android

Simplifying distribution and configuration of apps

Using managed Google Play, Android Enterprise empowers IT with app management that's standardized, consistent, powerful, and simple

The challenge

As IT administrators plan a mobility deployment, they must ensure that employees can quickly access the apps they need. The following requirements are critical:

- Securely distribute and remotely configure approved public and private apps for employees
- Manage permissions, privacy, security settings, and app updates
- Protect business data from leaks to other apps and cloud services

The Android difference

Android Enterprise delivers comprehensive features through managed Google Play that make app deployment and configuration easier no matter which devices or mobility management strategy you choose. With managed Google Play, an IT admin can choose from over 1 million available apps; approve, configure and distribute apps silently; or make them optional for users to install.

Beyond apps being publicly available on the Google Play Store, managed Google Play offers powerful in-house publishing features as well. IT teams can easily upload an app (APK file) and distribute it in minutes; private apps can be scanned and vetted by Google Play Protect; and these publishing tasks can all happen within the Enterprise Mobility Management (EMM) console.

Choosing, delivering, and remotely configuring apps

Once IT admins enable Android Enterprise within their EMM console, they can search for and approve apps for their users -- the entire Play Store catalog is available to choose from. For each app IT admins want to enable for users, they can choose the app and accept permissions on their behalf. Once deployed, IT admin approved apps are separated from personal apps on BYOD devices.

IT admins can set the selected apps to be pushed automatically (and silently), or to be available in the Play Store as optional for users to download. When updated versions of apps become available, a prompt can be sent to an IT admin to review the updates, or the new versions can be automatically sent to end users.

As IT admins curate apps for end users, they can customize the Play Store so only apps chosen by IT appear for users to download. They can also adjust the layout of the Play Store and how apps are grouped and organized.

Some apps support managed configuration, which are parameters that the IT admin can set within the EMM console. For example, with an email app, managed configuration can help save time for end users by pre-populating email addresses, server names, and authentication certificates. EMMs are able to detect which apps support these configurable parameters and can present them to IT admins when they are approving the app for distribution.

Managing and configuring accounts and identities

The Google Play store is the recommended mechanism for delivery and management of apps, and it requires each user to be logged in with a Google account. Having large numbers of users means that IT administrators need a dedicated method to manage the bulk creation of Google accounts.

Managing Google accounts starts inside the EMM console, which sets up a secure link to Google and uses APIs to create Google Play accounts. These accounts are then pushed out to devices to log in users automatically. Accounts can apply either to individual users with Android devices or to Android devices that might be shared among users.

Each user can use the same account on all their devices, and accounts can be deleted at any time when a user leaves the organization. By default, these accounts are anonymized and Google cannot see the user's identity, unless IT admins prefer to use Google Workspace accounts, which are also supported.

For users with work profiles, they will see a Google Play account for their personal Gmail and another for the managed Google Play account. IT admins also have the ability to add an account that can be used to bypass factory reset protection if desired.

Publishing private apps

One of the most useful features of the managed Google Play Store is the ability to easily publish in-house apps. IT admins that are familiar with using the EMM to directly distribute in-house APKs will find that managed Google Play extends this functionality by providing a private space on the Play store for their apps. Once uploaded, apps can be distributed to devices using the Google Play infrastructure.

Uploading apps on Google Play provides several advantages, including increased app security. All uploaded apps are scanned for malware, poor coding practices, and feedback is provided to developers. This process validates the security of the app itself before it is pushed out by Play's secure app distribution process.

When developers are ready to publish a private app, they can either upload the app via the EMM console, the Google Play Developer Console, or Play Developer APIs. The easiest process is to use the EMM console because EMMs have a direct interface to Google Play, where they can use a service account to upload apps. IT admins can upload APK files in just a few clicks via their EMM into the private Play Store, and publish quickly to their end users. If IT admins require more advanced publishing flows such as beta versions, this is also possible through the EMM interface.

Conclusion

Managed Google Play is one of the most powerful features of Android Enterprise, offering IT admins the ability to manage their most critical app publishing needs. Through an EMM management console, IT admins can choose, set permissions, remotely configure and deliver apps, and even publish private apps. Managing apps through an EMM enhances device deployment security and maintains privacy for the end user.

Contact your EMM to deploy Managed Google Play today