Android Enterprise:

Accommodating mobility in the Enterprise

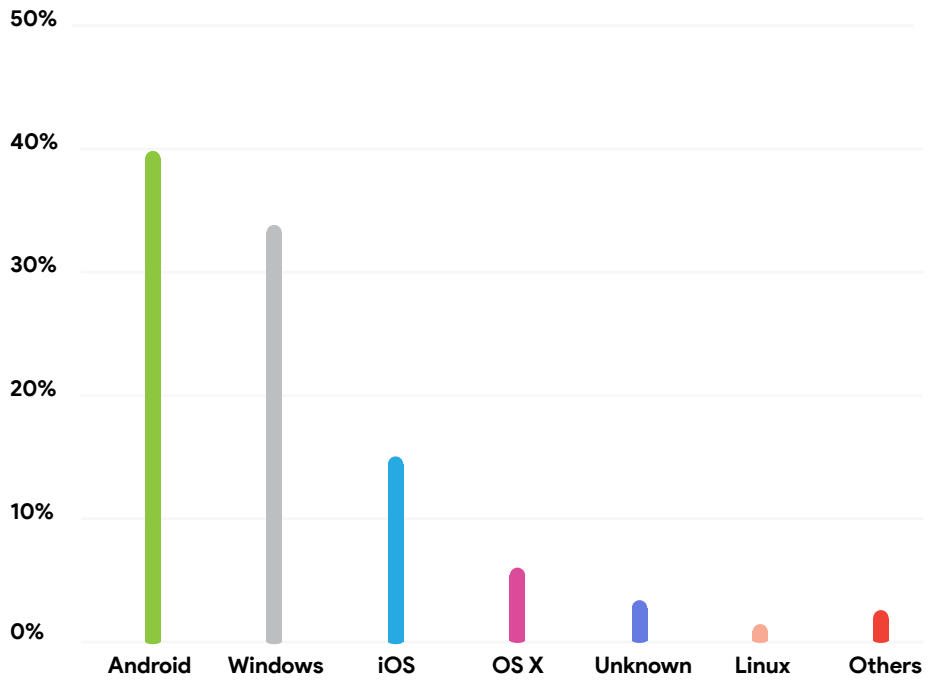
WHITE PAPER

hexnode

Table of Contents

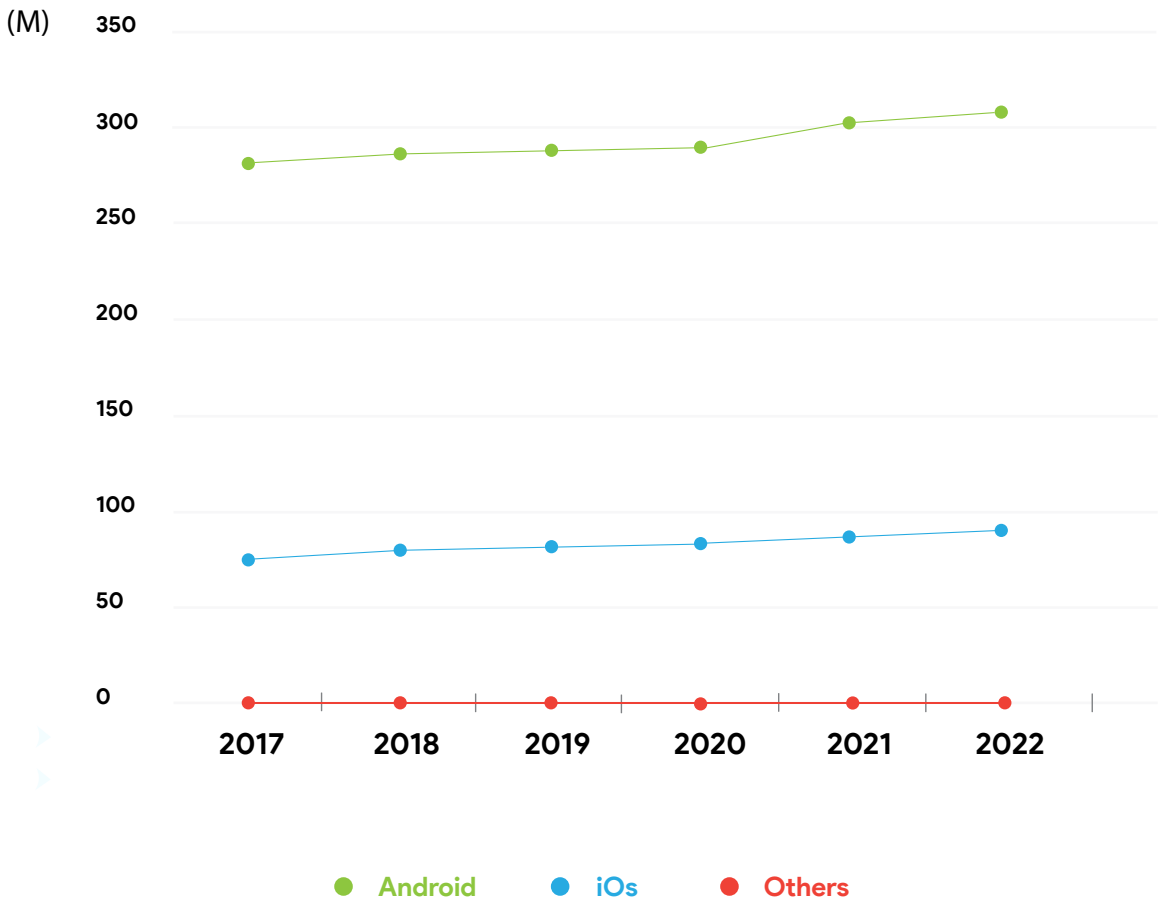
When Google started addressing the needs of the enterprise

