Android Enterprise Device Management with ZENworks 2017 Update 2

www.microfocus.com/opentext

Article

opentext™

Introduction

With the release of ZENworks 2017 and ZENworks 2017 Update 1 earlier this year, we have started our journey on executing our vision of ZENworks being an truly Unified Endpoint Management (UEM) solution that provides superior self-services and application management in an identity centric, location aware fashion thereby enabling customers to save money and improve productivity.

In this quest for UEM solution, I'm happy to announce that ZENworks 2017 Update 2 has been certified by Google for Android Enterprise Work Profile solution set and OpenText™ is now listed in the Android business partner directory as a solution provider. Let's now go through the capabilities of Android Enterprise and its features and how it's been integrated in ZENworks 2017 Update 2.

Android Enterprise Capabilities

Android in the Enterprise brings together Android and Play to enable users to work the way they want, using the devices and apps they love, while giving IT admins the security and management features they need.

With mobile first security, Android helps organizations confidently deploy devices for everyone, with multilayered protection, robust app security, and secure separation of business and personal data.

Data Security

Business data is separated in a work profile or protected device-wide on work managed devices with full disk and file-based encryptions.

App Security

Work apps are authorized and deployed through managed Google Play. IT can prevent installation of apps from unknown sources and apply app configurations, for full control over app usage.

Device Security

Android device integrity is protected and maintained with verified boot, lock-screen policies, remote SafetyNet attestation services, Google Play Protect and hardware root of trust.

Collective intelligence

Android incorporates the best of Google, from machine learning for malware detection and cloud Security to artificial intelligence for smart, contextual assistance.

Android Enterprise Apps

Android apps intended for enterprise distribution via managed Google Play can be public or private.

Public Apps

Any general app available in public Google Play store can be made available to the enterprise users from managed Google Play. Typically apps used in the enterprise can fall under categories such as email apps, productivity, and collaboration or file storage apps

Private Apps

Organizations that develop Android apps which needs to be distributed to its users, but don't want these apps to be available outside the organization can use Google Play Console to publish a private app to managed Google Play and distribute the apps to its users using OpenText™ ZENworks. To use the capability, organizations needs to register with the google Play console as an app developer through which they can publish a private Android app.

Private Apps can be categorized into two different types.

- **Google hosted private Apps:** Publishing private Apps using this method lets organizations utilize Google's managed Google Play infrastructure thereby giving its users faster apps downloads, reduced data consumption during app updates and IT admins benefit from Google's reliability of service, easy administration and security.
- **Self-hosted private Apps:** Organizations wanting to host a sensitive private Android App in their own IT infrastructure/servers can use this method of publishing a private app. Though the app apk file gets hosted in the IT infrastructure of the organizations, a definition file needs to be added to the managed Google Play so that such apps can be distributed to the users.

Android Enterprise Devices

Android Enterprise devices can be classified into Personal (Work Profile/BYOD), Work (Fully Managed/Company Owned) or Purpose-built (Kiosk type) devices. ZENworks 2017 Update 2 supports feature sets of Work Profile which are typically BYOD type devices.

What is a Work Profile?

Enabling a work profile on a BYOD/Personal device allows organizations to manage the business data and applications they care about, but leave everything else on a device under the user's control. IT Administrators control work profiles, which are kept separate from personal accounts, apps, and data. By default, work profile notifications and app icons have a red briefcase so they're easy to distinguish from personal apps. Work profiles allow an IT Administrators to securely manage a work environment without restricting users from using their device for personal apps and data.

Android Enterprise Management with ZENworks 2017 Update 2

Thus far, we went through what an Android Enterprise is, its features and its capabilities with Work Profile. Let me now highlight the key capabilities with ZENworks 2017 Update 2.

Profile Management

With a simple enrollment process, ZENworks agent creates a secure Work Profile on a BYOD/personal device. The work profile on an Android device separates and protects work data from personal apps and content.

Data Leakage Prevention

IT admins can apply policies to restrict the flow of data from the work profile to the personal profile by disabling copy paste or screen capture in work profile. From Android 7.0 onwards, a separate password challenge policy can be applied to work profile thereby ensuring robust security of work apps and data.

Business Data Remote Wipe

ZENworks lets IT admins to remotely wipe the business data & remove work profile on user's Android devices without affecting user's personal apps and content.

Managed Google Play

Using managed Google Play IT admins can discover and authorize business apps. Using ZENworks such authorized business apps can be distributed to users. IT admins can also silently install and uninstall these apps.

Prevent Install from Unknown Sources and Debug Capabilities

As soon as a work profile gets created on an Android device, ZENworks blocks side-loading and app installs from third-party marketplaces; thus ensuring that no rogue apps gets installed inside the work profile. IT Admins can also prevent geeks from debugging any apps or data inside the work profile.

Enforce Compliance

By using the new Compliance Policy, IT Admins can enforce and restrict corporate data if device security policies are not met.

Managed App Configurations

IT admins can auto-configure URL/port settings, email addresses, server details, login names etc and eliminate the need to educate end users about first time setup.

