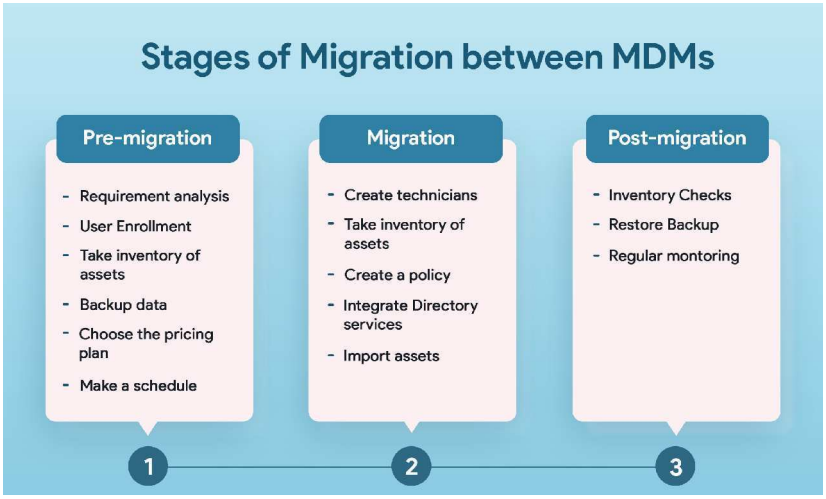
How to migrate managed devices between UEMs?

Managing devices for the enterprise has been considerably made easier with the advent of Unified Endpoint Management (UEM) solutions. While there are many options to choose from in the market, it is essential to choose the right one for your business. It is possible that your business needs have already outgrown your existing UEM. Migrating the managed devices between UEMs can seem like an exhausting task. However, it becomes a necessity in some cases.

When should you migrate from your existing UEM?

- Requirements are not met by the current UEM: The business and enterprise needs are constantly evolving. For example, if you are using an Apple device management solution, you would not be able to manage Android or Windows devices. Choosing a UEM with cross-platform support like Hexnode would let you manage all the devices under a single remote Web portal.
- The simplicity of use: Simplistic UI and ease of use is always desirable option. If the existing UEM is a complex solution demanding too much precious time, it makes sense to move on to a better solution.
- Financial Planning: The existing UEM could be too pricey considering your requirements. Switching to a lower-priced UEM with the required functionalities is a viable option in such a scenario.
- Product support: A good UEM is characterized by not only its functionalities and ease of use but also the support quality it offers. A live and hands-on support is a desirable option for easy troubleshooting.
- Scalability of the UEM: For growing businesses, the scalability of the UEM is a very important factor. The UEM solution should be able to accommodate any number of devices without any disruption in its services.

The Three Stages of Migration



Migrating all the managed devices to a new UEM seems like a daunting task. The process is actually simple if you follow a concrete plan. For reference purposes, we have assumed the new UEM to be Hexnode. There are three stages in migrating the managed devices:

1. Pre-migration: What to do before migrating your devices?

- Requirement Analysis: To decide on a new UEM, a detailed requirement analysis must be done. The different requirements can be categorized on the basis of how important they are.
- Testing the new UEM with a few devices: Before conducting a mass migration, testing with a few devices is absolutely necessary. Most of the UEM solutions provide a free trial during which you can test out the features and support before making a decision.
- Inventory of devices and users: The admin needs to make an inventory of all the devices and users to be migrated. Details such as the OS platform of the different devices and the number of devices used by a single user should be taken into consideration.
- Backup important device data: Migrating the devices often results in an initial factory reset of the device. Hence, it is important to backup the essential device data before the migration.
- Decide on the right plan for the organization: The UEM solutions provide different tiers of pricing plans. Identifying the requirements and choosing the pricing plan suited to those needs is an important step.
- Make a schedule for migration: Planning is an important phase in migrating the devices. A proper strategy and schedule has to be defined with a logically achievable timeline.

2. Migration: Steps to follow while migrating your devices

- Create the technicians/administrators in the new UEM: If there are multiple administrators for your organization, create the technicians and assign proper roles to them.
- Configure UEM settings: Before enrolling the devices, the UEM settings such as email and SMS settings have to be configured in the Web Portal.
- Create a policy with the required settings: A policy can be defined with the required settings such as Wi-Fi and VPN settings, app settings and configurations, and certificates to be installed on the devices.
- Integrate Directory services: For easy enrollment and policy assignation, the administrator should integrate the Active Directory and Azure AD with Hexnode.
- Import users and devices: The devices and users have to be removed from the existing UEM and imported into the new one. The process varies for different OS platforms.

