A Complete Guide to Mac Device Management

WHITE PAPER

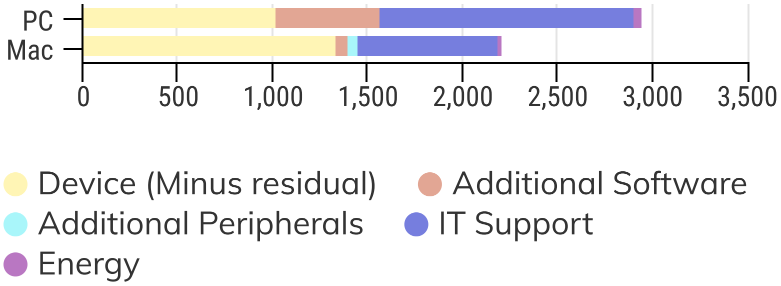
hexnode

Table of Contents

Introduction

SMBs and large-scale industries have begun accepting Mac devices within the workplace. Many users have found its total cost of ownership to be lower and the OS more dependable for work. The increased use of Macs within the enterprise can be partially attributed to the implementation of BYOD policies. Due to its high performance, security, compatibility and usability Macs are now favored by many employees. IT service tickets when compared to PCs are lesser as the employee's familiarity with the Mac devices gives them the flexibility to resolve some of the issues they may face on their own. One of the reasons that prevent businesses from adopting a Mac Enterprise Deployment is the cost. Apple devices on the whole still remain expensive but they offer a better TCO in the long run. Since Apple looks into the production of its own hardware and software, they offer long-term value to customers. This coupled with timely OS upgrades makes Mac devices a suitable choice for enterprises to use within the workplace.

Forrester did a research study commissioned by Apple. The study was a detailed comparison of the total economic impacts on Macs and PCs in enterprises that introduced employee choice programs where employees could choose a Mac or a PC as their work device.



Hardware, Software, Support Costs (Source: Forrester Total Economic Impact™ Study)

Cost Analysis

- Though the acquisition cost of Mac is $500 higher than that of PCs, when additional factors such as hardware and software costs are considered Macs turn out to cost $50 less.
- They have a higher residual value when compared to PCs.

IT Support and Operational Costs

Mac devices cost $628 less over a 3-year period. The important reasons behind this include:

- Setting up a new Mac takes less time
- Macs are easier to manage
- Mac users open fewer service tickets

Employee performance and engagement

The following statistics shows that Mac users are more productive:

- 20% improvement in retention rate
- 5% increase in sales performance
- 48 hours of increased productivity per employee

Security

- Mac devices have a more secure architecture when compared to PCs.
- Risk of a data breach per deployed Mac is reduce by 50%.

Chapter 1 - Services provided by Apple

With the services and programs provided by Apple, enterprises can effectively address a number of challenges they may face while managing Mac devices at a large scale.

Apple Business/School Manager

- Apple Business Manager (ABM) provides businesses with a centralized console to enroll devices and deploy the right apps and books needed by their employees. It includes DEP and VPP.
- Educational institutions can use Apple School Manager (ASM) to enroll devices and purchase necessary applications and books.

Zero touch deployment

- Automatically configure Mac devices purchased from Apple or from an authorized reseller.
- Organization should upgrade to ABM/ASM to make the devices ready for users upon unboxing.

- This deployment scenario is best suited for bulk enrollment where a large number of devices needs to be enrolled.
- Devices can be enrolled with its serial number or order number.
- Configure DEP with an MDM provider to deploy necessary configuration profiles.

Apps and Books

- Enables organizations to manage purchasing, licensing and distribution of apps and books required by users.
- MDM's integration with ABM simplifies this process and let admins have the necessary content ready for users right away.
- In addition to having instant access to Apple App Store and Apple iBook Store, admins can distribute custom B2B apps privately.
- Get more control over the distribution of apps by assigning apps directly to the devices without the use of Apple ID, revoke and assign apps to other devices and silently install applications.

Apple ID

- Apple ID is used to authenticate the user's identity.
- None of Apple's services such as the App Store, iCloud can be accessed without first logging in with your Apple ID.
- Apple IDs can be created for users as well as for an organization.
- Organizations can use their Apple ID within an MDM to create APNs certificates to enable communication between the MDM server and the Apple devices.
- The Apple ID is also used by organizations to login to the ABM/ASM portal to automatically enroll devices via zero touch deployment and to purchase and deploy essential books and apps in bulk.