Manage App Runtime Permissions

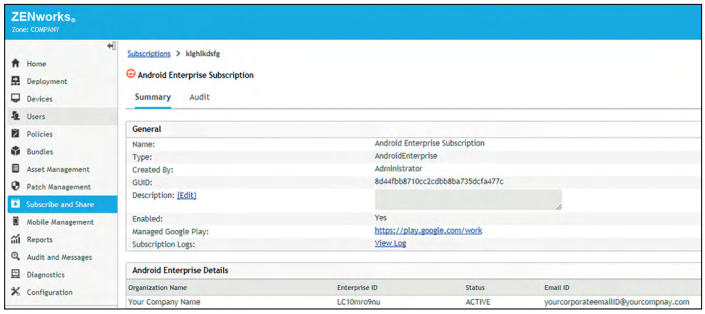
App Runtime permissions for each individual app can be easily controlled and pre-authorized/granted or denied by the IT admins using ZENworks.

Get. Set. Go!

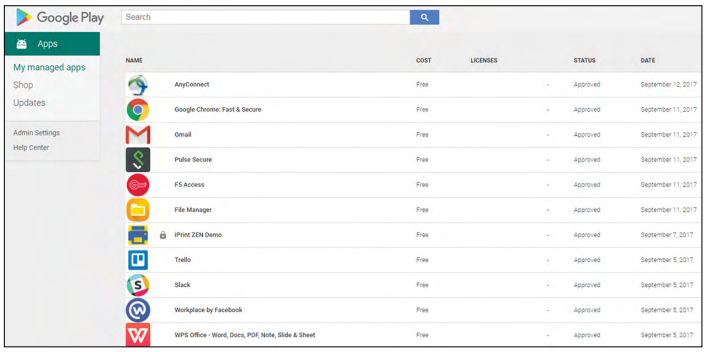
By now, you have learnt on the key capabilities of Android Enterprise and how ZENworks can manage them. Let's now go through how to get started in using these features and capabilities with ZENworks 2017 Update 2. I call it as GET, SET and GO!

GET

The first and key step is to create an Android Enterprise Subscription using a Corporate Google ID and associate a user context to it so that IT admins can manage the users and distribute apps.



Using Managed Google Play Store <**play.google.com/work**>, approve public or a private app. These apps are automatically imported into ZENworks which can be viewed from Apps Catalog page.



SET

With the Android Enterprise subscription created and work apps approved, the next step is to set various policies to ensure that IT admins have full control on the work profile and work apps.

ANDROID PROFILE ENROLLMENT POLICY

This policy lets users create a work profile on their devices. This policy works in conjunction with the Device Enrollment policy.

SECURITY POLICY

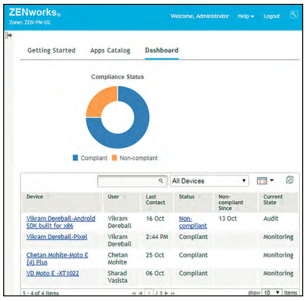
IT admins can specify various password or security restrictions for the device as well as security parameters for work profile.

DEVICE CONTROL POLICY

With this policy, IT admins can control various device capabilities such as access to camera or to prevent copy/paste and screenshot of work apps.

COMPLIANCE POLICY

IT admins can now enforce device compliance if security policy is not met. Compliance policy lets admins audit the non-compliance devices, enforce restrictions such as disabling work apps and take remediate actions such as removing the work profile, thereby ensuring that corporate data is secure. ZENworks now provides a dashboard view on the Compliance status of each device which was enrolled as a Work Profile Android device.

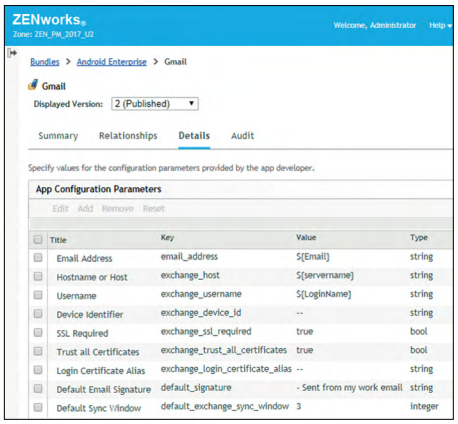


CONFIGURE MANAGED CONFIGURATIONS IN APP BUNDLES

IT admins can now easily manage and configure individual app parameters, for example, email ID, server names, login names etc using wild card parameters which ZENworks resolves based on the user sources and configurations. These resolved values gets sent to the respective app inside the work profile thereby pre-configuring the app automatically so that the app is ready to use without the need to users configuring themselves.

