

Mobile Management with Management

Managing and securing mobile devices can be a major challenge without the right tools. That's why Configuration Management (ZCM) is a major emphasis for us.

Product Highlights

With OpenText™ ZENworks Configuration Management, take control of your hybrid endpoint environment by leveraging the best of PC client management and mobile device management blended seamlessly across corporate and BYO devices from a single web-based management console.

Reduce costs by eliminating the need to buy new licenses, implement new systems, or manage multiple management solutions.

- Strengthen mobile security with greater device control and reach.
- Improve IT productivity with uniform identity-based, integrated management of all your iOS, Android, ActiveSync, Windows, MacOS, and Linux endpoint devices.

Key Features

- Mobile Devices**
Secure all your mobile devices from the same central location that you secure all of your desktops and laptops. The extent of some selected device types and OS versions.
- Enforce password restrictions, password complexity, encryption settings, screen locks, and device inactivity settings with mobile security policies.
- Implement iOS, Android, and ActiveSync device control policies, including allowing or restricting users from accessing certain features on your users' mobile devices. Depending on device type, this can

Quick View

- Expand endpoint visibility and simplify management.
 - Strengthen mobile security with greater device control.
 - Improve IT productivity with uniform identity-based, integrated management.
 - Reduce costs.
- include controlling use of device cameras, web browsers, and voice assistant.
- Remotely lock lost or stolen devices and allow users to unlock the device by entering their set passcodes.
 - Perform full wipes of fully managed or ActiveSync devices that have been lost or stolen.
 - Enhance control over iOS devices by enforcing MDM enrollment and MDM Apple Device Enrollment Program (DEP).
 - Easily leverage Android Enterprise Work Profile including separation of user personal

data and business data, remote wipe of business data only, leakage prevention controls of business data, blockage of side-loading apps and apps installs from unknown sources, full control over work app usage and runtime

- Manage and use iOS Activation Lock bypass codes to successfully reset and re-provision iOS devices without knowing previous users' credentials, including those of former employees.

ZENworks Configuration Management lets you manage all your mobile devices from a single console using role-based administrative capabilities.

- If desired, enroll Android and iOS device as fully managed devices to enable policy enforcement, facilitate application deployment and management, allow device inventory gathering, and manage Exchange ActiveSync capabilities.
- Pre-provision iOS mobile device devices or integrate with the iOS capabilities.
- Streamline deployment of multiple corporate owned iOS devices using
- Use native VPP integration to provision the licenses for your VPP purchased apps.
- Easily reclaim and reassign iOS VPP apps
- Manage and control public and private Android Work apps on users' devices, while leaving personal apps under their control.
- Silently push private, internally-developed Android Work apps to devices or make them available for users to download from your managed Google Play Store.
- Support settings, email addresses, server details, login names, and other settings, eliminating the need to educate end users
- Create Android Enterprise for Work and secure workspaces on users' Android devices and to allow you to manage those workspace environments without restricting users from using their device for personal apps and data.
- Create and assign a mobile compliance policy to Android devices enrolled in

compliance status of those devices from within the ZCM compliance dashboard.

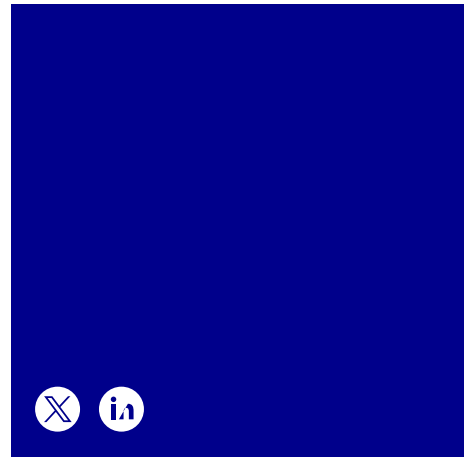
Gain Visibility into Mobile Device Information

Using the inventory framework in ZENworks you can provision iOS apps, Android Enterprise mobile device users and groups of users.

- Schedule mobile device inventory collection as part of your ZCM device refresh schedule.
- Collect information on managed and non-managed apps on iOS devices.
- Collect information on managed and system apps on Android devices in
- Use standard ZCM inventory reports to view mobile device information in your environment.
- Create and view custom inventory reports
- View what apps have been assigned to a device, but not installed.
- See how many of your purchased Apple Volume Purchase Program (VPP) licenses have been consumed and how many are still available, as well as license consumption by user and device.

Using the existing ZENworks bundles feature, you can provision iOS apps, Android Enterprise mobile device users and groups of users. Conditions needed to deploy and manage the apps

- Create App Store Bundles to distribute and manage apps purchased as part of your Apple VPP onto fully managed iOS devices.
- Create Android Enterprise for Work and secure workspaces on users' Android devices and to allow you to manage those workspace environments without restricting users from using their device for personal apps and data.



deployment of business apps to a secure workspace, and easy management of individual app parameters.

- Use native VPP integration to provision the licenses for your VPP purchased apps.
- Easily reclaim and reassign iOS VPP apps
- Manage and control public and private Android Work apps on users' devices, while leaving personal apps under their control.
- Silently push private, internally-developed Android Work apps to devices or make them available for users to download from your managed Google Play Store.
- Support settings, email addresses, server details, login names, and other settings, eliminating the need to educate end users

System Requirements

and system requirements, visit: www.microfocus.com/products/horunfromopdphow