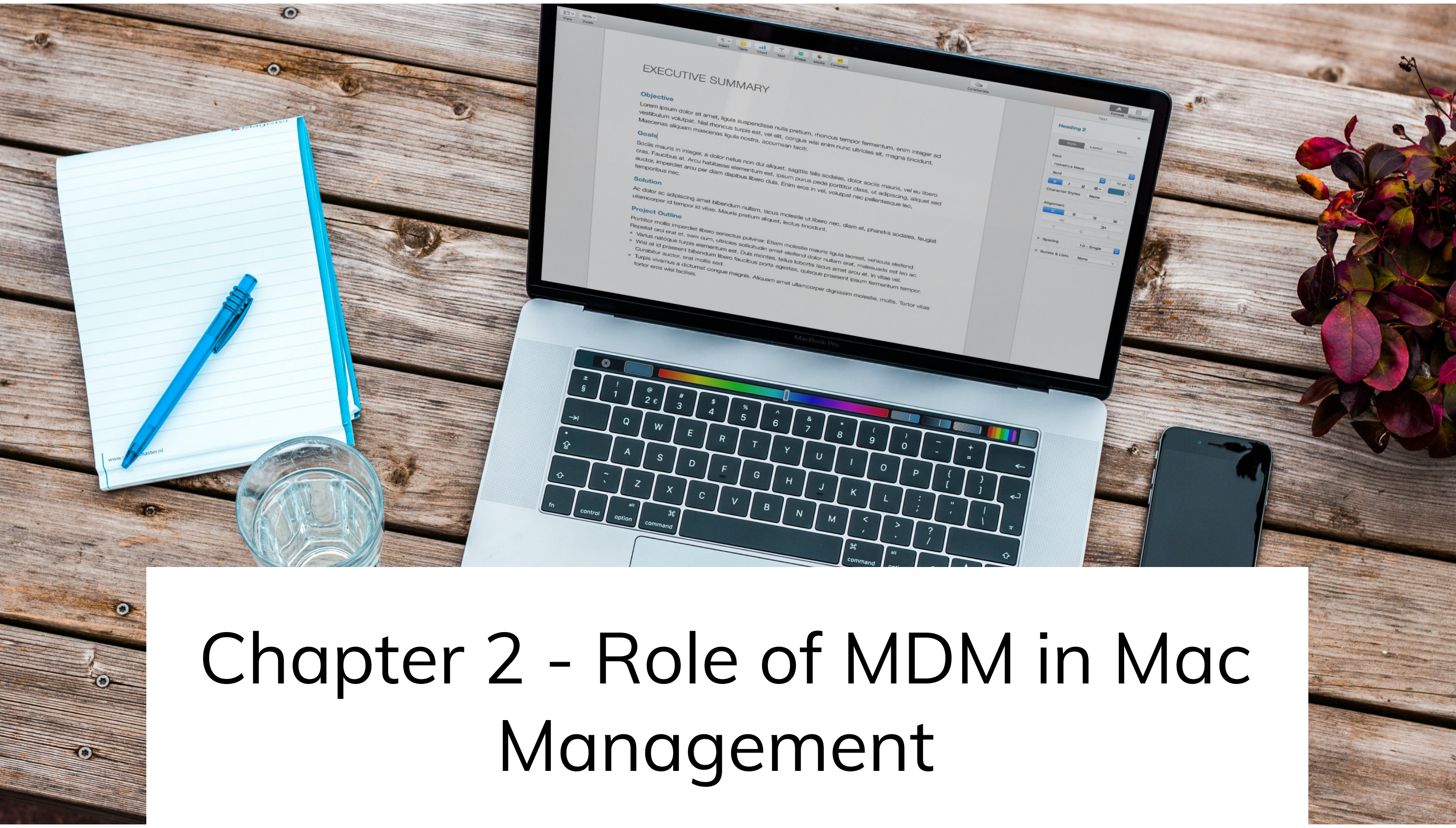
Managed Apple ID

- Introduced in ASM, Managed Apple IDs were initially created with the focus on minimizing distractions that put a damper on the learning experience of students.
- They limited app purchases and set restriction on services like Apple Pay and Face Time.
- Only contents approved by admins could be accessed on the devices.

- When Managed Apple IDs were later expanded into businesses, they were used by employees to easily access different Apple apps and services such as iCloud Drive, iTunes, Notes and iWork.
- Managed Apple IDs are owned and managed by the organization to ensure a smoother workflow. They can be used for app licensing, personalizing devices for employees, manage iCloud accounts and provide shared access to various enterprise accounts.
- In order to maintain productivity and ensure the integrity of the corporate resources within the enterprise, managed Apple IDs disables a number of features such as Apple Pay, iCloud Mail, iCloud Family Sharing, iCloud Keychain, App Store purchasing, iTunes purchasing, Find My services, FaceTime, iMessage and other media services such as Apple Music, Apple Radio etc.

Apple ID vs Managed Apple ID: Understanding the difference between the two

Apple ID	Managed Apple ID
Made for personal use.	Made for company owned devices with the aim to meet the organization’s requirements.
Created by the individual user. Once created, they can be used only by the person who creates it.	They can be created, managed and accessed by the user’s organization.
Leaves users with the responsibility to install the needed work tools by themselves.	Employees can have the work tools installed on the devices by the organization’s IT department.
Once an employee leaves an organization, it would be difficult to access their device.	Gives organizations the flexibility to access and manage the devices of employees who leave.
Less secure, as the work applications installed by users cannot be properly verified before it is pushed to the devices.	Enterprises can properly verify the applications before it is deployed onto the devices.