Mobility has always been key to embracing digital transformation and building a strong workforce. Outfitting employees with mobile devices allowed companies to get massive improvement in productivity, time management, and work-life balance - all of which contribute to the bottom line. Although Android was by far the largest OS system in the consumer world, the enterprise remained a different story. Most businesses preferred Apple's iOS platform (before the competitive entry of iPhone, Blackberry was the #1 choice of businesses) over Android. However, things took a different turn with the advent of BYOD. As employees started flocking in with their daily driver devices, organizations could no longer keep Android at an arm's length.



Operating System Market Share World Wide-January 2020

Source : StatCounter Global Stats

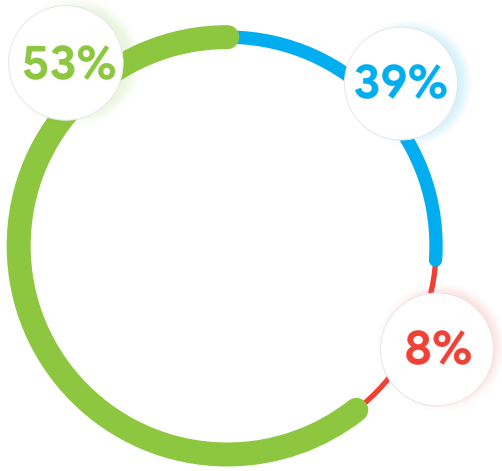


World Wide Buisness use smartphone forecast

Source : IDC

Traditional IT environments were inadequate to address the management challenges that came with the BYOD trend. To combat the associated security and fragmentation issues, Google started working on new solutions to make Android more enterprise-friendly and debuted Android Enterprise as a program to enable standardized management experience across Android devices. This white paper explores core management capabilities in the program and offers actionable guidance on getting the most out of your device deployments with Hexnode's Android Enterprise integration.

Android into the Enterprise: A little back story



Android tops CYOD choice

Source : IDC

The last decade has witnessed a clear shift in the enterprise mobility landscape – a transition from the legacy Windows OS to other prevalent platforms. The concept of Bring Your Own Devices has been there since 2004 but it took some time for it to become a real trend of the corporate world. Accommodating work and play on a single device became a necessity. Gradually, the line between work and life blurred and Android was one among the major choices of employees. The major concern of businesses was that these employee devices must adhere to strict security standards.

Finding its place in the corporate world, Google introduced the Device Administration APIs (Application Programming Interface) in 2010 with Android 2.2. With this, Android devices became open to being managed using a UEM solution though with very few management capabilities.

Before Android 4.0 Ice cream sandwich, Google offered less for enterprises as compared to its major and maybe the only rival Apple. Blackberry, the original leader in the enterprise realm had quickly been dethroned by Apple with the advent of BYOD. The consumer-focused Android operating system then added enterprise features in its later versions (4.2 Jellybeans and 4.4 KitKat releases). For many years, device administrator APIs had been the

standard method to deploy and manage Android devices in the enterprise. However, this approach was potentially too restrictive and has been more centered around corporate-owned gadgets. As Google always provided Android as an opensource operating system allowing others to build atop of it, many of the Android manufacturers like Samsung pioneered advanced security with custom APIs for their platform.

