Migrate your devices from Sophos Mobile to Hexnode UEM

Introduction

With a rapid rise in the never-ending technological advancements, the device management needs of your organization may continuously change. Hence, there's a good chance that your current device management solution may fail to satisfy your growing business needs. In that case, the best thing you can do is to switch your Mobile Device Management (MDM) vendor.

There are plenty of reasons why organizations migrate from one MDM to another. Overpriced plans, inefficient support, complicated steps, and cloggy UI are major reasons why enterprises think of migration.

Why Hexnode UEM?

If your current MDM does not meet your business goals or technical requirements, migrating to a more flexible and robust solution is always better. Hexnode, the award-winning UEM solution, helps you cover every feature for comprehensive device management.

Here's a list of Hexnode features that you've been missing out on your current vendor:

Unified management of devices: Hexnode manages all your endpoints from a single centralized console. It employs a holistic approach to control all endpoints and apps across the organization.

Multiple OS support: Hexnode extends its management capabilities to support almost all major platforms, such as Android, Windows, iOS, macOS, Fire OS, and Apple TVs.

Security: Hexnode secures your digital workspace without compromising the user experience. It includes a multitude of security features to secure apps, networks, and devices.

Zero learning curve: Hexnode is designed to minimize complex configuration steps, and thus, it has a gentle learning curve. Here, IT administrators do not require additional training to start managing endpoints.
Seamless onboarding of devices: Hexnode's UEM lets you onboard your devices with a wide variety of enrollment options ranging from zero-touch to minimal touch methods. It also lets you configure device settings before enrollment to make the devices ready for use right out of the box. In addition, Hexnode employs a top-of-the-line support team to readily fix and attend to customer requests.
Flexible pricing plans: Here at Hexnode, we offer a wide range of pricing plans specially designed to meet all your corporate requirements.
This migration guide will help you seamlessly cover all the necessary steps to migrate from VMWare Workspace ONE (formerly known as AirWatch) to Hexnode UEM.

Key points for a successful migration

Before starting the migration process, here are some tips that will help you migrate from Workspace ONE to Hexnode UEM successfully.

UEM Migration Checklist:

Follow the steps mentioned in the migration checklist to accomplish a successful migration. The checklist provides a list of tasks you must follow during the migration process.

Clear communication to end-users:

Inform your end-users about the transition clearly and provide details of the exact steps (device wipe, initial setup assistant, etc.), which they are expected to perform. Allow users to participate in the enrollment process to make them feel involved in the device management procedures.

Test migration processes using a few devices from all platforms:

Start your migration by testing with a few sample devices from all platforms to optimize the migration processes, if any, and to check for configuration errors. This will also help you to validate your migration plan.
We recommend migrating devices in an incrementing pattern. That is, migrate in groups such that the next group has more devices than the previous group. This helps identify and rectify issues associated with a smaller number of devices, rather than the entire device fleet.

Sign up for a free trial in Hexnode UEM:

Test the product for 14 days by signing up for a free trial to explore the rich features and functionalities offered by Hexnode UEM. This will help you understand the product better and makes migration processes fast and efficient.
The entire migration process can be grouped into three stages:

1. Pre-migration Phase
2. Migration Phase
3. Post-migration Phase

Pre-migration Phase

The pre-migration phase includes all the activities you must perform prior to the migration phase. The below list explains all the pre-migration events and activities:

- **Assess MDM requirements of your enterprise:**
  After all, the ultimate point of breaking away from your previous MDM vendor is to manage your organization's needs more efficiently. Hence, the primary concern must be about what the organization needs from an MDM solution. Ensure that the features lacking in your previous MDM solution are present in your new MDM provider.
  Evaluate your previous MDM solution based on the areas that need improvement, as well as the features that need to be carried over to the new MDM. Prepare for the transition only after deciding various criteria such as the OS platforms, device types, device choice – personal or corporate, and so on.
- **Identify the use-case of the organization:**
  While preparing for the transition, check that the new MDM service will meet and satisfy the organization's use case. Ensure that the MDM platform you are planning to migrate to can support your firm's growth requirements in the near future. Decide all the configurations and features you are going to use with the new MDM based on the use case of your organization.
- **Create a list of users:**
  Prepare a list of all users to be added to the new MDM solution. If possible, export the user data from the previous MDM provider's database. Identify specific users who require special privileges like admins and technicians.
- **Create a logical timeline:**
  The first step before heading to the migration phase is to create an effective timeline. Choose a time that is best suited for migration. It would be ideal to choose a time when your devices are out of use so that the IT team will have enough time for the transition without impacting users.

