Integrating ZENworks with Android Enterprise

November 2022

Android in the enterprise is a program for mobile devices that run on the Google Android operating system. This program enables IT admins to manage and secure mobile business applications on users' devices.

NOTE: Due to the deprecation of the Device Admin API, ZENworks now supports enrollment of Android devices using only the Android in the enterprise program

---

Modes of Enrollment

With this program, ZENworks lets you enroll your devices in two ways:

- **Work Profile Mode:**
  - **Scenario:** This mode is intended for the BYOD scenario.
  - **Purpose:** Enables organizations to manage only the corporate data, without compromising on the security of the users' personal data.
  - **How it works:** Creates dedicated containers on devices for corporate apps and data.
  - **Applicable for:** Android version 5.0 and newer devices.
- **Work-managed Device mode:**
  - **Scenario:** This mode is mainly intended for corporate-owned devices.
  - **Purpose:** Enables administrators to manage the entire device, thereby restricting the device to corporate use only.
  - **How it works:** The entire device is managed by ZENworks.
  - **Applicable for:** Android version 6.0 and newer devices.

Benefits of Android in the enterprise

By integrating Android in the enterprise with ZENworks, you can achieve the following benefits:

- **Data Security:**
  - Achieve complete control over corporate data on a device.
  - Restrict access to corporate data, if the device is found to be non-compliant, by using the Mobile Compliance Policy.

- Control data leakage and prevent app installations from unknown sources using the Mobile Device Control Policy.
- Remotely wipe corporate data or factory reset the device (based on the mode of enrollment) by using the Unenroll quick task.

- **Device Security**
  - Secure the device by applying separate passwords to the work profile and the personal space using the Mobile Security Policy.
  - Ability to white list corporate accounts to provision work-managed devices on which an unauthorized hard factory reset has been performed.
- **App Management**
  - Distribute and manage corporate apps through managed Google Play by using the existing Bundles feature.
  - Edit the app runtime permissions and remotely configure apps on devices.

Pre-enrollment Tasks

Before enrolling Android devices to ZENworks, you need to perform the following mandatory tasks:

- Enroll your organization in the Android in the enterprise program.
- Create and assign an Android Enterprise Enrollment policy.

Prior to commencing on the pre-enrollment tasks, you need to ensure that the basic configuration tasks to get started with the Mobile Management feature of ZENworks Configuration Management are in place. These include:

- Configuration of a user source
- Configuration of an MDM Server
- Creation of the Mobile Device Enrollment Policy
- Configuration of Firebase Cloud Messaging service

For more information on these tasks, see the Getting Started section in ZENworks Mobile Management Reference.

Enrolling your organization in the Android in the enterprise program

Before enrolling devices with Android in the enterprise, you first need to enroll your organization in the program. By enrolling in the program, Android recognizes ZENworks as the EMM vendor for your organization and thereafter any operation that has to be invoked on behalf of your organization, will be performed by ZENworks.

To enroll the organization, you need to create an Android Enterprise Subscription by navigating to the **Subscribe and Share** section in ZCC. While creating a subscription, you need to specify the Novell Customer Center credentials that have been provided to you, after which you will be re-directed to the sign-up UI hosted by Google. By registering your organization in this sign-up UI page, you access and distribute apps through

managed Google Play. You need to register your organization using your corporate Google account credentials. After registering, you will be redirected back to ZCC, where you can proceed with the remaining UI screens to complete the following:

- Association of a user context based on which only those users that are part of this user context will be allowed to enroll their devices to ZENworks.
- Selection of a language based on which the details of apps, meant for distribution, will be displayed in ZCC.
- Selection of a bundles folder where the bundles of apps will reside.

Creating and Assigning an Android Enterprise Enrollment Policy

Besides creating a Mobile Device Enrollment policy, you also need to create and assign an Android Enterprise Enrollment Policy. A Mobile Device Enrollment policy is required for the basic enrollment of any mobile device to ZENworks, whereas the Android Enterprise Enrollment policy is required for Android devices to be enrolled in the work profile or work-managed device mode. While assigning the Android Enterprise Enrollment policy, you need to ensure that it is assigned to the same set of users who are part of the user context associated with the Android Enterprise Subscription. After configuring these tasks, you can then have your users enroll their devices in one of the two modes detailed in the previous section.

Enrolling the device

The ZENworks server communicates with an Android device using the ZENworks Agent app. Therefore, to enroll Android devices in either the work profile or the work-managed device mode, you need to have the ZENworks Agent app installed on the device.

- For the work profile mode of enrollment, a new user can simply search for the ZENworks Agent app in the Play Store or can use the Invite Email to download the ZENworks Agent app. After logging in to the app, the user needs to follow the prompts, after which the device will be automatically enrolled in the work profile mode. Users who have already enrolled to ZENworks using the basic mode of enrollment and now have to be enrolled in the work profile mode, will receive a notification to set up the work profile when they open the ZENworks Agent app. Again, they need to follow the prompts to set up the work profile on their device. After the device is enrolled in the work profile mode, a badge icon is attached to the ZENworks Agent App icon and other system apps, which will help differentiate work apps from personal apps.
- For a work-managed device, a new or an existing user of ZENworks needs to factory reset the device (applicable for devices that have already been set up) or boot the device (applicable for new devices that have not yet been set up). The user needs to follow the initial setup prompts, till the user lands on the screen in which the Email ID needs to be specified. Here, instead of the email ID, the user needs to specify the ZENworks identifier for the Android enterprise program, which is **afw#zenworks**. When the user proceeds further, the ZENworks Agent app will be automatically downloaded and the user needs to simply follow the remaining prompts to set up the device as a work-managed device. Unlike in the work profile mode, work apps on a work-managed device will not have a badge icon attached to them.

