UEM Migration Handbook

An IT admin's guide for effective migration

WHITE PAPER

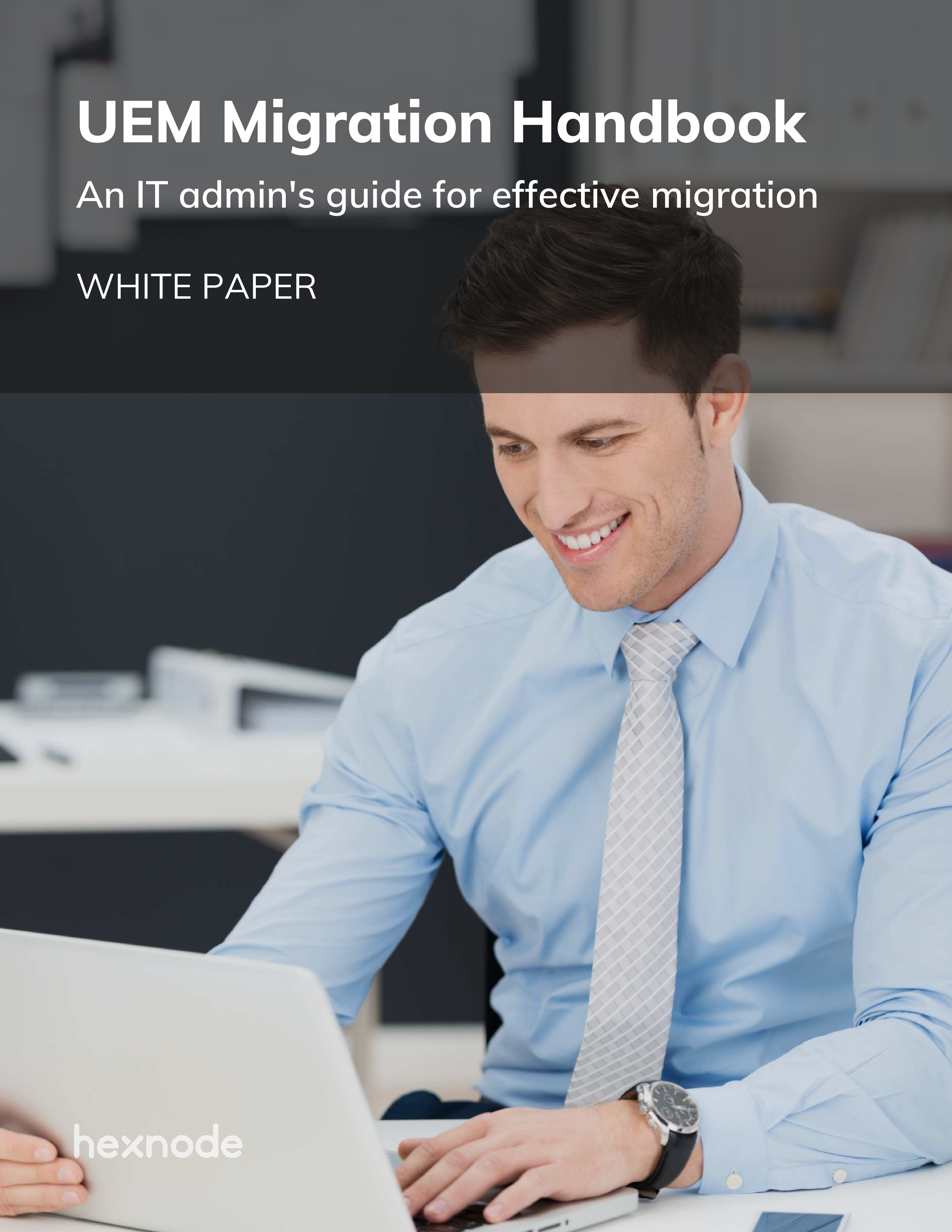


TABLE OF CONTENTS

Introduction

The dawn of the digital era marked the start of businesses employing a wide variety of devices for their personnel to work with. However, this gradual shift brought with itself the very real possibility of data leaks. Consequently, the idea of device management took root. Years of brainstorming making do with the existing technology, and constant evolution has now introduced the world to the concept of Unified Endpoint Management (UEM).

The road to Unified Endpoint Management (UEM) was one full of twists and turns. Yet it didn't take long to reach here.

- MDM or Mobile Device Management became important as mobile devices became more integrated into our daily lives.
- MCM, or Mobile Content Management, was developed to give end users access to exchange business data.
- Mobile Identity and Access Management (MIAM) was established to safeguard corporate networks by identifying and granting access to employees.
- Finally, Mobile Application Management (MAM) was developed due to the increased demand for deploying, updating, and securing mobile applications.
- In the end, Enterprise Mobility Management (EMM) emerged from the fusion of these solutions and MDM.

The development of device management reached the next level when Windows and macOS included Mobile Device Management features in their desktop operating systems. As a result, EMM companies began supporting desktops and laptops. As a result of this move, Unified Endpoint Management (UEM) was created.

UEM's rise was marked by many things, including technological developments and the rise of a remote work environment. Growing trends of BYOD (Bring Your Own Device) and the general notion of improving employees' work satisfaction have also played their parts.

The UEM market is anticipated to grow,

31.7%

by 2030, to reach

$53,656

million

A look at the most recent statistics shows that the market for Unified Endpoint Management is estimated to be worth $3,397.00 million in 2020 and is anticipated to grow by 31.7% by 2030 to reach $53,656.00 million.

1

Is it time to switch to Unified Endpoint Management?

Mobile devices have become key for businesses and employees. Organizations today are embracing mobile devices into the workplace due to its ability to offer a flexible work environment, reduce infrastructure costs, and improve employee productivity.

However, the challenge is to adopt the right tool to manage the different mobile device platforms and OS supported by an organization.

The current array of devices employed for business work is diverse enough to warrant a different type of management for each device group. However, different management systems for the different types of devices would mean trying to keep track of different consoles. This in itself is a hectic task.

Managing the different endpoints from a single console is more efficient and easier to handle, thus contributing to the popularity of Unified Endpoint Management.

FIVE REASONS WHY YOUR BUSINESS NEEDS A UEM SOLUTION

A thorough study of the market conditions and the kind of attacks businesses face in the wake of complete digitization is enough to present a thousand reasons businesses need a UEM solution. However, for clarity, these can be narrowed down to five main pointers.

Eliminate the risk of unmanaged endpoints

Fundamentally, UEM solutions market the improved security they provide across different endpoints. UEM solutions make it easy to enforce secure controls to all the devices within the organization's network. Additionally, they facilitate placing protocols to govern actions in case a security threat is suspected. Providing remote access to sensitive data, user authentication, and remote data wiping in case of lost/stolen devices are some ways UEM controls the flow of data between endpoints. They ensure that endpoints are up-to-date on software patches, thereby fixing known security vulnerabilities.

The wide variety of endpoints deployed across the organization provides an equally wide array of attack vectors. UEM solutions can provide consistent, best-in-class endpoint security from a centralized console.

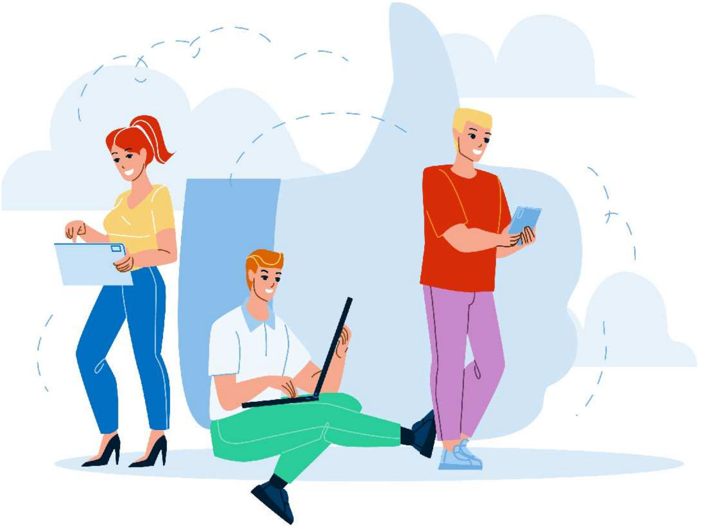
Automate IT operations

The IT department has its hands full with maintaining the security of data and networks in the organization. Some of the tasks they perform, like updating software, scheduling reports, and compliance checks, if automated, can free up their time which IT admins can then utilize for high-priority, better productivity tasks.