> "Together with a wide range of management, applications and device makers, we believe the Android for Work program provides businesses and workers with the choice and flexibility they need to get things done at work."

-Rajen Sheth

Director of Product Management, Android and Chrome for Work

The real solution for BYOD from Google actually came in 2014 with Android 5.0 Lollipop in which Android Enterprise (formerly Android for Work) was launched. The IT teams were provided with more flexible tools and policies to keep corporate and personal data safe and secure. With support for Android Enterprise, work data could be accessed from managed devices without compromising user privacy. Though it's a great effort to consolidate Android management, some manufacturers were so reluctant to integrate with the program immediately. However, beginning with Android 6.0 Marshmallow, Android made it a standard addition to its OS and mandatory for all the manufacturers. In 2017, Google has renamed Android for Work as Android Enterprise as a sign of its increased commitment towards enterprise mobility. Since then Google has been steadily improving its approach to device management.

Android Enterprise Evolution

2004

BYOD

2008

Android 1.0 -

Launched the first commercial Android device

2010

Android 2.2 -

Device Admin API

2014

Android 5.0 -

Launched Android for Work (Optional solution for manufacturers)

2016

Android 6.0 -

Made Android for Work a mandatory component for manufacturers

2017

Renamed Android for Work as Android Enterprise

2018

Android 9.0 -

Device admin is marked as deprecated for enterprise use. Deprecated some device admin policies.

2019

Android 10.0 -

Deprecated policies are no longer available to DPCs. Android Enterprise is made the default management solution.

Fostering work-life balance

As organizations are increasingly embracing enterprise mobility it's imperative to adopt a management approach which addresses the security concerns. With Android Enterprise, Google is addressing the issue of security on enterprise Android devices by giving enterprises the level of control they need at the same time preserving user's privacy. Basically, Android Enterprise is offering a way to separate work apps from personal apps on employee devices without enduring the security risks and hassles of the past. Android Enterprise features a few key components:

- Work profiles for non-enterprise device management which isolates and protects work data.
- Support for company-owned devices that enables secure device settings like Factory Reset Protection.
- Managed Google Play to approve and distribute work apps simplifying the process of app deployment and ensures that every app is approved by the enterprise.
- Silent app installation for both store apps and in-house apps.
- App configuration for pushing corporate settings to managed apps.
- Mandatory and automatic device-level encryption

When provisioning a device, an organization can have two different deployment scenarios to choose from:

- Work profile – A dedicated work profile is created that isolates and protects work data. IT can manage business data but have no visibility or control over the personal apps and data on the device.

- Fully managed device – Organizations have complete control over the device allowing no personal use by default. This provides a maximum level of management capabilities on devices. A subset of the fully managed device is the dedicated device.

  Dedicated device – Company-owned devices can also be locked down to a single app or a set of apps used for a specific purpose.

The Android Enterprise work profile has lessened the control and visibility that an organization can have to a dedicated work container. But the biggest issue with this approach is the limited control and visibility over the entire device as an organization cannot access anything out of the work container. For organizations looking for more of a traditional way of management with added security and visibility, it's better to choose a Fully managed mode.

Work profile (profile owner mode)	Fully managed device (device owner mode)
- Profile-based management.	- Complete management.
- Most suited for BYOD deployments.	- Apt for corporate-liable deployments.
- User privacy is respected.	- Priority to corporate security.
- Only the work profile could be managed by IT. Everything else is controlled by the user.	- IT can manage the whole device and apply all the possible policy controls.
- The device cannot be locked down to the kiosk mode.	- Can configure the device as a dedicated device. Kiosk mode can be configured to restrict the usage to a single app or a limited set of apps
- The device is controlled by the user and organization can have full management control over the work profile.	- The user's organization can have full management control over the entire device.
- The device can be used for personal purposes.	- Ensures that devices are used only for work purposes.
- IT can enforce work container restrictions such as copy/paste or screen capture, can selectively clear the work data keeping personal data intact and configure an access passcode for work containers for added protection.	- Device wide controls like complete device wipe and Factory Reset Protection are possible

Work profile (profile owner mode)	Fully managed device (device owner mode)
- Only a limited set of controls for IT admins.	- The company can have control over an extended range of features that are not available with the profile owner mode.
- Work apps run alongside personal apps but marked with a work badge.	- Only work apps can run on the device.
- Quick enrollment methods like QR code provisioning is not available.	- Fast and streamlined onboarding via Zero Touch Enrollment and QR Code provisioning is possible.
- No device resets are needed for enrollment.	- Can be assigned only during the initial device set up. A factory reset is needed.

