Android Enterprise Management Solution

Managing Android Enterprise enabled devices

Key Takeaways

- Multiple enrollment methods
- Customized configurations
- App management
- Endpoint and data security
- Kiosk device management
- Lost device management
- OEMConfig
- Compliance management

Despite the influx of other mobile devices in the workplace, Android continues to be the most dominant operating system as it supports a wide range of dedicated, rugged devices and digital signages. The increased number of personal devices and steady reliance on remote work poses a fresh new set of challenges for IT admins in terms of how the devices can be secured from a wide range of threats.

Android Enterprise (AE) known previously as Android for Work was first introduced in 2014 as an answer to the various challenges posed by the Android Device Admin API. Although the API made it possible for EMM agents to manage the device by enforcing policies on them, it still wasn’t enough to address all the difficulties organizations faced in keeping the devices secure and employees more productive.

Why use Android Enterprise?

The functionalities of AE incorporates the management of both corporate owned and personal devices of employees. It takes care of various privacy and confidentiality issues regarding the storage of business data on personal devices of employees.

Some of the other benefits of using AE includes multiple over the air device enrollment methods, enhanced security capabilities and silent app installation.

Onboard devices

Enrolling Android Enterprise device

- Android Enterprise supports the management of both personal and corporate owned devices. Admins could choose to enroll the devices either in a device owner or profile owner mode depending on the use case.
- Devices fully owned and managed by the organization would be enrolled in a device owner mode whereas personal devices or personally enabled devices can be enrolled in a profile owner mode. By enrolling the device in a profile owner mode, a work profile would be created on the managed device to containerize the work apps from the personal space of the user.
- Before the devices can be onboarded, the organization has to be enrolled within the Android Enterprise program. The final step of the onboarding process would include applying the necessary configurations to make the onboarding process easier for users.

Enrolling devices via profile owner mode

- As soon as the device is enrolled in a profile owner mode, a work container will be created on the device. All work apps would have a work badge making it easier for users to differentiate them from personal applications.
- The UEM agent used to manage the device would be made as the profile owner. This would give the agent full control over applying the necessary settings to secure the work apps and managed space on the device.

Enrolling devices via device owner mode

- Device owner mode is usually recommended for corporate owned devices or other devices fully managed by the organization. It restricts employees from accessing any application or enabling settings not approved by the organization.
- The device would have to undergo a factory reset in order to enroll in this method. The UEM agent would be made as the device owner.

Enrolling devices via Google Workspace

- A corporate owned G Suite account should be used to enroll the device via Google Workspace. The service account would be required by the UEM agent to push the configurations to the managed devices.
- Once the account has been set up, API access should be given to the UEM agent to simplify the process of applying the necessary configurations.

Enrolling devices via QR code

- In addition to being a quick and efficient way to enroll the devices, admins can remotely configure multiple settings during the enrollment process, such as the option to skip encryption, enable system applications and defining the Wi-Fi settings and security type.

Enrolling via Knox Mobile Enrollment (KME)

- KME is a zero-touch enrollment method that provides admins with the convenience to quickly enroll bulk number of corporate owned devices.

- This enrollment method entails a couple of requirements, which include a Samsung account, a Knox portal account and a UEM provider that integrates with KME.

Enrolling via Zero Touch Enrollment

- This is an automated over-the-air enrollment of corporate owned devices. It saves admins the need from manually configuring the devices to deploy the necessary restrictions and applications. The devices will be enrolled as device owner.

Enrolling devices without camera or Google Play Store

- Some organizations may have camera or Google Play Store disabled on the device. If your organization permits the use of Play Store but has the camera disabled, admins can download the Hexnode for Work app and follow the enrollment methods specific to device owner or profile owner mode.

- If cameras are allowed but Play Store is disabled, you could download the .apk file of the Hexnode for Work app and enroll the devices in a profile owner or device owner mode.

- If the use of both camera and Play Store is disabled, the device can be enrolled by following the steps mentioned above.

Securing endpoints with adequate restrictions

Most organizations find it challenging to deploy the right number of safeguards to secure the managed devices. Security requirements may differ depending on your business use cases. Configuring these settings manually can be difficult, especially if these requirements need to be rolled out quickly in a short amount of time. One of the important management capabilities of Android Enterprise are the restrictions it allows admins to set up to ensure data security and device protection.

Password security

Passwords are usually the first measure organizations take up to restrict the access of information to unauthorized parties. The more complex the password, the better protected the resources will be. Hexnode's password security functionalities include:

- Setting the password complexity requirements.
- Defining the password age to encourage users to update passwords at regular intervals.
- Automatically locking the device after a set period of inactivity.
- Defining the number of attempts a wrong password can be entered before data is wiped from the device.
- Securing the work container with a password to restrict other users from accessing the container.

Set various restrictions

Multiple restrictions on the device functionality, network and applications can be set up remotely to prevent users from enabling any settings on their own. These restrictions make it harder for external users to gain access to your systems thereby protecting your corporate resources from unauthorized modification and disclosure.

- Disable the use of camera, USB file transfer, microphone, screen capture and other device functionalities specific to your organization's policies.
- Enable or disable the use of mock location and enforcing GPS.
- Restrict the copying of sensitive information across work profile and personal space of the user.
- Disable users from sharing data via bluetooth and other file sharing options.

