Mastering ABM and ASM

The complete handbook

WHITE PAPER

hexnode

TABLE OF CONTENTS

Introduction

Apple Business Manager and Apple School Manager shorten your workflow by enabling direct shipping of devices to the end-users on purchase with secure configurations. The devices are ready for work right from the get-go.

The demand for efficient and secure device management has never been higher, and Apple has responded with their two management solutions: Apple Business Manager and Apple School Manager. These innovative platforms give an all-inclusive solution for deploying, managing, and securing the Apple device fleet of your organization. Whether you are an IT administrator aiming to streamline device deployment, or a school administrator looking to empower students with the latest technology, these tools can provide the perfect balance between simplicity and control.

With Apple Business Manager and Apple School Manager, you can effortlessly distribute apps, automate device enrollment, and easily manage your users and devices. These platforms offer a wealth of features, including app and book distribution, zero-touch device enrollment, and device management, all designed to make your job easier and more efficient.

This white paper will delve into the fundamentals of Apple Business Manager and Apple School Manager, exploring the features and capabilities that make them the go-to choice for organizations of all sizes. From setting up and configuring your devices to managing and protecting them, we will guide you through the process step-by-step, providing you with the knowledge and skills you need to make the most of these powerful tools. We will also look at how you can maximize the potential of these services by pairing them up with a UEM solution like Hexnode.

So, whether you're a seasoned IT professional or new to the world of device management, this white paper is the perfect guide for understanding the A-Z of Apple Business Manager and Apple School Manager and unlocking the full potential of your organization's Apple devices.

1

Unlocking the potential of ABM and ASM

By integrating ABM and ASM into your organization, you can streamline the management of your Apple devices, cut down on IT workloads, and boost productivity across the board. With these powerful tools, you can remotely provision devices before they're even turned on, ensuring they're ready to go for your end-users. Not only does this help your team hit the ground running, but it also means your devices stay up to date with the latest software and security updates.

Apple Business Manager and Apple School Manager are two powerful tools for helping organizations of all sizes to manage their Apple devices and apps. While the former is designed for businesses, the latter is meant for educational institutions. Although both of them belong to different spectrums of purpose, the capabilities are more or less the same.

Deploying configured devices to end-users can be strenuous without portals like ABM and ASM. After purchasing devices from the vendor, the IT team would have to manually configure them to prepare them for enterprise or school use, following the organization’s requirements. Afterward, they would be stored in a warehouse and would be shipped to the end user whenever required. This would also limit the scalability as manually managing several devices can be time-consuming and error-prone.

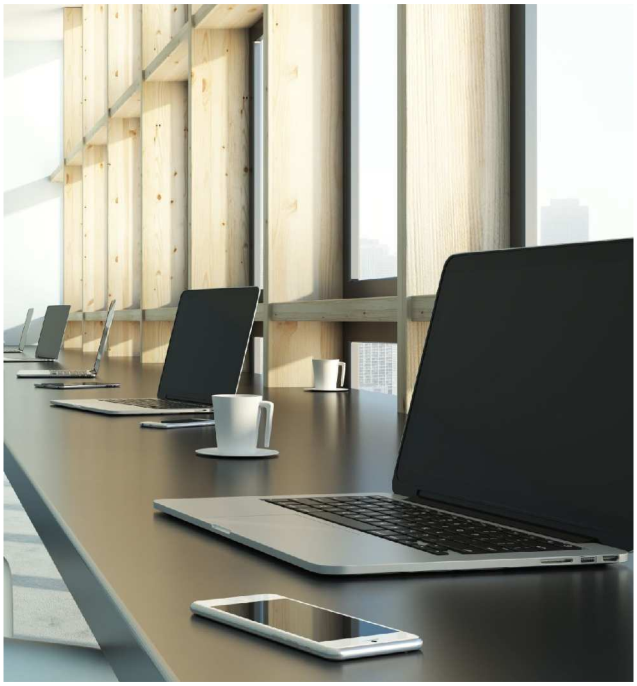
Apple Business Manager and Apple School Manager help to avoid the intermediate steps in the traditional provisioning workflow. This means that Apple devices purchased from an authorized reseller can be remotely provisioned before it is even turned on. This enables the devices to be corporate-ready for the end-users upon receiving them.

The web-based portals also offer various other capabilities other than zero-touch deployments. These tools allow IT administrators to enroll devices into their organization, assign them to specific users, and even remotely configure and update them. This means that users can get up and running quickly with their new devices and stay up to date with the latest software and security updates. By implementing these tools in your organization, you can help ensure that your users have the resources they need to be productive, while also keeping your organization's data secure.