Study the entire migration process and prepare an achievable schedule that includes important milestones, expenses, and other implementation factors. Divide the entire migration process into different segments, targeting a small group of devices to a higher number within various periods. This will optimize the process and help validate the migration plan.

- **Effective Communication:**
  It's essential to inform and educate your end-users about the migration processes. Describe the steps that your users must execute, including the details on whether the device will be wiped or not, whether the users are required to wipe and re-enroll the devices manually, and so on. Empower your users by providing thorough training sessions and in-depth help articles to seamlessly carry out the steps.
- **Backup data to cloud services:**
  Store sensitive data to cloud services before migration so that any data, if lost after migration, can be retrieved. Some examples of cloud services include iCloud, Google Drive, Dropbox, and Box.
- **Prepare devices for migration:**
  After completing the steps mentioned above, check your device for activation lock and factory reset protection. Back up your data to keep it safe, in case your device gets wiped. Make your devices ready for the transition. Help regarding device wipe and disenrollment from your previous vendor is explained in the next phase.

Migration Phase

The migration phase includes all the actions that the organization must carry out to migrate from one MDM to another. Make sure that you are right on the migration timeline and have completed all the pre-migration steps before entering the migration phase.
The first thing to do while planning the migration is to check out new MDMs. Here at Hexnode, we provide a 14-day trial period with the highest subscription plan, so that you can explore all the features and make sure we provide everything you need. If not, contact us directly and request new features that you find essential to meet your requirements. Since you have access to the Hexnode portal, identify which pricing plan you will choose when the trial period ends. Hexnode offers programs that are scaled across various price ranges. Refer to the pricing page if you are facing any difficulty in tracking down the features.
Steps to be followed in the migration phase:

1, Create technicians

Create technicians (same as Role-based admins in SureMDM) in Hexnode. They have at-most privileges and are responsible for managing users. The number of technicians

that you can add to Hexnode varies with your subscription plan.

2, Migrate Tokens

You can now migrate the tokens from the previous MDM vendor to Hexnode.
This includes Wi-Fi profiles (for enrollment via Apple Configurator), security certificates (certificates for Android, iOS, and macOS devices), apps, identity/user authentication certificates (VPN and Wi-Fi), and configuration profiles (DEP). Set up APNs, DEP, and VPP certificates/tokens in Hexnode.

APNs:

It is recommended to create a new APNs certificate in the Apple Push Certificate Portal, and add it to Hexnode.

DEP:

To sync your DEP account with Hexnode, create a new MDM server for Hexnode in your DEP portal and transfer devices from the previous MDM server to the newly created one.
To transfer devices from the previous MDM to Hexnode Server,

1. Login to your DEP portal.
2. Go to Settings, select the old MDM server and Download the devices list.
3. Go to Device Assignments and change the Choose Devices option to Upload CSV file.
4. Upload the downloaded device list and choose the Action as Assign to server.
5. Select the newly created server for Hexnode UEM as the MDM Server and click Done.

VPP:

To migrate the VPP token to Hexnode, clear the available VPP token on your SureMDM console and sync the VPP account with Hexnode.

3, Directory integration

Register your directory services like AD, Azure AD, G Suite, and Okta in Hexnode for easy and better management.

4, Import Assets

Bulk enrollment is a recommended method to import users' to Hexnode. This relieves you from importing individual users manually.
If you are integrating with AD, Azure AD, G Suite, or Okta please neglect the above mentioned, as users and groups will be directly synced with Hexnode.

You can also export device details from Workspace ONE and add them as pre-approved devices in Hexnode (Apple and Android). Adding a pre-approved device gives you the flexibility to pre-configure apps and policies in the devices even before enrollment initiation.

