hexnode mdm

Hexnode Windows Management Solution

Scaling Windows to best fit your business

Key benefits

- Manage Windows phones, tablets, laptops and PCs from a centralized admin console.
- Securely deploy corporate-owned devices and as well as personal devices.
- Lockdown your devices to a single app or multiple apps with Hexnode's kiosk solution.
- Set password rules with the desired password complexity, expiration and retry attempts for security enhancement.
- Remotely configure corporate Wi-Fi, Email and ActiveSync settings.
- Enable full-disk encryption to protect your on-device data.
- Track device locations in real-time and export the location history of devices.
- Automate device compliance checks.

Gone are the days when the Windows devices in an enterprise were configured and managed manually. Manually controlling the devices can put your organizational data at risk. Therefore, integrating your organization with an MDM solution is the best option to deploy and manage Windows devices and applications. The implementation of Hexnode in your enterprise will provide you with a strong and reliable MDM tool to make your enterprises secure than ever before.

Why Windows management?

The usage of Windows devices such as smartphones, tablets, and PCs in enterprises and schools has been increasing in recent years. Manually managing and securing the devices is an extremely tough task. Therefore, you will need an easy-to-deploy MDM platform which lets you enforce device compliance with corporate security policies. A comprehensive MDM solution can effectively implement the different enterprise strategies such as Bring Your Own Device (BYOD), Corporate Owned Personally Enabled devices (COPE) and Choose Your Own Devices (CYOD).

Features of Hexnode Windows device management

The functionalities described below empowers IT admins to efficiently manage, control and secure Windows devices, business applications, and data within an enterprise.

Enrolling Windows devices

- Windows mobile devices can be enrolled in 3 different ways.
  Enabling to manually enroll each device or deploy devices in bulk.
  - Enrollment without authentication
  - Email or SMS enrollment
  - Active Directory-based or Self-enrollment

Implementing BYOD

- Allowing users to work with the devices that are both familiar and convenient to them.

- Configuring policies to handle the less-restrictive settings for the personal devices in a BYOD program.

- Controlling even the most diverse fleet of devices is simple with the unique BYOD characteristics of Hexnode MDM.

Setting up Windows kiosks

- Restricting your Windows 10 devices to a single application while preventing access to all other apps.

- Locking down your Windows devices to a few selected applications.

- Employing the Assigned Access feature to run a specific application above the lock screen. When a user logs into his kiosk account, the device gets into kiosk mode by automatically launching the assigned application in full screen.

- Automatically opens the same application each time your Windows device loads.

- Enabling device location-tracking in real-time and configure Geofencing feature to monitor and control the operation of devices as they move in and out of the geofence.

- Enforce silent app installation on devices by configuring required applications as mandatory.

- Control access to the camera, manage Cortana settings, allow/deny SD card access, control basic device settings and much more.

Managing password policies

- Configuring strong device passwords to protect confidential corporate data from unauthorized access.

- Letting admins define the password policy explicitly.

- Enabling you to specify your requirements on automatically locking device screen, password complexity, expiration, password history, permissible retries, and almost everything you need to secure your devices in compliance with the corporate policies.

Enforcing device restrictions

- Getting complete control of all the devices that are associated with your network.
- Configuring restrictions enables you to prevent employees from accessing specific apps and services that are unnecessary in a work environment.
- Enabling administrators to restrict camera, screen capture, Wi-Fi, Bluetooth, NFC, browser, internet sharing, and numerous other device functionalities.

Configuring network settings

- Remotely configuring network settings and pushing it over-the-air.
- Setting up your corporate email on all your employee devices remotely. When an employee leaves your organization, you can perform a corporate wipe which safely removes the email settings from the device while leaving all personal data untouched.
- Setting up Exchange ActiveSync remotely and pushing it to the device over-the-air enables you to sync emails, attachments, calendar, contacts, etc. between a device and your email account server.

Managing apps

- Allowing you to deploy store apps on your Windows devices easily.
- Defining apps as mandatory ensure that the users have installed all the necessary apps on their devices.
- Restricting users from accessing specific applications on their devices by blacklisting or whitelisting apps.

Enforcing device encryption

- Ensuring the safety of your device by performing full-disk encryption on your device with the BitLocker feature of Hexnode MDM.
- Configuring encryption settings for the operating system, fixed data drives, and removable data drives on Windows 10 PC.

Monitoring device compliance

- Regularly tracking compliance across the entire range of enrolled devices.

Visit/learn more
www.hexnode.com

Sign up for a free trial
www.hexnode.com/mobile-device-man-age-ment/

Knowledge base
www.hexnode.com/mobile-device-man-age-ment/help/

- Weighing each device against the pre-set compliance parameters and custom ones defined in the policies.
- Alerting admin when a Windows device falls out of compliance so that remedial measures can be initiated directly from the dashboard immediately.

Auditing Windows devices

- Generating a wide range of reports incorporating security and compliance status.
- Allowing you to monitor user data, app statistics, security violations, and various compliance issues.
- Enabling you to export the reports for documentation purposes and future reference.