hexnode

Hexnode Fire OS Management Solution

Enabling simplified management of Fire OS devices

Key Takeaways

- Centralized management
- Simplified deployment
- Enterprise integrations
- 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

Fire OS is the operating system used by Amazon's tablets and other products, including TVs. It is an operating system that is similar to Android but has been altered to incorporate a completely different user interface. November 2011 saw the initial release of Fire OS, based on the Gingerbread 2.3.3 OS for Android. When the Amazon Fire Phone launched in July 2014, it ran on the Fire OS mobile operating system.

In recent years, Fire OS has seen its entry into the enterprise market. However, this sudden rise in Fire OS smartphones at work, brings in the need for effective management and security practices to protect these business devices and ensure zero security gaps within the enterprise environment.

Why Fire OS management?

Hexnode's Fire OS Management solution enables businesses to support any business model and unlock a plethora of endpoint management capabilities. Hexnode enable IT to exercise an extended level of control over every manageable aspect of a Fire OS device, and provision for simplified large-scale deployment of enterprise Fire OS devices.

Features of Hexnode Fire OS management

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

Enrolling Fire OS devices

There are several methods to enroll Fire OS devices in Hexnode, each suited for different use-cases. Both end-users and enterprise admins can enroll Fire OS devices into the Hexnode portal.

- The following methods are applicable for Fire OS device enrollment:
    - Quick enrollment
        - Enrollment without authentication
        - QR code enrollment (open)
    - Authenticated enrollment
        - Email or SMS enrollment
        - Enrollment via Active Directory/Azure AD/Okta
        - QR code enrollment (authenticated)

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.

- Enforce strong password policies and ensure they meet the corporate requirements.
- Set up password requirements that incorporate length, complexity, special characters, timeout periods, expiration dates and retry limits.
- Directly configure the password on Fire OS device from the Hexnode portal and if required, clear the passwords from specific Fire OS devices.

- Identify the devices that do not meet the password policy requirements and mark them as non-compliant.
- Automatically wipe the corporate data on the device after ‘n’ number of failed attempts.

Setting up Fire OS kiosks

With Hexnode, IT can lock Fire OS devices into kiosk mode and restrict the user from tampering with any device settings. Kiosk mode strips down the device's functionality to the bare minimum required to perform a specific task. Hexnode's kiosk management capabilities include the following functionalities:

- Configure a single app kiosk or multi-app kiosk with a customized user interface.
- Configure advanced website settings and browser properties to further fine-tune the website kiosk configurations.
- Convert Fire OS smartphones, tablets and TVs into transformable digital signages.
- Enable advanced single and multi-app kiosk configurations and customize the orientation, app placement, icon size, and grid view.
- Configure background apps in kiosk mode and prevent users from tampering with them.
- Customize the kiosk launcher and add elements including the app name, logo, font, and more.
- Enable or disable the option to manually exit from kiosk mode by configuring the global exit passcode.
- Remotely adjust peripheral settings such as device volume, screen brightness, Wi-Fi and Bluetooth access and so on.

Enforcing device restrictions

Configuring restrictions on Fire OS devices enables IT to control how the users access these devices. IT may allow or disallow device functionalities and features to secure organizational data and ensure that the devices are utilized safely.

- Maintain complete control of all the devices that are associated with your network.
- Enable administrators to configure restrictions such as turning off cameras, microphones, and other device capabilities to meet the needs of your corporate policies.
- Restrict users from tampering with sensitive device functionalities like USB debugging, factory reset, and more.

Configuring network settings

With Hexnode, enterprises can configure corporate network settings and remotely push the settings to the required Fire OS devices.

- Automatically connect the devices to Wi-Fi networks without prompting for a password.
- Specify minimum Wi-Fi security levels for Fire OS devices to successfully connect.
- Disable Wi-Fi connections, or alternatively, force Wi-Fi to be in ‘always-on’ state.
- Deploy network certificates for connecting to Wi-Fi for additional security.
- Disable access to suspicious and unproductive websites via blacklist/whitelist policies to enforce corporate security.

Managing apps and content on Fire OS

Using Hexnode's app inventory, administrators can easily manage and secure the apps and content on Fire OS devices, and ensure granular control of data at the application level. Fire OS app and content management in Hexnode include the following features and functionalities:

- Easily deploy store and enterprise apps on corporate Fire OS devices.
- Define specific apps as mandatory and ensure that they are automatically installed on end-user devices.
- Enable administrators to update or uninstall managed apps from Fire OS devices.
- Restrict users from accessing unproductive applications on their devices by blacklisting or whitelisting apps.
- Distribute your own enterprise (in-house) applications to the managed Fire OS devices.
- Organize the apps into various groups and categories and distribute them using custom app catalogs to help users easily find and download the apps they need.
- Restrict users from downloading harmful or unproductive apps on Fire OS devices by enforcing application blacklists / whitelists.
- Remotely launch apps on Fire OS devices and specify the duration they shall remain open.
- Deploy all types of files and content to Fire OS devices, including .apk, .pdf, .mp3/mp4, .mkv, and more, and specify the location and path for content deployment.

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.

- Enable real-time location tracking on any Fire OS device enrolled within the network.
- Track the movements of Fire OS devices through an unauthorized area and maintaining a history of their location information.
- Help the admins track lost or stolen devices and lock them down in lost mode, or in worst cases, wipe the corporate data stored on these devices.
- Configure geofences to monitor and control Fire OS devices as they move in and out of the geofence.
- Force Fire OS devices to set their GPS functionality to always-on mode, and restrict users from turning on mock location on these devices.

Managing OS updates

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

- View OS information of Fire OS devices and group them based on their OS versions to apply OS-specific policies and configurations.

- Remotely deploy OS updates to the specified Fire OS devices.
- Schedule and automate OS updates on Fire OS devices such that updates are performed during inactive hours, thereby reducing the load on corporate bandwidth.
- Delay OS updates on managed Fire OS devices, and provide 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 Fire OS devices, identifying apps with high mobile data consumption rates, and keeping track of data usage of individual devices.

- Track and manage Wi-Fi and mobile data usage across devices.
- Separately view the mobile data, Wi-Fi data and total data usage of individual devices as well as the data consumption 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 Fire OS device, or specific managed apps from using mobile data/Wi-Fi.

Managing visual configurations

Maintain uniformity in the enterprise by specifying wallpaper configurations on Fire OS devices including smartphones and tablets.

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/

- Remotely deploy wallpaper configurations to multiple Fire OS devices.
- Specify wallpaper configurations for both mobile and tablet devices.

Monitoring device compliance

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

- Monitor device compliance in real time and alert the administrators immediately at instances of non-compliance.
- Automatically round up non-compliant devices using dynamic groups to take quick remedial action.
- Enable real-time troubleshooting on Fire OS 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.

- Generate a broad range of reports incorporating security and compliance status.
- Enable administrators to monitor user data, app statistics, security violations, and various compliance issues.
- Export the reports as PDF or CSV files for documentation purposes and future reference.