UEM solutions provide the IT department with the scope and platform to automate several day-to-day IT operations and enforce them on the different endpoints distributed across the network.

Provide scalability and flexibility

Workers may complete their work from remote locations in addition to the office thanks to a UEM, which enables quicker, more effective communication and workflow management. Using a UEM, managers can swiftly set up project teams, allocate responsibilities to specific employees, and track the advancement of numerous initiatives at once. These productivity tools are a boon for businesses trying to use technology to improve the efficiency and effectiveness of their internal operations.



Increase productivity and efficiency

UEM software minimizes the time and resources needed for IT management because it is centrally managed. The program may install, update, and uninstall applications, rules, and settings from a single administration interface. This makes it simple to maintain security settings with current personnel, assure consistent mobile experiences for new hires, and restrict access to devices that are no longer in use. In addition, UEM offers asset management tracking, enabling your company to determine which employee uses which endpoint.

The program enables your IT team to give your workers upgrades and new devices. The amount of time and resources needed by IT departments to manage mobile devices is significantly reduced by UEM's central management and asset-tracking capability.

Save up on operational costs

Since UEM services for BYOD devices can be considerably more affordable than acquiring the devices and software for employees while still needing to provide the device management, many firms discover that a well-implemented UEM can save them money over time. In contrast, a UEM's cost reduction over the first few years of implementation can more than cover the cost of the service. According to the law, leaking private information is illegal. The last thing a business owner would want is to pay hefty fines and face accusations of a breach of client data that was sensitive.

The penalties are not only costly, but they will also damage a company's reputation and eventually hurt the business. Although adopting a UEM at the time of company formation may seem superfluous, doing so will reduce your business's need for working capital over time, making it a wise move.

WHY YOU MAY BE MAKING THE SWITCH TO A UEM

Reasons to switch UEM could be anything, from wishing for a change to fixing an issue. However, it mostly boils down to increasing productivity and efficiency.

1. **The company is switching from legacy management software:** Legacy or "on-premises" management systems frequently fall short of expectations, which damages the technology's reputation in the industry.

2. **The company has outgrown its current UEM vendor:** Technological developments are a constant. Every day something new pops up, creating new needs in the world of security and sometimes, the current UEM vendor may be unable to keep up with these changes. This necessitates switching UEMs if there is an alternative that fits the bill for the organization's requirements.

FACTORS TO CONSIDER WHEN SWITCHING UEM PROVIDERS

There are many things to consider when switching UEM providers. These might have been why the switch is happening in the first place. Each UEM solution, though working towards the same goal, provides different features and varying levels of support and infrastructure.

Supported devices

One of the most important things to ponder before switching or selecting a UEM vendor is to ensure it supports all the endpoints employed by the organization. Otherwise, the switch may be of little help. Different UEM solutions support different sets of devices. Only some UEMs handle all the different varieties there exist

User and device onboarding

Every UEM has a different process for the user and device onboarding. There is no right or wrong way, but only what works for you. An expanding company will require additional endpoints to be managed. At this point, the many deployment options offered by a UEM solution are essential. IT administrators overseeing an expanding fleet of endpoint devices find that Zero Touch Enrolment and pushing policies to device groups are of great assistance.

Inventory management

Device and inventory management are imperative as it is essential to know what assets are accessed by the different endpoints. In the current organizational structure, it would be desirable to have a security solution that enables concerned officials to identify all devices that access the organization's network and tag assets to specific users to understand who owns a device, how many devices they're using, and what applications they access.

This lessens the workload associated with device lifecycle management and removes the unpleasant surprise of unidentified devices accessing the company's apps.

Security management

UEM solutions were created to eliminate any threats that could result from endpoint device data and security breaches. The UEM system must be able to enforce policies to help secure devices and data remotely. To prevent any breach of devices or data, it must also be able to find missing devices, wipe off data, change the owner and password on devices, assist device encryptions, protect networks, conduct routine device monitoring, and more.

Policy enforcement and compliance

Any company that permits BYOD must be able to enforce security guidelines to lower the risk of data breaches and keep insecure or weak devices from accessing private information. Every firm has its own security policies that need to be altered based on the risk involved with particular applications.

Third-party integrations

Businesses already utilize various third-party services for daily operations. The suggested UEM approach should improve their functionality. Additionally, it should aid in seamlessly integrating with them.

Audits and reports

Some organizations may have to adhere to strict compliance regulations, such as HIPAA, PCI DSS, NIST, SOC 2 or ISO 27001. This can be achieved by ensuring employee-owned devices are always in compliance. Reducing the risk of data regulatory fines by aligning corporate policies to ensure that out-of-date and out-of-compliance devices do not have access to corporate applications is often a priority. Proper auditing and reports can help keep track of compliant and noncompliant devices along with other criteria.

2

Understanding your organization’s device management requirements

Companies recognize the need for adaptability when supporting and managing mobile devices. It would help to maintain a balance between what your employees want and your IT and security demand.

However, the greater challenge is to find the right device management solution that complements your organization and its infrastructure.

Device management is crucial for disaster recovery, business continuity planning procedures, and increasing the company's security infrastructure. To address device management concerns, IT teams want a comprehensive, standardized solution that meets employee and corporate goals while maintaining security and stability.

But first, it is critical to understand the devices, workplace models, and infrastructure that enterprises must manage and secure. Only then, can admins determine the solution that best fits your firm.

Here are the factors that must be taken into consideration:

ENSURE THE UEM CATERS TO YOUR ORGANIZATION'S DEVICE PREFERENCES

There are 4 primary models in which devices are used in the organization, and it is important that your UEM has the provisions to properly manage them. All of them offer unique ways that can benefit your business.

Bring your own device (BYOD)

BYOD refers to using a single device for both business and personal purposes. BYOD is a standard method of mobile device management. It enables you to access the company's data and systems using your personal devices. It urges employees to bring their own devices to work and use them for sending mail, producing presentations, communicating with clients, or any other task their profession requires.

Businesses that use BYOD programs in their offices do not need to purchase new devices or carrier plans for each employee. However, the IT department faces increased pressure since it is entrusted with implementing a uniform method to ensure the security and safety of the company's data and applications.

Using a device management solution to implement a BYOD policy increases data protection and privacy. Allowing employees to use their preferred devices allows them to do work-related tasks more conveniently and efficiently. BYOD allows individuals and enterprises to work remotely in today's corporate environment. This adaptability is critical to job satisfaction and good motivation.

$350

per year, per employee

Savings made by businesses that have adopted a basic BYOD policy.

Choose your own device (CYOD)

Some businesses see CYOD as a realistic alternative for providing employees with flexibility. Because the firm provides a variety of companies or models of mobile devices and tablets for workers to use as their personal and professional devices, CYOD allows the organization greater control than BYOD. The IT staff may completely lock down and monitor the device while allowing it for personal use. This systematic approach reduces support expenditures to a minimum. Service staff only need to be educated on those devices, and using fewer device kinds and configurations means they are less costly and easier to support.

CYOD gives users the power of choice while compelling them to stay inside the boundaries set by IT. Knowing which devices are being utilized throughout the enterprise considerably enhances device management for IT. Because the devices are corporate-owned in most cases, IT may set them up safely and promptly before the device reaches the end user.

Corporate-owned, personally-enabled (COPE)

The enterprise provides COPE devices to its employees. They are usually used for corporate goals, although individuals may also utilize them for personal reasons. Organizations may choose a COPE strategy if employees still need to utilize a mobile device or are not willing to continue paying for their personal device plans.

The corporate-owned and personally enabled policy transfers management and ownership of the device to the enterprise. Employees may not have had a say in the device's making and model. It's vital to highlight that privacy is at stake with COPE devices because the organization has insight into everything that happens on the device. However, by using containerization methods to isolate work-related data from personal data, privacy can be maintained to some extent.

COPE refers to a mobility program in which the balance is weighted toward the enterprise's demands for apps, integration, and security. Still, the end user is permitted to use the device for some personal needs as well. COPE programs should employ containerization techniques to separate personal and work data and apps, like the Work Profile in Android Enterprise or the User Enrollment for iOS.