The enterprise version of Google play

For devices enrolled in Android Enterprise, Managed Google Play is the enterprise app store. Managed Google Play is basically a version of Google Play which allows IT admins to securely deploy and manage apps across the workforce. It combines the advantage of familiarity with Google Play, the world's largest distribution platform, with a set of enterprise-oriented features. This makes it easy for the employees to see which all apps are allowed by their enterprise and install the apps they want onto their device. It's free to integrate into the EMM solution for Android Enterprise customers. IT admins can use managed Google Play to:

- Discover apps
- View app details
- Purchase app licenses

Typically, your enterprise purchase, manage and distribute apps via an EMM console. They can give their team full access to the right apps to get their job done. The Managed Google Play makes app distribution even easier by allowing IT admins to make all the configuration from the EMM console itself. It has tools to publish private and web apps and curate public apps needed for work. With Managed Google Play, enterprises can have choice and security at the same time. Undergoing SOC 2 and SOC 3 audits which are benchmarks of stringent privacy and security standards, Managed Google Play operates with a high level of privacy and security.

Hexnode for Android Enterprise management

Android Enterprise provides APIs and other tools for developers to build Enterprise Mobility Management (EMM) solutions that leverage the enterprise features built into Android devices and Google Play.

Onboarding

Device provisioning

Device management

App management

> Google has made Android Enterprise a mature enterprise-ready platform. Android Enterprise has been bound with Hexnode enabling organizations to cover all the deployment scenarios."

Onboarding

With a certified UEM solution in place, organizations can be enrolled with Android Enterprise program using any of the two methods:

Managed Google Play account

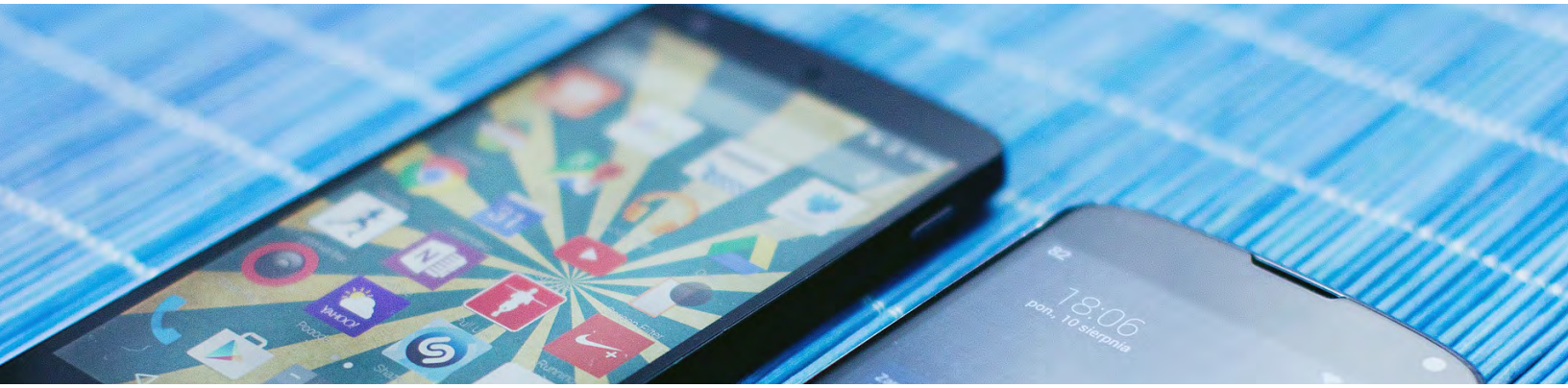
- For organizations that don't use any Cloud identity or G Suite.
- Simple to set up and works with any Google account.

