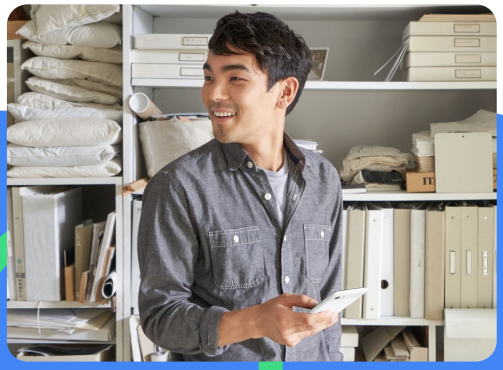
android

# Android Enterprise Deployment Guide

android

# Table of contents

android



# Introduction

Android Enterprise is a set of APIs and features included with Android and Google Play which offer comprehensive mobile device management, application management and security capabilities for a wide range of use cases, and for every employee-owned and company-owned device type. Companies gain a holistic solution for security, management, and app distribution for their Android devices.

This deployment guide is intended to provide guidance and best practices on how to deploy Android Enterprise to secure and manage Android devices. This includes instructions for Android Enterprise deployment, policy setup, change management, and onboarding best practices.

## Audience

This guide is intended for IT administrators seeking guidance for successfully deploying, securing, and managing corporate data on Android devices. It is not a general guide on using Android and does not explain how it works. Some topics mentioned here will occasionally fall outside the scope of this guide. In these cases, we will provide references to outside resources.

The documentation in this guide will at times be technical in nature so the reader is expected to have experience researching advanced mobility topics.

## How to use this guide

The sections are self-contained but ordered to be read sequentially from setup to provisioning to management steps. While reading every section is not required to progress, you should still understand all the concepts presented in them. These best practices are intended to supplement your enterprise mobility management (EMM) guide.

android

# Setup

## Enterprise binding

To manage Android devices with an EMM solution you will need to perform an enterprise binding that will connect your Google enterprise to your EMM server. The identity type selected during this process will determine how the binding is done.

### Managed Google Play Accounts (recommended):

This option is for organizations that ***don't*** use Cloud Identity or Google Workspace.

- With this identity an enterprise and enterprise ID will be created.
- Managed Google Play Accounts are automatically created by the EMM, and provisioned for devices and end users during EMM client setup.
- Managed Google Play Accounts cannot be used to identify a person.
- Managed Google Play Accounts provide access to managed Google Play, allowing users to install and use work apps selected by IT admins.
- No other Google service (like YouTube, Drive, etc.) can be used with this account.

**Best practices tip**

With managed Google Play Accounts you will be asked to provide a Gmail account for administrative purposes. We recommend creating a new Gmail account and setting the backup email on this account to a group in your IT department. Also consider setting up two-factor authentication for increased security while adding additional owners to maintain redundancy.

android

## Managed Google Accounts:

**This option is for organizations that use Cloud Identity or Google Workspace.**

Customers that use Cloud Identity or Google Workspace already have an existing enterprise ID and existing Google Accounts for users.

When setting up a device, each user must manually sign in with their existing Google Account. The account will give them access to managed Google Play in addition to the other Google services already provided by their organization's Cloud Identity or Google Workspace plan.

Because this type of identity is tied to a customer's existing domain, each domain can only be linked with one EMM console.

**A few things to keep in mind** concerning managed Google accounts:

### Configuration:

- For domain ownership claim and configuration you need to find your domain or Internet administrator to verify ownership of the domain (upload TXT record or html file).
- Google Service account and API integration need to be configured manually.
- Changing EMM requires unbinding your domain and removing every user from the EMM, which includes device reenrollment, factory reset (for corporate owned device) or work profile removal (for BYOD).
- You need to configure SAML connection for SSO with IDP provider.

### User Management:

- Users need to be created in Google for each Android user, or import users from active directory.
- Employees may have signed up for a Google account using their @mycompany.com email address.

android

## Networking

Most connections originate from the device, so Android generally does not require inbound ports opened on the network in order to function correctly. There are a number of outbound connections that administrators should be aware of when setting up their network environments for Android Enterprise.

It's recommended that you contact your EMM partner for additional information on their specific network requirements. General network requirements that apply regardless of EMM solution can be found in the Android Enterprise Network Requirements document.