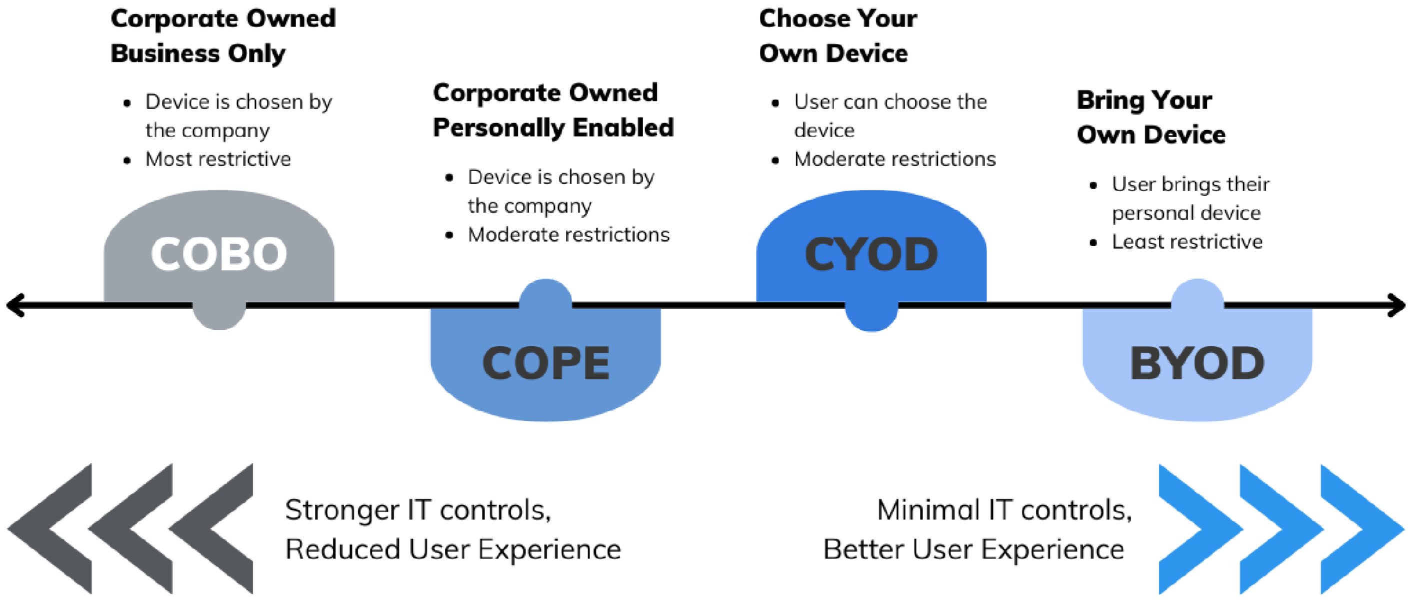
Corporate-owned business only (COBO)

COBO goes one step further than COPE by forbidding personal use of the devices. COBO is the most stringent policy for tablets, cell phones, and other devices. The gadgets are owned and controlled by the firm. The corporate-owned devices run business-only apps under a COBO policy.

While COBO devices are excellent for corporate security and productivity tracking, they severely limit user experience and eliminate the opportunity to utilize one single device for professional and personal needs.

COBO devices have the most restrictions of all device kinds, allowing IT to have complete control over how they are used, monitored, and controlled. Companies buying one device in bulk to comply with the COBO policy are likely to save a lot of money compared to other device solutions available.

Depending on their requirements, companies choose the strategy (or strategies) that best fits their firm. It also has to be ensured that the UEM solution you have or plan to have UEM complies with your chosen device strategy.


Corporate Owned Business Only
Device is chosen by the company
Most restrictive
COBO
Corporate Owned Personally Enabled
Device is chosen by the company
Moderate restrictions
COPE
Choose Your Own Device
User can choose the device
Moderate restrictions
CYOD
Bring Your Own Device
User brings their personal device
Least restrictive
BYOD
Stronger IT controls, Reduced User Experience
Minimal IT controls, Better User Experience

ENSURE THE UEM CATERS TO YOUR ORGANIZATION'S WORK MODEL

When the pandemic began, working from home became the new standard, and businesses had to adapt to maintain company continuity. Companies are now giving remote and hybrid alternatives as a retention tactic rather than for performance considerations.

Because of digital change, businesses are discovering new pathways for development and opportunity. Many sectors embrace digital offices and hybrid models to develop a dynamic workforce. Finally, digital transformation is causing industries to embrace new working methods and upskill their present workforce to meet future expectations.

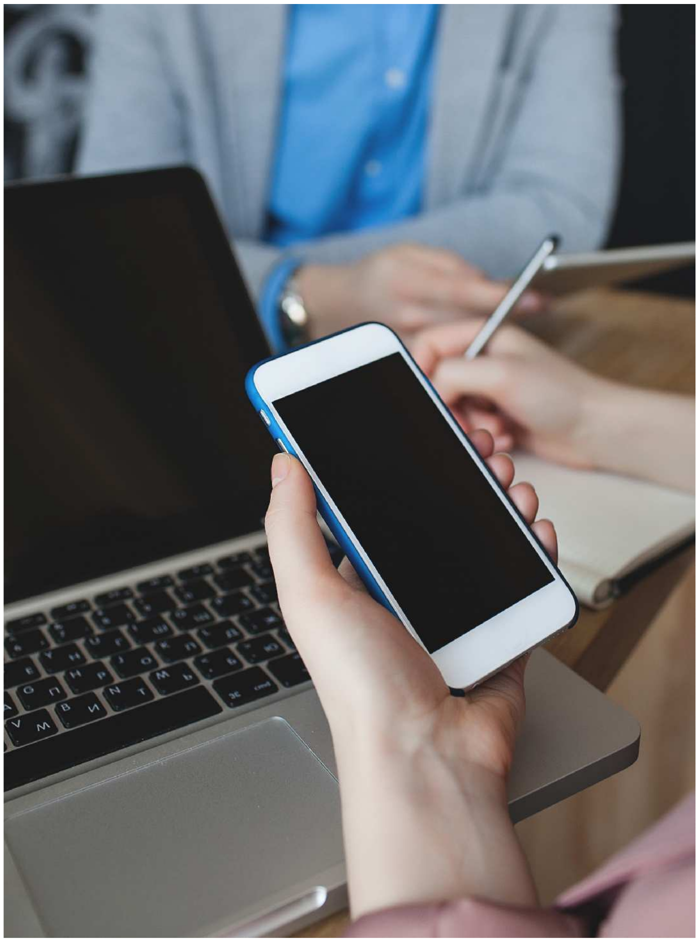
However, many firms continue to rely on on-site workforces, which is steadily changing as newer technology, artificial intelligence, and machine learning become prevalent.

On-site work model

Working in a particular area, such as a job site or an office, may give a united experience for the whole staff. Naturally, having workers work on-site fosters a deeper team relationship, resulting in an engaging working culture that employees look forward to being a part of every day. It gives everyone a better grasp of the organization's culture and a more coherent and united working experience. This concept is perfect for developing a collaborative environment among co-workers working toward similar goals and activities.

The on-site working model makes it easy to monitor and oversee employees' work. It also helps to maintain the confidentiality of sensitive information.

Furthermore, quick feedback and contact amongst professionals outside of the official team run well. Employees get easy access to company assets, equipment and facilities.



Remote work model

The employment scene changed radically and permanently when the epidemic began in March 2020. As the benefits for businesses and employees have become clear, the preference for remote work has substantially increased.

When trying to achieve a better work-life balance and considering new career options, many job seekers consider having the option of work environment and location. Employees utilize digital technologies to connect to work, engage with colleagues, and complete tasks instead of being physically present in an office environment.

As a result, organizations can access a broader and more diverse pool of talent and use this as a strategy to reduce the attrition rate. Of course, industries that require manual work cannot implement the remote work model.

Hybrid work model

The hybrid work model has emerged as the leading return-to-work strategy, with big firms such as Citigroup, Ford Motor Company, IBM, and others adopting it. A few years back, few people were familiar with this work mode, but now, it is preferred by many.