Chapter 2 - Role of MDM in Mac Management

With BYOD on the rise and remote work no longer being an option, one of the greatest challenges of being an IT admin is to secure the devices against unauthorized access. Mobile Device Management (MDM) has been instrumental in helping organizations set up adequate security configurations on the devices and also improve the productivity of employees by having the right application and files deployed at user end devices. Previously, device enrollment was a tedious process where admins had to manually provision the devices and get it ready for users. With Apple bringing its own hands-free enrollment like Zero Touch deployment, admins can spend more time on tasks that are of higher priority.

Managing Mac devices with MDM

- **Simplified deployment** – MDM combined with Apple's Zero Touch Deployment can significantly reduce the onboarding time and make the experience more agreeable for users. By associating your DEP registered Mac device to an MDM provider like Hexnode, necessary configurations can be set to ensure that the devices are already well secured when it reaches the hands of your users. All they have to do is to connect it to a corporate or school approved Wi-Fi network and the devices will be ready for use at once. DEP also offers the benefit of skipping unwanted setup assistant steps.

Enhanced security - It's not easy to keep a thorough watch on the devices when employees work remotely or when they take their personal devices back home after work. With MDM, you can set up adequate restriction policies to ensure that sensitive corporate data remain protected at all times. Strong passcode policies defining your organization's passcode rules can be enforced to make sure all employees follow them. There's always a higher risk for data breaches to occur if organizations implement lax security measures. Deploying a strong passcode policy helps secure your network and resources.

Refined App Management - It's vital to provide users with immediate access to the right applications. Apple store apps, apps purchased via VPP and enterprise apps can be seamlessly distributed to users to maximize productivity. App catalogs can be created to deploy individual apps or app groups to targeted users or teams within an organization. Hexnode also supports the distribution of enterprise apps in PKG format. Updating the enterprise applications remotely would ensure users have the latest version of it installed on their device. Making sure that employees stay completely focused on the tasks on hand will always be a challenge, the blacklisting feature can help admins black list applications that decreases productivity.

Deploy OS updates – Though updating the operating system is a good idea, they are not widely practiced in enterprises. Some employees would not be completely onboard with the idea either since they can sometimes cause incompatibility issues that may render users to lose valuable time and overwhelm the IT department with a flood of support tickets. Admins can schedule the OS updates after determining their organization's workflow and evaluating whether the new OS would be compatible for staff members to carry on their daily tasks. Updating your operating system to the latest version would be vital since they come with important security patches that can help fix any vulnerabilities hackers may use to exploit later on.

Remote management – With the increased reliance of remote work, it can be difficult for admins to monitor each device and ensure they stay compliant with the organization's policies. Hexnode offers a wide array of remote management capabilities that help admins to keep up a proper inventory on the managed devices.

These remote actions would also be extremely useful in locating misplaced or stolen devices and wipe sensitive corporate data to ensure it does not fall into the hands of unauthorized or malicious external parties.

Hexnode supports the management of Mac devices with OS X 10.7 Lion and above.

Hexnode MDM has a basic framework consisting of two components:

- Configuration Profiles
- Remote Management Actions

Configuration Profiles – They are integral in defining how the managed Mac devices must behave. Different network and security settings can be deployed as configuration profiles. Once the configuration profiles are installed, the devices will start functioning the way it's defined within the configuration profiles. Wi-Fi and VPN settings, passcode rules, app store and web browsing restrictions can be added into a single policy and pushed onto the devices.