APPLE BUSINESS MANAGER

Apple Business Manager is a cloud-based platform that enables businesses to manage their Apple devices, applications, and accounts in a single place. The platform provides a range of capabilities, including device management, app distribution, and security, that makes it simpler for businesses to manage their technology and boost productivity.

Administrators may also keep track of inventory, allocate devices to certain users, control device configurations and security settings, and track inventories. ABM also facilitates more robust security features such as device lockdown and remote wipe capabilities, when combined with device management solutions.



Additionally, administrators can control employee Apple IDs and accounts and integrate them with third-party MDM solutions. ABM also allows for custom app deployment, which allows administrators to distribute specific apps to specific groups of employees. This can be useful for businesses that have specific requirements for apps that are used by certain departments or teams.

APPLE SCHOOL MANAGER

Apple School Manager is a powerful tool for schools and educational institutions to manage their Apple devices. It also offers a central location to manage and distribute content to iPads, Macs, and Apple TVs.

One of the key benefits of using Apple School Manager is the ability to automate the creation of Apple IDs for students and teachers. This process can be time-consuming, but with the integration of Apple School Manager and the SIS, this task can be completed with just a few clicks. The Student Information System (SIS) is a platform that collects and stores school-wide data including administrative documentation, student enrollment data, classroom information, and so on.

Once the Apple IDs are created, schools can easily manage and distribute content to their students' and teachers' devices, including apps, books, and other educational materials. The platform is user-friendly and accessible, making it a cost-effective solution for educational institutions of all sizes.

HOW EFFECTIVE ARE ABM AND ASM ON THEIR OWN?

ABM and ASM provide enough capabilities to remotely deploy devices to your employees in bulk. However, they fall short when it comes to having advanced device management options. Having a qualified mobile device management solution (MDM) is an efficient method of recouping the shortcomings of ABM and ASM.

Even if your devices are not purchased from an authorized reseller or network provider, you can use Apple Configurator 2 to configure your Apple devices to ABM or ASM. Nonetheless, you would have to add all devices manually by plugging each device into a macOS computer that has Apple Configurator 2 installed.

Using an MDM solution alongside Apple's web portals will enable you to use some of the best management features that make business operations easier. Together, they eliminate so many manual processes, subsequently saving time and money. Moreover, ABM and ASM are designed to be used in conjunction with an MDM.

WHAT IS APPLE BUSINESS ESSENTIALS?

Apple Business Essentials (ABE) is a suite of products and services offered by Apple. Currently only available in the United States, ABE combines basic device management, 24/7 Apple support, and iCloud storage for organizations. It is specifically aimed at small and medium-sized organizations.

While ABE provides seamless integration with other Apple devices and software, it may not be compatible with other non-Apple products, which can be a drawback for businesses that rely on a mix of devices and software. Its limited scalability customization options might not be sufficient for organizations looking for more tailored solutions. However, ABE is still a very powerful tool for companies trying to streamline their operations, improve productivity, and provide a better user experience for employees.

2

The evolution of ABM and ASM

Before the advent of ABM and ASM, Apple had two programs which laid the groundwork for managing devices- the Volume Purchase Program(VPP) and Device Enrollment Program(DEP).

In the early 2010s, Device Enrollment Program (DEP) and Volume Purchase Program (VPP) were the tools used for deploying Apple devices and managing their content. VPP was a program that allowed businesses and educational institutions to purchase and distribute apps in bulk, while DEP was a program that allowed administrators to enroll and manage devices over the air. The consolidation of VPP and DEP into Apple Business Manager and Apple School Manager was a step to make it easier for businesses and educational institutions to manage their Apple devices and apps.

DEVICE ENROLLMENT PROGRAM

The Device Enrollment Program (DEP) was introduced in 2013 to make the device setup process faster and more efficient. The program allowed organizations to enroll their devices directly into management, eliminating the need for manual setup steps.

DEP also ensured that devices were enrolled in the right management system, saving administrators time and resources. This also makes it easier to set up new devices and deploy them to users.

VOLUME PURCHASE PROGRAM

The Volume Purchase Program (VPP) was introduced in 2011 to help organizations purchase and manage apps in bulk. With VPP, organizations could purchase apps for their users and distribute them directly to their devices. This made it easier to manage app licenses and reduce the costs associated with purchasing individual licenses. VPP was also beneficial for app developers, as it allowed them to reach a wider audience and sell more licenses.

