# PLATFORM GUIDE

## for macOS management

Optimizing macOS device management with Hexnode UEM

hexnode

# Table of Contents

# Chapter 1: Overview

## Introduction to macOS

macOS (formerly OS X) is a proprietary operating system developed by Apple Inc. for their Macintosh computers. It is based on the Unix operating system and provides a graphical user interface like of Microsoft Windows. macOS comes with built-in apps and features such as the Finder, a file manager, and the Safari web browser, as well as apps for tasks like email, calendar, and photo management.

## What is the importance of managing macOS systems?

In organizations, macOS management ensures that all macOS devices are configured and used in a consistent and secure manner. This includes tasks such as deploying software and updates, enforcing security policies, and monitoring device usage. Proper macOS management can help to:

- Ensure compliance with industry regulations and internal policies.
- Protect against security threats such as malware and unauthorized access.
- Improve efficiency and productivity by ensuring all devices are running the latest software and are configured optimally.
- Facilitate remote management and support for remote workers.
- Allow IT teams to centrally manage and monitor the macOS devices.

Overall, macOS management is an essential aspect of IT operations in organizations that use macOS devices. It helps to ensure that these devices are used effectively and securely, while reducing the workload on IT teams. A Unified Endpoint Management (UEM) solution like Hexnode can make macOS management seamlessly easy.

## Prerequisites

Before proceeding with the setup, it is important to make sure that you have already configured the Apple Push Notification Service (APNs) certificate in your server. This certificate is required for communication between Apple devices and the UEM server.

# Supported versions

Hexnode UEM supports the enrollment, configuration, and management of macOS devices with macOS version 10.7 and later.

# Key features of the macOS

macOS has evolved over the years to become a powerful and stable operating system. It is a reliable, intuitive, and versatile operating system that offers a seamless user experience and integrates seamlessly with other Apple devices. It has stood the test of time and continues to be a popular choice for both personal and professional use.
The operating system of macOS is constantly evolving and supports a wide range of third-party applications, making it a versatile and powerful platform for work, entertainment, and more. The main characteristics of macOS includes:

- Sleek and intuitive user interface
- Seamless integration with other Apple services, such as iCloud, iMessage, and FaceTime
- Efficient multitasking with features like Mission Control and Split View
- Robust security features, including built-in encryption and a firewall
- Continuity, allowing users to seamlessly switch between their Apple devices
- Built-in accessibility features, such as VoiceOver and dictation
- Siri, the built-in digital assistant for voice commands
- A wide range of pre-installed applications, including Safari, Mail, and Photos
- Customizable settings and preferences to suit individual user needs
- Regular updates and improvements to the operating system and applications
- Integration with Apple hardware, such as AirPods and the Touch Bar on MacBook Pro models
- Support for third-party applications through the Mac App Store
- Integration with cloud services, such as Dropbox and Google Drive
- Compatibility with a wide range of hardware and devices, including printers and cameras.

# Chapter 2: macOS enrollment

macOS enrollment refers to the process of setting up and configuring macOS devices within an organization or enterprise. Enrolling devices allows IT administrators to manage and secure them. But first, you need to configure an APNs certificate.

## Generate an APNs certificate for Hexnode UEM

APNs (Apple Push Notification Service) certificate configuration is a process of creating and installing a certificate on an MDM server that allows an organization to securely communicate with its enrolled macOS devices. The certificate is used to establish a secure and encrypted connection between the organization's servers and the devices, allowing the organization to push notifications, such as software updates and other management commands, to the devices.
The APNs certificate is usually valid for one year and need to be renewed annually. This certificate is essential for organizations using macOS and iOS devices for their operations and it is important to understand the process of APNs certificate configuration and management to ensure secure and efficient device management.

The process of APNs certificate configuration typically involves the following steps:

- Creating an **APNs certificate signing request** (CSR) on the organization's server.
- Submitting the CSR to the **Apple Push Certificates Portal** and generating an APNs certificate.
- Downloading and installing the APNs certificate on the organization's server.
- Configuring the organization's UEM solution to use the APNs certificate.

## Sync users, groups, and data from Identity Providers (IdPs)

Syncing users, groups, and data from Identity Providers (IdPs) involves integrating an organization's identity management system with external sources. This enables the transfer of user and group information, simplifies administration, and improves security and user experience.

# 1. Microsoft Directory Services

Microsoft Active Directory (AD) is a directory service that provides centralized authentication and authorization services for Windows-based computers. It manages users and computers, including their authentication, permissions, and access to resources such as files, printers, and applications. It also provides a hierarchical structure for organizing objects in the network.

Azure Active Directory (Azure AD) is a cloud-based identity and access management service provided by Microsoft. It provides a range of identity-related services, including user authentication, single sign-on (SSO), and access control for cloud-based applications and services. It's designed to work with both cloud-based and on-premises applications and services, allowing users to sign in once with their Azure AD credentials and access multiple resources across different environments.

Now, as for the integration of directory services (Microsoft AD and Azure AD) with Hexnode UEM, it allows organizations to manage and secure their mobile devices using the same identity and access management system they use for their Windows-based computers and cloud-based applications. This integration provides several benefits, including:

- **Simplified User Management:** With directory integration, administrators can manage user accounts and device access from a single location, reducing the need for multiple usernames and passwords.
- **Centralized Authentication:** Users can use their existing directory credentials to sign into their mobile devices, making the authentication process simpler and more secure.
- **Enhanced Security:** Integrating directory services with Hexnode MDM allows for advanced security features, such as multi-factor authentication, device enrollment restrictions, and device compliance policies.
- **Streamlined Device Enrollment:** The integration allows for automated device enrollment, making it easier for users to set up and use their mobile devices for work purposes.

# 2. Google Workspace

Google Workspace, formerly known as G Suite, is a suite of cloud-based productivity and collaboration tools offered by Google. It includes applications such as Gmail, Google Drive, Google Docs, Google Sheets, and Google Slides.

These applications allow users to communicate, create, store, and share content online. The integration between Google Workspace and Hexnode allows organizations to manage their Google Workspace accounts and devices from a single platform.

This integration enables administrators to:

- **Sync users and groups:** The integration allows administrators to sync their Google Workspace users and groups to Hexnode. This helps in managing access to applications and data on the devices.
- **Deploy apps:** The integration allows administrators to deploy Google Workspace apps such as Gmail, Google Drive, and Google Docs to the devices. This helps in improving productivity and collaboration among the users.
- **Configure policies:** The integration allows administrators to configure policies for Google Workspace apps. For example, administrators can set policies to restrict access to certain features or to enforce data encryption.
- **Track usage:** The integration allows administrators to track the usage of Google Workspace apps on the devices. This helps in identifying any issues or concerns related to productivity, security, or compliance.

***Prerequisite***

- *Your organization should have a Google Workspace Account.*

## 3. Okta

Okta is a cloud-based identity and access management solution that helps organizations manage user identities and access to applications and data. It includes features such as single sign-on (SSO), multi-factor authentication (MFA), and user provisioning. The integration between Okta and Hexnode allows organizations to manage user identities and mobile devices from a single platform.

This integration enables administrators to perform the following tasks:

- **Single sign-on (SSO):** This enables users to access their mobile devices with a single set of credentials, reducing the need for multiple passwords.
- **User provisioning:** The integration allows administrators to automate user provisioning for mobile devices using Okta. This helps in managing access to applications and data on the devices more efficiently.
- **Multi-factor authentication (MFA):** This adds an additional layer of security to the devices, reducing the risk of unauthorized access.
- **Group management:** The integration allows administrators to manage user groups in Okta and assign them to device profiles in Hexnode. This helps in managing access to applications and data on the devices more effectively.

# How to enroll a macOS device in Hexnode UEM

Once the APNs certificate is configured, the macOS devices can be enrolled to the UEM console. There are several methods for enrolling macOS devices, including:

## Open Enrollment

Users will be able to register their device in the Hexnode UEM console without entering any enrollment information.

## Authenticated Enrollment

- **Email/SMS enrollment:** Users can register their devices using the enrollment credentials that were emailed or sent to them via text. The email provides the username and password required for enrollment.