### Note

Traffic to Google endpoints should also bypass SSL inspection. SSL intercepted traffic to Google services are often interpreted to be man-in-the-middle attacks and are blocked.

android

# Provisioning

The provisioning method describes the way the EMM Device Policy Controller (DPC) is downloaded onto an Android device. A DPC app, sometimes called an agent, controls local device policies and system applications on devices. The provisioning method chosen depends on the device management mode, hardware capabilities, and the version of Android running on the device.

For work profile on employee-owned devices, there is one common option, and it does not require a factory reset on the device.

### Manual DPC install

This method involves having the DPC manually downloaded and installed from the Google Play store. In some cases the DPC installer is sideloaded onto devices but this is not recommended.

There are more provisioning options for company-owned devices but these can only be employed during initial device setup. This means that devices already in use will require a full reset.

### Zero-touch (recommended)

Zero-touch enrollment allows IT admins to create provisioning configurations and apply them to devices via a web console. These configurations are automatically applied to devices on first boot. There is no need for the admins to physically handle the managed devices making this the easiest deployment method in most cases.

**Note:** Devices need to be zero-touch compatible and purchased from authorized resellers.

- Ideal for most fully managed device deployment scenarios.
- Available on all Android 9.0+ devices with Google Play Services and on select 8.0+ and Pixel 7.1+ devices
- Samsung 9.0+ devices support zero-touch and Knox Mobile Enrollment.
- Find authorized resellers at the zero-touch page.

android

## NFC

Using a programmer app provided by the EMM, administrators can transfer information about DPC, Wi-Fi, and other EMM configuration parameters to another device using NFC tag.

- Ideal for “white glove prep” scenarios where a large number of devices need to be provisioned and the programming device can be physically present.
- **Available on Android 5.1+**
- Currently not supported for work profile on company-owned devices.

## QR code

Similar to the NFC method, QR code provisioning allows passing along configuration parameters to other devices but requires only a camera on the device being provisioned. In addition,  there is no need for a physical programming device to be present. The admin can generate a code and email it to an end-user or print it on a piece of paper. During device setup, a user taps on the welcome screen 6 times to initiate download of the QR reader app then scans the code. As of Android 9.0, the QR code scanner is built into the operating system.

- Ideal for devices that don’t support NFC and scenarios where devices are distributed remotely and a programmer device cannot be present.
- **Available on Android 7.0+**

## DPC Identifier

Also known as “afw#” method, during device setup, when prompted for an account to use, the user instead enters afw#<EMM code>. That is “afw#” and an EMM-specific code appended to it. The advantage of this provisioning method is that it’s available on the widest variety of Android devices. It requires no optional hardware such as a camera or NFC chip.

Unlike the ZT, QR, and NFC methods though, there is no way to provide extra parameters for configuration. This method requires the most manual steps and should be used when other methods are not readily available.

- **Available on Android 5.1+**
- Currently not supported for work profile on company-owned devices.

android

# Management

The management mode chosen determines the Android Enterprise features available for management, provisioning methods that can be used, and how devices can be enrolled.

There are two Android Enterprise management modes that can be chosen for a given use case:

- Work profile
- Fully managed device

If personal data will be allowed, we recommend work profile for employee-owned and company-owned devices to ensure employee privacy. If no personal data will be allowed, a fully managed device is recommended for work only and kiosk scenarios.

**Note:** Pre-Android 11 work profiles could be configured on fully managed devices which allowed IT admins full visibility on the device (including the “personal” profile). This led to potential confusion around privacy with personal usage on company-owned devices. Android 11 establishes consistency for customers needing to ensure employee privacy when personal usage is involved by introducing work profiles on company-owned devices.

**Features available for each management mode can be found below:**

Work profile

Fully managed device

android

## Application management

### Managed Google Play:

App management in Android Enterprise is centered around managed Google Play and merits some explanation here. Play is used for:

### App distribution:

Once an app is approved, admins can choose to have them automatically pushed to users' devices or simply make them available in in the managed Google Play Store for users to choose (more on this to follow).