Hybrid work models differ from one firm to the next. Employees are frequently allowed flexible working hours and remote work alternatives, while a portion of the workforce operates on-site. This system is switched based on the needs of the business. The hybrid work paradigm allows the business and the personnel to benefit from both on-site and remote working techniques.

An organization might be implementing more than one workplace model for its employees. The challenge is to manage these teams and their devices efficiently. Again, choosing the right UEM solution would make this task seamlessly easy.

ENSURE THE UEM COMPLIMENTS YOUR ORGANIZATION’S SOFTWARE AND INFRASTRUCTURE

Setting up your organization's infrastructure is a crucial strategic decision. But, deciding whether to stick to the on-premise mode or switch to the cloud might be a tough choice. Organizations may adopt on-premises or cloud-based corporate mobility solutions, but first, they must weigh the benefits and drawbacks of each option. Unified endpoint management (UEM) technologies provide almost 100% feature parity to either mode, so the optimum path for enterprises to pursue is generally determined by their current infrastructure.

On-premise UEM

The UEM server is deployed within the company's servers and computers in case of on-premise UEM arrangement. The firm controls its data, software, and hardware with no third-party access. The server must be managed, maintained, and backed up independently by the firm. This deployment option lets you control your company data without needing a third party. For a long time, on-premise hosting was the only choice for businesses searching for a dependable, safe solution to host apps.

Furthermore, on-premise infrastructure needs qualified staff to administer the on-premise solution internally without contacting the provider. For example, a large firm with a qualified IT team and adequate space could choose an on-premise solution. However, most businesses need to be equipped with all of those resources.

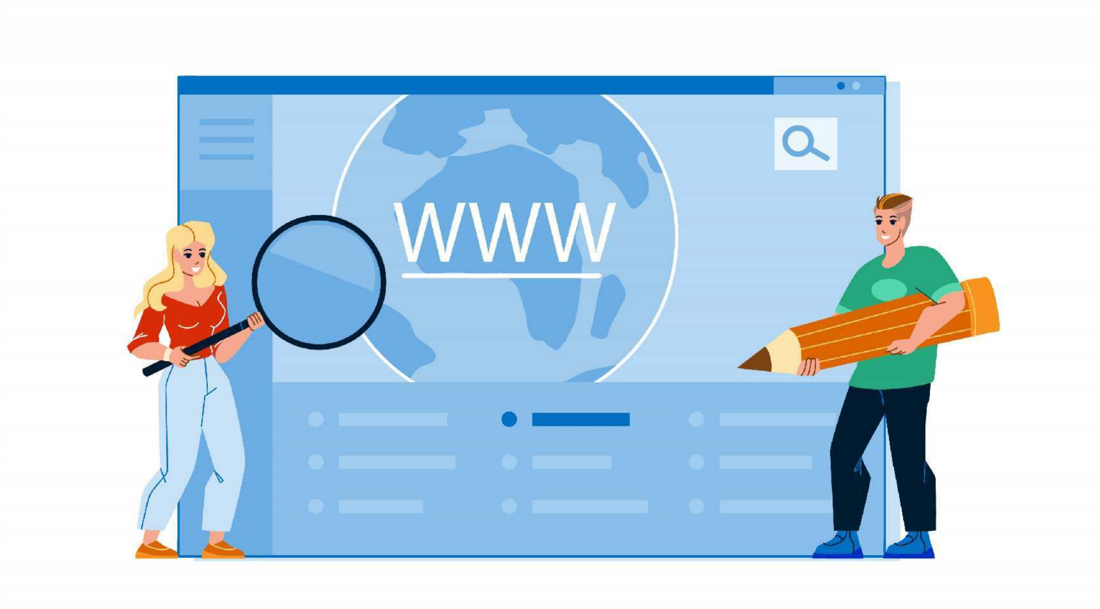
Cloud UEM

Cloud-based UEM allows you to connect to your device management vendor's server through the internet. You may enjoy the agility, comprehensive security, and flexibility of something like a subscription-based service with a cloud MDM solution. This is a ready-to-use deployment solution. It gives organizations more freedom because they don't have to worry about operating or maintaining servers.

Many large enterprises that operate several apps choose cloud-based device management services since they only pay for what they use and benefit from a quicker application rollout. The pricing gap between the Cloud and the On-premise option is the most significant. Indeed, an on-premise solution may appear reasonable at first glance, but this is because you do not see all the hidden charges driving up the price.

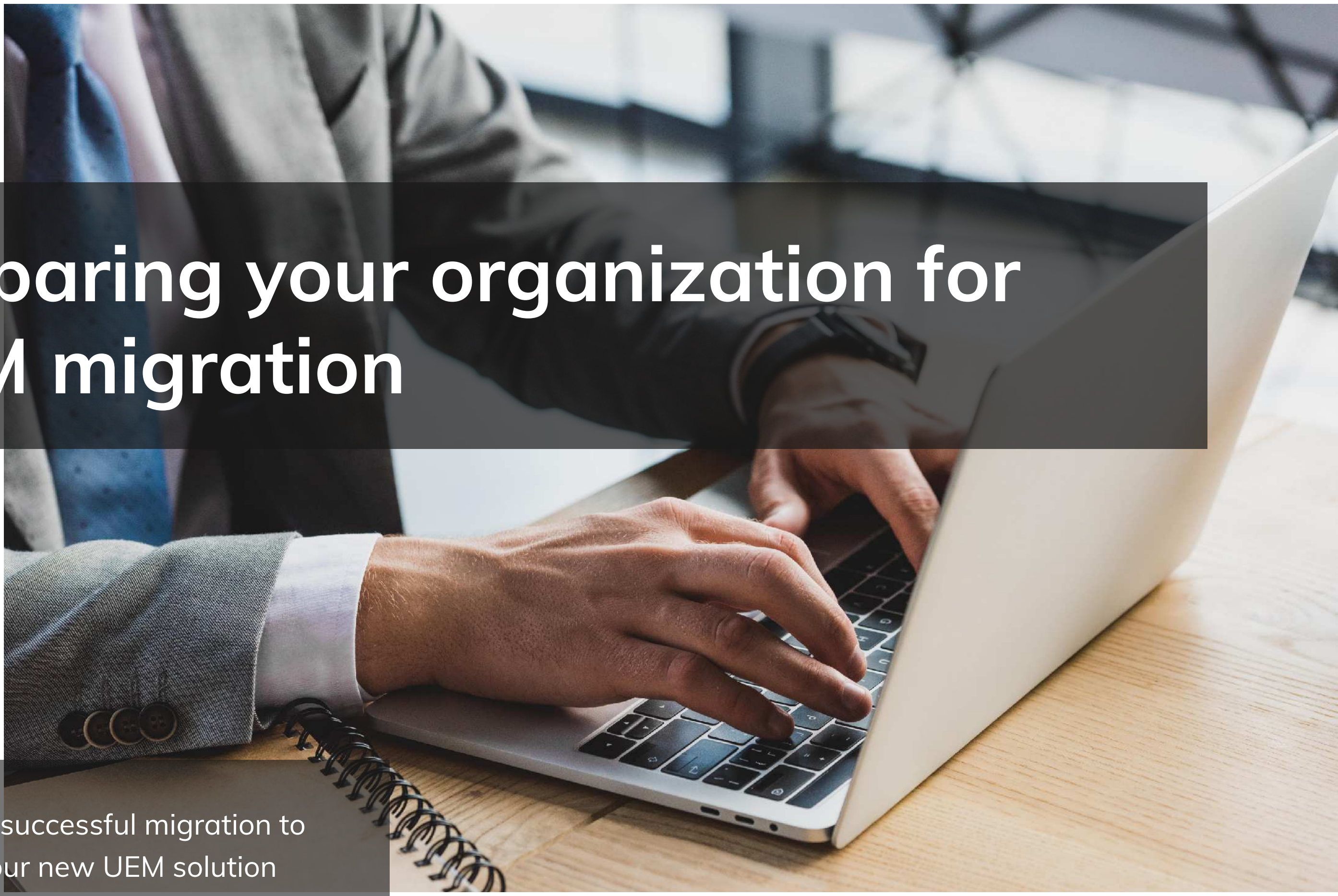
For example, spending on internal servers requires investing in the hardware and the implementation, workers, training, and maintenance expenditures. In addition, on-premise installations take longer than cloud deployments since the IT staff must set up ports, manually configure mail server settings and proxy settings, and much more.