- **Self Enrollment:** Users can self-enroll devices using their Active Directory/Azure AD/Google/Okta user credentials. For other users, the admin can either manually establish a default user with a dedicated password or give a common password. Hexnode also allows users to set individual passwords, which are then sent to them by bulk email. The admin will simply need to supply the users with the enrollment URL.

## Automated Device Enrollment (ADE)

Automated Device Enrollment (ADE) is a program offered by Apple to simplify the enrollment process for iOS, iPadOS, tvOS and macOS devices in businesses. With ADE, IT administrators can automatically configure and enroll devices in a mobile device management (MDM) solution without requiring users to manually enter their credentials or settings. Steps to enroll devices to the Hexnode server using Apple ADE:

**Step 1:** Enroll your organization in ABM/ASM.

- Go to ABM/ASM website and click "**Enroll now**".
- Enter your org's info. Apple will verify it via your rep and email you the approval.
- Sign in and add sales info.
- Get **Apple Customer Number** if you bought from Apple, or Org ID and Reseller ID if from a reseller.

**Step 2:** To add devices to Apple Business Manager, obtain the Apple Customer Number or Reseller ID from the supplier, then log in to the ABM account to add the number/ID.
**Step 3:** Configure the **DEP profile** by logging in to the Hexnode portal, downloading the certificate file, and adding the MDM server.
**Step 4:** Create a DEP account in Hexnode by obtaining the **MDM DEP certificate** and uploading the **public key**. Assign devices to the MDM by selecting the desired devices in the "**Devices**" section of the ABM account, then choose "**Assign to the following MDM**" and select an MDM server.
**Step 5:** Finally, sync devices to Hexnode by clicking "**Sync all DEP accounts**" and viewing the synced devices in the DEP Devices section.

***Prerequisite***

- *Hexnode allows ADE enrollment of macOS devices with OS X 10.9 or later.*

## ADE using Apple Configurator for iPhone

Before WWDC21, only macOS devices bought from Apple or their trusted resellers were eligible for ADE. Others couldn't enroll. But now, with Apple Configurator on an iPhone, any macOS device can be added to ABM, regardless of where it was bought. The steps for ADE using apple configurator are:

**Step 1:** Install Apple Configurator on iPhone and sign in using your managed Apple ID.
**Step 2:** Grant access to camera and configure a Wi-fi profile for your macOS (or you can also choose to share the network the iPhone is connected with by selecting Share network).
**Step 3:** Erase all content and settings using the System Preferences menu if the device is not new. (Skip this step if the device is new)
**Step 4:** Launch the Apple Configurator app on your iPhone and scan the image to assign the device.
**Step 5:** Verify that the device is added to DEP in ABM.

To assign a macOS device to the Hexnode UEM Server,

**Step 1:** Navigate to Devices in ABM and select Manually Added > Apple Configurator to find the device.
**Step 2:** Edit the MDM server to assign the devices.
**Step 3:** Select the required device and click Edit MDM server.
**Step 4:** Then, choose the MDM server to assign the devices.
**Step 5:** Check the devices are listed under DEP Devices in the Hexnode UEM portal.
**Step 6:** Navigate to **Enroll > All Enrollments > No-Touch > Apple Business/School Manager**.
**Step 7:** If the devices are not listed, click Sync with DEP to sync with ABM or ASM.

***ADE prerequisites***

- *Ensure that you are already registered in Apple Business Manager (ABM)/Apple School Manager (ASM).*
- *Make sure that Automated Device Enrollment is set up with Hexnode UEM.*
- *You must be an administrator in ABM with the Device Enrollment Manager Role.*
- *macOS 12 Monterey.*
- *iPhones running iOS 15 or later.*
- *Apple M1 Silicon or T2 Security chip.*

# macOS Onboarder

Hexnode Onboarder for Mac remotely migrates macOS computers to Hexnode UEM without wiping them. Hexnode Onboarder offers four enrollment methods, which include using an enrollment URL, a QR code, a token or Apple Configurator, to easily enroll macOS into Hexnode MDM and configure device settings, install apps, and deploy configurations. IT administrators can use Hexnode Onboarder to perform the following tasks:

- **Enroll macOS into Hexnode MDM:** With Hexnode Onboarder, IT admins can enroll macOS into Hexnode MDM with ease.
- **Configure device settings:** IT admins can use Hexnode Onboarder to configure device settings such as Wi-Fi, email, VPN, and more.
- **Install apps:** With Hexnode Onboarder, IT admins can install apps on the enrolled macOS automatically.
- **Deploy configurations:** IT admins can deploy configurations such as policies, profiles, and restrictions to the enrolled macOS.

Once enrolled, the organization or IT administrator can remotely manage the devices, including configuring settings, deploying apps and software updates, tracking inventory and usage, and providing support.

# Chapter 3: macOS device management

## Prevent MDM Removal

Administrators will be unable to control the device if a user manually removes the MDM profile. Users may delete MDM profiles by going to System Preferences > Profiles and tapping the'-'button, which will remove the chosen profile. You may prohibit end-users from removing the MDM profile on macOS devices by configuring the same in ABM/ASM. When this policy applied on the device, the '-' button to remove the profile is disabled, and thus the user is prevented from uninstalling the MDM profile. This is done by:

**Step 1:** Navigate to **Admin** > **Apple Business/School Manager** > **Apple ADE** on your Hexnode UEM portal.
**Step 2:** Select **ADE Configuration Profiles** > **Configure ADE Profile** from the drop-down menu.
**Step 3:** Disable the checkbox '**Allow MDM Profile Removal**'.
**Step 4:** Click the **Save** button.

**Note:**

- *Only macOS devices registered in Hexnode via Apple ADE can be stopped from removing MDM profiles.*

## Setting up a password policy for macOS

The macOS device password prevents unauthorised access to corporate resources and applications.  Using Hexnode UEM, you may remotely create an enterprise-grade password requirement for macOS devices. If the devices fail to fulfil the password criteria or if no password is setup on the devices, they will be categorised as non-compliant. To set-up a password policy:

**Step 1:** Log in to Hexnode MDM portal and go to **Policies** to create or edit an existing policy.
**Step 2:** Navigate to **macOS** > **Passcode** > **Configure** for passcode restrictions
**Step 3:** Go to **Policy Targets** within **Policies** tab
**Step 4:** Select devices and associate the policy with them.

All users on the targeted macOS will be subject to the password policy. If a user's current password does not comply with the settings, the user will be requested to change their password the next time they log in. If the user is already signed in, they will be unable to change any locked System Preferences settings until the password is changed. The user will also be prevented from storing a new password unless the entered password meets your requirements. When the compliance period expires, they must change the password again.

# Enabling Activation Lock in macOS

Activation Lock is a security feature on Apple devices that prevents people from deleting and reactivating Apple devices without the permission of the owner. IT administrators may use Hexnode to not only enable activation, but also to View Activation Lock Status, Clear Activation Lock, and Bypass Activation Lock.

| Sl.no | Settings | Description |
|---|---|---|
| 1. | Enable Activation Lock | • Go to **Policies** > **macOS** > **Advanced Restrictions**. Then allow the **Security** and **Privacy Settings**.<br>• Check the '**Activation Lock**' box to enable the functionality. To activate the function on the device, first disable and then reactivate **Find My Mac**. |
| 2. | View Activation Lock Status | • Navigate to the **Manage** tab and pick the desired device. You'll be taken to the **Device summary** page.<br>• Check the **Device Info** subtab and the "**Activation Lock**" section. |
| 3. | Clear Activation Lock | • Select your device from the **Devices** list on the **Manage** tab.<br>• Select **Clear Activation Lock** from the dropdown menu and complete the action by clicking on **Actions**. |
| 4. | Bypass Activation Lock | • Select your device from the Devices list and go to the Manage tab. You'll be sent to the **Device Summary** page.<br>• To access the section Activation Lock, navigate to the **Device Info** tab.<br>• By clicking on the eye symbol, you may discover the **Activation Lock Bypass Code**. |

**Note:**

- The methods described here are only applicable to devices already managed by Hexnode UEM.
- Requires macOS devices running 10.15+ with an Apple T2 security chip or enrolled in ABM/ASM.
- The Activation Lock Bypass Code is only valid on DEP-enabled devices.