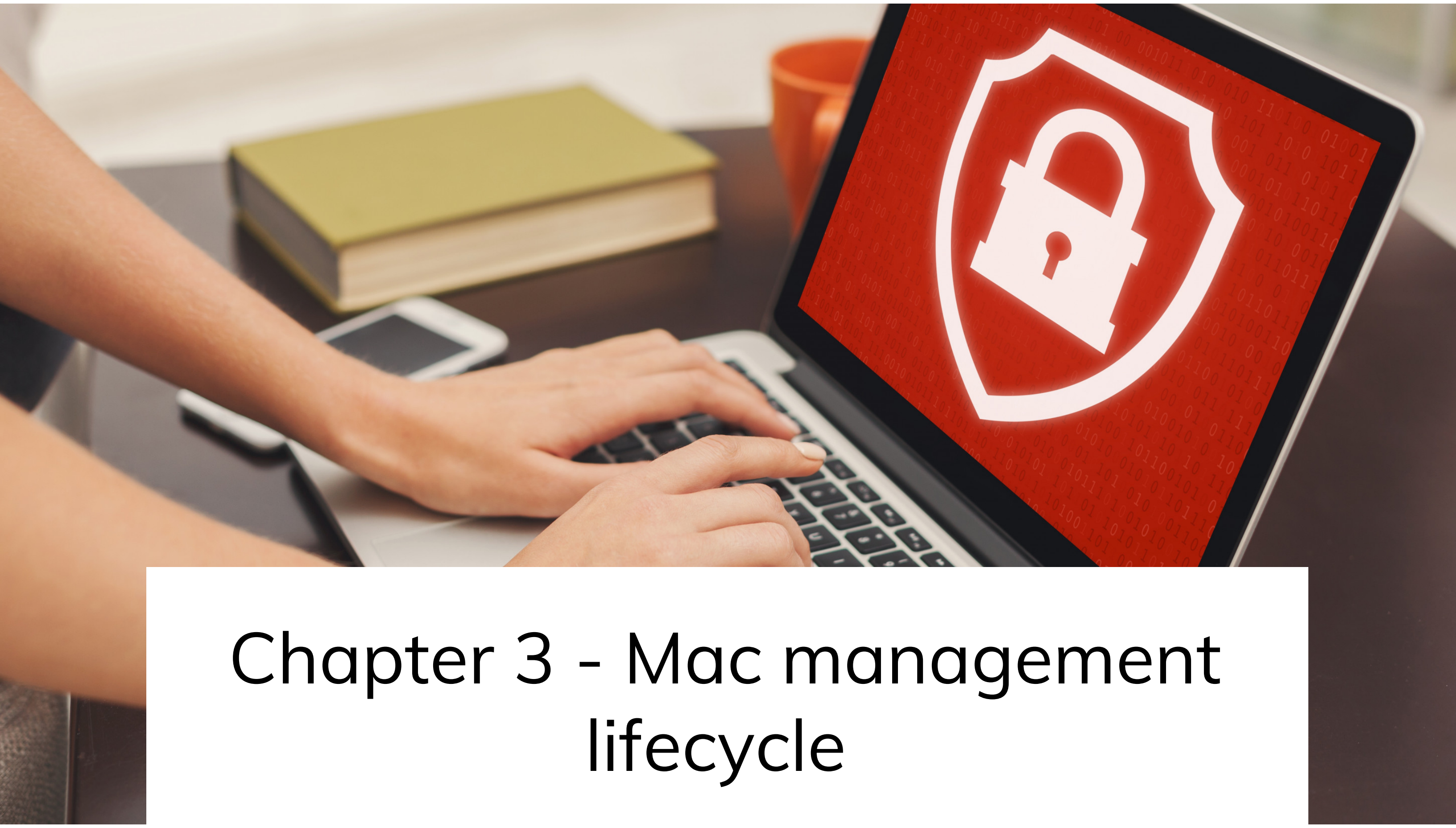
Remote Management Actions – These are unique commands which you can push onto the devices. If an employee reports losing their device, you can easily initiate a wipe device action from the MDM console to safeguard the confidential data. In order for users to use the device again after a factory reset, they will be required to enter their Find My Mac Pin. OS upgrades are vital to ensure the continuity of maintaining enterprise security, pushing OS updates remotely onto the DEP enrolled Mac devices can save admins the cumbersome task of reminding everyone to have their OS upgraded.

Apple Profile Manager vs Third-Party MDM providers

Profile Manager, Apple's native MDM may seem like a good choice to manage Mac devices within your organization, but admins can miss out on some essential management capabilities that third-party MDM providers like Hexnode offer. Apple Profile Manager only supports Mac computers, iPad, iPhone, iPad touch and Apple TV devices. This would be difficult for IT as they would have to resort to the use of other tools to manage other OS platforms. Going for third-party MDMs like Hexnode covering all popular device platforms would be a more convenient solution.

Apple Profile Manager vs. Hexnode

Apple Profile Manager	Hexnode
Does not support the option to associate profiles to domains.	Can associate policies to users, devices, groups and domains.
Does not have a dynamic group feature.	Can automate device grouping with dynamic groups.
When profiles are associated with devices, a notification will be sent to the device to download and install the profile. When profiles are associated with users, they will have to go to the user self-service portal to download it.	Policy is silently associated with the device.
Location of the device can be fetched only by enabling lost mode.	Location services can be enabled on mac devices. Real time updates of the device location can be fetched. Reports on the location history can be generated and stored.
Lacks Geofencing.	Has Geofencing.
Lacks the support of role-based admins.	Has multiple role-based admins.
Does not support app deployment through app catalogs.	Create individual apps and app groups in a catalog and distribute them to users.
Supports only the distribution of apps purchased through ABM/ASM and custom apps.	Distribute app store apps along with custom and ABM/ASM purchased apps.
Deploy in-store apps and apps purchased via ABM/ASM.	Distribute and manage store, enterprise, private and VPP apps.