5, Create Policies

Create policies in Hexnode that suit your use cases. Hexnode lets you configure policies for all supported Operating Systems from the same pane. This will come in handy if your organization is managing devices in more than one device platform. You can proactively attach users, user groups, domains, and pre-approved devices as Policy targets.

6, Disenroll From Sophos Mobile

As of now, you have a better understanding of Hexnode and if you find our software compatible for your use, disenroll your devices from Sophos Mobile and enroll them with Hexnode.
To disenroll devices from the Sophos Mobile,

1. On your Sophos Mobile portal, go to Manage > Devices.
2. Select a device that you want to disenroll, on the “Show device” page, click on Actions > Unenroll to remove device management.

You can also allow each device owners to disenroll their devices individually from their respective self-service portals,

1. Log in to the Sophos Mobile Control Self Service Portal using your credentials.
2. Select the device you want to remove.
3. From the Action choose Unenroll.

This is not supported for Android Work profile enrolled devices in Sophos Mobile. To remove such devices,

1. In the Self-Service Portal, click My devices and then select the device.
2. Click Actions and Wipe Android work profile to disenroll the device.

Now, let’s look at different methods to disenroll the devices or remove the MDM administration from the device.

Apple Devices

For Apple devices added to DEP (iOS and Mac)
Profile removal of a DEP enrolled device can be restricted by the admin via the DEP profile settings. This might restrict the disenrollment of the device via the Unenroll action. If this is the case, follow the steps below to disenroll the device from Sophos Mobile,

- Remove your devices from the current MDM server. This can be done in two ways. Either delete the previous_mdm_server from ABM, or you can remove/unassign/release devices from the previous_mdm_server.
- If you are deleting the server, reassign the devices to the new MDM server that you have created for Hexnode. If you are unassigning the devices, first download the device list using the Download button then unassign.
- Then carry out a complete device wipe (Erase all contents and settings) to remove the device management.

For Apple devices enrolled via Apple Configurator (iOS)

- Either use the Unenroll device option or carry out a wipe to remove the current MDM profile from the device.
- Create a new blueprint with Hexnode UEM details and apply it to the device that has to be migrated.

iOS Auto Enroll (using Apple Configurator)

Carry out a device wipe to remove MDM management of an Apple configurator enrolled device from the device end.

Using SMC App

You can remove the management of an enrolled device using the Unenroll button in the SMC app. If you have disabled unenrollment through the app, go to Settings > General > Profile > Remove Management. You can also carry out a device wipe to unenroll the device.

Android Devices

Legacy Android Device Admin Enrollment

Remove the device admin privileges from the device and uninstall the Sophos Mobile Control (SMC) app to remove management from the device end. You can also wipe the device to its factory settings to disenroll the device.

Sophos Mobile Control is the Sophos agent app present in the enrolled Android, iOS and Windows mobile devices that would help in managing the devices.

Work Profile Enrollment

In case of work profile enrolled devices, removing work profile (On your device, go to Settings > Accounts > Remove Work Profile) or factory resetting the device will also remove remote management.

Android Enterprise Fully Managed Device

To remove the management of a fully managed device from the device end you will have to reset the device to its factory settings.

Note:

While resetting, make sure that Factory Reset Protection (FRP) is disabled. You can also

remove the accounts associated with the device prior to factory reset.
Wipe or factory reset an Android Enterprise fully managed device after a disenroll action to re-enroll in Hexnode UEM.

Samsung Knox Enrollment

To remove the management of a Samsung Knox enrolled device, follow the below-mentioned steps;

1. Sign in to your Knox portal.
2. Go to Knox Mobile Enrollment > LAUNCH CONSOLE.
3. Go to Devices > ALL DEVICES.
4. Select the devices whose management has to be removed.
5. Click on Actions > Configure devices.
6. Change MDM Profiles to Clear profiles and Save.

Zero-touch Enrollment

To turn off Zero-touch enrollment for devices and remove the management,

1. Login to your Zero-touch portal.
2. Go to Devices, change the Configurations for the devices whose management has to be removed to No config.