## Configuring macOS restrictions

An administrator can impose a variety of basic and complex limitations on the macOS device, including app, security, privacy, and a variety of other settings. A good restriction policy protects company data and resources against device abuse and other security concerns. The device limits that can be specified are determined by your licence plan and macOS version. Using Hexnode, IT admins can enforce basic and advanced restrictions on:

- App Settings
- App Store
- Security settings
- iCloud services
- Device Functionality and Personalization Settings
- Security and Privacy Settings

The steps to configure restrictions on the macOS are as follows:

**Step 1:** Go to the Hexnode portal to create a new policy.
**Step 2:** To configure the settings, go to **Restrictions/Advanced Restrictions** under macOS and click on **Configure**.
**Step 3:** Configure both **Basic** and **Advanced Mac Restrictions** as needed.
**Step 4:** Associate the policy to the devices by navigating to **Policy Targets** and selecting the device/devices concerned.

## Setting up a Wi-Fi Policy

Configure minimal Wi-Fi security settings that must be met before a managed device may join to the network using UEM. This, in turn, minimises the likelihood of vulnerabilities occurring when devices connect to less secure Wi-Fi networks. Using the UEM interface to create macOS Wi-Fi setups allows devices to connect to the defined network automatically. With the use of rules, Hexnode assists administrators in configuring networks across many devices.

The following Wi-Fi settings can be configured using Hexnode:

| Sl.no | Settings | Description |
|---|---|---|
| 1. | Service Set Identifier | The name of a Wi-Fi network abbreviated as SSID. |
| 2. | Auto join | When the devices come into contact with the Wi-Fi network, they will immediately join to the network established here. By default, this option is enabled.<br>**Note:**<br>• This option might not be visible on devices running macOS v10.12.6. |
| 3. | Hidden Network | If your Wi-Fi network is hidden, enable this setting. Because a hidden network does not broadcast its SSID, it will not be included in the list of accessible wireless networks. |
| 4. | Security Type | The security type determines the authentication security protocol. Choose a security type and then customise the remaining parameters. None, WEP, WPA/WPA2, any (Personal), WEP Enterprise, WPA/WPA2 Enterprise, and Any (Enterprise) are the possible security types. |

You may set up several Wi-Fi networks and customise extra security settings for your organisation.

## Setting up a VPN on macOS devices

A Virtual Private Network enables users to connect to the organisational network from a remote location, ensuring safe access to company resources. Furthermore, the VPN may be set to redirect all traffic through the selected network. The IT administrator may setup VPN server settings on macOS devices using a policy in Hexnode UEM, which, when coupled with target entities, produces VPN configurations in the devices and new network connections.

Hexnode lets IT admins configure the following connection types:

- L2TP (default)
- PPTP
- IPsec (Cisco)
- Cisco AnyConnect
- Juniper SSL
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- Check Point Mobile VPN and
- Open VPN.

Once you've setup the necessary network security settings, you must guarantee that they are not tampered with. Through Hexnode, you can prevent your users from adding, altering, or resetting network settings. It also allows you to setup the proxy server settings. By serving as an intermediate between the device and the internet, a proxy server protects a macOS against malicious external files and websites. All communication between the device and the internet is routed through the proxy server, allowing dangerous websites to be blocked. None, Manual, and Automatic are the possible options. To setup the VPN settings:

**Step 1:** Go to the Hexnode portal to create a new policy.
**Step 2:** To configure the settings, go to **VPN** under **Network** in macOS and click on **Configure**.
**Step 3:** Configure the **connection name, type, server, account** as well as the **proxy server settings**.
**Step 4**: Associate the policy to the devices by navigating to **Policy Targets** and selecting the device/devices concerned.

# AD Asset Binding on macOS

Active Directory (AD) Asset Binding is a feature that allows an organization to associate a device with Active Directory user accounts, using a UEM solution. This is typically done by binding the device's unique hardware identifier (such as the MAC address) to a specific user account in AD. By binding the device to a specific user in AD, the organization can ensure that only authorized users have access to the device and its resources. The steps to configure macOS AD Asset Binding are as follows:

**Step 1:** Go to the Hexnode portal to create a new policy.
**Step 2:** To configure the settings, go to **AD Asset Binding** under **Network** in macOS and click on **Configure**.

**Step 3:** Configure both **Basic** (like domain, username, password and organization unit) and **Advanced** settings.
**Step 4:** Associate the policy to the devices by navigating to **Policy Targets** and selecting the device/devices concerned.

The **Disk Utility tool** creates a trusted binding between the macOS device and the organization's Active Directory server after the policy is linked with it.

## Remote management and troubleshooting

Hexnode's Unified Endpoint Management (UEM) solution provides your organisation with a set of Remote management functions to improve IT management. It allows you to administer tasks and manage endpoints from a single console. Hexnode's  remote management techniques give visibility into the health and state of your corporate devices, as well as reporting on the users' networks and systems. For example, Hexnode UEM's Remote View feature is a monitoring tool that allows administrators to remotely access to an endpoint's display in real time.

## Dynamic grouping of macOS devices

Dynamic device groups are an essential feature of macOS management that allows you to group devices based on various parameters. You can use dynamic device groups to automate the process of device grouping and apply policies to these groups, simplifying device management for administrators. To create a dynamic device group in your Hexnode MDM portal for macOS management, follow these steps:

**Step 1:** Log in to your Hexnode MDM portal and go to **Manage > Device Groups > New Dynamic Group**.
**Step 2:** Add a **Group Name** and **Description** for your new dynamic group.
**Step 3:** Configure the required criteria to create the group by selecting the available filters. The filters include Geofences/Location filters and Condition filters.
**Step 4:** To use Geofences/Location filters, select one or more locations (fences) already created under **Admin** > **Geofencing**. You can also create new geofences instantly by clicking on the **+Create New Geofences** button. The **Include filter** allows you to enforce policies or restrictions on devices present in the specified regions. The **Exclude filter** enables you to apply policies to a group of devices, excluding those located in the selected locations.

**Step 5:** To use **Condition filters**, specify the criteria required for grouping devices. You can add multiple conditions to filter out the required devices. Any devices satisfying the defined criteria will be automatically added to the corresponding dynamic device group.
**Step 6:** Add **Exceptions** to exclude the devices satisfying these conditions from the device group.
**Step 7:** Click on the **Preview** button to view the list of devices that match the criteria.
**Step 8:** Once you have confirmed that the criteria are correct, click **Save** group to save the group details. Your policies will now be automatically applied to all devices in the dynamic group that meet the criteria you specified.

Dynamic device groups are an excellent tool for macOS management that saves time and simplifies device management for administrators. By automating the process of device grouping and policy application, you can focus on more important tasks and ensure that all devices are up-to-date and secure.

## Configuring a geofencing setup

Geofencing is a powerful location-based service that can streamline the functioning of corporate endpoints based on the current location of devices. With geofencing, you can automatically group devices and apply configurations, as well as restrict corporate resources to devices based on their location. Some of the main benefits of using geofencing in device management includes:

- **Automatic device grouping:** Geofencing can automatically group devices based on their location. This means that you can create specific policies and apply them to devices in a particular area without the need for manual intervention.
- **Location-based restrictions:** You can use geofencing to restrict access to corporate resources based on the location of the device. For example, you can prevent devices from accessing sensitive information when they are outside of the office premises.
- **Increased security:** By using geofencing to restrict access to corporate resources, you can increase the overall security of your mobile device management strategy. This can help prevent data breaches and other security incidents.
- **Improved productivity:** Geofencing can also be used to improve productivity by allowing you to create policies that are specific to a particular location. For example, you can allow employees to access specific apps or resources when they are in the office but restrict access when they are outside of the office.

Overall, geofencing is a valuable tool for mobile device management. By using geofencing, you can ensure that your corporate endpoints are always secure and functioning optimally, no matter where they are located.

