ZENworks Modern Management

August 2023

The Getting Started with Modern Management page enables you to setup the zone and complete certain pre-configuration activities required to enroll Windows 10 MDM devices, Apple devices and Android devices. Subsequently, tasks required to successfully manage these enrolled devices are also displayed on this page.

Managing Windows 10 Devices

Windows MDM enrollment lets you enroll Windows 10 MDM devices to the zone without installing the ZENworks agent on the device. You can enroll Windows 10 devices to your zone in the following ways:

- Using a Provisioning Package (PPKG)
- Using Azure Active Directory (AD) Join
- Using Auto Pilot Enrollment

However, before enrolling these devices, you need to ensure that you have configured the following

- An MDM Server and checked the certificate requirements of this server
- Windows Notification Service (WNS) to send push notifications to enrolled Windows 10 MDM devices

After enrolling these devices, you can use the existing bundles feature to deploy MSI packages on these devices using the EnterpriseDesktopAppManagement Configuration Service Provider (CSP). You can also deploy other CSPs to deploy various configurations on these devices.

Additionally, using the Policies feature, you can also deploy the ZENworks agent on Windows devices that are already enrolled using the MDM mode of enrollment.

For more information on enrolling and managing Windows 10 devices, refer to the following:

- Windows MDM Reference

Managing Android Devices

ZENworks lets you enroll and manage Android devices. You can enroll Android devices in the following ways:

- **Work profile mode:** This mode is intended for the BYOD scenario. This mode of enrollment creates dedicated containers on devices for corporate apps and data, thereby enabling the organization to manage only the corporate data without compromising on the security of the users' personal data.

  Work-managed device mode: This mode is intended for corporate-owned devices. This mode of enrollment enables administrators to manage the entire device, thereby restricting the device to corporate use only.

However, before enrolling these devices, you need to ensure that you have configured the following

- An MDM Server and checked the certificate requirements of this server
- Firebase Cloud Message (FCM) to send push notifications to enrolled Android devices
- User Source
- Android Enterprise Subscription
- Mobile Enrollment Policy
- Purchase Android Application from Google Play Store

After enrolling devices, you can assign the bundles associated with the approved play store apps to these devices. You can also distribute various corporate resources like Wi-Fi configuration profiles and Web Apps to the enrolled Android devices. Additionally, you can apply the security and control policies to enforce security settings and apply certain restrictions on these devices.

You can also provision an email account on the enrolled devices, such as, the Gmail account.

For additional information, refer to the following:

- ZENworks Mobile Management Reference

Managing iOS/iPadOS Devices

ZENworks lets you enroll and manage iOS/iPadOS devices. You can enroll iOS/iPadOS devices in the following ways:

- **Apple Deployment Programs (DEP):** The Device Enrollment Program (DEP) is part of the Apple Deployment Programs and provides administrators with a streamlined way to deploy multiple corporate owned iOS devices. Upon device activation, over-the-air configuration of the device is immediate and enrollment with the MDM server is automatic. There is no need for IT administrators to physically access each device to complete the setup.

  Apple Configurator: Using the Apple Configurator, a Mac OS X tool, you can deploy iOS devices in business or education settings. Apple Configurator makes reassigning devices quick and simple, allowing the next user to start with a clean slate of content.

  ZENworks User Portal: To enroll BYOD devices, users can manually enroll their devices using the ZENworks user portal.

However, before enrolling these devices, you need to ensure that you have configured the following

- An MDM Server and checked the certificate requirements of this server

- Apple Push Notification service (APNs) to send push notifications to enrolled Apple devices
- User Source
- Mobile Enrollment Policy
- (Conditional) Enroll in the Device Enrollment Program
- (Conditional) Purchase apps using Apple's Volume Purchase Program (VPP)

After enrolling devices, you can assign the bundles associated with Apple's VPP to these devices. You can also distribute App Store apps, and various corporate resources like Wi-Fi configuration profiles and Web Apps to the enrolled Apple devices. Additionally, you can apply the security and control policies to enforce security settings and apply certain restrictions on these devices.

You can also provision an email account on the enrolled devices and manage emails using ZENworks.

For additional information, refer to the following:

- ZENworks Mobile Management Reference

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see (https://www.microfocus.com/en-us/legal).