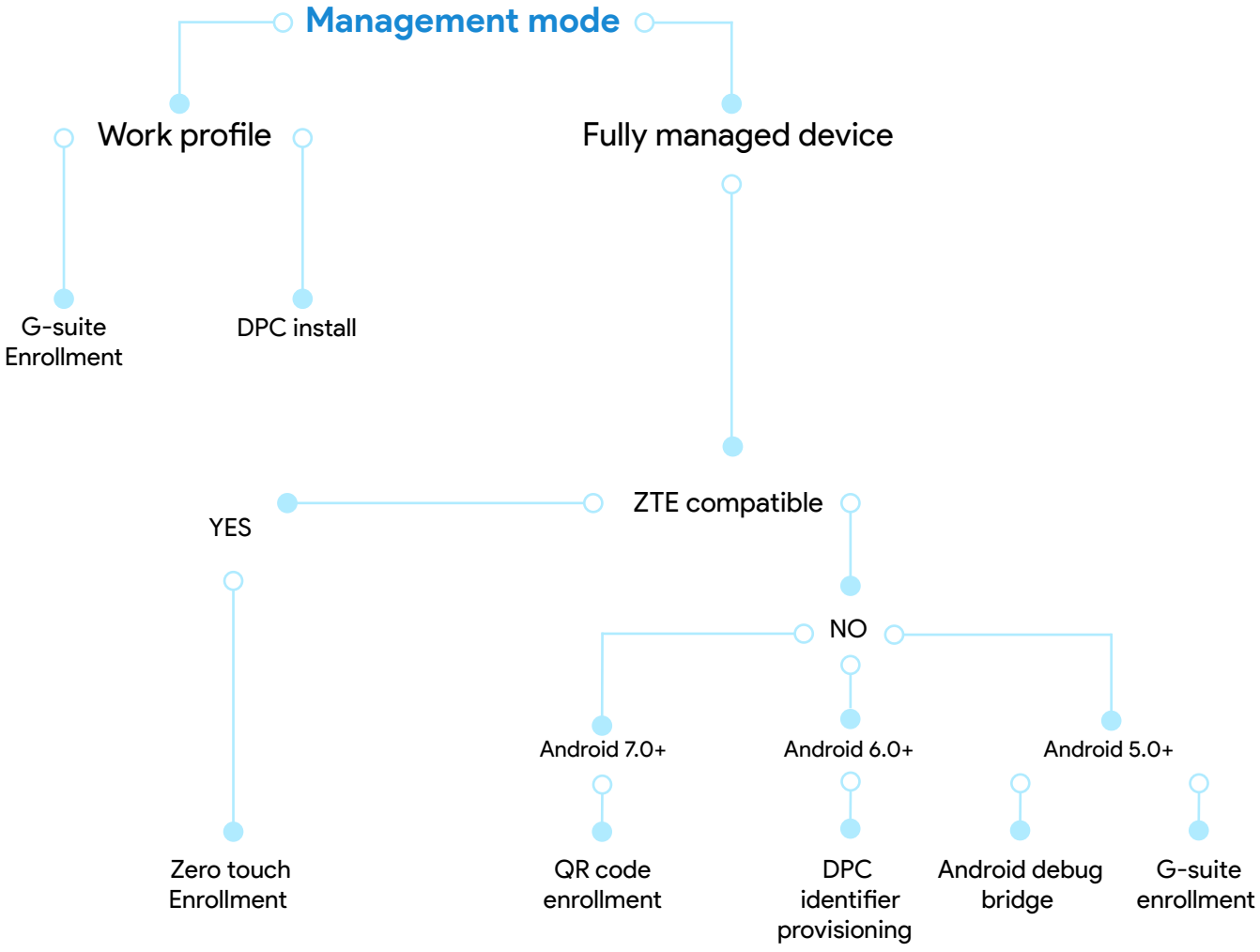
- No need to claim a domain or set up a service account.
- No domain verification required during enrollment

Google account

- For organizations that use a Cloud identity or G Suite.
- Requires company domain to be claimed.
- Must retrieve the Google account information using the Google directory API.
- Manual sign into Google account is required during the device set up.