Chapter 3 - Mac management lifecycle

Cyberthreats and various other social engineering attacks targeting enterprise users are continually on the rise. Though Macs are known to be more secure, it wouldn't be a bad idea to stay on guard and ensure maximum security on the enrolled Mac devices anyway. Understanding every stage of the lifecycle of the Mac device would give admins a better idea of how the devices ought to be managed. In addition to enhancing security, you can also ensure a smoother workflow with the timely deployment of apps to users.

Stage 1 - Integration and set up

The entire process of managing your Mac devices with an MDM begins with the Apple Push Notification service (APNs), a service created by Apple to enable Apple devices to communicate with other third-party services. The Hexnode MDM server first sends a notification to the APNs server, the server subsequently communicates with the device. In order to start to manage Macs with Hexnode MDM, you must first configure the APNs certificate. This certificate authorizes the communication from Hexnode to the Mac devices. Once the certificate is created it will remain valid for a period of one year from its date of creation. After every 365 days, the certificate has to be renewed.

Steps involved in configuring APNs:

- Create a certificate signing request from Hexnode's MDM portal.
- Upload the self-signed certificate in the Apple Server.
- Upload the APNs certificate back to the portal.

Stage 2 – Deploy and Provision device for users

Devices can be deployed to users via hands-free enrollment options like Zero Touch Deployment or user-initiated enrollment through URL. Going for Zero Touch Enrollment not only offers the convenience of enrolling bulk number of devices at once but it also leaves your employees free from the onboarding process. This deployment method would be ideal for organizations handling a large number of devices. You could also have a more user centric approach by letting users enroll their devices via Email or SMS consisting of the enrollment request.

Hexnode MDM offers the following deployment methods for Mac devices:

Open Enrollment

- Users can enroll their devices without entering any enrollment credentials.
- Enter the enrollment URL in Safari to download and install the MDM profiles.
- Enter the Mac admin's username and password.

Authenticated Enrollment

The enrollment credentials are sent to the mail used for enrollment. Users will have to enter those credentials to enroll the devices.

- Enter the enrollment URL in Safari.
- Type the username and password received in the mail.
- Download and install the MDM profiles.
- Enter the Mac admin's username and password.

Self-Enrollment

Users can enroll the devices with their Active Directory or Azure Active Directory, Google or Okta credentials.

- Enter enrollment URL.
- Select the right domain.
- Enter the credentials.

- Install MDM profiles.
- Enter Mac admin’s username and password.

Zero Touch Deployment

Known previously as DEP, Zero Touch offers a more streamlined approach for the enrollment of large number of devices. Necessary configurations and settings can be automatically applied on the device on its start up. This reduces user dependency on IT admins to get the device ready for work.

Apple has brought in DEP and VPP under a single web console known as ABM. In order to deploy the devices via DEP, organizations have to enroll in ABM. Only devices purchased from Apple or an authorized dealer on or after March 1st 2011 can be added. The Mac devices should be running on an OS version of OS X 10.9 and above.

Integrating DEP with an MDM solution like Hexnode, would give organizations a more individualistic approach to define the right settings and configurations that is tailor-made to their workflow and security requirements.

Configuring DEP with Hexnode

1. Login to Hexnode MDM portal and download the certificate file.
2. Sign in to ABM, add the MDM server and upload the downloaded certificate file.
3. Download the new server token from ABM and upload it Hexnode server.
4. Once you have uploaded the token in Hexnode server, you would be able to configure the options listed below:

- Add DEP devices as pre-approved device
- Create a new DEP configuration profile or select a previously created one
- Choose the user authentication type

Assign devices to Hexnode Server

1. Sign in to the ABM account.
2. Click on Devices and select the required devices.
3. Choose the MDM server to assign the devices to that server.
4. Once the devices have been assigned, you will be able to see the devices in the Hexnode MDM portal.

Benefits of enrolling with DEP:

1. Installation of non-removable MDM profiles.
2. Prevent users from manually removing the MDM configuration.
3. Preconfigure and setup devices for users.
4. Silent app installation and upgrades.
5. Access to more security capabilities.

G Suite Enrollment

Allow admins to assign Mac devices to G Suite users. The whole process can be briefly condensed down to two steps, which involves:

- Configuring G Suite with Hexnode MDM
- Enrolling Mac devices with G Suite Authentication

This enrollment approach is yet another convenient way for admins to manage the Mac devices as the required policies and remote actions can be associated not just with the devices but with users and the whole domain as well.

Prior to going for this enrollment method, you have to make sure that your organization has a G Suite account. A service account needs to be created and API client access should be given to the MDM provider to provide them with specific API access to apply the required configurations onto the managed Mac devices.

