hexnode

Hexnode Windows Management solution

Scaling Windows to best fit your business

Key Takeaways

- Centralized management
- Zero-touch deployment
- Application management
- Kiosk lockdown
- Enforce restrictions
- Enforce strong passwords
- Enable encryption
- Deploy custom scripts
- Enforce network security
- Configure Microsoft Defender
- SCCM migration
- Track real-time location
- Monitor compliance
- Schedule and generate reports

Windows devices come equipped with a variety of tools for effectively managing your enterprise system. These include tools for managing hardware and software configurations, disks and file systems, apps and content, network configurations, and more. Hexnode UEM provides enterprises with a robust set of mobility management solutions for enrolling, securing, configuring, and managing Windows 10 devices. With the help of Hexnode's Windows management solution, enterprises can easily manage the entire lifecycle of corporate and employee-owned Windows 10 devices.

Why Windows management?

The usage of Windows devices in enterprises and schools have been increasing in recent years. Enabling users to operate these devices unmanaged can severely put your organizational data at risk. Hence, integrating your organization with a UEM solution is the most suitable option to secure and manage Windows devices in the enterprise.

Although traditionally, enterprises managed Windows devices using agent-based client management techniques including group policies, Active Directory, and custom images, the use of personal devices for work, as well as employees working outside the office, has changed how organizations control devices. Managing and securing these devices via traditional techniques could pose a rather laborious task.

Hexnode's comprehensive Unified Endpoint Management solution equips enterprise IT with the flexibility to respond to these changing requirements.

Features of Hexnode Windows 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

Hexnode UEM enables organizations to enroll Windows devices using a multitude of methods. Both end-users and enterprise admins can enroll Windows devices into the Hexnode portal.

- The following methods are applicable for Windows device enrollment:
    - Enrollment without authentication
    - Email or SMS enrollment
    - Enrollment via Active Directory/Azure AD
    - Enrollment via Google Workspace/Okta
    - Enrollment using provisioning package (PPKG)
- With Hexnode, enterprises can enable co-management of Windows 10 devices. This enables Windows 10 devices enrolled in another MDM/UEM portal, to be co-managed by Hexnode.

Implementing BYOD

Hexnode allows users to work with the devices that are both familiar and convenient to them, by employing BYOD polices and configurations on Windows devices. Hexnode's BYOD management policies include the following functionalities:

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

- Encrypt corporate data on BYOD devices.
- Controlling even the most diverse fleet of devices is simple with the unique BYOD characteristics of Hexnode UEM.

Setting up Windows kiosk

The kiosk mode in Windows 10 aims at creating a confined environment where IT can configure Windows devices to be locked within a specific set of apps. With Hexnode, implementing kiosk lockdown in Windows devices is a straightforward process. Hexnode's kiosk management capabilities include the following features:

- 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.
- Enforcing the Assigned Access feature to run a specific application above the lock screen. When a user logs into the kiosk account, the device automatically launches the assigned application in full screen.
- Configure the start menu layout for multi-app kiosk on Windows.
- 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

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:

- Enables IT admins to define the password policy explicitly.
- Enables IT to specify requirements on automatically locking device screen, password complexity, expiration, password history, permissible retries, and almost everything you need to secure your devices and maintain compliance with corporate policies.
- Wipes corporate data on the device after 'n' number of failed attempts.

Enforcing device restrictions

Configuring restrictions on Windows devices enables you to enforce control on how the users access these devices. You may allow or disallow Windows functionalities and features on managed devices to secure the organizational data on the device and determine whether they are utilized safely.

- Obtaining 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 and account settings

With Hexnode, enterprises can remotely configure network settings, email and ActiveSync account configurations and push them to the required Windows devices:

- Remotely configuring network settings including Wi-Fi and VPN and pushing it over-the-air.
- Setting up your corporate email on all your employee devices remotely. When an employee leaves your organization, IT can disassociate the policy 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 applications

Hexnode's app management functionality provides IT administrators with the ability to manage, control, and secure apps on Windows devices. Windows app management in Hexnode includes the following features:

- Enabling IT to deploy store and enterprise apps on your Windows devices easily.
- Defining apps as mandatory ensure that the users have installed all the necessary apps on their devices.

- Enabling you to update or uninstall managed apps from Windows devices.

Enforcing device encryption

Hexnode UEM enables you to set up and manage BitLocker configurations on Windows devices. When used in conjunction with TPM versions 1.2 and above, BitLocker can also validate system files and boot activity.

- Ensuring the safety of your device by performing full-disk encryption on your device with the BitLocker feature of Hexnode UEM.
- Configuring encryption settings for the operating system, fixed data drives, and removable data drives on Windows PC.
- Providing the option to save the recovery information to Azure AD.

Monitoring device compliance

Hexnode UEM enables you to define a host of rules and settings to ensure an optimal level of security and conformity with your corporate regulations, and flags devices as non-compliant if they fail any of the selected compliance checks. Hexnode enables you to maintain compliance with the help of the following features:

- Regularly tracking compliance across the entire range of enrolled devices.
- Marking Windows devices as non-compliant when blacklisted apps are installed on the device.
- Alerting admin when a Windows device falls out of compliance so that remedial measures can be initiated directly from the dashboard immediately.

- Weighing each device against the pre-set compliance parameters such as encryption status, geofence position, installed apps, along with custom ones defined in the policies.
- Automatically round up non-compliant devices using dynamic groups and take quick remedial action.
- Enabling real-time diagnosis of Windows devices by initiating remote view.

Auditing and managing reports

Hexnode enables you to generate a wide range of reports on the go, enabling you to view granular reports and audit history based on specific actions.

- 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.
- Scheduling reports to be sent via the configured email at specific time intervals.
- Enabling you to export the reports for documentation purposes and future reference.

Managing threats and malware

Hexnode UEM enables administrators to configure various Microsoft Defender settings on Windows 10 devices enrolled in the portal. Microsoft Defender with Hexnode includes the following functionalities:

- Providing real-time protection of Windows devices against threats and malware.

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/

- Enabling Microsoft Defender Application Guard to open suspicious webpages in an isolated container.
- Enabling administrators to disable or hide Windows Defender Security Center functionalities including the user interfaces and settings.

Deploying custom Windows scripts

With custom Windows scripts, Hexnode enables enterprises to save time and effort by reducing most administrative tasks to just a few lines of code. Hexnode's Windows scripting feature includes the following functionalities:

- Automating routine and time-consuming operations on Windows devices by pushing script files with custom configurations to the required devices.
- Enabling IT to use wildcards pass arguments to scripts.
- Providing the ability to check the output of the pushed script files directly from the Hexnode portal.

Integrating SCCM

Hexnode's integration with Microsoft's System Center Configuration Manager (SCCM) equips you with the ability to migrate, enroll, and manage Windows 10 client devices registered in the SCCM server directly from the Hexnode portal.

- Migrating Windows 10 devices from the SCCM server to the Hexnode portal.
- Directly enrolling Windows client devices to the Hexnode portal by downloading and installing the Hexnode MDM app for Windows, and specifying the necessary configurations.