Windows (Tablet/ PC: 10

Manual Device Enrollment (Adding Work Profile)

To remove the management of a Windows PC and tablet, go to Settings > Accounts > Access Work or School and remove MDM profile.

Automatic enrollment by installing Sophos Mobile app

To remove Sophos Agent from Windows PC, go to Control panel > Programs and Features. Select the SMC app from the list and click on Uninstall to remove it from the device.

7, Enroll in Hexnode

To manage the disenrolled devices from the previous MDM vendor, you need to enroll them with Hexnode UEM. Hexnode UEM supports enrollment of iOS, Android, Mac, Windows 10 PCs & Tablets, Apple TV, and Fire OS devices. Here, devices can be registered using a plethora of enrollment methods ranging from zero-touch to minimal touch enrollment options. Before enrolling your devices, make sure that you configure the Enrollment Settings on the Hexnode portal.
The platform-specific instructions for enrolling devices in Hexnode UEM are given below:

iOS Devices

Devices can be enrolled in iOS through various enrollment techniques. Which includes,

Apple Business Manager/Apple School Manager

The most recommended in case of bulk supervised enrollment. To assign the devices to the newly created MDM server for Hexnode,

1. In the Apple Business Manager page, go to Device > Device Assignments.
2. Upload the CSV file that you have downloaded in Step 2: Migrate Tokens.
3. Choose Action as Assign to server and choose that you created for Hexnode as the MDM Server.

Apple Configurator

Each device has to be individually accessed to enroll in Hexnode using Apple Configurator. Use this method to enable device supervision on enrollment when the device cannot be enrolled using Apple DEP.

Pre-approved

Use in case you want to pre-approve devices or pre-assign policies to devices before enrollment.

Email/SMS

Users will get enrollment request with login credentials via email/SMS to guide them through the enrollment procedure.

Enroll in DEP via Apple Configurator

Previously, Apple allowed only the devices purchased directly from Apple to be enrolled in DEP. But now you can add any Apple devices running iOS 11 or later to DEP regardless of how or from where it is purchased, using Apple Configurator 2.5 or later.

Enrollment without authentication

Users can directly enroll in Hexnode with no authentication.

Self enrollment

Users can enroll with the directory or local credentials.

Mac Devices

Mac devices can be enrolled in Hexnode through any of the following ways.

Email/SMS

Devices can be enrolled by entering the credentials that are sent to users via email or SMS.

Enrollment without authentication

With this enrollment method, users can directly enroll their devices without any authentication.

Apple Business Manager/Apple School Manager

This method is recommended to enroll a large number of devices in bulk.

Self enrollment

Users can directly enroll in Hexnode with their local or directory credentials.

Apple TV Devices

Use any of the following methods to enroll Apple TV in Hexnode UEM.

- Apple Configurator
- Apple Business/School Manager

Android Devices

1, Android Legacy

Self-enrollment

Self-enrollment allows the users to enroll devices with their Active Directory/Azure Active Directory/Google/Okta/local user credentials.

QR code

Scan a QR Code to enroll via the Hexnode app.

Email/SMS enrollment

An Email/SMS with the enrollment credentials and instructions on how to enroll devices will be sent to the selected users. They can use this information to enroll their devices in Hexnode.

Pre-approved

Upload a CSV file with device details in Hexnode so that, you can attach policies and applications to devices prior to enrollment.

2, Android Enterprise

To enroll a device in AE,

1. Enroll your organization in the Android Enterprise program via the Google or Managed domain.
2. Enroll the devices using either the Profile owner or device owner enrollment methods.

Zero Touch Enrollment

Zero-touch enrollment is a bulk device enrollment method. To enroll a device using Zero-Touch enrollment method,

1. Login to your zero-touch portal and create a configuration for Hexnode UEM.
2. Upload the device list in CSV format and apply the configuration to the devices.
3. All the devices will now be assigned to that specific configuration.