**Web App distribution** - Web apps are published to managed Google Play and can be distributed like other Android apps.

### App approval:

Admins browse Play and choose the applications that they would like their users to have.

### Approving app permissions:

Admins can accept app permissions on behalf of the user.

**Best practices tip**

Managed configurations allow admins to set configuration properties for applications that support them

android

Another aspect of managed Google Play is the managed Play Store client on the user's device. When admins approve apps that their users can install, the Play Store client is where users can choose to install them, assuming the apps aren't already pushed automatically by the admin.

**A few things to keep in mind** concerning apps on the managed Play Store:

- Managed Play store defaults to an allowlist. Every app that is allowed to be installed by users must individually be chosen by the admin. Optionally, the admin can choose to enable access to all applications available on Play.
- IT admins can approve any app that is available in public Play or private apps that have been shared with their enterprise.
- Managed Play does not support paid applications.

**EMMs use the Android Management APIs or the Play EMM APIs** to communicate with Play directly or integrate the managed Play iFrame in their consoles.

| | | |
|---|---|---|
| Android Management API | Play EMM API | Managed Play iFrame |

android

## Private applications and Play Developer Console

Organizations that develop custom apps that they need to distribute to their users (and only their users) need to become familiar with the Google Play Developer Console. The console allows you to:

- Upload custom apps.
- Mark custom apps as private so they're only available to specific enterprises.
- Manage multiple development channels for custom apps to enable beta testing before wider distribution.

**App submission process from managed Google Play iFrame:**

1. Log in to EMM Console and open the managed Google Play iFrame.
2. Upload and and give a "Title" to your custom app.

There are other aspects of managed Google Play not covered here like custom store layouts, system update management, and Google Play Protect. A thorough understanding of managed Google Play is highly recommended.

### Best practices tip

If your EMM integrates the managed Google Play iFrame in their console, you can manage your organization's custom apps and access the Play console directly from your EMM console. This enables faster publishing of custom apps, and it does not require you to pay the one time fee of $25 for creating a Play Developer account.

**App submission process from Google Play Console:**

1. Log in to the Google Play console with the same account that was used to bind your organization to an EMM. It isn't mandatory to use the same account, but it's the best practice.
2. Upload your custom app.
3. Select the checkbox that denotes the app is for private distribution.
4. Create separate distribution channels for development and production.

android

# Policy management

Android Enterprise provides a variety of productivity and security features. We recommend working with your EMM vendor to determine the best policies to meet your management needs. Below are some policies we suggest our customers consider:

## Control Google Factory Reset Protection

Factory Reset Protection (FRP) is a consumer security feature on Android devices, aimed at preventing reuse of a device if it is stolen. FRP is enabled automatically when a Google account has been registered on the device and will be disabled if the Google account is removed from the device prior to the Factory Data Reset. Once FRP has been activated, it will prevent use of your device after an untrusted Factory Data Reset. This means if your device has been Factory Reset in any other way than manually through the device settings or via EMM command, the FRP Lock will be enabled.

If Google FRP is enabled, customers that allow personal Google accounts on managed devices will need to enter credentials for that account after a hard reset.

### Recommendations:

- Remove personal Gmail accounts before hard resetting and turning device back to IT.
- In fully managed device mode, EMM can control or turn off factory reset protection.
- The IT admin sets a different Google account, which acts as a recovery account, to unlock the device after a reset.

android

## Device Security

### Specify Device Unlock or Work Challenge

We recommend setting a password policy to secure your corporate data. Android devices support PIN, pattern, password, and biometrics that can be set at the device or work profile level.

For fully managed devices the IT admin can specify a device password. For work profile devices, the IT admin can allow a single password for the entire device or specify a second password or “work challenge” to unlock work apps separately, with different complexity requirements.

### Enforce Google Play Protect

Google Play Protect is Google’s built-in malware detection for Android. This Anti-Malware scanning and remediation service is installed by default on every device (both corporate and consumer) that's running Google Play Services.

EMMs can enforce that Play Protect’s app scanning feature is enabled on employee-owned and company-owned devices.

### Disallow Unknown Sources

Allowing users to install applications from anywhere other than a known source (Google Play Store, OEM store, EMM) can introduce security vulnerabilities.

The EMM can disallow app installations from an unknown source on employee-owned and company-owned devices.

