Hexnode UEM

Feature Matrix

Managing devices is no small feat.

Which is why choosing the right UEM solution is key to a strong device management strategy.

	REQUIREMENTS	FEATURES
DEVICE ENROLLMENT	**Provide self-service enrollment options:** Enable end-users to enroll their devices to Hexnode without administrator involvement.	• Authenticated enrollment • Email/SMS enrollment • QR code enrollment
	Enroll devices out-of-the-box: Automatically enroll devices to Hexnode when users turn on the device for the first time.	• Android Zero-Touch Enrollment • Android ROM enrollment • Samsung Knox Mobile Enrollment • Apple Automated Device Enrollment
	Enforce BYOD enrollment: Enable users to enroll their personal devices to Hexnode, giving admins minimal control over device functionality.	• Apple User Enrollment • Android Enterprise Profile Owner enrollment
	Enforce device restrictions: Configure restrictions on devices to enforce control on how users access them. You may allow or disallow functionalities to secure data and ensure devices are utilized safely.	• Modify device functionality • Modify security/privacy settings • Modify connectivity options • Modify location settings • Modify display & personalization • Modify account & auto-sync settings
ENDPOINT SECURITY	**Enforce strong password policies:** Configure strong device passwords to protect confidential data on the device from any form of unauthorized access	• Specify minimum password length, alphanumeric values, and complex characters • Specify minimum password age and password history • Specify time for device auto-lock • Erase device data after specified number of failed attempts
	Enable encryption: Ensure the safety of data-at-rest on your devices by configuring and managing encryption policies on endpoints.	• Configure BitLocker and FileVault encryption • Manage recovery options and safeguard recovery keys

	REQUIREMENTS	FEATURES
	Manage software and OS updates: Enforce or schedule updates on endpoints so that the device will stay immune to bugs and vulnerabilities.	• Schedule, enforce, or delay OS updates on managed devices • Configure updates to be automatically downloaded and/or installed
	Enable kiosk lockdown: Lock down endpoints into kiosk mode to strip down the device's functionality and create a restricted purpose-specific environment with easy access to work resources.	• Configure single or multi-app kiosk lockdown • Configure website kiosk lockdown • Enable background apps in kiosk mode • Configure kiosk launcher and modify kiosk home screen settings • Convert devices to Digital Signages • Enable & configure kiosk exit settings
NETWORK SECURITY	**Automatically connect devices to corporate networks:** Configure corporate network settings including Wi-Fi, VPN, HTTP proxy, and more and push them over-the-air.	• Securely deploy Wi-Fi configurations • Specify minimum Wi-Fi security levels • Securely push VPN configurations • Deploy network certificates for Wi-Fi and VPN • Push global HTTP proxy configuration
	Block access to suspicious websites: Restrict end-users from visiting harmful or unproductive websites on work devices.	• Enable website blacklist policy and block access to the specified websites • Enable website whitelist policy and approve access to just the specified websites
	Track and manage network data usage: Identify and restrict apps and devices with high data consumption and notify admins when limits are crossed.	• Track per-app data usage • Track data usage over the entire device • Specify limits on data usage • Notify admins/users and restrict data once specified limits are crossed
IDENTITY AND ACCESS MANAGEMENT	**Manage a directory of users and their information:** Automate user onboarding and group assignments using integrations with directory services.	• Integrate directory services (Active Directory, Azure AD, Okta, Google Workspace) with Hexnode • Configure and/or sync user and device groups on Hexnode

	REQUIREMENTS	FEATURES
	Configure user accounts: Ensure secure access to corporate accounts, including email, contacts and calendars on corporate-owned and personal devices.	• Configure user accounts on devices • Use wildcards to auto-populate fields and configure accounts in bulk • Configure accounts for email, ExchangeActive sync, Calendar and Contacts.
	Manage access privileges: Create user and device groups and enforce policies and configurations based on their assigned roles and permissions.	• Restrict admin access on user accounts • Deploy certificates to manage access to corporate tools and services. • Enforce MFA and SSO when logging in to Hexnode portal.
APP MANAGEMENT	**Assign users with the required apps:** Enable administrators to automate the deployment, updation, and retirement of apps and resources on managed devices.	• Add, remove, and update store and enterprise apps on end-user devices • Specify mandatory apps and automate app installation • Deploy self-service app libraries for end-users • Remotely launch apps on end-user devices
	Customize apps to suit enterprise requirements: Assign configurations and manage permissions in bulk on the managed apps installed on end-user devices, to ensure granular control of data at the application level.	• Manage app configurations • Manage app permissions • Manage app notifications
	Restrict users' access to unproductive apps: Manage and secure the apps installed on endpoints to block users from accessing harmful and unproductive applications.	• Enable app blacklist policy and block access to unproductive apps • Enable app whitelist policy and approve access to just the specified apps
REMOTE MONITORING	**Monitor the location of endpoints:** Enable organizations to fetch the real-time location information of devices, thereby helping administrators evaluate and make better business decisions.	• Enable real-time location tracking • Maintain a history of location information • Force GPS functionality to always-on mode. • Restrict users from turning on mock location

	REQUIREMENTS	FEATURES
	Remotely troubleshoot endpoints: Gain insight into your devices' health and status and resolve end-users' technical issues in real-time to ease the process of troubleshooting devices.	• Enable remote view and/or remote control • Push remote actions including remote ring, power off/restart, and more • Broadcast important messages to your devices • Deploy custom scripts to devices
	Remotely lock and/or wipe endpoints: Identify, track and lock/wipe the data on stolen or lost devices to protect the corporate data in them from falling into the wrong hands.	• Enforce geofences and lock down devices outside geofence • Push remote wipe or device lock actions on stolen/lost devices
COMPLIANCE MANAGEMENT	**Monitor device compliance:** Define a host of rules and criteria for monitoring compliance on managed devices and notify admins on non-compliance	• Monitor specified compliance parameters on endpoints • Alert admins and/or users via email on device non-compliance
	Perform automated remedial actions: Automatically round up non-compliant devices using geofencing policies and dynamic groups to perform automated remedial actions.	• Use dynamic groups to automatically group non-compliant devices • Execute specified policies on non-compliant devices
AUDITING AND REPORTING	**Generate automated reports:** Create a wide range of on-demand and scheduled reports to help admins monitor the key metrics of devices and enable IT teams to always be in the know on any issues that may arise.	• Generate reports on device status, user actions, app statistics, and more • Schedule daily, monthly, or weekly reports • Control access to view and manage reports
	Send and/or export reports: Assign technician roles to manage access privileges to view and manage reports, send reports to specified email addresses, and easily export reports in the form of PDF or CSV files.	• Export reports in the form of PDF or CSV files • Specify the email address to which the reports may be sent