hexnode

Hexnode UEM for Healthcare

Secure healthcare devices with Unified Endpoint Management

Key Takeaways

- Centralized management
- Multiple enrollment methods
- Push policies and configurations
- App management
- Data restriction and tracking
- Data expense management
- Kiosk management
- Device compliance monitoring
- Schedule and generate reports
- Lost device management
- BYOD management
- Media management

As remote healthcare gains ground, the need for a UEM solution in hospitals and healthcare institutions is at an all-time high. Healthcare facilities with a significant workforce can be easily monitored and managed using UEM solutions.

Hospitals primarily use tablets and smartphones for ongoing patient health and vitals monitoring. These devices must adhere to privacy regulations like HIPAA and be safe to prevent the leakage of protected health information (PHI). Therefore, these devices should be effectively maintained and controlled under any circumstances.

Hexnode UEM effectively helps to control healthcare equipment and safeguard patient data. It allows IT admins to easily track each healthcare device's status and control smart TVs, IoT devices, desktops, laptops, smartphones, and tablets from a single console. Additionally, Healthcare firms can accomplish HIPAA compliance with the help of Hexnode.

Why Hexnode for healthcare?

- Hexnode UEM manages mobile devices at the corporate level, thereby adjusting device features to suit healthcare requirements.
- IT admins benefit greatly from using Hexnode's integrations with Apple Business Manager (ABM), Android Enterprise Recommended, Google Workspace, and Azure AD.
- IT admins can deploy new devices, distribute policies, enforce restrictions and security configurations, monitor and troubleshoot devices, and lock down devices into kiosks.

- Using a single centralized console, Hexnode's Unified Endpoint Management solution enables healthcare institutions to secure and manage devices running any operating system (including iOS, macOS, tvOS, Android, and Windows).

The core features of Hexnode UEM

Hexnode offers an endpoint management solution that is cloud-based and accessible from any internet-capable device, effectively enabling quick access to the UEM console. In addition, administrators can streamline and automate the deployment, management, and configuration of managed devices in a healthcare institution by using the core feature of Hexnode mentioned below.

Cross-platform enrollment

Hexnode provides a range of enrollment methods, each of which supports various use cases. Hexnode UEM additionally provides zero-touch enrollment techniques for the hands-free, out-of-the-box deployment of devices in the healthcare sector. The following are the main enrollment methods supported by the Hexnode UEM:

1. ***Zero-touch enrollment***

Zero-touch enrollment enables administrators to deploy devices quickly over the air without end-user involvement. Hexnode provides a selection of zero-touch device enrollment methods for multiple purposes.

- With Hexnode's integration with Automated Device Enrollment, IT admins can deploy macOS, iOS, iPadOS, and tvOS devices bought directly from Apple or a certified reseller.
- Using Hexnode's integration with Android Zero Touch enrollment, Android devices can be deployed out of the box and automatically enrolled in the Android Enterprise program.

- Hexnode's integration with Knox Mobile Enrollment (KME) helps admins distribute Samsung Knox devices in large quantities to end-users.
- Admins can enroll Android devices hands-free by setting up ROM or Android firmware so that the Hexnode Agent app is pre-installed on the device.
- IT admins can pre-approve devices running Android, iOS, macOS, and tvOS in Hexnode. Once enrolled, Hexnode will automatically link them to pre-configured policies.

2. Quick enrollment

IT admins who must set up learning devices themselves may employ quick enrollment. This is because device enrollment and individual authentication would require time and effort. However, enrolling devices via this method may limit the device management functionalities performed on them.

3. Authenticated enrollment

When medical staff must set up and enroll their devices to Hexnode UEM, authenticated enrollment may be employed. It may also be utilized if admins are required to authenticate the devices before enrollment securely. Hexnode supports the following authenticated enrollment techniques.

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

Device restriction policies

- Hexnode UEM's platform-compatible restriction set allows admins to impose strict control over the device.
- Using the restriction policies, IT admins can ensure that the medical staff is always connected to a secure network.

- Device features, including the camera, call and messaging, social networks, screenshots, and other unsuitable features for a medical setting, can be disabled using the restriction policies available for each platform.

Privacy protection for patients

- Hexnode makes it possible for healthcare facilities to meet HIPAA-required standards.
- Access to ePHI (Electronically Protected Health Information) on the devices is safe by enforcing secure containers.
- The IT admins can ensure that confidential information is secured on healthcare devices.
- Admins can stop medical staff from accessing ePHI on unauthorized devices, thereby preventing the chances of data leakage.

Single or multi-app kiosk mode

- Using kiosk mode, healthcare devices can be locked down to a single app, multiple apps, and/or web pages.
- In this mode, the device's functionality can be constrained by enforcing hardware and software restrictions.
- Additionally, Hexnode provides a controlled peripheral option in its kiosk that enables remote control of device volume and screen brightness and blocks access to Wi-Fi, Bluetooth, flashlight, and other peripheral features.

Crisis control and management

- Enforce quick security controls like device lock, wipe, and lost mode when devices are misplaced or lost.
- Implement strong password policies to protect the data on the devices.

- Location history and live location tracking features of Hexnode help to locate a misplaced or lost device easily.

Network configuration management

- Hexnode streamlines IT operations by actively tracking and identifying device issues and providing real-time troubleshooting guidance.
- Even when medical staff is working remotely, a VPN can be remotely configured to give them secure access to company resources.
- With Hexnode, IT admins can ensure the security of files or application data by granting users permission over any apps or procedures requiring access to protected data.