Post Enrollment Tasks

After users enroll their devices in either of two modes, you can perform the following tasks that are relevant to both the enrollment modes:

- Distributing work apps to users
- Securing the device
- Monitoring device compliance

App Distribution

ZENworks distributes apps to users through managed Google Play, which is Android's app management platform for enterprise users. Subsequently, all app licenses are managed using managed Google Play. To distribute apps, you need to first approve these apps in managed Google Play.

Types of Apps

You can approve the following types of apps:

- Public apps that are available to the general public in Google Play.
- Private apps that are customized apps developed for specific enterprise customers. These apps are of two types; Google-hosted private apps and Self-hosted private apps.

As soon as the apps are approved in managed Google Play, ZENworks identifies these apps and populates them in ZCC. You can view these apps in the Apps Catalog page in ZCC. Simultaneously, bundles are automatically created for these apps within the Android Enterprise Subscription folder, thereby enabling you to distribute the apps to users

Distributing work apps to users

ZENworks allows you to distribute Android apps to only users and not directly to their devices. Before distributing these apps, you can choose to edit the default runtime permissions of these apps. ZENworks also provides you with the ability to remotely pre-configure a work app, so that the settings are applied automatically, as soon as the user launches the app on the device. In this case, the user is not required to take any action to set up the app on the device.

Securing the Device

You can secure work profile and work-managed devices by configuring password restrictions, device inactivity restrictions and by applying other additional restrictions. To do this, you need to create and assign the following policies:

- **Mobile Device Security policy:** Enables you to configure password restrictions and device inactivity settings.
  - Password restrictions include mandating a specific password length and including complex characters in the password.
  - Device inactivity restrictions include mandating an inactivity lock after a specific period of timeout.

- **Mobile Device Control Policy:** Enables you to apply additional restrictions on the device. These restrictions differ based on the mode of enrollment, which can be determined based on checkmark under the work profile and work-managed device columns. Some of these restrictions are as follows:
  - Device restrictions such as restricting the device camera, the copying and pasting of data between the work profile and the personal space of the device, and enabling factory reset protection.
  - App specific restrictions such as the editing of default Runtime permission values, restricting access to the public play store and restricting the modification of the app data.
  - Network restrictions such as restricting the editing of mobile network settings, restricting cellular data while roaming and restricting outgoing calls.
  - Audio restrictions such as muting the master volume and restricting the editing of volume settings.
  - Date restrictions such as allowing the configuration of the date, time and timezone.
  - OS Update restrictions to determine when OS updates should be installed on the device.
  - Keyguard restrictions such as disabling Smart Lock agents.
  - Display restrictions such as setting the brightness on the device, restricting ambient display and configuring screen timeout.

Monitoring the Compliance of the Device

To ensure that devices are compliant with the assigned rules and policies, you can create and assign a Mobile Compliance Policy to the Android devices. The Mobile Compliance Policy contains a pre-defined event based on which the compliance of a device is monitored. This policy enables you to audit, restrict and remediate devices that do not comply with the pre-defined event.

If a device is non-compliant and if the restrict action is imposed on the device, as configured in the policy, then the work apps on the device are restricted. As a remediation action, the work profile is removed from the device and work-managed devices are factory reset. These devices are subsequently unenrolled from ZENworks and retired.

Unenrolling the Organization

To unenroll the organization from the Android in the enterprise program, you should delete the Android Enterprise subscription from ZENworks Control Center.

Important Considerations Prior to Deleting the Subscription

Before deleting the Android Enterprise Subscription, administrators should be aware of the following:

- NCC credentials are required to delete the subscription.
- By deleting the Android Enterprise Subscription, your enterprise will be unenrolled from managed Google Play. However, data associated with this subscription will be deleted only after 30 days. Within the next 30 days, if you create a new Android Enterprise Subscription using the same email ID, ZENworks might be able to recognize the enterprise details and restore the subscription data.
- The user context associated with the deleted subscription, cannot be associated with the new subscription. You can select an alternate user context. To use the same user context, you need to either wait for 30 days or run the `zman subscription-clear-ae` command.

- You can also delete the organization from managed Google Play. The subscription and its data will be deleted from ZENworks only after 24 hours. To delete the organization from managed Google Play:
    1. Navigate to Managed Google Play and log in using the credentials that you had used to create the Android Enterprise Subscription.
    2. On the left panel, click **Admin Settings**.
    3. In the Organization Information panel, click the hamburger menu and click **Delete Organization**.
    4. Confirm your action in the **Delete Organization** pop-up.

For detailed information on each of the topics presented in this article, see ZENworks Mobile Management Reference.