# Tracking location of managed macOS

Location tracking is an essential feature of mobile device management that enables organizations to monitor and track the location of their managed devices. With Hexnode, you can easily configure location tracking policies for macOS devices. These policies enable the periodic collection of location details from devices, eliminating the need for manual intervention. Additionally, Hexnode allows you to track the location of devices instantly whenever you need it. This feature can come in handy in a variety of situations, such as when you need to locate a lost or stolen device, or when you need to track the location of a remote employee for safety or compliance reasons.
Before setting up location tracking with Hexnode MDM, there are a few prerequisites that must be met. They are as follows:

- Hexnode UEM must be installed on the managed devices.
- The devices must always have an internet connection.
- Location Services must be enabled on the devices.
- For macOS devices, the Hexnode UEM app should be installed with Location permission granted.

Hexnode UEM offers many features under the location tracking domain. This includes:

- **Periodic Location Tracking:** With Hexnode, you can periodically collect the location details of macOS devices. This policy remedies the issue of manually collecting the location details of individual devices at periodic intervals of time.
- **Enabling Location Services on Devices:** During the initial setup of the Hexnode UEM app, users will be prompted to enable location permissions. However, if the user forgets to grant the necessary permissions during this process, they will need to enable the permissions manually. The following steps outline the process for enabling location services on macOS devices:

  **Step 1:** Open **System Preferences** on your macOS.
  **Step 2:** Click on **Security** and **Privacy**.
  **Step 3:** Select the **Privacy** tab.
  **Step 4:** If the padlock icon is locked, click on it and enter your admin username and password to unlock it.
  **Step 5:** Check the box next to **Enable Location Services.**
  **Step 6:** From the list of applications, select the Hexnode UEM app.

- **Instantaneous Location Tracking:** Hexnode enables you to instantaneously track down the location of your macOS devices every time you need it. Location is tracked when the Hexnode UEM app is running in the background. However, when there is a significant change in location (500 meters or above), the app wakes up on its own, and the location is tracked even if the app is not running in the background.

**View Device Location:** You can view the location details of your macOS devices on the Hexnode UEM console. The device location details include latitude, longitude, and the last location update time.

**Disable Location Tracking:** You can disable location tracking for your macOS devices from the Hexnode MDM console. Once disabled, the location tracking policy will not be applied to the device, and the device location will not be tracked.

## Remote view and remote control

Hexnode UEM provides Remote View and Remote-Control features that allow administrators to monitor and connect to endpoint displays in real-time. By initiating a remote view session, you can diagnose and detect device issues in real-time. With the Remote-Control feature, administrators can access and control remote devices, enabling them to troubleshoot and fix errors on the device in real-time. It is important to note that Remote View for macOS is available on Ultimate and Ultra subscription plans, while Remote Control is only supported on the Ultra subscription plan of Hexnode UEM. In addition, certain system requirements must be met, that includes:

- macOS 10.12 or higher
- Hexnode UEM app v7.0.0 or higher and
- Hexnode Remote Assist app v4.1.0 or higher.

For the Hexnode Remote Assist app to use the Remote View and Remote-Control functions, users must allow Screen Recording permission and Accessibility permission on macOS 10.15 or higher. Administrator roles under **System Preferences > Security & Privacy > Screen Recording** can manually provide access to Remote View. Similarly, **System Preferences > Security & Privacy > Accessibility** in System Preferences allows the admin to directly grant permission for Remote Control.

## Remote actions for macOS devices

They are Instantaneous commands which is used to manage devices remotely from the Hexnode UEM portal. Administrators can perform remote management operations on devices, users, groups, and domains within the organization. The organizations can choose to execute actions individually or in bulk on selected devices based on their needs.

The following list shows some of the remote actions supported by Hexnode for macOS devices:

| Sl.no | Settings | Description |
|---|---|---|
| 1. | Scan Device | Basic information about the registered devices is retrieved via the Scan Device activity. Based on each action executed, the site updates data such as battery level, list of installed apps, device details, etc. |
| 2. | Scan Device Location | The purpose of this activity is to retrieve the device's current position. Admins can perform this function only if a location tracking policy is linked to the device. This feature is supported by macOS 10.11+ or later. |
| 3. | Lock Device | With the use of this function, administrators can lock devices so that only those who know the device password can unlock them. |
| 4. | Broadcast Message | Admins have the ability to message the device. On the device, this message appears as a pop-up or notification. |
| 5. | Power Off Device | The administrator can remotely shut down devices by taking this step. This feature is supported by macOS 10.13+ or later. |
| 6. | Restart Device | The administrator can remotely restart the devices by taking this step. This feature is supported by macOS 10.13+ or later. |
| 7. | Export Device Details | Using this feature, you can export information such hardware information, enrollment information, device information, network information, etc. as a pdf file. |

Apart from these features, there are many more offered by Hexnode UEM for macOS devices. To know more about the other features under this domain, click here.

## Executing custom scripts on macOS

Hexnode UEM empowers IT administrators to remotely execute custom scripts on macOS devices. This feature enables admins to perform system-level configurations on macOS devices without requiring any user interaction. With this feature, admins can carry out a range of actions, including shutting down/restarting devices, installing/uninstalling apps, pushing updates, setting up app configurations, and more. This capability takes macOS management to the next level by allowing administrators to configure additional settings that may not be natively available in UEM's feature stack.

Before using the custom script feature on macOS, make sure that your devices meet the following requirements:

- They run on macOS 10.11 or later.
- The script file is in one of the supported formats, such as Perl (.pl), Bash (.sh), or Python (.py).
- The latest version of the Hexnode MDM app is installed on each device.
- The required binary for the script is installed on each macOS.

Note that this feature is only available on the Ultimate and Ultra subscription plans. Also, be aware that before running a script on multiple devices, it's important to validate the script manually on a macOS to avoid unexpected issues.

## Local User Management on a macOS device

Hexnode allows for seamless management of all user accounts on a macOS device. This includes creating new accounts, changing passwords, granting secure tokens, disabling users, and tracking local account information such as the last login session. It is important to note that the device must have the latest version of the Hexnode Agent app installed to utilize these features. To create a new local user account on a macOS device using Hexnode, follow the steps below:

**Step 1:** Log in to your Hexnode portal.
**Step 2:** Navigate to **Manage** > **Devices**.
**Step 3:** Select the macOS device to which you want to add a new user.
**Step 4:** Click the **Local Accounts** tab.
**Step 5:** Click the **Add User** icon.
**Step 6:** A dialog box will be opened. Configure the following settings for the new user account:

- Account Name
- Password
- Password Hint
- Account Type
- Secure Token
- Aliases

**Step 7:** Hide account from Login Window and Users & Groups
**Step 8:** Once you have configured the settings, click on the **Create** button to create the new user account on the macOS device.

The following features can be also performed by the admins using Hexnode UEM:

- Sync Local Accounts
- Grant Secure Token
- Force Log Out User
- Unlock User Account
- Change User Role
- Change Password
- Disable User
- Enable User and
- Delete User

With Hexnode UEM, it is effortless to retrieve a comprehensive report that displays all the user accounts on various macOS devices enrolled in the system. This report provides valuable information about each local user account, including session type, sync date, login and logout time, session duration, and more. To access this report, simply go to **Reports > Device Reports > Local Accounts (macOS).**

## Monitoring compliance metrics

Hexnode UEM allows administrators to enforce a list of rules and settings to ensure that devices comply with the organization's security and regulatory requirements. The compliance status of a device reflects whether it adheres to the enforced policies.

Hexnode UEM will flag a device as non-compliant if it fails any of the selected compliance checks. The Device compliance pane and non-compliant widgets on the dashboard display key metrics related to device compliance. The Compliant devices report enables administrators to document compliance for audits accurately. Dynamic grouping can also be used to automatically group non-compliant devices separately for quick remedial actions.

# Chapter 4: macOS device configurations

Hexnode UEM helps in configuring many features of macOS from a single console, making the work of IT admins much simpler. Creating setup assistants, deploying custom configurations, dock and wallpaper preferences all come under this shade. Details about each feature are stated below:

## Deploying custom configurations on macOS devices

With the Custom Configuration capability of Hexnode UEM, IT admins can distribute several configurations to a fleet of devices. It is easier for administrators to create profiles using various tools to customize enterprise settings for macOS devices. IT admins can then deploy profiles directly from the Hexnode console.

