hexnode

Hexnode Android Management Solution

Ensuring hassle-free management of Android devices

Key Takeaways

- Centralized management
- Zero-touch deployment
- Enterprise integrations
- OEMConfig support
- Manage rugged devices
- Android Enterprise management
- BYOD management
- Enforce network security
- Manage apps and content
- Track real-time location
- Manage OS updates
- Control data expenses
- Kiosk lockdown
- Push remote actions
- Manage visual configurations
- Enforce restrictions
- Monitor compliance
- Schedule and generate reports

Without question, the impact of Android smartphones and tablets in the enterprise has revolutionized the workplace in recent years. They have enhanced employee productivity and significantly improved the current business workflow. However, this radical entrance of Android smartphones also introduces the possibility of potential security gaps and vulnerabilities in device management. Hence, there emerges the need to efficiently manage and secure Android devices in the enterprise.

Why Android management?

Hexnode's Android Management solution enables businesses to extend enterprise flexibility to support any business model and unlock a plethora of endpoint management capabilities. The seamless integration of Hexnode UEM with Android Enterprise enables businesses to enforce BYOD policies while securing any mission-critical corporate data. Android Enterprise (AE) and Hexnode also enable businesses to exercise an extended level of control over every manageable aspect of an Android device, and provision for simplified large-scale deployment of enterprise devices.

Features of Hexnode Android management

Hexnode supports an entirely cloud-based Android management console which can be accessed from any internet-enabled device. The functionalities described below enables IT administrators to securely deploy, manage and configure Android devices, business applications, and data within an enterprise.

Enrolling Android devices

There are several methods to enroll Android devices in Hexnode, each supporting different use-cases. Both end-users and enterprise admins can enroll Android devices into the Hexnode portal. Hexnode UEM also offers no-touch enrollment methods to streamline the deployment of Android devices.

- The following methods are applicable for Windows device enrollment:
    - Quick enrollment
        - Enrollment without authentication
        - QR code enrollment (open)
    - Authenticated enrollment
        - Email or SMS enrollment
        - Enrollment via Active Directory/Azure AD
        - Enrollment via Google Workspace/Okta
        - QR code enrollment (authenticated)
    - No-touch enrollment
        - Android Zero-touch enrollment
        - Samsung Knox Mobile Enrollment (KME)
        - ROM/OEM configured enrollment
- Hexnode also supports the enrollment of Android devices via Android Enterprise Profile owner and Device owner enrollments. The above-mentioned zero-touch enrollment methods, including Samsung KME, and Android zero-touch, also supports the Android Enterprise enrollment process.

Implementing BYOD

Hexnode's BYOD management helps organizations to strike the perfect balance between security and privacy. Enterprises can secure corporate data without compromising the privacy of their employees with the help of work containers. Hexnode's Android BYOD management policies incorporate the following functionalities:

- Allowing users to work with the devices that are both familiar and convenient to them.
- Implementing Android Enterprise to separate work apps and data from personal apps and data by creating app containers.
- When the device needs to be released from management, only this work container needs to be removed, leaving personal apps and data untouched.
- Configuring policies to handle the less-restrictive settings for the personal devices in a BYOD program.
- Providing a seamless and secure integration of BYOD and corporate devices, regardless of the device model or manufacturer.

Setting up Android kiosks

With Hexnode, IT can lock Android devices into kiosk mode to restrict the user from tampering with any device settings and strip down the device's functionality to the bare minimum required to perform the specified tasks. Hexnode's kiosk management capabilities include the following functionalities:

- Configuring a single app kiosk or multi-app kiosk with a customized user interface.

- Configure advanced website settings and browser properties to further fine-tune your website kiosk configurations.
- Converting your Android smartphones, tablets and TVs into transformable digital signages.
- Enabling advanced single and multi-app kiosk configurations including orientation, app placement, icon size, and grid view.
- Configuring background apps to hide apps in kiosk mode and prevent users from tampering with them.
- Customizing the kiosk launcher including the app name, logo, font, and more.
- Enabling or disabling manually exiting from kiosk mode with the global exit passcode
- Remotely adjust the peripheral settings such as device volume, screen brightness, Wi-Fi and Bluetooth access and so on.