THE FORMATION OF ABM AND ASM

In 2018, Apple introduced Apple Business Manager (ABM), which combined the features of DEP and VPP into a single, unified platform. ABM was designed to simplify device management for organizations and make it easier to manage devices and apps in one place. Shortly after, Apple introduced Apple School Manager (ASM), as an ABM alternative for education organizations. By merging these two programs, Apple aimed to provide a centralized, web-based portal for IT administrators to manage their organization's Apple devices and apps more efficiently.

The evolution of ABM and ASM from DEP and VPP has been a significant milestone for Apple's device management strategy. These platforms provide organizations with a single, unified platform for managing devices and apps, making it easier for administrators to manage devices and reducing the amount of time and resources required to do so. As organizations continue to adopt Apple devices, ABM and ASM will become increasingly important tools for managing these devices and ensuring that they are deployed effectively.

3

A deep dive into the capabilities of ABM and ASM

IT administrators are drawn to the cutting-edge web portals of Apple Business Manager and Apple School Manager. It helps to simplify each step in a device's lifecycle, starting from remote deployment and enrollment to getting granular control over the device through managed Apple IDs.

Apple Business Manager and Apple School Manager can simplify the whole device provisioning process of your organization if used in the right way. Onboarding your organization into ABM or ASM along with your users and devices takes a few steps. In this section, we will focus on what ABM and ASM are capable of and how you can leverage their features to make the most out of them for your organization.

Even though the use cases fall into two different spectrums, the underlying objectives of both portals are the same – deploying devices remotely and managing the devices and the content distributed to them. Hence, most of the features included in ABM and ASM are similar. So, please keep in mind that the features mentioned below will be common to both otherwise specifically mentioned.

BROWSER REQUIREMENTS

The following are the browser versions required for the working of ABM and ASM:

- Safari on iOS 12 or later, or iPadOS 13.1 or later
- Safari 9 or later on Mac
- Microsoft Edge on Windows
- Google Chrome 35.0 or later

SIGNING UP YOUR ORGANIZATION

Signing your organization up for ABM or ASM can be done in a few steps. First, open the website (https://business.apple.com/ for ABM and https://school.apple.com/ for ASM). Click on Enroll now and enter your organization's details. You will have to enter information such as the organization's legal name, website, and details of the individual enrolling on behalf of the organization.

Initial administrator account

While setting up the user account, you should use the name of a person, and not the name of a group or role. This account will be the Administrator account. Once the enrollment is complete, you can give the Administrator role to up to four managers. Also, you should ensure the email address you use for signing up has not been used as an Apple ID for any other Apple website or service.

D-U-N-S number

While signing up for ABM, you should also enter your organization's D-U-N-S number. A D-U-N-S number or Data Universal Numbering System number is a unique numeric identifier assigned to business entities by Dun & Bradstreet. It is considered the standard for tracking businesses and their business credit activity.

MANAGING DEVICES

Once you have enrolled your organization in ABM or ASM, you can start managing your devices remotely. Not only can you deploy devices, but you can also tailor each device to fit the specific needs of your organization by configuring settings and restrictions to optimize productivity and security. This includes controlling access to certain apps and features, setting up email accounts and VPNs, and customizing device configurations to meet the unique needs of your organization.

Device enrollment

The first step in managing devices is to enroll them in your ABM or ASM account. This can be done using two methods:

Automated enrollment

Devices purchased directly from Apple or through authorized Apple resellers can be automatically enrolled in ABM or ASM during the setup process. Once you provide your Apple Customer Number or the Reseller ID to the ABM or ASM portal, they will fetch the details of the devices you have purchased, including serial number, order number, assignment date, and so on. You can also assign these devices to your MDM server during this process or after it. This allows for the zero-touch deployment, with devices being pre-configured and ready for use as soon as they are turned on.

Manual enrollment

If the devices are not purchased directly from Apple or its authorized resellers, you can still add them to the ABM and ASM portals using Apple Configurator. Although time-consuming, you can also resort to another method of adding device details such as the device's serial number and IMEI number to manually enroll the devices.

Device management

Configuring devices that are enrolled in ABM or ASM requires them to be assigned to an MDM (Mobile Device Management) server as well. With this solution, you can set up policies, restrictions, and configurations on the devices to meet the specific needs of your organization.

For instance, you can configure Wi-Fi and network settings, ensuring that devices automatically connect to your organization's secure network. You can also establish passcode requirements, such as minimum length and complexity, to safeguard sensitive information stored on the devices.