On the other hand, setting up cloud-based deployments is not as tricky because this model is entirely housed in the Cloud, allowing employees to access corporate data from anywhere and at any time.



3

Preparing your organization for UEM migration



A successful migration to your new UEM solution starts with a well thought-out plan. This plan depends on your business environment and your technical requirements.

However, some factors remain common for all approaches. This includes developing a migration timeline to help with setting up goals, while identifying and resolving any potential delays in implementation.

Implementing a digital workplace transition can take months, if not years, and the very last thing stakeholders wants to face is a major hurdle towards the end. Unexpected problems may arise, but UEM migration should never be one of them. While leadership concentrates on higher-level challenges, IT managers frequently see the need for a simplified UEM migration solution.

Decision-makers must work directly with IT teams, end-users, and the necessary business units to implement a successful UEM migration strategy.

GENERATE A MIGRATION TIMELINE

UEM migrations involves substantial amount of planning. There are many factors that make migrations complicated for the IT team and end-users. Formulating an appropriate migration timeline can help admins gain a clear idea of the processes they must involve, and the approximate time it takes to complete each process. Here's a sample timeline to help you get started:

WEEK1	WEEK2	WEEK3	WEEK4	WEEK5
DAY: 1 Identify the need for a new UEM for your organization	**DAY: 8** Educate users on why the transition is taking place	**DAY: 15 - 16** Disenroll all endpoints from the existing UEM.	**DAY: 22** Enroll a few devices to perform a trial run.	**DAY: 29 - 31** Restore all backed up data to the devices and check for any failed action.
DAY: 2 - 6 Find a suitable UEM based on what your organization needs.	**DAY: 9 - 10** Document your present workflow and create a list of all your users and devices.	**DAY: 17 - 18** Create admin accounts and assign them roles, migrate all necessary tokens and certificates	**DAY: 23 - 24** Perform a testrun by creating and enforcing policies.	**DAY: 32- 35** Enforce monitoring policies and set support channel.
DAY: 7 Purchase your new UEM and familiarize yourself with the new features	**DAY: 11 - 14** Backup all existing data, and remove all third-party integrations.	**DAY: 19 - 21** Collect the devices and prepare them for the enrollment process.	**DAY: 25 - 28** Enroll all devices, push the policies and sync the third party integrations with the new UEM	

PREPARE END-USERS FOR THE TRANSITION

While UEM migration is technically complicated, it is more of a people problem than an IT challenge. It is important to groom the end-users and keep them well prepared for the transition

Educate them on why this transition is taking place

Some people don't prefer change, especially when it involves moving out of their comfort zone. It is tricky and essential to explain the motive behind switching UEM to the end-users. Leaders should be able to explain how it would benefit each of them in the long run.

Provide a timeline for the process

These changes can take time to happen. For example, re-enrolling a device could take a couple of hours, and management usually underestimates the actual extent of the operation while overvaluing the IT team's and current infrastructure's capabilities to support that move. Two hours per device equates to several months of downtime for a complete enterprise fleet, even if we don't consider each employee's delay while making the switch.

Therefore, it needs to be a well-thought-out process and providing your end-user with a timeline of the migration helps them to be aware of the steps that would follow.

Describe what users can expect throughout the migration

The purpose of providing a timeline for the migration process is to let the users know what to expect throughout the migration. They should be able to continue their regular work while the migration is happening. At the same time, they also need to be involved with the migration process if and when required.

Explain what a user’s role is in the process

The end-users should know their part in the transition process. Only if they know their part can the process happen smoothly. Furthermore, once the migration is over, the user should know how to work with the new UEM. The management should be responsible for educating them and letting them know their part. Clear communication across different management levels is vital for a seamless UEM transition.

CREATE A MIGRATION CHECKLIST

While undertaking UEM migration, preparing and following a migration checklist can provide admins with the insight and confidence necessary to simplify the migration process. The checklist should provide a brief overview of the general steps involved to prepare for UEM migration. Here's a sample for reference:

1: Have you prepared a list of your user and devices?

A list of all the devices and users should be prepared. This would help keep track during the entire off-boarding and on-boarding procedure. In addition, this would help ensure that all devices and users are included during the migration process.

2: Have you documented your present workflows?

Documenting your current workflows is essential as it helps to retain how the business is running presently. In addition, once the new UEM is running, referring to these workflows would help to configure the policies and the new workflow even better.

3: Have you made a backup of your essential data?

The last thing you would want is to lose your critical business information. Backing it up in the Cloud is a safe way to retain your data. In addition, it is easily retrievable when you need it.

4: Have you prepared the devices, policies and configurations for the new UEM?

The devices have to be prepared for enrolling in the new UEM. Configurations and data of the previous UEM should no longer be present as they might show errors during enrollment. The policies and configurations should be prepared beforehand to push as soon as the devices get enrolled to the server.

5: Have you set up a support team to assist and troubleshoot migration issues?

Unexpected errors might pop up during or even after the migration is over. Companies need to have a dedicated support team to help take care of these issues. In addition, they should be able to assist in troubleshooting the issues when needed.

4

The 3 phases of UEM migration

The overall UEM migration process comprises of 3 distinct phases.

- Phase 1: Pre-Migration
- Phase 2: Migration
- Phase 3: Post-Migration

PRE-MIGRATION PHASE

The pre-migration phase is where admins must evaluate their current device management strategies, identify the areas that require improvement, and formulate updated strategies they plan to implement once migration is complete.

Here's a detailed list of steps IT executives must undertake to prepare their organization for UEM migration.

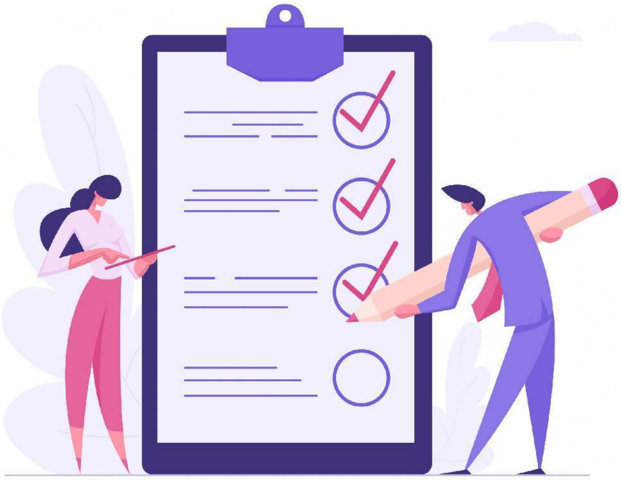
Admins should prepare their environment for UEM migration, take inventory of all the assets, tools, and resources that are present in their current ecosystem, and backup all essential data before going ahead with the migration process.

Here's the detailed list of steps involved during the pre-migration phase.

Step 1: Create a list of users and devices

The first step in preparing for UEM migration involves identifying the different device platforms and operating systems you will need to support, and determining which devices are to be corporate-owned, or personally-enabled.

You must then identify the number of individual devices along with their users, and determine which devices are to be used in a shared environment. You must also group these devices/users based on their departments and/or any other criteria in your organization.



Step 2: Define your enrollment strategy

Step two involves determining your enrollment strategies based on your enterprise device environment. Does your organization support corporate devices, BYO devices, or is it a mix of both? You must identify who is going to carry out the enrollment process - is it the IT team, or the end-users? If it’s the end-users, you must provide technical assistance, and generate support documents to guide them through the enrollment process.

You must also determine if your organization supports zero-touch deployment strategies. If yes, you must identify the right methods and/or vendors to provide a seamless out-of-the-box experience for your end-users. Some popular zero-touch enrollment techniques include - Apple Business Manager (ABM), Apple School Manager (ASM), Google Workspace, Samsung Knox Mobile Enrollment (KME), and Windows Autopilot.