### User Experience

Android provides many options for securing and configuring your devices. When considering your configuration options, finding a balance between security and productivity can help to greatly improve user experience. This section will highlight a few of those considerations.

android

## Cross-profile considerations

**Contacts:** By default, corporate contacts from the work profile are available to personal applications as read-only. End users can search their corporate contacts from the personal contacts application. Additionally, corporate contacts will be displayed in caller ID for incoming phone calls.

- Determine if the default behavior meets your requirements. Admins can disable this behavior so that corporate contacts are not available from the personal contacts app or caller ID.
- Bluetooth: Determine if bluetooth devices should be able to access corporate contacts. This can be enabled/disabled by policy.

**Sharing & Views:** By default users are allowed to share files/pictures/data from the personal profile into the work profile. Sharing from the work profile to personal profile is disabled by default.

- Determine if the default behavior meets your requirements. Admins can allow/disallow sharing across profiles by policy.
- Widgets: Determine if users should be allowed to use widgets from work apps. This can be enabled on a per app basis.
- Connected Apps: Android 11 introduces a framework for apps to interact across profiles. For example, a calendar app installed on work and personal profiles could display all (work & personal) types of events in a single view. This can be enabled on a per app basis.

### Default File Handler

In order to provide a seamless user experience consider including a default file handler application in your configurations. This will allow users to easily open basic file types (documents, images, audio, video, etc) that they may receive in email. We recommend using Files by Google for this.

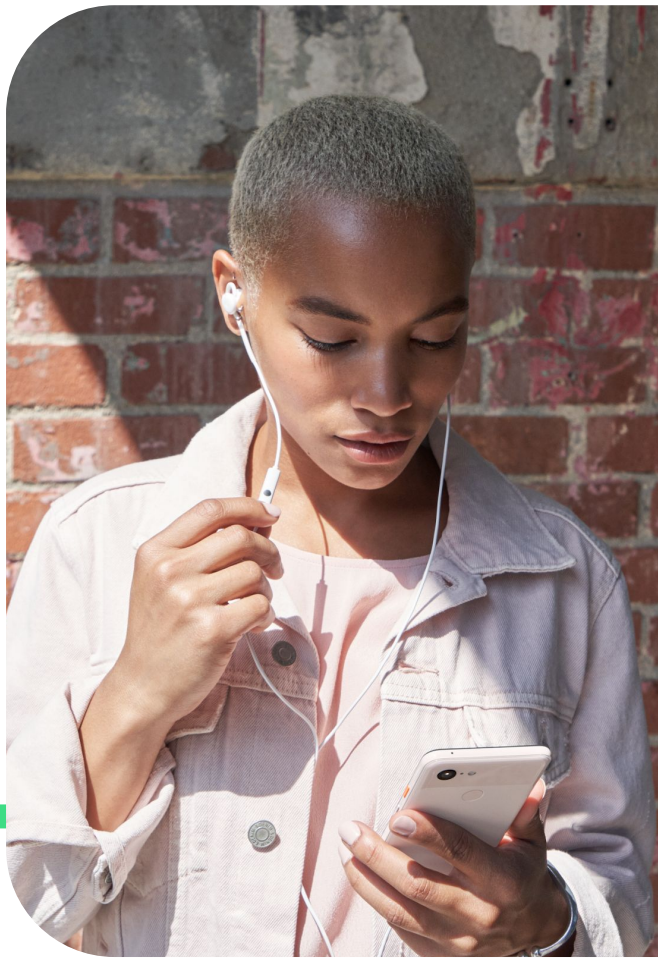
android

## Requirements mapping and proof of concept (POC)

Above we outlined a few of the main policy considerations when configuring your Android deployment.

But there are many more that can be implemented by your EMM. We recommend working with your EMM to map your requirements to their supported features.

Set up a proof of concept to evaluate your configurations and ensure the success of your deployment.



android

# Get help

### Resources

- Android Enterprise Help Center
- Android Enterprise Help Community
- Android Enterprise User Adoption Kit
- Android Enterprise Security

The Android Enterprise Help Community and your EMM can help you with the rest.

### Solutions directory

Android Enterprise Recommended Devices

Validated list of EMMs