These custom configuration profiles can be created using Apple Configurator, profile editor apps, or similar tools. In addition, Hexnode UEM offers support for non-encrypted .mobileconfig, .xml, and .plist files for deploying custom configurations to the devices.

When you apply a custom configuration profile on a device using Hexnode, the Action History page will show a "Success" status even if the device is running on a different operating system. But keep in mind that only the devices running the corresponding operating system will be affected by the custom configuration profile.

To deploy custom configurations, follow the steps:

**Step 1:** Create a device policy for macOS by navigating to the “**Policies**” tab.
**Step 2:** Choose an existing policy or create one by clicking on **New Policy** and name it.
**Step 3:** Select the “**macOS**” tab and configure the custom configuration feature under configurations from the left panel.
**Step 4:** Select configuration profiles directly from the device or from those previously added to the portal.
**Step 5:** Navigate to the “**Policy Targets**” tab, add devices or users' groups as required, and save it.

# Setting a Wallpaper on managed macOS devices

Using this feature, the organization can set up desktop wallpaper on all their enterprise devices to promote corporate branding on managed devices. IT admins can configure the company's logo or any other image to appear on a fleet of devices. With this customization, admins can also decide whether wallpaper should be applied to each user on the device and how often it should be changed.
Devices connected to Hexnode running macOS 10.11 or later can use this capability. JPG, JPEG, and PNG are the supported file formats for the image files. To use this feature, follow the steps:

**Step 1:** Log in to the Hexnode console.
**Step 2:** Navigate to **Policies > New Policy.**
**Step 3:** Provide a policy name and description.
**Step 4:** Next, go to **macOS > Configurations > Wallpaper** and click **Configure**.
**Step 5:** Select **Add Folders/Files** to add folders or image files on the target devices. Admins can also add Images to choose among images submitted to the portal.
**Step 6:** Configure the features like image position, apply wallpaper to all users, change the picture and choose wallpaper randomly.
**Step 7:** Click **Configure** to save the policy.

***Note:***

- *The option of Image position is available only on macOS 10.13+ devices.*

# Customizing the macOS dock

The dock is a convenient feature on macOS devices that allows easy access to apps, files, and folders. By default, the dock is located at the bottom of the screen and includes apps such as Launchpad and Siri on the left side and downloads, files, and minimized folders on the right side.

With Hexnode, you can easily customize the dock to suit your needs and preferences using the macOS dock preferences feature. This allows you to change the appearance of the dock and the way applications are displayed, adjust the dock's size, position, and visibility, and add animation when opening applications. To utilize this feature, follow the steps mentioned below:

**Step 1:** Create a device policy for macOS by navigating to the “**Policies**” tab.
**Step 2:** Choose an existing policy or create one by clicking on **New Policy** and name it.
**Step 3:** Go to **macOS > Configurations > Dock** and click on **Configure**.
**Step 4:** Set up the features as required.
**Step 5:** Navigate to the “**Policy Targets**” tab, add device or user groups as required, and save it.

# Configuring Setup Assistant for macOS

When a user first logs in to a macOS device, the Setup Assistant guides them through initial setup procedures such as configuring Apple ID and iCloud, enabling Siri, and more. Hexnode UEM allows admins to customize this experience by skipping unnecessary setup options and simplifying the process for both users and IT admins. With the Setup Assistant configuration feature, the admins can streamline device setup for new user accounts and simplify remote management for your organization. This feature can be enabled by following the steps mentioned below:

**Step 1:** First, create a device policy for macOS by navigating to the "**Policies**" tab.
**Step 2:** Choose an existing policy or create one by clicking on **New Policy** and name it.
**Step 3:** Go to **macOS** > **Configurations** > **Setup assistant** and click **Configure**.
**Step 4:** Configure the following features as per requirement:

| Sl.no | Setup Assistant Settings | Description |
|---|---|---|
| 1. | Skip Privacy setup (Supported on macOS 10.13.4+) | Allows to skip the Data and Privacy setup window during the initial setup process. |
| 2. | Skip Signing in with Apple ID (Supported on macOS 10.12+) | Allows to skip the Apple ID sign-in setup window. |
| 3. | Skip iCloud Storage setup (Supported on macOS 10.13.4+) | Allows to skip the iCloud Storage setup window. |
| 4. | Skip Siri setup (Supported on macOS 10.12+) | Allows to skip the setup option to enable Siri. |
| 5. | Skip Choose Your Look setup (Supported on macOS 10.14+) | Allows to skip the setup window option allowing the user to choose the appearance of the macOS. |

**Step 5:** Navigate to the "**Policy Targets**" tab, add devices or users' groups as required, and save it.

# Configuring screensaver for macOS devices

Screensavers provide a visually pleasing display or a security measure by requiring a password to access the device when it has been inactive for a certain period. In addition, Hexnode allows IT administrators to remotely configure screensaver settings for macOS devices, providing an added layer of security and customization for end-users. To enable this feature, follow the steps below:

**Step 1:** First, create a device policy for macOS by navigating to the "**Policies**" tab.
**Step 2:** Choose an existing policy or create one by clicking on **New Policy** and name it.
**Step 3:** Go to **macOS** > **Configurations** > **Screensaver** and click **Configure**.
**Step 4:** Configure the following features as per requirement:

| Sl.no | Screensaver Settings | Description |
|---|---|---|
| 1. | Enable Screensaver | Allows the activation of the screensaver on the macOS device. |
| 2. | Login window screensaver idle time | Allows setting the duration of inactivity at the login window before the screensaver activates. The options range from 5 seconds to 5 minutes, with a default value of 30 seconds. |
| 3. | Screensaver idle time | Allows setting the duration of inactivity before the screensaver becomes active. The options range from 1 minute to 1 hour, with a default value of 1 minute. |
| 4. | Require password to unlock the screen (Available on macOS 10.13+) | Enabling this option prompts the user to enter a password for the device to wake from screensaver/sleep mode. This option is enabled by default. |
| 5. | Set delay for password prompt (Available on macOS 10.13+) | Allows choosing the time of inactivity before the password prompt appears to unlock the screen. The options range from 5 seconds to 5 minutes, with a default value of 30 seconds. |

These settings can be configured only when the enable screensaver option is checked.
**Step 5:** Navigate to the "**Policy Targets**" tab, add devices or users' groups as required, and save it.

When the Auto-Lock feature is enabled in a policy, the device's screensaver will be activated without the need for it to be set up separately through the Hexnode portal. If both the screensaver and Auto-Lock are configured, the setting with the shorter time limit will take precedence on the device.

With Hexnode, IT administrators can set and enforce screensaver policies on target devices, ensuring that users cannot alter the screensaver timer settings. This allows for a uniform user experience, as all devices have the same screen saver settings specified in the policy.

## Setting up AirPrint on macOS

With Hexnode UEM, IT admins can easily set up AirPrint on macOS devices for seamless printing experiences. In addition, the AirPrint policy allows for pre-configuration of settings, enabling macOS devices to connect to known AirPrint printers on the same network without the need for additional drivers or software. This streamlines the process and eliminates the need for manual setup on each device, making printing from macOS devices a breeze. This feature is supported on macOS v10.10 and later devices.

To create the AirPlay policy, follow the steps below:

**Step 1:** Log in to the Hexnode MDM portal.
**Step 2:** Navigate to **Policies** > **New Policy** and assign a name and description for the policy or choose an existing policy.
**Step 3:** Under **macOS** > **Configurations**, select **AirPrint** and click **Configure**.
**Step 4:** Click on **+Add AirPrint** device.
**Step 5:** Enter the AirPrint printer information, including the IP address and Resource Path.
**Step 6:** Click **Add**.

Once the AirPrint policy is applied, the specified printers will be automatically added to the "Printers & Scanners" section of the System Preferences on the managed devices and labeled as "AirPrint Profile".

