hexnode

Hexnode for Samsung device management

Secure your Samsung devices with Unified Endpoint Management

Key Takeaways

- Multiple enrollment methods
- Enterprise integrations
- OEMConfig support
- Samsung Knox Validated Program
- Android Enterprise management
- BYOD management
- Network management
- Kiosk management
- Monitor compliance
- Schedule and generate reports
- Data expense management
- App management

Efficient management of Samsung devices using UEM enables enterprises to manage each device in an organization with excellent flexibility and ease. IT admins can manage devices with strict policies and limits maintained using an effective device management solution. UEM solutions assist organizations in ensuring smooth end-user device deployment, configuration, control, monitoring, and supervision.

Smartphones and tablets with Samsung Knox capabilities offer security features that help safeguard private and business data on the device, without needing an additional agent. Knox, a highly secure platform integrated into Samsung devices, includes several defenses against unauthorized access and cyberattacks. In addition, Samsung Knox offers the most advanced management and configuration features, showcasing strong security. In combination with a Unified Endpoint Management system, Samsung Knox can enhance the security and isolation of corporate data.

Why Hexnode UEM for Samsung device management?

Due to constantly expanding technology standards, businesses need a flexible endpoint management solution. Using traditional device management techniques brings up many difficulties for the administrator.

Hexnode's UEM solution helps to manage the endpoints seamlessly. Hexnode UEM's integration with Samsung Knox offers a wide variety of capabilities in application management, kiosk management, web filtering, security management, remote view and control, and more.

Hexnode UEM features for Samsung device management

Hexnode supports an Android management console that can be accessed from any internet-capable device. IT admins can securely install, manage, and configure Samsung devices, enterprise applications, and data using the below-mentioned features.

Enrollments

Samsung devices can be added to Hexnode via various methods, each supporting a particular use case. The Hexnode portal allows both end users and enterprise administrators to enroll these devices. To streamline the deployment of Samsung devices, Hexnode UEM also provides no-touch enrolling techniques.

1. Quick enrollment

Quick enrollment can be used by IT admins who must set up devices directly. This is because device enrollment and personal identification will be time-consuming and impractical. However, using this way to enroll Samsung devices might restrict the functions of device management that are applied to them.

2. Authenticated enrollment

Authenticated enrollment may be used if employees need to set up and enroll their devices in Hexnode UEM. It can also be used if admins need to securely authenticate the devices before enrollment. Hexnode UEM supports the following authenticated enrollment methods.

- Local user enrollment with email or SMS authentication.
- User enrollment for Google Workspace/Okta with email or SMS-based authentication.

3. Zero-touch enrollment

Admins can rapidly deploy devices over the air without the involvement of end-users using zero-touch enrollment. Hexnode UEM offers a variety of zero-touch enrollment methods for the hands-free, out-of-the-box deployment of Samsung devices.

I. Android Zero-touch enrollment

- Samsung devices can be deployed right out of the box and instantly signed up for the Android Enterprise program using Hexnode's integration with Android Zero Touch enrollment.
- Admins can quickly deploy over the air with zero-touch enrollment by avoiding end-user involvement.
- Depending on the use case, administrators can enroll the devices in device owner mode through this enrollment.

II. ROM/OEM configured enrollment

- A secure way to enroll is to flash a custom ROM onto a Samsung device with Hexnode UEM as a system or privileged app. Enterprises working with OEM vendors may employ this enrollment strategy.
- In this case, a device is produced with a specially designed ROM (Android firmware) that gives Hexnode UEM access to all permissions and privileges.
- When the user turns on the device for the first time, Hexnode UEM will be immediately installed on it.

III. Samsung Knox Mobile Enrollment (KME)

- The quickest and most effective way to enroll Knox-enabled devices in the workplace for corporate use is through Samsung Knox Mobile Enrollment (KME).

- KME supports various MDM configurations for each account.
- Multiple MDM profiles can be hosted by a single Samsung account and made available to various users.
- Utilize the UEM panel to automatically install software and turn on the security settings the organization has provisioned.
- Devices can be reenrolled even after a factory reset and deletion of all data.
- This eliminates the errors that may occur with manual enrollment and makes the process streamlined and easy.
- Although not all Samsung devices are compatible with Knox, enrolling the device through Samsung Knox Enrollment of Hexnode UEM guarantees that the network and data are more protected.