Device provisioning





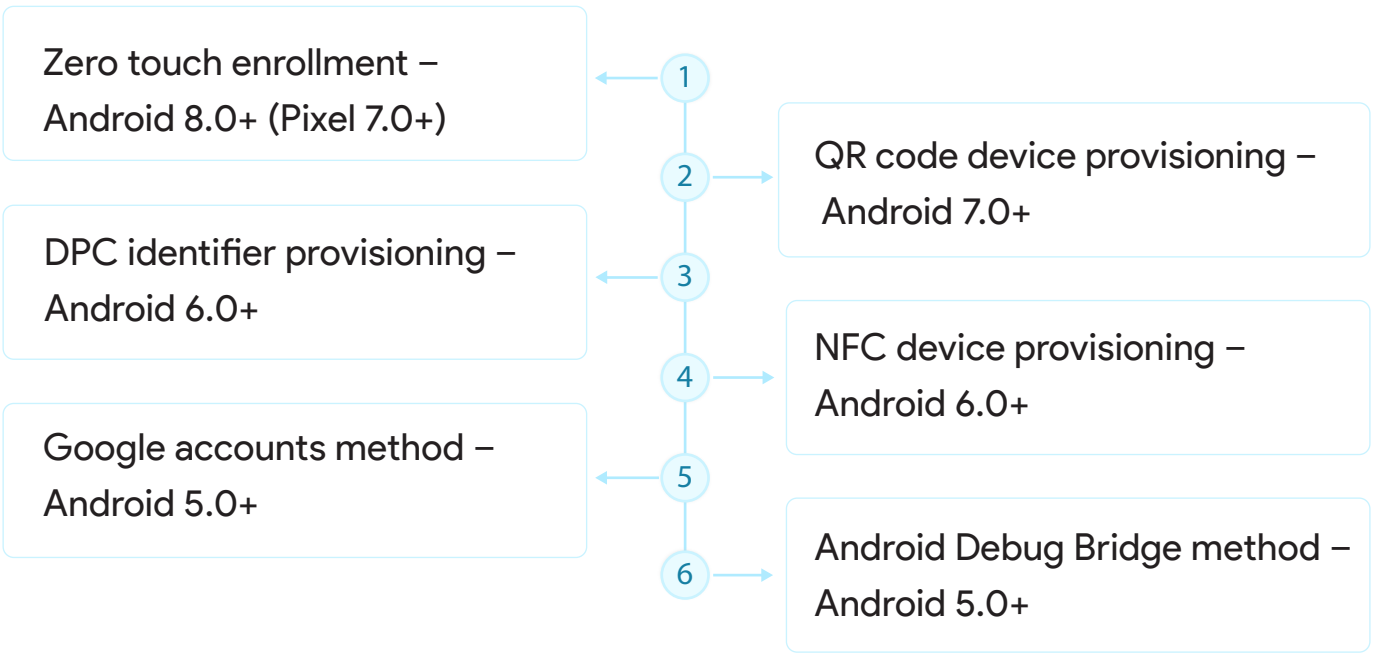
Different options are available for device provisioning according to the device management type.

Work profile

- DPC-first work profile provisioning – Enrollment by downloading the UEMs DPC (Device Policy Controller) from Google Play.
- Google account work profile provisioning – Enrollment using G Suite credentials.

Fully Managed Device

- DPC identifier provisioning – Enrollment using a DPC identifier (afw#hexnodemdm).
- NFC device provisioning – Bump devices using the UEMs NFC provisioning app
- QR code device provisioning – Scans a QR code generated by the UEM.
- Zero touch enrollment – No touch enrollment for devices purchased from authorized resellers.
- Google account device provisioning – Enrollment using corporate G Suite credentials.
- Android debug bridge method – Useful in cases where the number of devices to be enrolled is less.
- Samsung Knox Mobile Enrollment – Out-of-the-box enrollment for Samsung devices running Knox version 2.8 or later.



Android Zero Touch Enrollment

Zero touch enrollment where the device comes configured out of the box to enroll onto a UEM is the quickest provisioning method for corporate-owned Android devices. It offers a seamless deployment method making large scale rollouts fast, easy and secured for IT. Organizations can purchase devices from an authorized reseller and have them shipped with enforced management so employees can open the box and get started. When the device is first turned on, it's forced into the settings pre-configured by the IT admin.

Requirements:

- Compatible Android device with Android 8.0 (Oreo) and above or Google Pixel phone with Android 7.0 (Nougat) and above, purchased from an authorized reseller partner
- An EMM provider like Hexnode that supports fully managed device provisioning

Device management

Admin can configure management, security and usability features for users and devices. Apart from the basic management features, Android Enterprise enrolled device has a set of additional management capabilities. IT can protect corporate data with custom policy enforcement.

- Enforcing an additional set of restrictions like factory resetting, connectivity settings, and FRP
- Configuring password protection for work container.

> “A successful deployment is about more than just selecting the right devices; it's about getting them configured and rolled out into the hands of users as quickly and easily as possible.”

-James Nugent
Google Product Manager

App management

Using Managed google play - the enterprise version of Google play, EMM console can distribute apps to managed devices. Managed Google Play can be accessed directly from the EMM's console. Users can install only what's whitelisted for them.

