

# Android for Work Applications Overview

Deploy, manage, secure, and publish work applications using Google Play for Work

Last updated: June 2015

# Contents

[About this guide](#)  
[Introduction](#)  
[Google Play for Work](#)  
    [Application discovery and licensing](#)  
    [Application distribution](#)  
    [Application configuration](#)  
    [Application security](#)  
    [Private application publishing](#)  
    [Android for Work App support](#)  
[Additional resources and support](#)



## About this guide

This guide is designed to help IT decision makers and implementers understand how Android for Work empowers companies to securely distribute business applications on their Android devices. It includes information about:

- Deploying and managing third-party and internal applications for Android for Work native management
- Enabling applications through the [Android for Work App](#)

## Introduction

Android was built to help people connect and give them amazing mobile experiences. Today, it's the world's most popular mobile platform with more than 1 billion active users worldwide. Android's application platform has made it possible for people worldwide to communicate, play, entertain, and educate themselves. Users can install the latest in mobile productivity—from trusted independent software vendors and promising startups—to their own IT organizations.

Android for Work creates a secure framework for companies to put any application in Google Play to work, making it easy for IT administrators to approve and distribute Android app to users' verified-safe devices. With Google Play for Work, you can browse, purchase, deploy, and manage work applications while ensuring malware and other threats are minimized.

## Google Play for Work

Google Play for Work brings the best of Google Play to work and is available free of charge to Android for Work customers. This extension of Google Play enables Google Play functionality for the enterprise. For Android for Work customers, Google Play for Work is the trusted gateway for enterprise application distribution. In the native Android for Work configuration, Google Play for Work allows you to easily distribute any Play app to users' devices, without the need for proprietary wrappers or custom development.

In addition to the public Google Play catalog, you can utilize Google Play for Work to distribute private, enterprise-specific applications to employees. Google Play for Work brings together each step in the lifecycle of an application rollout, from browsing and comparing applications, to approving updates for your users. Each step integrates with [partner Enterprise Mobility Management \(EMM\) platforms](#) to deliver a consistent Android experience.

To learn more about how applications work on Android for Work, review the following topics:

- [Application discovery and licensing](#)
- [Application distribution](#)
- [Application configuration](#)
- [Application security](#)
- [Private application publishing](#)
- [Android for Work App support](#)

## Application discovery and licensing

With Android for Work, you can:

- Discover business applications in the new enterprise-oriented Google Play for Work store.
- Review the permissions required to install an application and approve applications for distribution by accepting these permissions.

Google Play for Work also introduces a new bulk purchasing model, which allows app developers to offer user licenses for purchase on the Google Play for Work store. You can then allocate those licenses across your user base on a per-user basis, and reclaim or reallocate licenses from users that no longer require that app.

Learn about [Google Play Services](#) and [App Licensing](#) on the Android Developer's site, or visit the [Google Play Help Center](#).

## Application distribution

Once applications have been selected and approved for your domain, you can distribute those applications to customizable groups of users through an EMM console. You can push the installation of business mandatory apps on a user's device or simply make an app optionally available for the user to browse and install. Installations require no user intervention for the app to appear on their device.

If an app is made optional, it appears in the Google Play for Work store on the user's device. Users can browse their available work applications within the Google Play for Work store client, which is fully curated and only displays those applications specifically selected for them by their administrator.

## Application configuration

After an app is installed, you can configure that app for each individual user if that app has built in support for app configurations. Developers can add configuration options to their apps and easily publish those options to be seamlessly displayed within a [partner EMM](#) console. You can then define and pass custom configurations to different users or devices remotely, allowing applications to push configure settings themselves and modify behavior without any user interaction. Configurations are always tailored to any specific app, because developers build support for and publish the app configuration details themselves.

## Application security

Google Play for Work provides a trusted delivery mechanism to get work applications on employee devices by allowing you to explicitly approve which applications are deployed to the Work Profile. You can also disable installs from unknown sources and the use of developer tools to sideload applications. Even private, enterprise-developed applications can leverage this trusted distribution mechanism, based on your approval.

You can rely on Google services-based protections, such as Google Play's ability to detect vulnerabilities and potentially malicious code within applications through regular scanning of Google Play.



Learn more about security by reading the [Android for Work Security white paper](#).

## Private application publishing

You can use Google Play for Work to distribute internally developed or enterprise-specific applications in addition to Google Play's catalog. You can use Google Play for Work's hosting capabilities to conveniently and securely distribute apps. Alternatively, you can host an app and utilize the Google Play infrastructure only for delivery to devices.

Hosting with Google gives you several benefits, including sophisticated vulnerability scanning, production management tools like alpha and beta channels, automated device compatibility testing, and Google Play's high server uptime and global server distribution.

## Android for Work App support

For devices that don't natively run Android for Work, the Android for Work App can be downloaded from Google Play to provide many of the same features, including application deployment through Google Play for Work. You can leverage the Google Play for Work store on devices for optional applications and silently push mandatory applications using the same Application Programmer Interfaces (APIs) and management interface used in the native solution.

Unlike the native solution, the Android for Work App requires applications to integrate with the Android for Work Software Development Kit (SDK). Google's partners leverage this SDK in their existing security technologies to enable you to produce Android for Work App-compatible versions of internal applications, which can then be hosted using the same private app publishing mechanisms and deployed to Android for Work App users.

For third party developers integrating with the SDK, Android for Work App-compatible versions of their applications will also be available on Google Play, though visible only in the Google Play for Work admin console or when deployed to user devices using the Android for Work App.

## Additional resources and support

- Get support from your EMM provider
- Consult the [Google Play for Work Help Center](#)
- Review the Google Play [Developer Distribution Agreement](#), [Google Play for Work Developer Distribution Agreement Addendum](#) (paid apps only) and [Developer Program Policies](#)
- Check out the [Android for Work Security white paper](#)