## System extensions for macOS

The Hexnode System Extension policy enables IT admins to manage and control the system extensions on macOS devices. By applying this policy, admins can ensure that the necessary extensions are loaded and activated on the end-user devices while also having the ability to deactivate extensions that were previously enabled through the policy. This allows for more streamlined and efficient management of the native capabilities of the operating system.

To configure macOS system extension settings, follow these steps:

**Step 1:** Access the **Policies** tab on the Hexnode portal.
**Step 2:** Select an existing policy or create a new one by clicking on the "**New Policy**" button.
**Step 3:** Give the new policy a name if creating a new one.
**Step 4:** Go to **macOS** > **Configurations** and select **System Extensions**.
**Step 5:** Click "**Configure**" and set the System Extensions settings.
**Step 6:** Click "**Save**" to apply the changes.

If you apply this policy to devices with versions lower than 10.15, the policy will be pushed from the console and the payload will be visible in System Preferences > Profiles, but it will not take effect on the device. The following configuration options are available:

| Sl.no | Configurations | Description |
|---|---|---|
| 1. | User Override | Check this box to allow all users of the macOS to approve additional system extensions that are not specified in the policy, allowing applications to be installed without approval for a system extension. |
| 2. | Team Identifiers | Enter the Team identifiers of validly signed system extensions that should be allowed to load on the macOS. The team identifier must be alphanumeric and should have ten characters. |
| 3. | System Extensions | List specific System Extensions that you want to approve for the macOS. Add the Bundle identifier and Team identifier of a system extension to load. For unsigned system extensions, leave the field empty. |
| 4. | System Extension types | This option allows you to specify specific System Extension types you want to be installed for the team identifier. You can enable System Extensions for each team ID: Endpoint Security Extension, Driver Extension, and Network Extension. By default, all extension types will be allowed if you haven't specified the extension type for a given team ID. |

Devices may need to be restarted for the modifications to take effect if the System Extension policy that was already connected to them has been updated.

# Kernel extensions for macOS

Kernel extensions (KEXTs) are powerful tools that allow users to enhance the capabilities of their operating systems. These extensions can access parts of the operating system that regular applications cannot and execute code at the kernel level, allowing for modifications to the core OS components required to run an application. However, with the upgrade to macOS High Sierra, these extensions now require user authorization to load.

Hexnode UEM allows you to create a whitelist of approved Kernel Extensions that can be loaded without user approval on macOS High Sierra 10.13.2 devices. Additionally, IT admins can also give users the ability to override KEXTs and add team identifiers. To configure macOS kernel extension settings, follow the steps below:

**Step 1:** Navigate to the **Policies** tab on the Hexnode MDM portal.
**Step 2:** Select an existing policy or create a new one by clicking on the "**New Policy**" button.
**Step 3:** Give the new policy a suitable name if creating a new one.
**Step 4:** Go to **macOS > Configurations** and select **Kernel Extensions**.
**Step 5:** Click "**Configure**" and set the KEXTs settings.
**Step 6:** Click "**Save**" to apply the changes.

The following options are available in the KEXT settings:

| Sl.no | Configurations | Description |
|---|---|---|
| 1. | User Override | Enable this option to allow users to approve kernel extensions that have not been whitelisted in the policy. |
| 2. | Team Identifiers | Add Team IDs one by one. Then, all kernel extensions signed by the listed Team IDs will be approved. The Team ID must be alphanumeric with ten characters. |
| 3. | Kernel Extensions | Provide the Team ID and Bundle ID to allow specific kernel extensions for each app. For un-signed legacy kernel extensions, provide only the Bundle Identifier field leaving the Team Identifier field blank. |

On devices running macOS 11 and higher, installing or updating Kernel extensions via policy requires the device to be restarted for the changes to take effect. If the Kernel extension includes unsupported or deprecated Kernel Programming Interfaces (KPIs), it will not work correctly. To resolve this, you can use the alternatives suggested by Apple and deploy them using System extensions.

## Setting up email accounts on macOS devices

Hexnode UEM provides a solution allowing IT admins to set up email accounts on macOS devices remotely, saving time and effort. With Hexnode, admins can easily configure POP or IMAP mail accounts on macOS devices, set up incoming and outgoing mail server settings, choose different user authentication types, and more.

The wildcard functionality allows for the automatic population of data, such as usernames or email addresses, based on the details provided during device enrollment in Hexnode UEM. In addition, this feature enables users to send and receive emails with their corporate email accounts, making it a highly beneficial solution for organizations.

To add mail accounts to macOS devices using Hexnode UEM, follow these steps:

**Step 1:** Log in to the Hexnode UEM portal using your credentials.
**Step 2:** Once logged in, navigate to the **Policies** tab. IT admins can create a new policy by clicking on the "**New Policy**" button or continue with an existing one. Assign a suitable name and description (optional) for the policy.
**Step 3:** Navigate to **macOS > Accounts > Email**.
**Step 4:** Click on the "**Configure**" button. This will allow us to set up email accounts on macOS devices remotely, saving time and effort.
**Step 5:** From this point on, the admins can set up email accounts on the devices, configure incoming and outgoing mail server settings, choose different user authentication types, and more.
**Step 6:** Navigate to the “**Policy Targets**” tab, add devices or users' groups as required, and save it.

Hexnode UEM provides many more options for setting up incoming and outgoing emails. Remember that if the email account has multi-factor authentication enabled and is not supported by the native email app, use the app password instead of the account password.

# Configuring Exchange ActiveSync settings on macOS

Exchange ActiveSync allows for the automatic setup of Exchange server settings on macOS devices remotely, making it easy for organizations to keep their employees connected and productive. In addition, with Exchange ActiveSync, users can seamlessly sync mail and other web services such as Calendar, Contacts, Reminders, and Notes hosted on an Exchange server with their enrolled devices.

Hexnode UEM provides an easy-to-use platform for creating an Exchange ActiveSync policy for a corporate account, enabling users to access these services even when working offline. This feature streamlines the process of setting up and maintaining Exchange accounts, helping increase organizations' efficiency and productivity. To configure Exchange ActiveSync Account via policy, follow these steps:

**Step 1:** Log in to the Hexnode UEM portal
**Step 2:** Once logged in, navigate to the Policies tab. Here, admins can create a new policy by clicking on the "**New Policy**" button or continue with an existing one. Assign a suitable name and description (optional) for the policy.
**Step 3:** Next, navigate to **macOS** > **Accounts** > **Exchange ActiveSync**.
**Step 4:** Click on the **Configure** button. This will allow you to remotely set up the Exchange ActiveSync settings on macOS devices.
**Step 5:** In the configuration menu, IT admins can configure various features such as email account settings, synchronization settings, and more as per requirements.
**Step 6:** Once configured, navigate to the "**Policy Targets**" tab. Here, admins can add the devices or user groups they want to apply the policy.
**Step 7:** Finally, save the policy to apply the changes.

When the policy is applied, the target device will automatically configure the Exchange ActiveSync account according to the specified settings.

# Configuring CardDav, CalDav and LDAP on managed macOS

CardDAV (vCard Extensions to WebDAV), CalDAV (Calendaring Extensions to WebDAV) and LDAP (Lightweight Directory Access Protocol) are protocols that allow users to access and share contacts, calendars, events, and notifications on a server.

Hexnode UEM allows administrators to configure CardDAV, CalDAV and LDAP settings for macOS devices remotely from the Hexnode console. This allows administrators to add contact and calendar accounts to user devices, enabling them to synchronize their data with any server that supports CardDAV and CalDAV. Additionally, LDAP allows syncing contacts from the corporate Active Directory to macOS devices, which can be accessed from the contacts app.

