a boundary between a trusted internal network and untrusted external network.
- Set up web content filtering to obstruct users from accessing undesirable websites. Blacklisting a site stops the users from reaching any page on that website whereas Whitelisting blocks the users from entering any of the websites besides the whitelisted ones.
- Restrict and control basic features like device functionalities, app settings, app store, security settings, iCloud services etc., to prevent users from accessing non-work-related aspects.
- Limit user access to Mac devices for a specified amount of time.
- Remotely lock or completely wipe the devices in case your device is either lost or stolen.
- Set up advanced restrictions configure advanced security and privacy options like activation lock and password sharing.

- Create a virtual geofence to limit access to corporate data to users within the fence.

### **Enhance user experience through personalization**

- Customize your Mac's Dock settings such as size, position, magnification, animation settings of opening and closing applications and much more.
- Manage the login window on your Macs by configuring preferences for user login, specifying the information to be displayed on the login window and so on.
- Configure Setup Assistant utility on your Macs to manage the series of setup assistant windows that lead a user in setting up a new Mac.
- Remotely set up screensaver with an appropriate idle time and choose whether a password is required to unlock the screen.
- Enable users to print full quality photos and documents from known Air Print printers on the same network.
- Setup desktop wallpaper on all your enterprise devices to promote corporate branding on managed devices.

### **Identity and Access Management**

- Control identity thefts and malicious attacks by enforcing strong password policies on Mac devices and sustaining all the corporate regulatory requirements.
- Offer greater security for your corporate resources with two-factor authentication.
- Automated and periodic compliance checks ensure that the necessary corporate security controls are in place.

- App catalogs provide instantaneous access to required apps by creating a custom app store thereby ensuring that the workforce doesn't waste time searching for the apps they need.
- Implement certificate-based authentication for Wi-Fi and Virtual Private Network (VPN) settings.

### Mac scripting

- Automate processes to perform specific operations which otherwise needs to be executed one-by-one on Apple's terminal.
- Perform system level configurations on Mac devices without user intervention.
- Enhance Mac management by configuring settings that may not be a part of UEM's features.
- Perform a series of actions like shut down/restart devices, install/uninstall apps, push updates, set up app configurations and a lot more.

### Custom configurations

- Easier for administrators to create profiles using various tools to customize enterprise settings for various device platforms.
- Create custom configuration profiles using tools like Apple Configurator, profile editor etc.
- Deploy custom configurations using non encrypted .mobileconfig, .xml, or .plist files to the devices from Hexnode
- Customize enterprise settings for macOS by deploying profiles directly from the Hexnode console.

## Visit/learn more

[www.hexnode.com](http://www.hexnode.com)

## Sign up for a free trial

[www.hexnode.com/mobile-device-management/](http://www.hexnode.com/mobile-device-management/)

## Knowledge base

[www.hexnode.com/mobile-device-management/help/](http://www.hexnode.com/mobile-device-management/help/)

## AD asset binding

- Administrators can easily bind each Mac machine with Active Directory remotely with Hexnode.
- With AD Asset Binding, users can easily log in to their devices with AD credentials.
- Bind any LDAP with your Mac machine easily.
- Choose policy targets as per the requirement be it devices, users, groups, and even domains

## Media management

- Secure your corporate data by controlling access to corporate content.
- Configure advanced settings for media usage for external drives, internal drives and optical media to ensure corporate data security.
- Prevent instances of unauthorized access by restricting media access to authenticated users alone.