Report generation

- IT admins may quickly generate a variety of reports along with the capability to view and export detailed report data.
- Reports can be generated using Hexnode to track user information, app statistics, security breaches, and medical device compliance levels.
- Reports can be scheduled and emailed to administrators on a regular basis.
- IT admins can export the reports as PDF or CSV files for documentation and future use.

Data usage tracking

- Hexnode helps to manage per-app data usage on medical devices, to prevent healthcare institutions from incurring high data expense costs.
- Track monthly and daily usage limits and restrict the connectivity when the particular limit is reached.

- Monitors the mobile data and Wi-Fi data usage.

App management

It is essential to have a robust app and content management strategy so the medical staff can easily access the apps and resources they may need. Hexnode UEM makes it easier to distribute apps and app catalogs to devices in mass. IT admins can manage, control, and safeguard the data on medical devices using the app and content management functionalities of Hexnode UEM as described below:

- Hexnode can silently install, update, and delete apps and resources on the devices used by medical staff.
- IT admins can automatically configure a list of mandatory apps downloaded and installed on the listed medical devices.
- The custom app catalog feature can categorize and group the required apps, allowing staff to search and download the apps they need quickly.
- IT admins can configure app permissions and remotely push managed app configurations to have more control over the apps installed on medical devices.
- The blacklist and whitelist policies help to prevent medical staff from downloading or installing particular apps on their devices.

BYOD management

BYOD (bring your own device) practices are becoming more popular in the IT industry. However, healthcare institutions have historically needed help implementing BYOD due to the difficulty in ensuring sufficient security.

- Using Hexnode, Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) schemes are effectively managed.

- Android Enterprise offers admins the option of enrolling the devices in either a profile owner or device owner mode, depending on the use case.
- The managed device will build a work profile to separate the work apps from the user's personal app by enrolling the device in profile owner mode.
- Business containers and managed domains can limit data transfer between personal and corporate spaces.
- Integrating Hexnode UEM with Apple Business Manager/Apple School Manager also enables users to enroll and configure iOS and macOS devices automatically.

Remote access and management

The medical devices in the healthcare industry must be easily monitorable and manageable. Any data leaks should be prevented because this is sensitive information.

- Hexnode UEM provides remote view and control capability that help administrators remotely manage devices given to patients.
- Additionally, technicians can be granted access to medical staff devices to maintain and support them, review usage statistics, and respond to alerts.
- With Hexnode UEM, administrators can remotely lock devices, change owners, erase passwords, and maintain overall control over medical devices.
- Using Hexnode UEM, tight password policy, data loss prevention measures, and network limitations can be applied to these devices for security.
- Remote updates for the OS and apps are also made effortless.
- These devices are not allowed to connect to an unmanaged Wi-Fi network so as to enhance security.

Single console

Hexnode provides a single console for the entire IT infrastructure of the healthcare center. A portable tablet is utilized to gather patient data and carry out surveys rather than needless paperwork and filling out forms.

- Management of business applications, emails, and security is all possible from the main admin console.
- More restrictions on functions like keyboard shortcuts, messaging, Airdrop, erasing data, and changing passcodes can also be imposed by admins using Hexnode.
- It can deploy several Wi-Fi configurations to the devices, configure online content filtering to restrict access to malicious/unwanted websites, schedule OS updates, and monitor each device's status remotely from the console.
- Direct access from the admin's central console can be enabled to configure and restrict device features that go against corporate policies.
- The console also provides managed app summary, compliance breakdown, device check-ins, endpoint summary and many more.

Compliance monitoring and custom scripts

Hexnode UEM helps to monitor the enrolled devices in real-time and ensures they always adhere to corporate regulations. It also allows IT managers to automate device policies, configurations, and limits to help manage end-user access.

- Devices that fail one of the pre-configured compliance parameters (like installed app, geofence position, encryption status) will be notified to the admin and be marked as non-compliant.
- Custom scripts help IT admins automate time-consuming and repetitive operations.

- It uses geofencing policies and dynamic groups to identify non-compliant devices and take remedial action against them automatically.
- Some of the powerful compliance management features of Hexnode UEM include monitoring password policy compliance, app compliance and limiting Wi-Fi access to targeted users.

Geofencing and dynamic groups

In Hexnode UEM, location tracking enables administrators to locate lost or misplaced staff devices, retrieve their location information, and retain the history of areas visited by the device.

- Geofencing can be set up to lock down the devices when they leave the confines of the healthcare zone.
- It forces the device to have its GPS enabled all the time and prevents users from activating mock locations.
- Create dynamic groups, apply rules and criteria, and set up pre-configured actions like policy assignment, auto lockdown, and more that are activated when a particular criterion is matched.

Media management

- Configure advanced media usage settings for external drives, internal drives, and optical media to maintain data security.
- Hexnode protects the data by limiting access to corporate content.
- By only allowing authenticated users access to media, unauthorized access and data transfer can be avoided.

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/

Configure user accounts

- To sync Emails, Contacts, Calendars, Tasks, Reminders, and Notes with healthcare devices, admins can configure an Exchange ActiveSync account over the air.
- With secure access to the corporate inbox, healthcare device email configurations are simple to set up.
- To synchronize user data to the particular endpoints, utilize wildcards to configure user accounts in bulk on managed devices, including email, calendar, and contacts.