The configuration settings policy for macOS devices in Hexnode facilitates an interface for profile setup and deployment, which makes it easy for organizations to set up and maintain the protocols. To configure these settings via policy, follow the steps below:

**Step 1:** Log in to the Hexnode UEM portal.
**Step 2:** Navigate to **Policies** > **New Policy**. Assign a suitable name and description (optional) for the policy. Alternatively, you can choose to continue with an existing policy.
**Step 3:** Go to **macOS** > **Accounts** > **CardDAV** or **CalDav** or **LDAP**. Then, click Configure to set up the settings for the protocol.
**Step 4:** IT admins can configure various features from the configuration menu as per requirements.
**Step 5:** To associate the policy with the target entity, navigate to **Policy Targets** > +**Add Devices.** Choose the target device and click OK. Click **Save**.
**Step 6:** You can also associate the policy with Device Groups, Users, User Groups, or Domains from the left pane of the **Policy Targets** tab.
**Step 7:** Alternatively, the policy can be associated from the **Manage drop-down** of the **Policies** tab. Click **Manage** > **Associate Targets**. Choose the target entity and click **Associate**.

When the policy is associated with the macOS device, the configured CardDAV, CalDAV and LDAP accounts will be added and the contacts, calendars and other data will sync with the device. The synchronized contacts and calendars can be accessed from the Contacts and Calendar app on the macOS. The LDAP account settings can be found under **System Preferences** > **Internet Accounts**. Once the policy is associated successfully, the user will be able to access the contacts, calendars and other data from the device and will be able to work offline as well.

# Chapter 5: macOS app management

Managing apps on macOS devices is essential to maintain security and ensure productivity in organizations. Hexnode UEM offers a range of features to manage apps on macOS devices effectively. These features include enforcing mandatory app installations, blacklisting or whitelisting apps, providing an app catalog for users to install approved apps, and configuring app settings. These features help organizations maintain the integrity of their IT environment while providing a seamless user experience.

## Adding mandatory apps for managed macOS

Hexnode UEM simplifies app management for companies with its mandatory application feature for macOS devices. With a simple policy push to the target entities, all the necessary apps are installed on the devices without any user intervention. Hexnode UEM supports adding several versions of an app to the app inventory, whether retail or corporate (however, only one version of the app can be installed on the device at a time).

The Hexnode UEM Mac app management tool streamlines the process of upgrading important apps required by your firm. The mandatory apps configurations can be found in the App Management tab of macOS policies. If you wish to upgrade a previously deployed business app, you must replace the old PKG file with an updated version of the PKG file. If several versions of an app are added to the Mandatory Apps policy, only one version of the app will be sent to the devices for installation. There are multiple scenarios for this:

| | |
|---|---|
| First case | If the business app version is the same as the retail app version, installation will be prioritised in the following order:<br>1. Non-Ad-Hoc Enterprise version<br>2. Store version<br>3. Ad-Hoc Enterprise version |
| Second case | When the corporate (or enterprise) app version exceeds the store app version, the enterprise version is installed on macOS devices. |
| Third case | If the store app version is newer than the enterprise app version, the store app version will be downloaded and installed on the devices. |

***Note:***

- *Apple only permits the deployment of*
  *(1) store applications purchased through the Volume Purchase Program (VPP) and*
  *(2) corporate apps to macOS devices.*

## Blacklisting/Whitelisting applications on macOS

The Blacklist app policy in the Hexnode UEM interface allows you to block apps on macOS devices. When the user tries to launch the blacklisted apps, it displays a blocked-access prompt on the device. Whitelisting restricts users' access to just those apps that the company has specifically defined. Users can easily install/access them without any limitations. Except for the whitelisted apps, all other apps will be prohibited on the device. You may define which apps are forbidden or granted access on macOS devices based on the requirements. Once you log in to the Hexnode portal, the steps to whitelist or blacklist the applications are as follows:

1. Go to **Policies > New Policy > macOS > App Management > Blacklist/Whitelist** and click **Configure**.
2. Enter policy name and description.
3. Click **Whitelist (for allowlist) or Blacklist (for denylisting)** depending on what you need and **+Add** to select apps or groups to be whitelisted.
4. Associate policy with target devices by selecting Devices/Device Groups/User/User Groups/Domains.
5. Click Save to push policy to device.

***Note:***

- *Only macOS 10.11 and later are supported.*
- *The Blacklist/Whitelist policy necessitates the installation of the most recent version of the Hexnode agent app on the devices.*
- *Enterprise apps, Store apps and VPP apps can be whitelisted on the devices.*
- *The Hexnode MDM agent on the device is in charge of transmitting app paths (app IDs or bundle identifiers) to the portal. Apps from the policy can be selected for blacklisting/whitelisting only when a macOS device has been registered in the UEM console, the device scan has been performed, and the agent has updated the app paths with the portal.*

## Creating an app catalog in macOS

The 'App catalog' feature in Hexnode allows administrators to construct a customized app store with a range of applications that can fulfill an organization's needs. An end-user may easily download all the necessary applications from the app library. Users may browse the app catalog using the Hexnode app, which is loaded on their devices.

To successfully provide corporate, store, and VPP apps for distinct sets of targeted customers, an administrator can build up numerous app catalogs including app groups and individual apps. By providing employees with a centralized location to download apps, it becomes easier to ensure that employees are only using approved apps. To create an app catalog in Hexnode,

1. Log in to the Hexnode portal and go to "**Apps**."
2. Click "**Add App**" and select "**Web App**" or "**Enterprise App**."
3. Fill in the necessary details and **configure the app permissions and settings.**
4. Click "**Save**" to create the app.
5. To add the app to the catalog, go to "**App Catalog**" and click "**Add Catalog Item.**"
6. Select the app from the list and configure the settings for the app catalog item.
7. Save the changes and publish the app catalog for users to access.

***Note:***

- *Store apps published to the App Catalog on macOS devices will redirect the user to the App Store when clicked.*

## Setup app configurations for managed macOS devices

The app configuration feature allows IT to offload app configuration from the user end. It is only applicable to apps that have been authorized with configurations built in by the app developers. IT may pre-configure usage parameters like port numbers or server addresses for supported apps, avoiding the risk of wrong setup by leaving it to end-users. With Hexnode, you may use app configuration files to specify basic settings like accounts, logins, and so on on apps. These app configuration files are distributed in XML format and contain the keys and values that are used to indicate the customized parameters.

To set up app configurations on macOS devices:

- On the Hexnode portal, go to the **Policies tab** to select an existing policy or create a new one.
- Choose App Configurations from the **macOS > App Management** menu.
- Choose **Configure** and then click the **+ Add New Configuration button** to select the app to be customized.
- Download the sample XML file to see how to prepare an application configuration file.
- By selecting the **Choose File option**, you may **upload the necessary XML file** for the selected app.
- Select the devices or device groups to which the policy will be linked on the Policy Targets tab.
- Select the Save option.

# Chapter 6: macOS device and data security

Securing macOS devices is crucial for any organization to protect sensitive data and maintain a secure IT environment. Hexnode UEM offers a comprehensive solution to manage and secure macOS devices with its range of device security features. These features include privacy preferences policies, certificate management, web content filtering, OS updates, media management, time limits, smart card authentication, firewall configuration, FileVault management, and login window preferences configuration.

With Hexnode UEM, IT teams can remotely manage and configure macOS device settings, deploy security policies, and enforce compliance regulations to keep their devices and data secure.

## Setting up privacy preferences

A Privacy Preferences Policy Control (PPPC) profile enables administrators to remotely manage the Privacy tab of the Security & Privacy pane under System Preferences. Admins may remotely accept or refuse certain apps' requests to access different macOS services like as Calendar, Camera, and so on. Allowing an application access to certain services via a PPPC profile simplifies app deployment.

For example, providing the app remote access to all protected files on the device allows the chosen app to access any private-sensitive data without prompting the end-users. With the Privacy Preferences Policy Control payload for macOS and Hexnode's UEM technology, companies may remotely handle these approvals on behalf of users.

**Note:**

- *The PPPC profile necessitates the installation of the most recent version of the Hexnode UEM app on the devices.*
- *Supported on macOS 10.14 or later devices.*

## Adding certificates for macOS devices

A digital certificate installed on a device enables safe internet access to business resources. Since safeguarding corporate data has always been an important and high-priority duty for macOS administrators, there is a rising demand for digital certificates in the company.