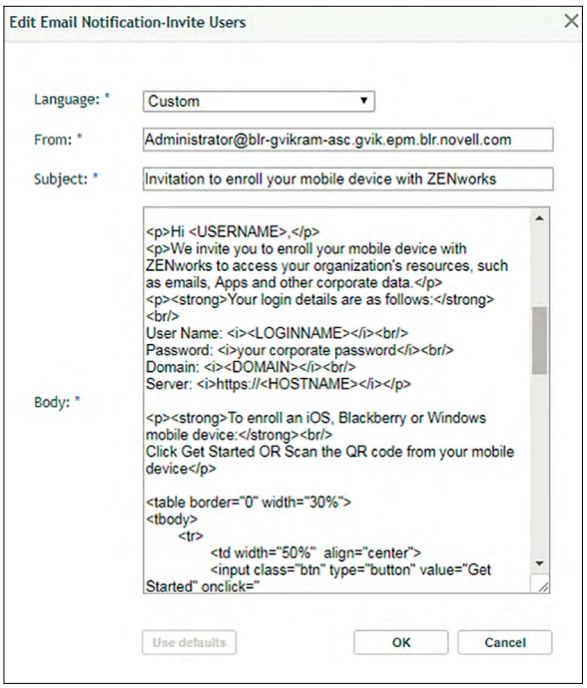
APPROVE AND CONTROL APP PERMISSIONS

Some of these runtime permissions include access to contacts, storage, camera, microphone, location etc. Based on the set values by IT Admins, whenever an app runs inside a work profile, either the runtime permission is automatically granted or automatically denied.



CONFIGURE INVITE LETTER

One of the new features in ZENworks 2017 Update 2 is the ability for the IT admins to configure and send an Invite Letter which lets users to easily enroll their devices into ZENworks. IT admins can choose whom to send invite letters as well as define which language this letter gets sent.

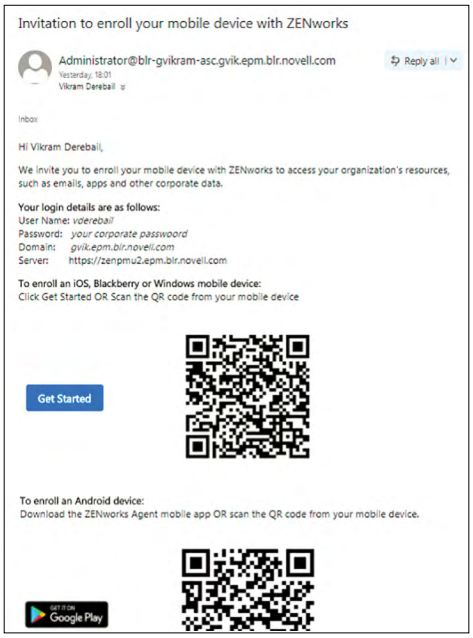


GO

Now that ZENworks has been set and made ready to manage devices using Work Profile, let's look at how you go about managing and distributing apps.

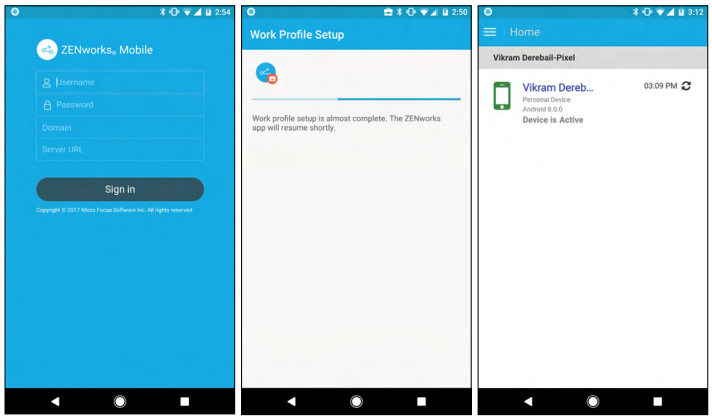
INVITE USERS

The first steps is to invite users to enroll their devices into ZENworks. Users receive an email with details of the server which they have to enroll into and links to download the ZENworks agent app.



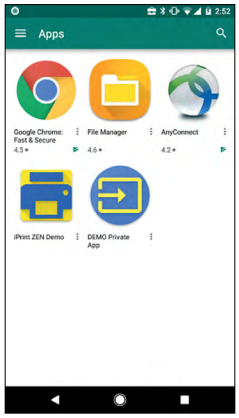
ENROLL USERS

Once the users download the ZENworks agent app and enter their credentials, work profile setup begins automatically and device gets enrolled into ZENworks.



APP DISTRIBUTION

IT admins can silently push install mandatory apps or make available Apps for users to install from badged Play Store. IT admins can also silently uninstall apps within the work profile.



UPDATE APP CONFIGURATIONS FOR DIFFERENT SET OF USERS

By creating multiple Android App bundles for the same app, IT admins can apply different set of managed configurations for different users or departments.

REMOTELY WIPE BUSINESS DATA

If a device is lost or based on user's request, IT admins can use the Un-enroll quick task to remove the work profile on the device thereby removing the business data. ZENworks does not erase the Personal apps and data and it remains intact on the device.

With these work flows and features, IT admins will be able to start using ZENworks to manage Android devices enrolled into the Work Profile mode of device management.

Learn more at
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™