App management features

- Silent app installation
- App configurations for deploying corporate settings to applications.
- Customized Managed Google Play store layout.
- App permissions to set up what a specific app can do and have access to right before they're assigned to any device.
- Manage and publish self-hosted private apps

App configurations and permissions for managed apps

With Hexnode, it's easy to limit the features that a managed app can have, and IT can even pre-configure the app before pushing them onto the user devices. App permissions allow organizations to pre-configure permissions for Managed Google play apps to access Android device features. By default, apps that require access permissions will prompt users to accept or deny permissions. By defining app permissions, organizations can remotely manage this and make sure that apps can't access unnecessary features keeping sensitive corporate data protected.

App configurations let the admin remotely configure features for Managed Google Play apps. Once the app is installed, all the settings will be supplied automatically. As all apps don't support configurations, it's essential to consult with the App developer to see whether the app is designed to support configuration settings. Within the supported apps, the developer specifies which options can be configured and IT can use the options displayed in the Hexnode console to define custom configurations. This saves a lot of time for IT who can pre-configure apps and distribute them to multiple users in a single stretch as well as users who can use the apps without any further configurations.

OEM Config

OEM Config is a new Android standard defined by Google that enables device makers to differentiate their devices with specialized functionalities at the same time guaranteeing immediate and unified management support by UEMs. With OEMConfig, Hexnode can now offer its customers the full range of fine-grained hardware and security features for Android Enterprise devices without having to build each and every OEM-specific setting into the product. It leverages managed app configurations as a way to push OEM-specific features to the managed devices.

Why OEMConfig?

- A standardized way to build and support OEM-specific features
- Addresses the dilemma of fragmentation in the Android ecosystem and unlocks a level of management beyond the Android Enterprise program
- Ensures zero-day support for new updates. There's no need to wait for EMMS to specifically integrate new features
- Developmental costs for supporting new features are minimized for UEMs
- No need to upgrade the UEM agent app to access new features

This is how it works:

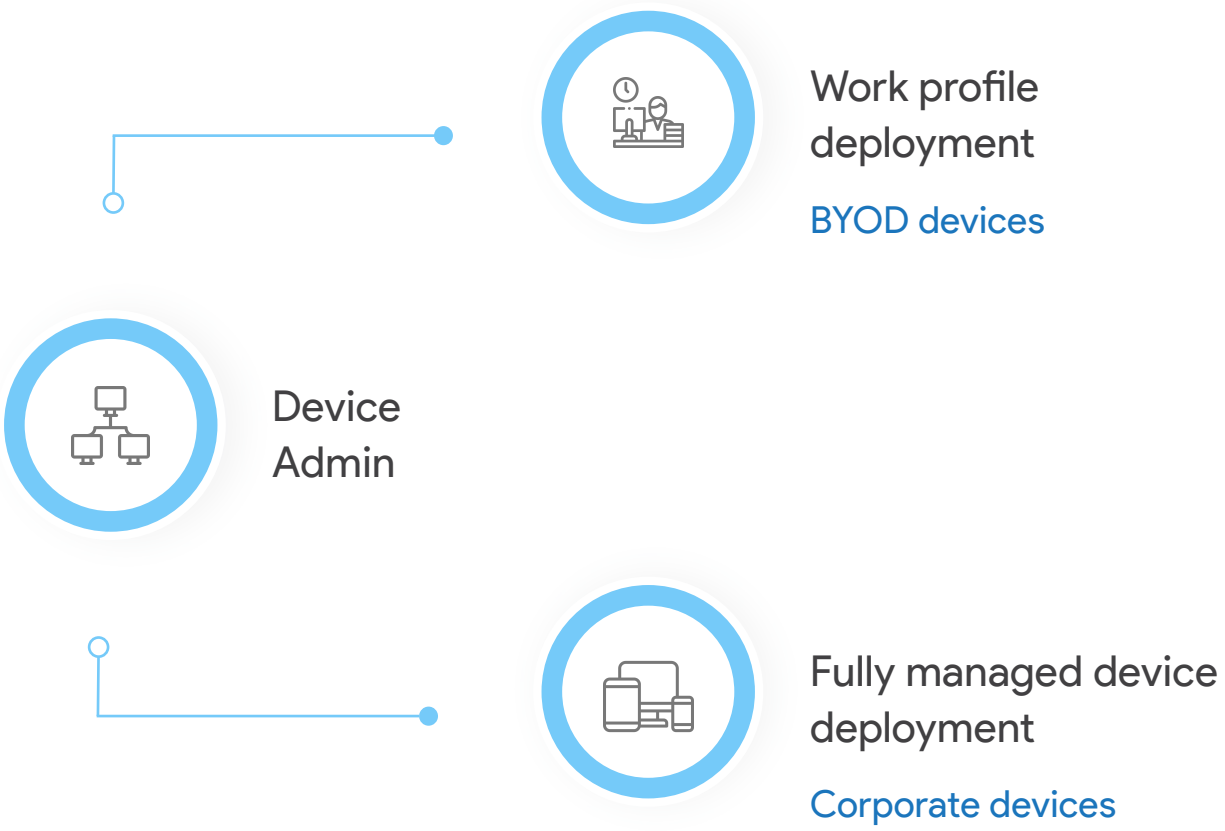
- Device manufacturers that support OEMConfig build their own OEM-Config apps with their APIs and host them on Google Play
- The organization approves and adds the OEMConfig app to the UEM console
- Hexnode allows administrators to customize the settings using managed app configurations
- Silently push the app to the Android Enterprise devices via Hexnode
- The customized OEMConfig app gets installed on the device and uses the configured settings to manage the device.
- Once a new feature is added, the OEM updates the app and Hexnode automatically adds support to the new feature