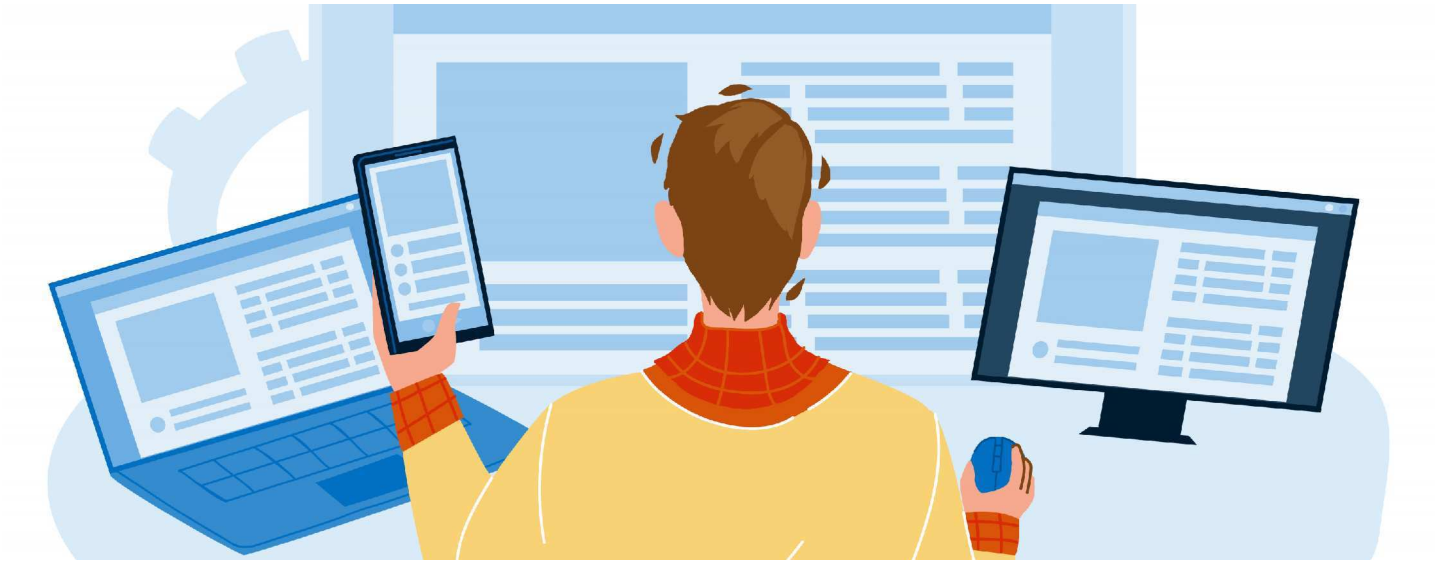
Step 3: Evaluate and document existing device management workflows

This step involves identifying your current device management policies and determining if it meets the device and data security requirements of your organization.

You must review your existing UEM solution's strategies and identify areas that need improvement. You must then update your current policies based on the results you receive, and list out the features you require from the new UEM. Once you've reviewed your options, determine the suitable device management strategy in the new UEM.

Step 4: Back up all important data to your preferred cloud service

Migrating devices usually requires an initial factory reset. Ensure you backup all critical business data on to a cloud storage service before wiping them. Moreover, certain apps sync data on the local storage as opposed to the cloud. Identify such apps in your inventory and perform the necessary actions to backup important data to the cloud. Here are several types of data that might be on the device, which you must back-up: Photos, notes, messages, apps and app data, critical resources and files.



Step 5: Maintain an inventory of all necessary certificates, usernames and passwords

When migrating from your existing UEM, you must create a detailed inventory of all the certificates, tokens, and user accounts that are linked with your existing UEM. This includes, security certificates such as Wi-Fi and VPN profiles, identity configurations including Google/iCloud, email, ExchangeActive accounts, workflow objects such as scripts, packages, configuration profiles, and more.

Step 6: Identify and disconnect all third-party integrations and external connections from the current UEM

This step involves identifying and documenting your existing UEM integrations such as your Microsoft Active Directory accounts, Google Workspace, Apple School Manager (ASM)/Apple Business Manager (ABM) accounts, your configured Apple Push Notification Services (APNS) tokens, and more.

Once you've taken inventory of all third-party integrations and external connections, you must disassociate them with the current UEM solution and prepare them for the migration process.

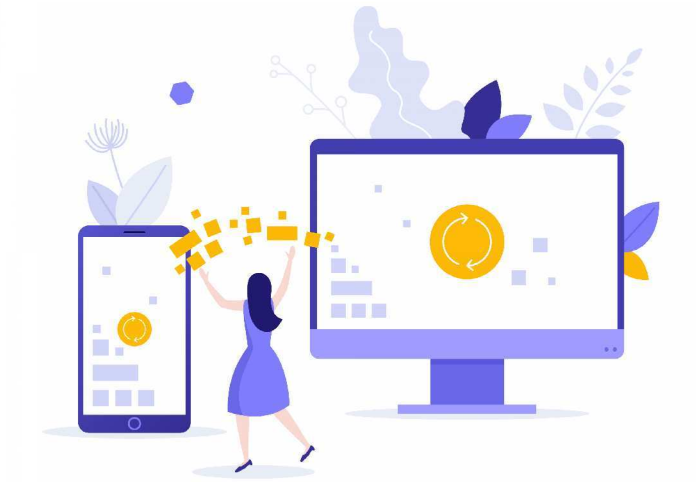
Step 7: Remove all assets from the current UEM and prepare for transitioning to the new UEM

The final step involves dissociating all your assets - including the managed applications, software, resources and endpoints – from your existing UEM solution, and preparing them for migration to the new UEM.

MIGRATION PHASE

Once the preparations are ready, it's time to begin migration. You must set up the UEM portal (the steps involved in setting it up may vary depending on the vendor). Then, you must configure the UEM settings to fit your organizational needs.

Once configured, you must import the users, devices, apps, resources, certificates, and more. Finally, perform a test rollout with a few devices before going all-out.



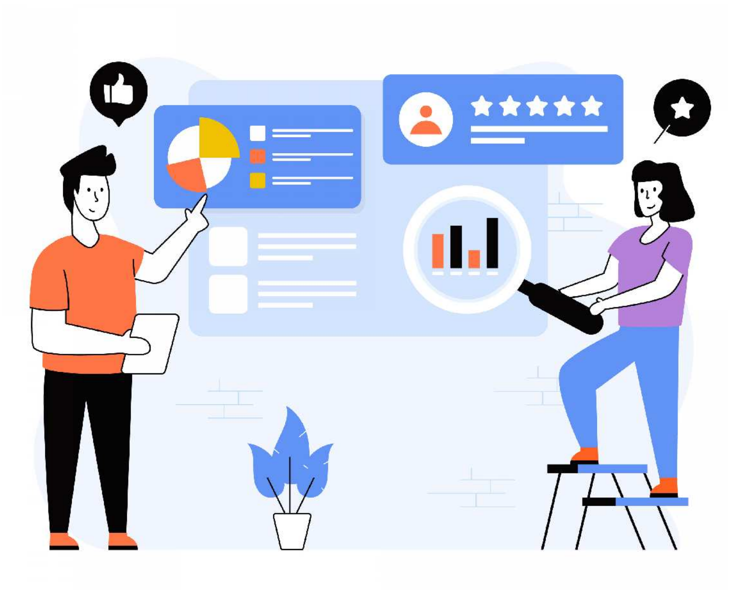
Step 1: Create admin accounts in the new UEM and assign them with the right roles

The first step to kicking off the migration process involves the creation of admin accounts in the new UEM. If you have multiple technicians to manage your UEM portal, you must then create additional technicians and assign them with the appropriate roles.

When assigning roles to technicians, first, determine the permissions that should be available. These permissions specify various functionalities that the technician can view or modify. Some UEMs also offer the ability to create custom roles based on the needs of an organization, and assign them to specific technicians. The best practice is to ensure that each technician is assigned with just the necessary roles and permissions to perform their specified tasks.

Step 2: Configure UEM settings, migrate tokens, and sync your native/third-party accounts with the new UEM

Next, you must configure the admin settings for the UEM, such as the email settings, SMS settings, and more, and migrate your third-party integrations and external connections, along with your security certificates, identity configurations, workflow objects, and more, (which was previously documented in 'pre-migration - step 5 and step 6'), to your new UEM solution.



This will sometimes require you to create new tokens (especially for APNS, ABM/ASM), renew specific certificates, and repeat the steps to reconnect your third-party services to the new UEM.

Step 3: Import all the necessary apps, resources, and tools to the new UEM

This step involves uploading all the software, applications, and resources that were removed from the previous UEM, to the new UEM solution. Make sure to set up the appropriate configurations for the app and content repository, enforce the necessary application groups, and manage permissions and controls for the uploaded apps and resources.