Samsung Knox Enrollment

Samsung Knox devices can be enrolled in Hexnode via Knox Mobile Enrollment, a no-touch enrollment solution by Samsung Knox. To enroll in Knox,

- Login to your Knox portal account and create a profile for Hexnode UEM.
- Upload the device list in CSV format and assign the profiles to the devices.
- For reseller purchased devices, the reseller will add the devices to the Knox portal.

Then the profiles can be applied to the devices.

- For non-reseller devices, associate the created Hexnode profile to the devices via Knox Deployment Application and deploy them using either Bluetooth or NFC.

Android ROM/OEM Enrollment

Android ROM/OEM enrollment unlocks a lot of features like non-removable MDM even after device wipe, silent app installation, etc.
You can make the Hexnode system agent app as a privileged app during Android ROM/OEM enrollment. This will grant system permissions to the Hexnode UEM Android app as new versions are being installed.

Windows Devices

Enroll using Hexnode Installer

Recommended for devices running Windows 10 v1803 or later.
Enter the enrollment URL (www.portalname.hexnodemdm.com/enroll/) on the browser to download the Hexnode Installer app on the device. Install the app and follow the on-screen instructions to complete the device enrollment.

Open enrollment & Authenticated enrollment via Email/SMS

Recommended for Windows 10 v1709 or below.
The major difference between open enrollment and Email/SMS is that users will be asked to authenticate for enrolling their device via the Email/SMS enrollment method.
To enroll a device using Open or Email/SMS enrollment methods, go to Settings > Accounts > Access Work or School > Enroll in device management on the device. Enter the enrollment URL and the user authentication credentials (required for Email/SMS enrollment) whenever prompted. Follow the on-screen instructions to complete the device enrollment.

Self enrollment

Users have to enroll in Hexnode by authenticating with their organization's directory credentials or local user credentials.

PPKG Enrollment

Use the PPKG enrollment technique while bulk enrolling Windows devices in Hexnode. End-users need to just power on the device, get connected to the network, and install the ppkg file to get enrolled with Hexnode UEM.
To enroll devices via PPKG enrollment,

1. Create a ppkg file using Windows ICD.
2. Distribute this ppkg via external media/email.
3. Click on the ppkg file and follow the on-screen procedure to get the devices enrolled with Hexnode.

8, Migration Fallback

There is a possibility that some of the device enrollments may end in failures. This may set back your whole productivity. We suggest some easier enrollment techniques as a workaround to roll back your devices to the MDM console quickly.

For Apple Devices use:

1. Email/SMS (Use either open/authenticated enrollment)
2. Pre-approved
3. Apple configurator (For supervised enrollment – iOS only)

For Android Devices use:

1. QR Code
2. Email/SMS (Use either open/authenticated enrollment)
3. Pre-approved

For Windows Devices use:

1. Enroll using Hexnode Installer

9, Monitor enrollment process

Monitor the whole enrollment process and track newly enrolled users using various analytics methods. Identify the devices still in unenrolled/enrollment failed state. Use any of the methods mentioned in migration fallback to enroll it back in Hexnode UEM.

Post-Migration Phase

This phase includes all checks and surveys to be carried out to ensure that all devices are migrated from your previous vendor to Hexnode UEM successfully.

- Device Inventory checks: Export the details of all devices enrolled in Hexnode UEM from the Reports tab. Compare this list with the exported legacy MDM provider's device database. This will help to find out all the devices which are still not enrolled in Hexnode UEM.
- Restoring back-up data: For Apple devices, you can restore saved data by logging into your devices using your iCloud or Managed Apple ID. Cloud-hosted data can also be retrieved from cloud services like Google Drive, Dropbox, Box, etc. This will ensure no data loss after the migration process.
- Unsubscribing the services of old MDM: Decommission the services of your previous MDM provider.
- Surveys and feedback on new MDM: Collect users' feedback to identify any issues or new requirements in your new MDM solution. Conduct surveys regularly to analyze the user experience so that training sessions can be arranged, if needed, for new areas and use cases.

- Troubleshooting / Support plan to assist with migration: Equip yourself with the world-class support team from Hexnode UEM to assist you in issues regarding migration. Clear your queries by referring to the published FAQs and other how-to articles to mitigate troubleshooting issues.