- Restrict users from disabling Factory Reset Protection and initiating a factory reset on their own.
- Blacklist websites that hamper productivity and compromises the security of your organization.
- Configure the Wi-Fi settings to enable users to connect to corporate network without prompting users for a password.
- Configure the minimum security type of the Wi-Fi network.
- Configure the VPN settings to ensure remote access to corporate resources is done in a secure manner.
- Configure the APN settings to make sure devices connect to secure gateways.
- Set up a global HTTP proxy to make sure all network connections pass through it.

Application management

Android Enterprise comes with multiple app management capabilities that help admins to manage application in all stages of its management lifecycle, right from deployment to uninstallation from the end user device.

A single application or a set of applications can be rolled out to individual and multiple users at the same time. Various store apps and enterprise apps can be silently installed on the device without requiring any user intervention. This minimizes any possibility for human errors to occur and ensures all users have the necessary applications installed on the device. An app catalog can be created and customized according to your organization's specific requirements. Hexnode's app management capabilities include the following:

- Set essential applications as mandatory and install them over the air without any user intervention.
- Silently install Play store and Managed Google Play apps in devices enrolled as profile owner and device owner mode. Enterprise apps have to be published as private apps within the Google Play console before they can be pushed silently to the devices.
- Publish in-house (enterprise) apps and make them available to users via the Managed Google Play store catalog.
- Blacklist and whitelist applications.
- Create a customized app store on the device of the user.
- Configure Android Enterprise applications with configurations specific to your organization.
- Permit or deny permission required by work apps or enterprise applications.

Ensure security of endpoints

Although, setting an adequate amount of restrictions is a great place to start. It's always good idea to implement additional security measures to ensure the endpoints are completely protected from a number of insider threats and other cyberattacks.

The use of identity certificates for example adds in an extra layer of protection as it authenticates users before they are granted access to corporate resources. Similarly, hackers always exploit vulnerabilities that can arise from using an old and outdated software within the systems. Admins can keep the devices secure by scheduling OS updates remotely. In this way, all users would have the latest software installed within the system.

- Deploy identity certificates to authorize user access to corporate resources.
- Schedule OS updates on the device.
- Group devices based on their OS and deploy policies specific to those devices.
- Restrict data usage across network and applications.
- Remotely deploy files to devices and restrict access to those files only to authorized employees.

Managing kiosk devices

Multiple industries incorporate the use of kiosk and digital signages to improve brand awareness and to quicken up their operations. Hexnode supports the management of single app kiosk, multi app kiosk and digital signages. The devices need to be enrolled in a device owner mode in order to function as dedicated devices.

Secure browsing has always been a priority for many especially those within the education industry, where additional measures have to be taken up to minimize student’s exposure to insecure websites. Hexnode has an in-built kiosk browser that offers a secure browsing experience. The browser can also be customized to align with your organization’s specific requirements. In addition to this, the peripheral settings of the device can be configured and password for exiting the kiosk can be defined to ensure only authorized users or the admin exists the kiosk mode from the device.

- Configure devices to run in single app or multi app kiosk mode.
- Set apps to run in the background without displaying the icon on the screen.

- Easily convert devices into digital signage displays, supports multiple file formats.
- Customize the kiosk launcher settings and auto launch settings for whitelisted applications.
- Configure the peripheral settings of the device.
- Set the kiosk exit password and define the kiosk exit settings.
- Configure the website kiosk settings.
- Define how the web browser should look like by configuring the toolbar settings. Schedule refresh at periodic intervals and disable a number of media options.
- Display images and videos as a screensaver. Customize the kiosk screensaver settings.

Secure lost devices

Lost device is a common occurrence in any organization. It's always best to anticipate this situation and be prepared to combat such risks by implementing enough security controls to safeguard the device and data present within the lost device.

In addition to tracking the device in real time, a host of other remote actions can be deployed to prevent external parties from accessing sensitive data and tampering with the device settings. Admins can make use of Hexnode’s following management capabilities to secure lost devices:

- Track the location of the device in real time.
- Get the location history of the device.
- Enable lost mode on the device to initiate remote lock and data wipe.
- Wipe corporate data from the lost device.

Visit/learn more

https://www.hexnode.com/

Sign up for a free trial

https://www.hexnode.com/mobile-device-management/

Knowledge base

www.hexnode.com/mobile-device-management/help/

Rugged device management with OEMConfig

OEMConfigs are applications developed by Original Equipment Manufacturers (OEMs). They consists of OEM specific configurations and published in Google Playstore. Before OEMConfigs was introduced, organizations had to wait for their EMM provider to integrate the features. Instead, all they are required to do now is to download the OEMConfig app from the Playstore to configure various device functionalities. The process can be summarized as follows:

- The OEM vendor develops an OEMConfig app consisting of a set of common APIs. The app is published in Managed Google Playstore.
- Organizations install the application from the Playstore and add it within the app inventory. Begin setting up the OEM specific configurations by pushing it remotely from the UEM console.

The benefits of managing devices with OEMConfig include:

- Zero day support for new features.
- Improved security of devices.

Ensure compliancy of devices

Monitoring the compliancy of the devices is important as it gives admins an idea of the number of devices that are out of compliance with your organization's deployed policies. Devices that fall out of compliance due to some error can be immediately enrolled within the UEM agent again.

- Monitor the devices on a continual basis by checking their compliance with the deployed policies.
- Deactivation of work container of devices not compliant with organization's policies.
- Get reports in real time or at periodic intervals to check the number of compliant devices.