hexnode

Hexnode UEM Remote Device Management

Enabling seamless remote management for enterprises

Key Takeaways

- Remote enrollment
- Managing password policies
- Enforcing device restrictions
- Configuring network settings
- Remote actions
- Managing apps and their deployment
- Custom scripting
- Monitoring device compliance
- Real-time location tracking
- Reports

With the global transition to remote work, the need for a comprehensive endpoint management solution is at an all-time high. IT admins need a unified solution that can seamlessly monitor and manage their assets while being completely remote. Deploying dedicated software services for device management, asset tracking, employee monitoring, application management etc., can be a challenge to manage.

Things get incredibly tricky for enterprises that have a vast workforce that is scaling exponentially. Data security becomes the primary concern when a large chunk of the force goes remote. Technical assistance for corporate-enabled devices ends up being a significant headache for admins to manage. Compliance policies often stir up confusion for enterprises that have employees that travel to other countries.

Remote device monitoring and management with Hexnode UEM

Device management often stirs up the unwanted image of connecting new devices to PCs and pushing complicated codes to said devices. Hexnode UEM simplifies the entire process with the bonus of carrying everything out remotely. In addition, the remote monitoring and management capabilities delivered by Hexnode ensures that no end-user intervention is needed for the setup and management process.

Hexnode UEM supports the remote management of Android, iOS, iPadOS, macOS, FireOS, Windows, and tvOS devices. With Hexnode UEM, you can achieve continuous monitoring and reporting, management of mobile devices, enterprise security management, seamless integration and onboarding, and automated software and patch updates. BYOD management is also simplified with the introduction of Hexnode UEM; the enterprise only controls the corporate partition of the device, enabling the user to work on their devices securely.

Key features of Hexnode UEM that assist with remote device management and monitoring

Remote enrollment

- Complete remote device deployment via the several enrollment options
- Pre-configure devices to provide an out of the box experience for newly deployed devices
- Streamlined and rapid over the air deployment eliminating the need for direct access to the device
- Deploy devices manually or automatically in bulk without end-user intervention.
- The various enrollment options enabled by Hexnode UEM include:
- No authentication enrollment
- Email/SMS enrollment
- Self-enrollment
- QR code enrollment

- ROM enrollment
- Android Enterprise enrollment
- Zero-touch enrollment
- Samsung Knox Mobile Enrollment

Managing passwords

- Ensure device security from brute force attacks with advanced password policies through Hexnode UEM.
- Regular password updates with time and complexity-based password policies.
- Password history feature to prevent credential recycling on corporate endpoints.
- Set passwords for work profile without affecting the user profile.
- Remote device wipe can be programmed to take effect after multiple failed login attempts to secure enterprise data.

Enforcing device restrictions

- Comprehensive remote management of corporate assets regardless of platform and device type.
- Admins can restrict features like camera, microphone, apps and, other services that threaten enterprise security and productivity.
- Remote blacklisting and whitelisting of websites can be enforced for enhanced security.
- Rooting/jailbreaking can be restricted on corporate enabled devices
- Telecom expense management.

Configuring network settings

- Over-the-air network configuration for enhanced remote management.
- Devices can be configured to connect to trusted networks without password prompts automatically.

Remote actions

- Remote wipe can be used to send a wipe command to devices remotely.
- Live viewing the device screen through the remote view option can help admins resolve technical issues providing a comprehensive remote troubleshooting experience.
- Most devices also support the remote-control feature from Hexnode UEM, allowing remote access to the end user's device.
- Remote management of all the deployed endpoints from a single unified console.
- Hexnode UEM console also provides detailed stats on device health which assists in minimizing downtime.
- File manager allows access to device files for remote checks and audits.
- Hexnode messenger can be used as a one-way communication method between the admin and the target user.

Managing apps and their deployments

- Distribute in-house applications to enrolled devices.
- Bulk deployment of applications to devices.
- Whitelisting and blacklisting of applications to restrict

potentially harmful applications.

- Create and distribute app categories to user groups remotely.
- App catalogs can be created and associated with devices to ensure users only see the apps that are made available to them.
- App configuration can be leveraged to manage applications that are deployed on work devices.

Custom scripting

- Execute custom scripts on Windows and macOS devices directly from the Hexnode UEM console.
- Configurations and other remote actions can be executed via custom scripting.

Monitoring device compliance

- Define compliance settings to ensure that your devices are adherent to corporate regulations.
- Real-time alerts to track and neutralize compliance breaches and policy violations.

Real-time location tracking and geo-fencing

- Track lost/stolen devices with Hexnode's real-time location tracking.
- Secure devices with geo-fences. Admin alerts for breaching the geo-fence.
- Policies associated with the devices can be set to change based on device location.

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/

Reports and audits

- A wide array of detailed reports can be generated via the Hexnode UEM console.
- Compliance statuses, device health, app statistics, user data, violations, and more can be monitored via reports.
- Customization of reports helps document the stats for audits or analysis.