Stage 3 – Configure the devices

Applying necessary configurations onto the managed devices prevents users from tampering with the device settings and ensures that the devices stay secure against prying from unauthorized sources. The configuration profiles can be associated to a single device as well as groups of devices. Admins who want a more organized device management approach can group the devices or users into static groups or dynamic groups. A static group will consist of a fixed number of devices or groups, they are ideal for organizations managing a small or fixed number of devices. On the other hand, devices or users present within a dynamic group will keep changing based on the requirements of the conditions set. In addition to being adept for managing a large number of devices, dynamic groups can give admins timely updates on the status of the devices they manage.

Policies that define your organization’s security requirements can be pushed onto the devices as configuration profiles. This ensures users are equipped with all the right settings the minute they start using the devices for work. Adequate settings on Wi-Fi and VPN can be set to ensure users stay safe online and are connected to a corporate network. With Hexnode, admins can also remotely bind the managed Mac devices to Active Directory with minimal manual intervention. Deploying restrictions on device settings will be useful in stopping users from changing any of the settings that has been previously configured by the admin. In order to ensure the managed Mac devices stay protected, you can lock the MDM profile to make it unremovable, this however can only be done on devices enrolled via DEP.

Restrictions

Set restrictions on:

- Device functionality
- App settings
- App store
- iCloud
- Security and Privacy settings

Network

- *Wi-Fi* - set up the Wi-Fi so users can automatically connect to it without entering any password.
- *VPN* - send data through a private network so employees working remotely can access corporate data securely.
- *AD Asset Binding* – bind the managed Mac devices to Active Directory.

Accounts

- *Email* - remotely set up email accounts on the devices.
- *Exchange ActiveSync* - sync Mail and web services such as Calendar, Contacts, Reminders and Notes hosted on an Exchange server with the managed Mac devices.
- *CardDav* - add contact account to user's device and enable them to synchronize contact data with any server supporting CardDAV.
- *CalDAV* - sync organizational calendars, reminders and notifications to the device.
- *LDAP* – sync contacts stored on an LDAP server.

Configurations

- *Dock* - personalize the screens by setting up various dock preferences to define its size and repositioning. Define the animation setting of opening applications.
- *Setup Assistant* – simplify setting up the devices for users by skipping unwanted Setup Assistant steps.
- *Screensaver* - define the screensaver settings for the managed devices.
- *AirPrint* – remotely add AirPrint printers.
- *Kernel Extensions* – load kernel extensions on user end devices and set restrictions on loading user-approved kexts.

With the help of an MDM solution, admins can whitelist kernel extensions and prevent risks that come with loading third-party extensions on the devices. Admins can make use of the kernel extension policy provided by Apple to prevent users from enabling kernel extensions on their own and define a list of whitelisted kernel extensions that can be loaded without the user's consent. The mac kernel extension policy can be applied to devices running on macOS 10.13.2 and above. In addition to whitelisting kernel extensions, admins can also add team identifiers and permit users to override kernel extensions. Allowing users to override the kernel extensions will enable them to approve additional kernel extensions not added within the policy.

Stage 4 – Manage Applications

Seamless distribution and management of applications needed by users is one of the key things that most admins look forward to while managing Mac devices. Getting the right applications deployed at the right time wouldn't be a hassle if you have an MDM on board. With Hexnode, both store apps purchased via VPP (now Apps and Books) and enterprise apps can be pushed onto the devices without any user intervention. The apps can also be set as mandatory to ensure that all users have it installed. If any of the device reports having the apps as missing, they will be marked as non-compliant thus alerting the admin of the missing applications.

In order to silently install VPP applications via Hexnode, you need to make sure that your corporate VPP account is integrated with Hexnode MDM. The custom B2B apps that organizations wish to deploy to users must first be built by a third-party developer. The developer needs to be enrolled with the Apple Developer Program. The developer submits the custom app to the App Store connect which then goes through Apple's review. The application will then have to be approved and priced. Once that's done, the developer shall assign the app to your organization's ABM account and you can access the app from the Apps and Books section of ABM. Just log in to the ABM portal, purchase the apps you need for your employees and distribute them using MDM. If required, the distributed apps can later be revoked and reassigned to different devices or users.

Enterprise applications being custom-made to meet the specific needs of the organization are not available publicly. Thus, relying on MDM ensures easy distribution and upgrade of enterprise applications. Prior to installing the enterprise application on the Mac devices, it should first be added to Hexnode's app inventory. Upload the PKG file from your system and select the category to which the app needs