Administrators can remotely distribute and install certificates to macOS devices using a Mobile Device Management system such as Hexnode UEM. A digital certificate can be used to encrypt network connections (VPN and Wi-Fi) and ensure that only the users or devices specified have access to company data. After adding the certificates to the Hexnode gateway through policies, you may use them in any other macOS capability that requires a certificate. The steps to add certificates are as follows:

- On the Hexnode portal, go to the **Policies tab** to select an existing policy or create a new one.
- Navigate to **macOS Security > Certificates**. Select **Configure**.
- To import a new credential certificate profile from your device, tap the **Add Certificate** button. You may enter as many certificates as you like.
- Then, **Select the devices or device groups** to which the policy will be linked on the Policy Targets tab.
- Select the **Save option** to associate the policy to the devices

The following choices will be displayed by the newly added certificate:

- **Credential Name:** The display name of the certificate is referred to as the credential name. When you submit a certificate by selecting Add Certificate, this area becomes accessible.
- **Credential Details:** You may examine the subject, issuer name, and expiration date by clicking on the '+' button next to Credential Details. To close the details section, click '-'. Click the 'x' button in the top-right corner of each certificate listing to delete it.

***Note:***

- *Keep in mind that you must maintain the existing Certificates policy in macOS in order to access the list of certificates for other capabilities like as Wi-Fi, VPN, and so on.*

# Web content filtering on macOS devices

Web content filtering allows your company to control who has access to which websites on macOS devices. It helps organizations secure their devices by blocking access to potentially harmful or malicious websites.  Additionally, web content filtering can also be used to block access to non-work-related sites, such as social media or streaming services. You may set rules across your devices to block users from viewing certain URLs with the Safari browser.

Hexnode also offers the option to '**Blacklist by Content**'.  It is enabled by default on macOS devices and cannot be disabled. This setting automatically limits the explicit content. However, administrators can provide users access to certain websites by whitelisting them. This capability comes in handy when you need to offer access to websites that are prohibited due to their content type.

**Note:**

- *URLs should start with http://, ftp://, or https://*
- *You can whitelist multiple URLs by separating them using comma or semi-colon*

## Scheduling OS updates for managed macOS

Hexnode assists IT managers in scheduling macOS upgrades on devices by policy or remote action. On managed devices, you may simply restrict or postpone available OS upgrades. When a system update is available, IT admins can schedule any of the following actions:

- Notify only
- Download only
- Download and install
- Install
- Install later

The action specifies how the update is to be handled on macOS devices.

**Note:**

- *UEM can automatically distribute macOS upgrades to monitored macOS devices.*
- *Before you begin, ensure that the device is linked to the internet. It ensures the installation of all available macOS and firmware upgrades for the macOS.*
- *Before delivering a macOS upgrade, ensure that your organization's process is compatible with the new macOS version. As a result, a methodical approach to OS upgrades is required to guarantee macOS security.*

## Setting up media management

Securing data is a crucial aspect in any business setting. To ensure the safety of information stored on corporate devices, organizations must have control over access to their content. Hexnode offers the ability to set up advanced media management settings for external and internal drives, as well as optical media on macOS devices.

These settings allow the organization to decide whether to allow or deny media use or limit it to only authorized users. By denying media usage, it is not possible to mount it and transfer data from the devices, thus providing an added layer of security and protecting against unauthorized access.

**Note:**

- *This feature is supported on macOS 10.13.6+*

# Restrict user login time on macOS devices

On macOS devices, Apple has implemented built-in restrictions that allow administrator users to control the actions of other user accounts. These restrictions are beneficial for organizations as they can set specific times for when corporate-owned macOS devices can be accessed. This ensures that the devices are only used during designated hours, minimizing the risk of unauthorized access, even in the event of compromised user credentials.

The Time Limit policy for macOS specifically limits the time when users can log in to the device, reducing the potential for misuse. This eliminates the need for administrators to manually configure usage limitations for each individual account on the device.

**Note:**

- *Ensure that Parental Controls are enabled for the user in the respective device's System Preferences.*
- *You can set time limits from 15 minutes up to 8 hours.*
- *If "–" is selected no access limits are enforced on the user.*
- *User login is restricted after the allowed time limit. If the device is in use, the user will be logged out automatically.*

# Smart card authentication for managed macOS

A smart card is a physical device, that contains one or more security certificates. These certificates can be used for various types of authentications, such as logging into a computer or accessing a network. The user's smart card PIN is also required to access the certificates and authenticate the user.

Smart card authentication for logging in to a macOS device provides an extra layer of security by requiring possession of both the smart card and the PIN. Unlike a traditional password, which can be easily compromised, this method uses encryption and makes it difficult for unauthorized access.

Hexnode UEM allows IT administrators to remotely manage the smart card authentication settings for macOS devices. This includes configuring the settings so that users are required to use a smart card to log in, enforcing the use of a specific smart card, and verifying the authenticity of the security certificates. This simplifies the management process for IT admins and improves the security of macOS devices.

**Note:**

- *This feature works on devices running macOS 10.12.4 and later*

# Setting up Firewall on macOS

Using Hexnode UEM, you can configure the Firewall on your macOS to block or allow connections between your network ports and applications. This can prevent third parties from exploiting your device and protect your macOS from security attacks by creating a barrier between internal and external networks.

It's recommended to enable the Firewall when connecting to a public network as it can block unauthorized incoming connections from the internet without affecting outgoing connections or network access. Additionally, you can enable Stealth Mode to prevent others from discovering your macOS by blocking it from responding to probing requests.

***Note:***

- *The Firewall on a macOS device cannot be turned off by removing the device from Policy Targets or deleting the associated policy. Instead, it must be manually turned off by going to* ***System Preferences > Security & Privacy > Turn Off Firewall*** *and clicking the lock to prevent further changes.*
- *If Stealth Mode is enabled in the Hexnode MDM console, users will not be able to manually turn off the Firewall unless the device is removed from the associated policy.*
- *Similarly, if all incoming connections are blocked using Hexnode UEM, users will not be able to manually turn off the Firewall unless the device is removed from the associated policy.*
- *The list of blocked apps can also only be removed manually from the device settings.*

# Managing FileVault for macOS devices

FileVault is a disk encryption program in macOS OSX 10.3 and later that protects data and prevents unauthorized access. It requires a password or recovery key to log in and encrypts all new files saved on the device. FileVault is useful for preventing data compromise in case a macOS is lost or damaged. Hexnode allows IT administrators to choose to allow users to enable or disable FileVault on their work devices and offers options for encryption using:

- Institutional recovery key
- Personal recovery key
- Institutional and personal recovery key.

When using Hexnode, users can escrow the recovery key, within the Hexnode system. This allows for retrieval of the key from the UEM platform if the original key is lost and the encrypted disk needs to be unlocked. Additionally, Hexnode also enables users to retrieve the personal recovery key if they have chosen to encrypt their device using either the Personal Recovery Key or the Institutional and Personal Recovery Key options.

**Note:**

- *FileVault works on Mac OSX 10.3 and newer versions.*
- *Once enabled, removing the policy or disassociating devices will not disable FileVault.*
- *To create an encryption certificate, use one of the following file formats: .cer, .crt, .pem,. der,. p7b, .p12. A computer running macOS 10.8 or later is required.*
- *If exporting certificate without private key, store it securely for decryption.*
- *Check name and format of startup disk before proceeding.*
- *Institutional Recovery Key cannot decrypt macOS devices with M1 chip or macOS Big Sur and later, admin credentials or Personal Recovery Key is required.*
- *Re-encrypting an already encrypted macOS will generate a new personal recovery key.*
- *Applying another FileVault policy has no effect on an encrypted device with a FileVault policy already in place.*
- *Any changes made to FileVault escrow key configuration after encryption will not update the escrow recovery key in the portal.*

## Login window preferences settings for macOS

The login window screen settings on macOS devices allow for customization of the login screen. These settings can be found in the System Preferences and include options such as displaying a list of users, adjusting the appearance of the login window, and showing control buttons.

Depending on the configured preferences, the login window may appear when the user logs out, when the device wakes up from sleep mode, or when exiting screensaver mode. Hexnode UEM solution allows for remote configuration of these settings across multiple macOS devices.



Mitsogo Inc., United States (HQ), 111 Pine St #1225,
San Francisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151