Step 4: Import all your users and groups to the new UEM

Next, it's time to add all the necessary users to the new UEM solution. Make sure to assign the users to the right groups based on their departments and/or any other criteria in your organization. You can also import users and user groups to the UEM portal by integrating with your Directory service.

Step 5: Pre-approve your endpoints and prepare for enrollment to the new UEM

Many UEM solutions offer the option to pre-approve your devices, enabling admins to import devices into the UEM portal even before the enrollment is performed. Admins can then assign the necessary policies and configurations on these pre-approved devices, which will automatically take effect when the devices complete enrollment.

Step 6: Create and enforce policies and configurations for your users and devices

This step involves enforcing the necessary policies and configurations to successfully implement your organization's device management strategy in the new UEM. Admins must create platform-specific policies for all their devices, and enforce appropriate configurations for both BYOD and corporate endpoints.

Step 7: Perform a test rollout with a few devices

It is important to allot time for testing throughout the migration process to help admins catch any potential issues before the devices are completely migrated. Admins must perform a test rollout with just a few sample devices from all platforms.

This will also help you to validate your migration plan and ensure that you've accounted for all use-cases and variables. This includes testing on BYO devices, corporate devices, on older operating systems, and more. Once all the potential issues have been ironed out, it's time to deploy your strategy at scale.

Step 8: Enroll all your endpoints to the new UEM

Once you've set everything up, it's time to enroll your devices. Make sure you've integrated with the necessary deployment platforms, including Google Workspace, Android Enterprise, Samsung KME, Android ZTE, ABM/ASM, and/or Windows Autopilot. Then, enforce the necessary configurations and enroll the devices. If the enrollment must be done by end-users, send the appropriate enrollment instructions to users, and give a deadline for completing the enrollment process.

POST-MIGRATION PHASE

Migration doesn't end with simply enrolling devices to the new UEM server. You must compare your device inventory from your previous UEM with the device inventory in Hexnode to confirm that all endpoints have been successfully enrolled.

You must restore your users' previously stored backups; you must set up appropriate channels to help users with migration issues. The UEM migration process can be marked successful only after resolving any such issues.

Step 1: Monitor the enrollment process

Check your UEM portal to see the list of enrolled devices. Ensure that all devices have been successfully enrolled. There is a possibility that some of the device enrollments may end in failures. In such cases, you troubleshoot the issue, or identify and adopt easier enrollment techniques for these devices, as a workaround.

Step 2: Restore the data backups on the devices

Once the devices are successfully enrolled in the new UEM, the backed-up data that's stored in the preferred cloud server can be restored to the devices, to ensure a smooth and productive workflow while avoiding any loss of data.

Step 3: Monitor devices and enable periodic compliance checks

Device compliance with organizational policies must be monitored by admins. The most effective way to do that is through routine compliance checks. Admins must enforce policies to monitor compliance, identify instances of non-compliance, and automate remedial actions on the newly enrolled endpoints.

Step 4: Schedule appropriate auditing and reporting workflows

Scheduling appropriate inventory checks, and performing regular audits and reports is key to a successful migration. Admins must generate a wide range of reports to monitor device enrollment, app installation, network traffic during migration, and more.

Step 5: Set up dedicated support channels to receive user feedback and troubleshoot migration issues

Admins must maintain a dedicated support channel to gather information from users on potential issues that may arise, before, during, or after migration, and perform troubleshooting operations to resolve the issues ASAP.

In order to get user feedback on the migration process, administrators can launch a post-migration survey.

5

How to migrate your endpoints to Hexnode UEM

Hexnode is a SaaS company headquartered in San Fransisco specializing in providing Unified Endpoint Management (UEM) solutions to companies worldwide.

Hexnode's customers range from small and medium sized businesses to Fortune 500 companies

While UEM migration may seem complex, choosing the right solution helps you streamline the process significantly. Hexnode UEM is designed to minimize complex configuration steps, thus enabling administrators to easily migrate and deploy managed devices.

However, it must be noted that the migration process is not exactly the same for all the device platforms. Managed devices usually fall under three catagories: Apple devices (iPhones, iPads, macOS devices, Apple TVs), Android or Windows devices.

Let's have a look at the migration steps for these device platforms.

COMMON ENROLLMENT OPTIONS

Hexnode offers a host of quick enrollment options that lets admins enroll iOS, macOS, Android, Fire OS, and Windows devices to Hexnode UEM via a single enrollment URL or application. Here are the options available.

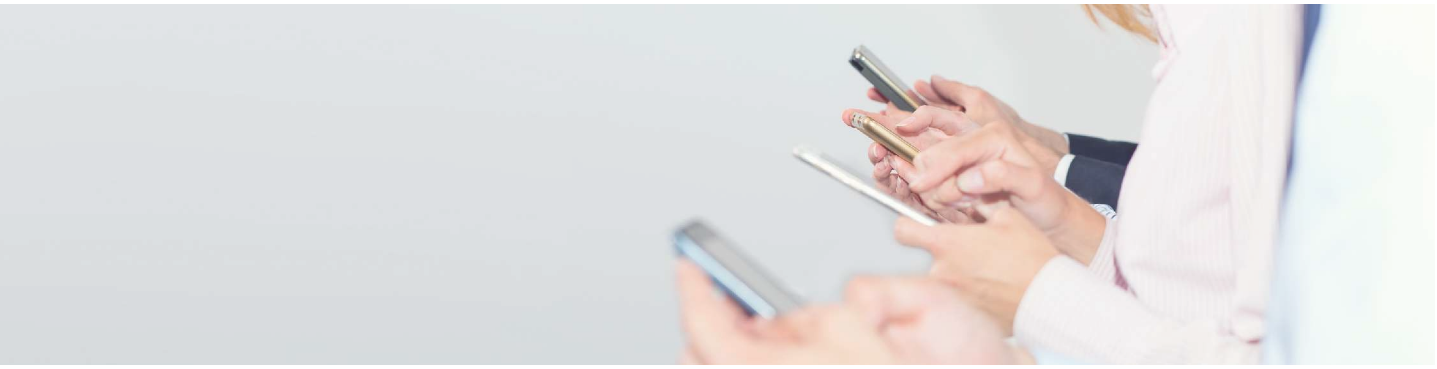
However, it must be noted that device management capabilities may be limited when enrolling devices via these methods. *(Except in the case of pre-approved enrollment. Here, the device management capabilities available would depend on the enrollment method that's adopted along with the pre-approved enrollment technique.)*

Open enrollment: This enrollment technique enables users to enroll their devices without providing any authentication credentials.

Email/SMS enrollment: This enrollment method delivers an enrollment request via email or SMS to the users which includes the enrollment URL, username, password, and a QR code.

Self enrollment: Self-enrollment is a type of authenticated enrollment by which users will enroll their devices using their preassigned passwords (for local users) or their directory passwords (for AD, Azure AD, Okta and Google users)

Pre-approved enrollment: Pre-Approved enrollment enables admins to import devices into Hexnode UEM, even before the enrollment process is completed. Admins can proactively group devices and assign policies with all the configurations, restrictions and apps. Upon enrollment, the policies automatically take effect on the devices. This enrollment method must be used in combination with a device enrollment technique such as DEP, or standard enrollment. *(Pre-approved enrollment is not supported on Android 10+ and Windows.)*



MIGRATING APPLE DEVICES

Migrating Apple devices (macOS, iOS/iPadOS, tvOS) from one UEM solution to another often involves the reassignment of tokens and certificates for services such as, Apple Push Notification service (APNs), Automated Device Enrollment (DEP), Apple Apps and Books (VPP), and more. Let's take a look at the steps involved.

- **Step 1:** Disenroll the Apple devices and remove the APNS, DEP and VPP accounts configured in the current UEM.
- **Step 2:** Create an APNS certificate for Hexnode UEM. To do this, create and download a Certificate Signing Request from the Hexnode portal.
- **Step 3:** Go to Apple Push Certificates Portal, upload the self-signed certificate and download the APNs certificate generated by Apple.
- **Step 4:** Upload the APNs certificate back to the Hexnode UEM portal.
- **Step 5:** Migrate your organization's DEP and VPP tokens to Hexnode UEM. Your DEP token keeps a record of your organization's devices and your VPP token keeps track of all app purchases.