to be placed. Once you have added the enterprise application within the app inventory, you can push the application to user end devices via a mandatory app policy.
To upgrade an enterprise application, you could either replace the old PKG file with the new one within the inventory and distribute it or push the new app consisting of the higher version by adding it in the inventory and distributing it directly to the devices. App catalogs can be created to deploy individual apps or app groups to targeted users or teams within the organization. The catalog acting as a customized app store provides users with quick access to the apps they need and also prevents them from unintentionally installing application not approved by their organization. Users can install the apps from the catalog found within the Hexnode MDM Agent App in their Mac devices.
Hexnode also offers the convenience for admins to configure various settings such as accounts and logins on apps with the aid of app configuration files. The files will be deployed in an XML format with keys and values to define the configured settings. The app configurations can only be applied to apps that are provisioned with configurations built in by the app developer. The blacklisting and whitelisting feature would add in extra layer of protection over the managed devices by allowing admins to permit or deny access to specific applications or app groups. This is supported on macOS 10.11+. Enterprise applications uploaded with DMG files cannot be blacklisted nor whitelisted since the app identifier cannot be fetched for DMGs. To ensure smoother deployment and management of enterprise applications its best to convert the DMG files to PKG. Signing the PKG files is vital to ensure security. By signing the file, it shows that the app is safe for use and free from malware.

Stage 5 – Secure devices

Keeping a constant watch on the devices and safeguarding the integrity of the corporate networks is no easy task, especially when hackers are always on a constant lookout to spot any vulnerabilities within the systems and networks. MDMs can help lighten this heavy responsibility on IT admins to ensure that corporate resources stay safe. In addition to defining strong passcode rules and network settings, admins can also upload certificates from the MDM portal to enable users to safely access corporate resources while using the internet. A digital certificate can help secure network connections such as VPN and Wi-Fi to ensure only specified devices and users have access to confidential enterprise data. Once the certificates are added to the portal, they can be used in other macOS functionalities that requires a certificate.

Having unrestricted access to the internet will eventually open up possibilities for users to fall victim to various cyber-attacks. Setting up web content filtering in place can ensure users stay within the confines of websites that are not known to harbor any malicious intent. Setting aside security concerns, admins may also wish to restrict access to certain websites due to bandwidth usage or other compliance regulations. Multiple URLs can be blacklisted at the same time by separating them with a comma or a semi-colon. The ‘Blacklist by Content’ option is enabled by default on Mac devices and cannot be disabled. This automatically restricts user access to explicit content. However, access to those websites can be gained by whitelisting them. This would come in handy in situations when you need to access websites that are blocked based on their content type. Whitelisting a set of websites will give users access to only the whitelisted websites, all the other sites will be blocked.

OS upgrades are crucial in securing the managed devices since they come with security updates that fixes various vulnerabilities. OS updates on Mac devices can be scheduled either as a policy or pushed to the devices as a remote action. The various OS update settings include:

- Notify only - the user is notified of the update through App Store
- Download only – the software update will be downloaded but not installed
- Download and Install – the update will be downloaded and the installation will start immediately.
- Install – installs the software update that has been downloaded previously
- Install later – downloads the software update and installs it later

MacOS updates can only be automatically pushed to devices that are enrolled via DEP.

Encryption can be better in securing the confidential data present inside. While passwords can only stop unauthorized users from accessing the managed devices, they can be easily hacked or employees may unknowingly share it online. Encryption on the other hand will change the data into an unreadable form, thus giving access to just the authorized person. FileVault, a full disc encryption program found in macOS versions 10.3 and above can prevent external parties from retrieving any sensitive information stored within the device. Admins can improve their workplace security by deploying a policy via Hexnode to ensure all the managed devices are encrypted. Once the Mac devices are encrypted, they cannot be used without the user entering the password or recovery key. Encryption can help secure data on lost or stolen devices.

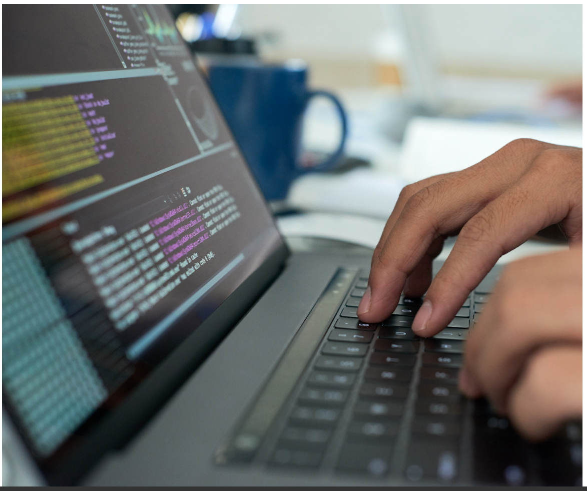
Admins can elevate enterprise security even further by configuring settings on the usage for external media, internal media, disk image and optical media. Denying media usage would prevent the transfer of sensitive information from the managed devices and hinder unauthorized users from accessing it. Configure the Firewall settings to prevent external applications and unauthorized services from accepting incoming connections. The Firewall protects the Mac devices by creating a secure barrier between the internal and external networks. It's good to enable firewall when users are connected to a public network. Admins can also enable stealth mode to prevent the devices from being discovered. It is recommended not to enable stealth mode if the devices are not frequently connected to external networks. Incoming connections to specific applications can be permitted or denied. Some users may prefer using their smart cards to login to their devices. With Hexnode MDM, preferences on the smart card authentication can be set such as - enforcing a smart card only authentication to ensure users only use their smart cards, force users to pair with a single smart card, verify the authenticity of the certificate and enable screensaver on smart card removal.