Managing password policies

With Hexnode, enterprises can configure strong device passwords to protect confidential data on the device from any form of unauthorized access. Hexnode's password policies allows you to enforce the following configurations.

- Ensuring that a device password meet complexity requirements based on corporate policies.
- Setting up password requirements that incorporate length, complexity, special characters, timeout periods, expiration dates and retry limits.

- Directly configure the password on Android device from the Hexnode portal and if required, clear the passwords from specific Android devices.
- Marking the devices that do not meet your password policy requirements as non-compliant.
- Setting up separate passwords to access the work container on Android Enterprise profile owner devices.
- Automatically wipe the corporate data on the device after ‘n’ number of failed attempts.

Enforcing device restrictions

Configuring restrictions on Android devices enables you to enforce control on how the users access these devices. You may allow or disallow Android functionalities and features to secure the organizational data and ensure that the devices are utilized safely.

- Maintaining complete control of all the devices that are associated with your network.
- Enabling administrators to configure restrictions such as turning off cameras, microphones, and other device capabilities to meet the needs of your corporate policies.
- Disabling access to suspicious and unproductive websites via blacklist/whitelist policies to boost corporate device and data security.
- Restricting users from tampering with sensitive device functionalities including USB debugging, disable FRP, perform factory reset, and more.

Configuring network settings

With Hexnode, enterprises can remotely configure network settings including Wi-Fi, VPN, HTTP proxy, and more along with email and ActiveSync account configurations, and push them to the required Android devices.

- Remotely configuring global HTTP proxy settings and pushing it over-the-air.
- Automatically connecting the devices to Wi-Fi networks without prompting for a password.
- Specifying minimum Wi-Fi security levels for Android devices to successfully connect.
- Disabling Wi-Fi connections, or alternatively, forcing Wi-Fi to be in 'always-on' state.
- Configuring email settings on your Samsung Knox Android devices to synchronize emails between the device and the email server.
- Enabling Exchange ActiveSync to access all emails, attachments, calendars, notes, etc. from a Samsung Knox Android device and store them safely on the device.
- Setting up Virtual Private Network (VPN) configurations for Samsung Knox Android devices.
- Configuring Access Point Names (APN) on Samsung Knox Android devices to access the internet and send/retrieve multimedia messages (MMS).
- Deploying network certificates including Wi-Fi and VPN for additional security.

Managing apps and content on Android

Hexnode's app and content management functionalities enable administrators to manage and secure the apps and content on Android devices, and ensure granular control of data at the application level. Android app and content management in Hexnode include the following features and functionalities:

- Allowing you to deploy store and enterprise apps on your Android devices easily.
- Defining apps as mandatory ensure that the users have installed all the necessary apps on their devices.
- Enabling administrators to update or uninstall managed apps from Android devices.
- Restricting users from accessing specific applications on their devices by blacklisting or whitelisting apps.
- Distributing your own enterprise (in-house) applications to the enrolled devices.
- Organizing the apps into various groups and categories and distributing them using custom app catalogs enable the users to easily find and download the apps they need.
- Restricting users from downloading harmful or unproductive apps by enforcing application blacklists/whitelists.
- Remotely launch apps on Android devices and specify the duration they shall remain open.
- Retrieve app logs from managed Android devices and easily identify and abnormal behaviours.
- Deploy all types of files and content to Android devices, including .apk, .pdf, .mp3/mp4, .mkv, and more, and specify the location and path for content deployment.

Managing apps with Android Enterprise

Android Enterprise is a device management framework used to manage and secure Android devices in the work environment. Devices enrolled in the Android Enterprise program supports a suite of additional functionalities, thereby expanding the administrator's arsenal of app management capabilities to even greater limits. Android Enterprise app management with Hexnode incorporates the following features and functionalities.

- Allowing administrators to enforce silent installation of store and enterprise apps on Android devices.
- Pushing managed app configurations and specifying app permissions to gain greater control over the apps installed on Android devices.
- Set up and deploy Managed Google Play and Store layouts to provide users with a custom app store with limiting them with access to just the required apps.
- Push remote actions and restrictions including clearing app data, hiding Google Play Store, verifying apps before install, disabling app install from unknown sources, and more.
- Enabling organizations to easily collect the status and log information of specific apps installed on an Android device using the Android app feedback channel.