Android Enterprise

- The seamless integration of Hexnode UEM with Android Enterprise enables businesses to enforce BYOD policies while protecting corporate data.
- Hexnode also supports Android Enterprise Profile owner and Device owner enrollments for Samsung devices.
- Devices owned by businesses or those under their management should generally be in device owner mode. It prevents employees from using applications or enabling settings that the company has not authorized.
- A work container will be generated on the device as soon as it is registered in profile owner mode.
- The device management UEM agent would be designated as the profile owner. The agent would then have complete control over the settings required to secure the controlled space on the device and the business apps.

Samsung Knox Platform for Enterprise (KPE)

- KPE provides a complete set of security management tools for several Samsung devices used in businesses. Hexnode UEM enables these features, easing bulk deployment and facilitating simple device integration with the current business architecture.
- The Knox Platform offers best-in-class hardware-based security, policy administration, and compliance capabilities beyond the basic features in the mobile device market.
- The Knox Platform for Enterprise Premium license can be used on numerous devices over different periods. The legacy Enterprise License (ELM) and Knox License (KLM) keys will be replaced by this KPE license key.
- Containerized workspace, remote management, and application programming interfaces (APIs) with total control over all the apps and settings are all parts of KPE's comprehensive device management.
- It offers all-round credential, certificate management and hardware-based security that disables a device if it detects tampering with certificates or kernels.

OEMConfig and Knox Service Plugin (KSP)

- KSP is Samsung's original equipment manufacturer (OEM) app for EMM providers to give their users access to Knox Platform for Enterprise (KPE) features as soon as they become available.
- By reducing the gap between the introduction of a device-specific feature and its adoption into the UEM, users can quickly roll out feature customization.
- This guarantees that IT administrators can utilize the most recent Knox features the moment it emerges.

- The KSP app helps ensure that the UEM solution is continuously updated with the newest Samsung management options.
- Firmware Over-the-Air (FOTA) updates on Samsung business devices are made simple using the Knox Service Plugin app.
- Improve the delivery and configuration of KPE capabilities for enterprise customers by utilizing the Hexnode UEM's framework and user interface.
- Through this, the enterprise can obtain early access to all the new features, functions, and configurations that the OEM vendors introduce.

Samsung Knox Validated Program

- The Samsung Knox Validated Program is the verification and authentication program for Mobility Management (EMM/MDM/UEM) solution providers who satisfy Samsung's Knox platform and product requirements.
- This assures end users that the UEM vendor supports Samsung enterprise-grade security features.
- It assists partners in developing more distinctive management solutions and expanding their customer base.
- Hexnode UEM is dedicated to supporting business clients and customizing management solutions to meet their unique requirements with end-to-end security and simple-to-use features.
- Hexnode UEM delivers a consistent user experience on Samsung Knox devices regarding setup procedures, controls, security features, timely feature upgrades, and patches.
- Through this Knox Validated Program of Samsung, Hexnode UEM provides full support for Samsung Knox Mobile Enrollment (KME) and the Knox Platform for Enterprise (KPE).

Integrations

- Multiple directory services are integrated with Hexnode, and admins can export users and user groups from these directories to the Hexnode interface.
- Integrate directory services to automate user onboarding, group assignment, and access management (Active Directory, Azure AD, Okta, Google Workspace).
- Assign devices to the user groups, push policies and configurations, and export users and user groups from the enterprise directory.
- Create dynamic groups, assign rules and criteria, and then set pre-configured actions, such as policy assignment, auto lockdown, and more, that are activated when the conditions are met.

BYOD management

- With the help of Hexnode's BYOD management, enterprises achieve the perfect balance between security and privacy.
- This enables users to work with devices that are both comfortable and familiar to them.
- Android Enterprise is being used to implement app containers to isolate work apps and data from personal apps and data.
- This work container must be deleted to free the device from management, leaving personal apps and data in place.
- Hexnode UEM configures policies to manage the less-restrictive settings for personal devices in a BYOD program.
- It provides a seamless and secure integration of BYOD and corporate devices, regardless of the device model or manufacturer.