You can also implement other security policies and restrictions on the devices, such as blocking access to certain websites or limiting the types of apps that can be installed. This helps to safeguard your organization's data and network from potential threats.

Shared iPad

The Shared iPad feature is a unique feature available within Apple School Manager and Apple Business Manager, allowing several users to use a single iPad tablet. This functionality is particularly beneficial in schools, where several students may use the same iPad throughout the day. Shared iPad creates a personalized experience for each user by allowing them to access their apps and data on the same device.

When a user logs in to a shared iPad, they can access their home screen, apps, documents, and settings. They can also access their iCloud Drive storage and managed Apple ID. The iPad will automatically download and install the user's apps and content, so they have access to everything they need. After a user signs out, the iPad deletes their data and resets to a clean state, ready for the next user.

MANAGING USERS

One of the key functionalities of ABM and ASM is that it enables administrators to seamlessly manage users within the organization. Administrators may use it to establish and manage user accounts, assign roles and permissions, and allocate devices to users.

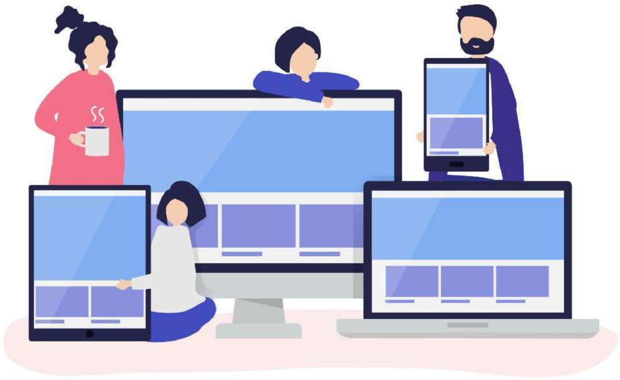
The first step in managing users in ABM and ASM is to create user accounts. When creating a user account, administrators can specify the user's name, email address, role, and permissions. Once user accounts have been created, administrators can assign devices to users. This allows users to use the devices and access the services associated with those devices. You can easily revoke users' privileges or remove the user from the organization too, making it a useful tool for employee onboarding and exiting.

Roles and privileges

There are multiple roles available in both ABM and ASM to be assigned to the users. Each role has different levels of privilege.

- **Administrator**: Administrators have the highest level of access after the Account Holder. They can perform tasks like enrolling devices, creating Managed Apple IDs, and managing content and settings.

- **Device enrollment Manager**: This role is responsible for managing the enrollment of devices in Apple Business Manager. They can also create and manage enrollment profiles and assign them to devices.



- **People Manager**: People managers can act on all other roles apart from administrators. They can aid in the management of employee access and rights by assigning and modifying the roles, statuses, and passwords of other users. However, they cannot manage devices or content.

- **Content Manager**: Content managers can purchase and distribute apps, books, and other content to users and devices. They can also create and manage Managed Apple IDs for users.

- **Staff**: Staffs are basic-level end-users. They can use the managed devices, apps, and books using the managed apple IDs assigned to them.

Apart from these, two more roles are exclusively available in Apple School Manager.

- **Instructor**: This role is for educators who will be managing classes and course material. They will have access to features such as creating classes, inviting students to join classes, creating course materials, assigning and grading assignments, and monitoring student progress.

- **Student**: The Student role is designed for students who will be using the assigned devices and participating in classes. Students have access to features such as viewing course materials and communicating with their instructors.

MANAGING CONTENT

ABM and ASM provide a way for organizations to purchase apps and books in volume for distribution to their devices. This allows administrators to purchase and distribute content to multiple users at once, rather than requiring each user to purchase their copy. This feature also enables enterprises to manage app licensing centrally, making it simple to revoke licenses if a user leaves the organization or a device is no longer in use.

Distributing apps and books

The Apps and Books section in the portal lets you search for the content that you require. Once you find your desired application or book, you can simply purchase the required number of licenses. ABM and ASM also allow you to transfer licenses from one location to another.

Distributing custom apps and books

ABM and ASM allow you to distribute custom apps and books that are tailored to meet the requirements of your organization. The steps required for making this possible include adding the app or book to the ABM or ASM portal and waiting for Apple's review process. Once approved, the apps and books will be available in the portal for you to assign to devices.

ABM AND ASM INTEGRATIONS

ABM and ASM in themselves are two powerful tools for automating device and content deployment. However, it also lets you integrate into several other platforms to unlock a multitude of features. Let's look at some of the integrations you can leverage with ABM and ASM;

Identity providers

Identity providers (IdPs) are services that provide authentication and authorization services for users in an organization. Integrating identity providers with ABM and ASM enables federated authentication, which simplifies the login process for users.