Supported OEMConfig vendors

Vendor	OEM config App
- Samsung	- Knox Service Plugin
- Zebra	- Zebra OEMConfig powered by MX
- Honeywell	- Honeywell OEM config
- Kyocera	- Device Config Plugin
- Datalogic	- Datalogic OEMConfig
- Spectralink	- Spectralink Device Settings
- Lenovo	- Lenovo OEMConfig
- Unitech	- Unitech OEMConfig
- CipherLab	- CipherLab OEMConfig
- Seuic	- Seuic OEMConfig

The future of Android in the enterprise - Phasing out Device Administrator

Recognizing that legacy management have not much to do in a BYOD environment, Google announced its intention to deprecate some of the Device admin APIs in 2017 to promote Android Enterprise adding a wealth of more comprehensive features. Starting with Android 9, the admin policies like password enforcement, disable keyguard features, disable camera, etc. are marked as deprecated. With the release of Android Q in 2019, those APIs are no longer available to DPCs. As Android Enterprise is mature to meet the management requirements of all enterprises, Google recommends migrating from legacy Android management to Android Enterprise



Android Enterprise Recommended: where IT gets expert guidance for Android device management

A certification program for devices and services that are recommended for business use by Google. Help businesses to confidently choose the devices, enterprise mobility management services, and carrier services meeting the highest standards for the optimum enterprise experience best suited for their needs.

The elevated set of features for devices as required by Google:

- Minimum hardware specifications for Android 7.0+ devices.
- Support for bulk deployment including Android Zero Touch Enrollment.
- Unlocked device availability.
- Security update delivery within 90 days of release.
- Consistent application experience within the Android Enterprise work profiles and on fully managed devices.

  etc.,

Enterprise features recommended by Google:

- Advanced features across at least two of the below management scenarios:
  - ✓ Work profile
  - ✓ Fully managed device
  - ✓ Dedicated devices
- Proven ability to deploy Android Enterprise with advanced security and management features.

- Documentation and guides on how to enroll with Android Enterprise management sets.

- Knowledgeable teams to assist with deployment.

etc.,

Conclusion

During the last decade, Android has aligned its platform to modern-day security best practices to become the clear choice of businesses in a variety of sectors. There is a strong desire to push past the idea of "Android is ready for work" in an era where businesses have woven BYOD into the fabric of what they do. Recommending Android Enterprise as a viable alternative for legacy management (Device Admin API), Google is acknowledging that the needs of the modern business world will be better served by the Android Enterprise fully managed device and work profile modes. Work Profile mode is ideal to provision the device a dual persona which feels like a perfect blend of separating personal and work data while still making them easy to access.

> "Hexnode MDM with Android Enterprise leverages the robust security and management capabilities in the Android platform."

Hexnode has integrated everything under Android Enterprise to its comprehensive platform. Hexnode has solutions tailored for every roles and business processes within an organization, for both BYOD and corporate-owned device deployment scenarios. Right from the process of onboarding to app management and configurations, Hexnode covers every phase of Android lifecycle management. The goal of an effective UEM solution is to strike a balance between privacy and security. With the minimal effort of configuring and highest flexibility for device management and user privacy, organizations should be seriously looking into a UEM solution which can support Android Enterprise which is the default Android management tool of the near future.

Mitsogo Inc. Unites States (HQ) 111 Pine St #1225, San Fransisco, CA 94111
Tel: Intl +1-415-636-7555 Fax: Intl +1-415-646-4151

Copyright © 2019 Mitsogo Inc. All Rights Reserved.