3. Post Migration: The work after migration

- Inventory checks: The admin should make a detailed comparison between the initial inventory of the devices and users exported from the previous UEM for checking if all the devices have been enrolled properly. With Hexnode, the admin can make use of the reports for this purpose.
- Restoring backup: Now that the devices are successfully enrolled in the new UEM, the important backups can be restored to the devices to ensure smooth working flow and avoid any loss of data.
- Regular monitoring: The job is only half done after the migration. The devices should be regularly monitored for any misbehavior. Regular and scheduled device scans ensure that the device is checking in with the UEM server. Lost devices can be either put into Lost Mode or entirely wiped remotely.

Migration for different OS platforms

The migration process is not exactly the same for all the device platforms. The managed devices usually fall under three categories: Apple devices (iPhones, iPads, macOS devices, Apple TVs), Android, or Windows devices. Let's have a look at the migration steps for these OS platforms

Migrating Android devices between UEMs

1. Remove the devices and users from the current UEM by disenrolling the devices and backup the device data.
2. Configure GSuite, Samsung Knox Mobile Enrollment, Android Zero-Touch Enrollment, and Android Enterprise as per your requirements.
3. Sync users from the Active Directory to Hexnode UEM.
4. Enroll the devices into Hexnode UEM using a suitable enrollment method.

Enrollment methods for Android devices

There is no dearth of enrollment methods for Android devices with Hexnode UEM. The devices can be enrolled using no-touch enrollment methods like Android Zero-Touch Enrollment or Samsung Knox Enrollment. Android phones and tablets can be enrolled without any authentication or with authentication. The admins can send an enrollment request via email or SMS to the users with the credentials required for authentication. For a few devices, the admins can simply scan the QR code in the web portal for enrolling the devices. The users can also go for self-enrollment and authenticate with their AD/Azure AD/User credentials.

Migrating Apple devices between UEMs

1. Disenroll the Apple devices from the current UEM. Wipe the devices after backing up the data and delete the Device Enrollment Program (DEP) account configured in the current UEM.
2. Create DEP and VPP accounts for your organization.
3. Migrate the APNs certificate, DEP, and VPP tokens to Hexnode UEM.
4. Sync the users from the Active Directory to Hexnode UEM.
5. Enroll the devices as either supervised or unsupervised devices as required using a suitable enrollment method.

Enrollment methods for Apple devices

For the automatic enrollment of Apple devices, configuring Apple DEP is essential. Using the Apple DEP, the Apple devices can be enrolled over the air using just the serial number or the order number of the devices. The Apple devices would be automatically enrolled in Hexnode UEM on their initial setup.
There are also enrollment options like open enrollment using just the enrollment URL, self-enrollment, and email/SMS enrollment for authenticated enrollment.

Migrating Windows devices between UEMs

1. Back up all the required data of the Windows devices. Remove all the management profiles and users from the current UEM. Disenroll the device from the current UEM by using either the disenroll action or removing the device management profile from the settings.
2. Sync the users from the Active Directory to Hexnode UEM.
3. Unbind the current UEM from Microsoft's System Center Configuration Manager (SCCM) and integrate it with Hexnode UEM to sync the Windows devices from the SCCM server.
4. Enroll the Windows devices using either bulk enrollment or Email/SMS enrollment.

Enrollment methods for Windows devices

To bulk enroll Windows 10 devices into Hexnode, the admin can go for ppkg enrollment or bulk enrollment with CSV import. In ppkg enrollment, a customized ppkg file created using the Windows Configuration Designer is applied to the device for enrolling it in Hexnode. The enrollment options like self-enrollment with the AD credentials, open enrollment using server URL and email address, and enrollment using the credentials received via email or SMS are also available for Windows devices.

There are numerous options in the market for endpoint management. There is no need to settle for a UEM that does not satisfy your requirements. Businesses evolve and so does the enterprise mobility management industry. It is not advisable to be stuck with legacy UEMs that do not get updated with the changing times. It may not be the easiest solution to change the UEM solutions but it can be of benefit, in the long run, depending on the enterprise's needs. Migrating between UEMs would cease to be a herculean task if you get proper resources and support. It is also essential to have clear communication with the end-users about the migration process. The empowerment and inclusion of users lead to a smoother transition and higher acceptance of the device administration.