With this integration, users can sign in to Apple services using their existing credentials from their organization's identity provider. IT administrators can maintain control over user accounts and access to resources, providing added security and management capabilities. ABM and ASM support integration with popular identity providers such as Microsoft Azure Active Directory and Google Workspace.

Federated authentication

Federated authentication is a technology that allows users to access multiple tools, apps, and domains with a single set of credentials. This feature eliminates the need of having different login credentials to access different tools in an organization. You can use federated authentication to link your ABM or ASM portals with Google Workspace and Microsoft Azure Active Directory (Azure AD). This will enable your users to leverage their Google Workspace or Azure AD credentials as managed Apple IDs. They can then use those usernames and passwords to sign into their assigned iPhone, iPad, or Mac and even to iCloud on the web.

Student Information Systems (SIS)

A Student Information System (SIS) is a computerized database that schools manage and maintain to efficiently monitor all of their student data, including personal information, grades, attendance, and more. Integration with SIS is majorly intended for Apple School Manager for streamlining devices and user management for educational institutions. By integrating these systems, administrators can automate the process of creating and updating accounts and device assignments, saving time and reducing errors.

SIS integrations allow administrators to create and manage classes, rosters, and user accounts in Apple School Manager automatically. Student, instructor, and class data can be synced between systems, and assignments and grading can be shared. This integration simplifies the task of managing accounts and permissions while also offering access to Apple's ecosystem of educational apps and content.

Unified Endpoint Management solutions

We have already mentioned in multiple instances the need to have a UEM solution along with ABM or ASM. Apple Business Manager and Apple School Manager do offer a range of features to help manage devices, but for more complex environments, integrating with a Unified Endpoint Management (UEM) system becomes imminent.

For beginners, a Unified Endpoint Management (UEM) system is a software solution that enables organizations to manage and secure a diverse range of endpoints, including mobile devices, laptops, desktops, and servers from a single console. It provides IT administrators with a unified view of all the endpoints in their environment and allows them to apply policies and configurations to all these devices from a centralized location.

By integrating ABM with a UEM system, administrators can gain additional management and security capabilities which will come in handy throughout the devices' lifecycle. It helps you to enroll and deploy devices remotely while granting you granular control over its capabilities. Additionally, it gives you a unified view of all devices in an organization, regardless of operating system, allowing for consistent management policies and configurations. This can include device enrollment, app deployment, security policies, and compliance monitoring.

Overall, integrating ABM with a UEM system can help organizations streamline device management, and improve security while simplifying the administration of multiple platforms and operating systems.

4

Joining forces: when ABM and ASM meet a UEM

Hexnode UEM is a top-rated solution for managing and securing endpoints, including mobile devices, laptops, and desktops, in an enterprise environment. With a comprehensive suite of features, Hexnode caters to businesses of all sizes, from small start-ups to large enterprises.

While Apple Business Manager and Apple School Manager provide a great deal of control over Apple devices, there are limitations to what they can do on their own. Even though you will get an overview of all the devices registered to your organization, you will not be able to know more about the status and health of each device.

Another important aspect is configuring each device to meet the organization's requirements. This requires having control over what the device can and cannot do, while continuously monitoring it. All these facets point towards the importance of pairing ABM and ASM with a complementary solution that can provide additional capabilities, such as more robust device management, advanced reporting and analytics, and integration with other business systems. Unified Endpoint Management systems are the perfect solution to these hurdles.

HOW TO CHOOSE YOUR IDEAL UEM?

Selecting the best Unified Endpoint Management (UEM) solution for your organization might be difficult. With so many providers and features to consider, it can be overwhelming to select the ideal solution that meets your business requirements. Some of the factors that you need to bear in mind are scalability, compatibility, and ease of use it offers. Security features such as password enforcement, remote wipe, and data encryption are also some must-haves regardless of the type of organization.

Figuring out the requirements of your organization in terms of device and user management capabilities will be the starting point. A good recommendation is to always have your organization future-proof, providing leeway for its growth. Choosing a comprehensive and robust solution such as Hexnode will be beneficial in that regard.

HEXNODE’S VALUE PROPOSITION

Integrating your ABM and ASM portals to Hexnode enables you to leverage all its native device management features to monitor and control your Apple devices. Let’s look at some of the capabilities it unlocks;

Configuring accounts

Quickly setting up user accounts in apps such as email and calendar is a boon to all organizations having several users and devices. Hexnode lets you set up each device with the respective user’s account remotely. This saves a lot of time and effort for the administrators by getting the devices up and running as soon as they are switched on by the user.