Kiosk management

- Hexnode facilitates the management of digital signages, single app kiosks, and multi app kiosks for Samsung devices. The devices must be registered in device owner mode to act as dedicated devices.
- Hexnode offers a secure browsing experience using an in-built kiosk browser. IT admins can also modify the browser to meet the organization's unique needs.
- To ensure that only authorized users or admins can access the kiosk mode from the device, the peripheral settings of the device can be controlled and a password can be defined for exiting the kiosk.
- Create background-running apps that don't show their icon on the screen.
- Configure the kiosk launcher's settings and the auto-launch options for the whitelisted program.
- Display images and videos as a screensaver. Customize the kiosk screensaver settings.
- Configure the toolbar options to specify the web browser's appearance. Disable several media options and schedule refresh at regular intervals.

Restrictions

- Several restrictions on device functionality, network access, and application functionality can be set up remotely to prohibit users from changing any settings on their own.
- Hexnode helps to maintain total control over all the devices connected to the enterprise network.
- Enable admins to set limits, such as disabling cameras, microphones, and other device features, to comply with enterprise standards.

- To improve corporate device and data security, blacklist/whitelist policies can block access to suspicious and inefficient websites.
- Restrict users from accessing device functionalities, including USB debugging, disabling FRP, performing a factory reset, and more.

Network management

- Hexnode UEM helps push network settings over the air while remotely-configuring it.
- Allow users to join the network without being prompted for a password by configuring the local Wi-Fi settings.
- The VPNs of Samsung devices can be configured remotely by IT admins through Hexnode.
- Adjust email settings on Samsung Knox devices to synchronize emails between the device and the email server.
- Enable Exchange ActiveSync to access and securely store all emails, attachments, calendars, notes, etc., from a Samsung device.
- Establish Access Point Names (APNs) on Samsung devices to connect to the internet and send/receive multimedia messages (MMS).

Password policy

- Enterprises can set up strong device passwords with Hexnode to shield sensitive data from unauthorized access.
- It ensures that a device password complies with company policy-based standards for complexity.
- Establish password specifications incorporating length, complexity, special characters, timeout intervals, expiration dates, and retry restrictions.

- Identify the devices as non-compliant if they don't follow your password policy guidelines.
- Set up unique passwords for Android Enterprise profile owner devices to access the work container.
- After "n" failed tries, automatically erase the corporate data from the device.

App management

- The app and content management features of Hexnode allow administrators to govern data at the application level and manage and secure the apps and content on Samsung devices.
- Hexnode UEM can silently install, update, and delete apps and resources on Samsung devices.
- Mandatory apps are defined to ensure users have installed all the necessary apps on their devices.
- Enable managers to update or remove managed apps from Samsung devices.
- Restrict users from accessing particular apps on their devices by adding or removing apps to blacklists or whitelists.
- Distribute enterprise (in-house) applications to the enrolled devices.
- Users can easily search and download the apps they need if they are distributed using custom app catalogs and divided into different groups and categories.

Geofencing and Location tracking

- The network administrator can retrieve a Samsung device's location to determine whether it is inside a restricted area.
- Allows the admin to find lost/stolen Samsung devices.

- Using geofencing, Hexnode can associate the enterprise policies with specific geolocation, allowing it to enforce those restrictions in that location.

Device compliance

- IT admins can define various rules and settings with Hexnode to guarantee the highest level of security and compliance with the enterprise’s regulations and flag devices as non-compliant if they don't pass the chosen compliance checks.
- Alert IT admins when the devices violate the policies.
- When a device is inactive or non-compliant, the Android Enterprise container is locked.
- Enables remote view and remote control to enable real-time diagnosis of Samsung devices.
- Dynamic groups can automatically gather non-compliant devices and take immediate corrective action.
- Monitoring app compliance, detecting rooted devices and blocking Wi-Fi access for specific users.

Report generation

- Hexnode allows the company to produce a variety of reports instantly, allowing admins to inspect detailed data, reports, and audit history depending on particular activities.
- It helps to keep an eye on user information, app statistics, security breaches, and numerous compliance problems.
- IT admins can export the reports as PDF or CSV files for future usage and documentation.

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/

Data expense management

- Hexnode UEM enables IT admins to control network data costs by monitoring and limiting data usage across Samsung devices, identifying apps with high mobile data consumption rates, and keeping track of data usage on individual devices.
- View the mobile data, Wi-Fi data, overall data usage, and data consumption details for each installed application separately for each device.
- Establish email alerts for administrators or users when their mobile data use exceeds the predetermined limit.
- Block the Samsung devices or particular managed apps from using mobile data or Wi-Fi.