Stage 6 – Remote Management

A wide array of remote actions can be pushed onto the devices to get more granular control over their management. These include:

- **Scan device** – initiate a remote scan to fetch various device details and check whether the devices are compliant with the deployed policies.
- **Scan device location** - scan the device location to get real-time updates.
- **Lock devices** - ensure only authorized users have access to the device.
- **Assign devices to new users** – when a device is assigned to a new user, all the policies associated with the old user will be removed and policies associated with the new user will be pushed onto the devices. The device-based restrictions, however, shall still be retained.

- **Modify device attributes** – remotely modify device attributes in bulk. The attributes are used to uniquely identify each device. When applying the configurations onto the devices, the attributes can be included as wildcards to pass device-specific values.
- **Device wipe** - wipe data on lost or stolen devices to minimize the risk of a corporate data leak
- **Bypass activation lock** – activation lock prevents your Mac from being used by someone else in the event if it gets lost or stolen. Once locked, you will be required to enter your Apple ID and password to use the device again. This safety measure can prevent other external parties from resetting your Mac device. However, you may want to bypass the activation lock in case if an employee suddenly leaves the organization. You can remotely clear the activation lock from the MDM console. This is supported on Mac devices running 10.15+ with Apple T2 security chip and enrolled in ABM/ASM.
- **Disenroll and delete a device** – remotely disenroll a device that does not need to be managed anymore. Use 'Delete Device' to delete a pre-approved device from the list. Only pre-approved devices can be deleted from the device list.
- **Add user account on Mac devices** – remotely set up multiple accounts on the same device to give multiple users an individualistic login experience. Specify the account type while creating the account to ensure users do not access any data beyond the confines of the privileges assigned to them.
- **Broadcast messages** – keep staff updated on meeting schedules by broadcasting messages.
- **Power off or restart devices** - remotely power off or restart devices from the MDM console. Depending on the action you choose, the device will either power off or restart within 5 to 10 minutes once the action is executed. Supported on macOS devices running 10.13 and above.
- **Roll out OS updates** - keep your enterprise data secure by updating the Mac devices to their latest OS versions.



- **Execute custom mac scripts** – get a more enhanced experience in managing Mac devices by executing custom mac scripts. These scripts can help automate various processes to perform specific operations such as powering off and restarting devices, deploy updates, install and uninstall applications, setting app configurations and more. Supported on macOS 10.11+

Stage 7 – Manage Inventory

With Hexnode MDM, admins can generate various reports to properly monitor the corporate assets they manage. Admins can either generate the reports on the go or schedule them to receive the reports on a periodic basis. While creating a new scheduled report, you can set the report type as private or public. Setting the report type as private will require the recipient to login into the MDM portal to view the report. You can also set the download link validity for 1, 2 or 3 months. The reports can be easily exported in a PDF or CSV file format.

A broad range of reports can be generated from Hexnode MDM's portal, these include:

Device Reports

- All devices
- Disenrollment pending devices
- Enrolled devices
- Non-compliant devices
- Inactive devices
- Password protected devices
- Non-encrypted devices
- Compliant devices
- Personal devices
- Corporate devices
- Devices missing mandatory apps
- Devices with blacklisted apps
- Camera disabled devices
- Recently enrolled devices
- Policy free devices
- Active devices

User Reports:

- Users with non-encrypted devices
- All users
- Non-compliant users
- Unenrolled users
- Active Directory users
- Users with no passcode devices

- Users with inactive devices
- Users with camera disabled devices
- BYOD users
- Enrolled users
- Users with corporate devices

Compliance Reports:

- Compliant devices
- Profile-compliant devices
- Passcode-complaint devices
- Non-compliant devices
- Profile non-compliant devices
- Non-passcode compliant devices
- Inactive devices

Location Reports:

- Location history

Application Reports:

- All Applications
- Popular Applications

Audit Reports:

- Audit History
- Action History

Conclusion

Managing your Mac devices with an MDM solution that is well suited for your organization’s requirements can greatly reduce the workload on IT admins and easily provide users with access to all the resources they need. With security being a top priority for many, enterprises should always be on guard to secure the corporate networks from any unforeseen attacks. With Hexnode, organizations can ensure that their networks and corporate assets are accessed only by authorized parties. There's always that underlying risk where employees may leave their Mac devices unprotected while leaving their workstations. By deploying stringent passcode policies, admins can make sure that the devices remain protected even when employees become neglectful. Relying on an MDM solution like Hexnode that has integration with ABM and ASM not only ensures a smoother onboarding for users but it also streamlines the process of distributing and managing necessary applications.