



powered by Notify Technology



ANDROID ENTERPRISE MOBILE MANAGEMENT (EMM) OVERVIEW

What is Google EMM and why do I need it?

Android Enterprise is a Google-led initiative to enable the use of Android devices and apps in the workplace. The program offers APIs and other tools for developers to integrate support for Android into their enterprise mobility management (EMM) solutions. The Android Enterprise solution is a combination of three components: your EMM console like **Notify's MobileRMM™**, Android Device Policy, and managed Google Play.

How do I sign up to start using Google EMM?

To set up Android Management Account, you need to register your company using a Google Account this can be a standard G-mail account. The account must be one that is not already associated with an enterprise or managed by an EMM. If you need to setup a Google Account you can click [here](#).

Once you have a Google Account you can use the setup wizard in Notify's MobileRMM™ console to complete the setup. For detailed instructions on how to complete this setup click [here](#).

Now that you have a Managed Google EMM account what are the key benefits?

There are two main components that we will focus on. The first is Device management for corporate owned and personally owned devices. The second is application management using the Managed Google Play store.

- **Device Management:** All Android devices that an organization manages through your EMM console must install the Device Policy Controller (DPC) during setup. The DPC is an app supplied by Notify's MobileRMM™ that automatically applies the management policies set in your EMM console to devices.
- **App Management:** Managed Google Play is an enterprise version Google Play that facilitates certain app management capabilities for Android Enterprise solutions. It combines the familiar user experience and app store features of Google Play with a set of management capabilities designed specifically for enterprises.

Device Enrollment

Notify's MobileRMM™ supports both Corporate owned or bring your own device (BYOD) device enrollment types.

BYOD devices can be set up with a **work profile** — that allows work apps and data to be stored in a separate, self-contained space within a device. An employee can continue to use their device as all their personal apps and data remain on the device's primary profile. An employee's organization has full management control of the apps, data, and settings in their device's work profile, but has no visibility or access to the device's personal profile. This distinct separation gives enterprises control over corporate data and security without compromising employee privacy.



Fully managed deployments are for company-owned devices intended exclusively for work purposes. With a fully managed device, organizations can enforce Android's full range of management policies, including device-level policies that are unavailable to **work profiles**.

► For a detailed walk-through on how to enroll Android devices with Notify's MobileRMM™ platform click [here](#).

Managed Play Store

Managed Google Play is Google's enterprise app store of applications for Android Enterprise. You can use Notify's MobileRMM to manage app deployments through Managed Google Play for any Android Enterprise scenario. How you add Managed Google Play apps to MobileRMM differs from how Android apps are added for non-Android Enterprise. To access the Managed apps store simply navigate to <https://play.google.com/work> and login with the Google account you created. Store apps are approved in or added to Managed Google Play, and then synchronized into MobileRMM so that they appear in the Apps list. Once they appear in the Apps list, you can manage assignment of any Managed Google Play app as you would any other app.

► For a detailed walk-through on how to manage Apps with Notify's MobileRMM™ platform click [here](#).