Deploying network security configurations

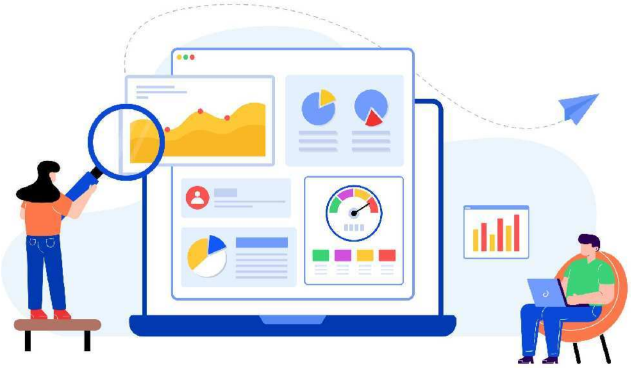
The network management options available in Hexnode let you safeguard your organizational devices by making sure that their connections are secure. You can configure the credentials of your VPN or Wi-Fi network from the Hexnode portal and push it to the devices, enabling it to automatically connect to the network, once available.

Silent app deployment

This configuration lets you silently install in-house apps and store apps without interrupting the user. You can also utilize other app management features such as allow-listing and deny-listing to gatekeep only the apps necessary for your organization.

Remote device monitoring

With Hexnode, you can monitor device health and performance, including battery life, memory usage, and storage capacity, and proactively address issues before they impact users. Additionally, you can monitor app usage and data usage to ensure compliance with company policies and regulations.



Geofencing

With geofencing, administrators can create virtual boundaries around specific locations, such as office buildings or schools, and automatically trigger actions when a device enters or exits those boundaries. This opens up the ability to lock devices once they leave the school or office premises.

Schedule software updates

Software updates that come impromptu can affect employees' productivity and students' learning experience. With Hexnode, administrators can schedule updates in devices during off-hours after making sure the update is compatible with the existing devices.

Custom configurations

The ability to remotely add custom configurations to the devices opens up new possibilities for facilitating numerous device actions. This can be used to seamlessly automate tedious tasks on a large number of devices.

Bolster the use of Apple classroom and Schoolwork app

Using Hexnode, you can automatically configure the Classroom/Schoolwork app with student and class data retrieved from SIS or Azure AD. The only requirement is to connect the instructor's and student's devices to the same network.

STEPS TO INTEGRATE ABM/ASM WITH A UEM

Integration of Apple Business Manager and Apple School Manager to Hexnode, or any other UEM solution for that matter, can be configured in a few minutes. Linking ABM or ASM to a third-party UEM server majorly consists of two steps.

1. **UEM server certificates**: After creating a new server in your UEM portal, you should get a public key certificate file (.pem or .der) from your UEM vendor for each server you want to add. This public key certificate will be used to encrypt the Authentication Token file for secure transfer to the UEM server.

2. **Server tokens**: Once you upload the server certificate into the ABM/ASM portal, you will be able to generate a new server token from the ABM/ASM portal. After downloading the server token, you should install it on the UEM server, completing the integration process.

With these two steps, the UEM server will be added to the ABM or ASM portal. Now you are free to add any number of devices to the UEM server and open the door to numerous device management capabilities.

Conclusion

Mastering the intricacies of Apple Business Manager and Apple School Manager to meet your organization's needs will unlock a world of opportunities. For instance, you wouldn't have to scratch your head when you hire a bunch of new employees and are required to fully configure devices for each of them. You can seamlessly purchase devices and content in bulk, and using a capable UEM like Hexnode, apply all the pre-existing device configurations in a snap.

With digitalization taking the world by storm, more devices are being used in corporate and educational environments. However, managing and securing these devices can be challenging for IT personnel. ABM and ASM provide a unified solution to this challenge, offering powerful tools to manage, deploy, and secure devices with ease.

A fully optimized environment consisting of ABM or ASM along with a UEM solution such as Hexnode can enable employees to easily connect to shared devices, collaborate on projects in real time, and access secure cloud-based applications from anywhere. The integration of these platforms with other solutions such as identity providers and student information systems further enhances their capabilities and enables a more comprehensive management suite. These benefits not only increase efficiency and reduce downtime but also promote a culture of innovation, where employees and students are encouraged to push boundaries and create new solutions to challenges.