Managing rugged devices with OEMConfig

OEMConfig is a standard used to configure OEM-specific settings on OEM supported devices enrolled in the Android Enterprise program. Hexnode UEM enables organizations to secure and manage rugged devices in the enterprise, by customizing OEM-specific configurations straight from the Hexnode portal with the help of OEMConfig apps. The following are Hexnode's rugged device and OEMConfig functionalities:

- Managing and configuring all the OEM-specific settings on Android Enterprise devices.
- Provide OEM-specific configurations for Smasung Knox, Kyocera, Honeywell, LG Gate, and a variety of manufacturers and rugged devices.
- Gaining first-day access to all the new features, functionalities and configurations that are introduced by OEM vendors.

Enabling real-time location tracking

Location Tracking in Hexnode UEM enables organizations to find the lost or misplaced devices, fetch the real-time device location information, and the store the history of locations traversed by the device previously. This information thereby helps administrators evaluate employee performance and make better business decisions.

- Enabling real-time location tracking of any device enrolled within the network.
- Tracking the movements of devices through an unauthorized area and maintaining a history of their location information.
- Helping the admins track lost or stolen devices, locking them in lost mode, and in worst cases, wiping the corporate data stored on these devices.
- Tracking the movements of devices through an unauthorized area and maintaining a history of their location information.
- Helping the admins track lost or stolen devices, locking them in lost mode, and in worst cases, wiping the corporate data stored on these devices.

- Configuring the geofencing feature to monitor and control the operation of devices as they move in and out of the geofence.
- Forcing devices to set their GPS functionality to always-on mode, and restricting users from turning on mock location on Android devices.

Managing OS updates

Hexnode UEM provides information on OS versions for enrolled Android devices, and enables enterprises to enforce or schedule updates on their corporate Androids remotely.

- View OS information of Android devices and group them based on their OS versions to apply OS-specific policies and configurations.
- Remotely deploying OS updates to the specified Android devices.
- Scheduling and automating OS updates on Android devices to update during inactive hours, thereby reducing the load on corporate bandwidth.
- Delaying OS updates on corporate Android devices, thereby providing technicians with time to test the new OS for bugs and vulnerabilities.

Managing network data expenses

Hexnode UEM enables administrators to manage network data expenses by tracking and restricting data usage across Android devices, identifying apps with high mobile data consumption rates, and keeping track of data usage of individual devices. Hexnode's network expense management capabilities includes the following functionalities:

- Track and manage mobile data usage across Androids.
- Separately view the mobile data, Wi-Fi data and total data usage of individual devices as well as the data consumption details of respective applications installed on devices.
- Set alert notifications to administrators or users via email when the mobile data usage crosses the set limit.
- Block either the Android device, or specific managed apps from using mobile data/Wi-Fi.

Managing visual configurations

Maintain uniformity in the enterprise by specifying visual configurations on Android devices including wallpaper and boot/shutdown animation with Hexnode UEM.

- Remotely deploying wallpaper configurations to multiple Android devices.
- Specifying wallpaper configurations for both mobile and tablet devices.
- Personalizing boot and shutdown animations on Android devices with custom sounds and animations.

Monitoring device compliance

With Hexnode you can define a host of rules and settings to ensure an optimal level of security and conformity with your corporate regulations, and flag devices as non-compliant if they fail any of the selected compliance checks. Hexnode UEM enables you to maintain compliance on Android devices with the help of the following features:

Visit/learn more

www.hexnode.com

Sign up for a free trial

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

Knowledge base

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

- Monitoring the compliance in real time thereby efficiently maintaining data and network security.
- Alerting the administrators immediately at the instances of policy violations.
- Automatically rounding up non-compliant devices using dynamic groups to take quick remedial action.
- Monitoring password policy compliance, app compliance, detecting rooted devices, disabling Wi-Fi access to targeted users.
- Locking the Android Enterprise container when device inactivity or non-compliance is detected.
- Enabling real-time diagnosis of Android devices by initiating remote view and remote control.

Generating reports

Hexnode enables you to generate a wide range of reports on the go, enabling administrators to view granular details, reports, and audit history based on specific actions.

- Generating a broad range of reports incorporating security and compliance status.
- Allowing administrators to monitor user data, app statistics, security violations, and various compliance issues.
- Exporting the reports for documentation purposes and future reference.