Now, admins can enroll the devices as either supervised or unsupervised devices (as required) using a suitable enrollment method.

Automated Device Enrollment

Automated Device Enrollment (Apple DEP) helps in deploying Apple devices in bulk, by automatically applying settings and configurations upon the initial device start-up. These devices are then made ready for use right out of the box. Over-the-air supervision of these devices is possible only if they are enrolled in ABM/ASM.

Requirements

Your organization must be enrolled in ABM/ASM
Devices must have been purchased on or after 1st March 2011
Device must be running an operating system that meets the following requirements:

- *iOS 7 or later (for iOS devices)*
- *OS X 10.9 or later (for Mac devices)*
- *tvOS 10.2 or later (for Apple TV)*

Hexnode Onboarder for Mac

The Hexnode Onboarder app enables you to easily migrate your macOS devices enrolled in another MDM, to your company's Hexnode portal. Admins can generate a custom PKG file from the Hexnode console and specify the Hexnode Onboarder settings, along with any optional network configurations. The Hexnode Onboarder app can also automatically detect device capabilities and initiate either standard or Automated (DEP) enrollment.

User Enrollment for iOS and iPadOS

User Enrollment is a feature offered by Apple that helps organizations manage personally-owned iOS/iPadOS devices. With User Enrollment, the iPhone introduces a separate volume on the device that contains managed apps and data. All it requires is a Managed Apple ID to authenticate the enrollment. Being a BYOD-specific feature, User Enrollment supports only a limited set of payloads and restrictions on the device. However, with the end-user's permission, you may install the Hexnode UEM agent on the iOS/iPadOS device (using VPP app licenses) to achieve advanced device management capabilities.

Requirements

The iOS/iPadOS device must be unsupervised and running iOS 13.0+ or iPadOS 13.1+.
User Enrollment requires Managed Apple IDs to authenticate the user for device management.

Enrollment via Apple Configurator 2

Apple Configurator 2 is a macOS app that enables admins to deploy iPad, iPhone, and Apple TV devices for businesses, by creating and pushing configuration profiles to the devices. You can supervise iOS devices with Apple Configurator. Apple Configurator 2 enables you to add iOS and tvOS devices to ABM/ASM. You can also use Apple Configurator for iPhone to add macOS devices to ABM/ASM.

Requirements

Apple Configurator 2 for macOS runs on devices with OS 10.15.6 or later.
Supported devices:

- *iOS devices running OS version 6 or above (requires iOS 11.5+ to add to ABM/ASM).*
- *Apple TV (2nd generation or later).*

Apple Configurator for iPhone runs on devices with iOS 15 or later.
Supported devices:

- *macOS 12 Monterey with Apple M1 Silicon or T2 Security chip*

MIGRATING ANDROID AND FIRE OS DEVICES

When migrating Android/Fire OS devices from one UEM solution to another, you must consider the reassignment of certificates for services such as Google Workspace (G Suite), Android Enterprise, Samsung KME, and Android ZTE. Here are the steps.

- **Step 1:** Disenroll the Android devices and remove the Google Workspace (G Suite), Android Enterprise, Samsung KME, and Android ZTE accounts configured in the current UEM.
- **Step 2:** Configure Google Workspace in Hexnode UEM by uploading the JSON key downloaded from the Google Developers Console.
- **Step 3:** Next, paste the EMM token generated from the Google Admin Console. Your organization will be enrolled in Android Enterprise program using the Google domain.
- **Step 4:** Go to Knox portal and create a new UEM profile with your Hexnode UEM server URL in the MDM server URI column. Provide other profile details and URL for the Hexnode UEM APK in the MDM Agent APK column.
- **Step 5:** Sign in to Zero Touch Portal and click on Add MDM configuration, select Hexnode for Work app from the list of EMM apps and provide the JSON data available in the Hexnode UEM portal.

Now, admins can enroll Android devices to Hexnode using a suitable enrollment method.

Android Enterprise enrollment

Android Enterprise is an initiative developed by Google that enables the use of Android devices and applications in the work environment. It provides a set of consistent APIs to manage and secure Android devices for corporate usage.

Corporate devices can be enrolled as a device owner and personal devices as a profile owner in the Android Enterprise program either using the managed domain or google domain.

Requirements

Samsung Knox devices: Android version 6.0 and above, or Knox SDK 2.6 and above.
General Android Devices: 5.0 and above

Android Zero-Touch enrollment

Android ZTE is a secure device deployment method that's used to enroll corporate-owned devices without manually configuring each of them. It is an out-of-box enrollment method where the devices will be enrolled in the UEM once it is powered on and connected to the network.

Requirements

- *Google account associated with corporate email. Ensure that you don't use your personal Gmail account.*
- *Devices should be purchased directly either from a Zero touch reseller partner / Google partner and not from a consumer store.*
- *Phones/tablets should be running Android 9.0 or above*
- *Ensure that the device is compatible with ZTE from the list of Android Zero Touch Devices.*

Samsung Knox Mobile Enrollment

Samsung Knox Mobile Enrollment (KME) helps in deploying supported Samsung Knox devices in bulk, by automatically applying settings and configurations upon the initial device start-up. These devices are then made ready for use right out of the box. It is also possible to enroll Samsung Knox devices via KME to Hexnode using the Knox Deployment App (KDA).

Requirements

- *Devices running Knox version 2.4 or higher support Android Device Admin enrollment using KME.*
- *However, Knox Mobile Enrollment no longer supports Device Admin on Android 11 or above.*
- *Knox devices above 2.7.1 purchased from a reseller participating in the Knox Deployment Program (KDA), will support Knox Mobile Enrollment (KME) using the Knox Deployment app.*
- *Knox devices running Knox version 2.8 or higher can support Android Enterprise Device Owner enrollment using KME.*
- *Knox devices running Knox version 2.8 or higher, along with an Android 10+ Operating System, will be able to support Android Enterprise Profile Owner enrollment using KME.*

MIGRATING WINDOWS DEVICES

Windows devices have been around for a long time. When migrating Windows devices to a UEM solution, admins must consider several key elements – Especially when migrating from legacy management software. Here are the steps to follow.

- **Step 1:** Disenroll the Windows devices from the current UEM.
- **Step 2:** Create a .ppkg file using Windows Configuration Designer to enable large scale roll-out of Windows 10 devices. If using SCCM, Unbind your current UEM from SCCM and integrate Hexnode UEM to sync the devices from SCCM server to the Hexnode portal.

Enrollment via Provisioning Package (PPKG)

Using Windows provisioning, administrators can quickly and seamlessly set up the configurations and settings required for the Windows enrollment process. A provisioning package file (.ppkg) is a container for a collection of configuration settings. It can be created using a Windows 10/11 device, which can later be used for the bulk enrollment of Windows devices without any user intervention.

SCCM migration

Microsoft's System Center Configuration Manager (SCCM) is a system management software that manages devices and servers, either included within your network or in the cloud. Hexnode's integration with SCCM helps in migrating the Windows devices from the SCCM server to Hexnode.

Co-management

Co-management enables Windows devices enrolled in another UEM solution to be concurrently managed by Hexnode UEM. Such devices are provided with conditional access to the device management functionalities supported by Hexnode. Co-management is one of the primary ways to streamline migration to Hexnode from other UEM vendors.

Requirements

Co-management is supported on:

- *Windows 10 v1803+*
- *Windows 10 v1703 to Windows 10 v1709 (if .NET Framework v4.7.1+ is installed)*
- *Windows 11*

Conclusion

The beginning of the 21st century heralded the era that has seen the fastest-changing communications and technology landscape. Suffice to say, business security also undergoes a near-constant change. Consequently, the advent of technology to make life easier also brought in scope for exploitation and an incessant need for better data protection and devices.

This is a world of constant change, a very cliched way of looking at the world and yet an honest observation. This need to constantly change has seeped into every aspect of life, especially the business world.

A heightened need to protect corporate data and devices has indeed resulted in a boom in the UEM markets. But with the wide variety of options comes great confusion about what to choose. The key to solving this confusion is knowing your requirements and what made you want to switch UEM solutions in the first place. Once the requirements are listed out, it's all a matter of aligning them with the features offered by the different contenders and choosing the best fit.