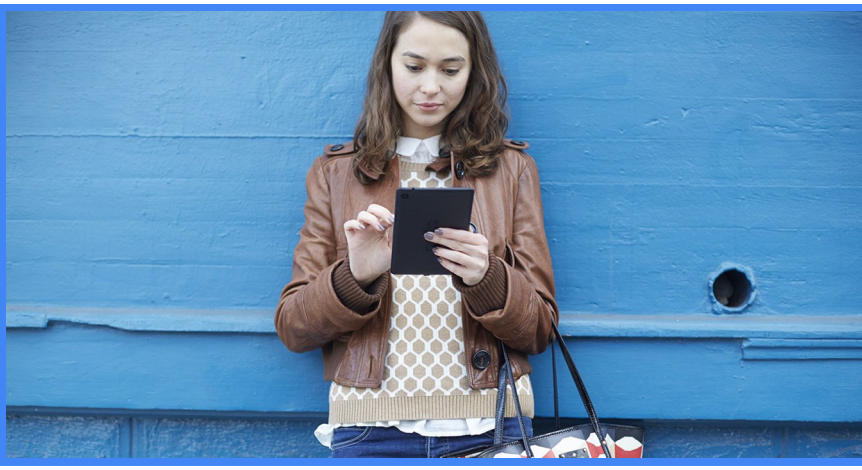
android

stratix

Enabling your BYOD program with the Android work profile



Android allows an enterprise to not only secure corporate data, but also respect enterprise employees' personal privacy, across a broad range of devices with a consistent management approach

The Challenge

BYOD is often promoted to IT as an opportunity for cost savings. But, in many cases, the promised reduction in device purchases are overshadowed by the cost of supporting a complex, heterogeneous device fleet. Furthermore, users of BYOD often raise questions about employer's visibility over personal data, and motivations to get them to do more work in their personal time. Data regulation and concerns about personal data loss mean companies are very cautious when managing users' personal devices.

The Android difference

With Android, the original promise of BYOD can be realized. Android allows an enterprise to not only secure corporate data, but also respect employees' personal privacy, across a broad range of devices with a consistent management approach. With over 85% of the world's smartphones using Android, it is critical to support Android in your BYOD program. Let's see how it works…

Android's work profile

From Android 6.0 Marshmallow and later, Android devices support an OS-level container called a work profile. The work profile contains all corporate applications and data and ensures that the data is separated from any personal apps and data a user may have.

The two profiles run side by side in the home screen of the device, with work apps and notifications badged with a briefcase. Users can arrange apps however they wish without affecting where data is stored. Users can also multi-task between work and personal apps through the familiar 'recents' screen while data remains separate.

Securing work data

Separation between a user's personal data and work data is enforced at the OS kernel level across processes, memory and storage. All applications from Google Play work out of the box with separate data storage and there's no need for modification of applications.

The lifecycle and policies for the work profile are managed through a comprehensive range of EMM providers that integrate with Android. IT admins can enforce a range of policies, including the following critical elements for preventing data loss:

- **Screen lock** - Enforce a minimum lock complexity or set a lock screen just for the work profile.
- **Encryption** - Ensure compliance with encryption policies.
- **Copy/paste** - Prevent data being copied from work apps And pasted into personal apps.
- **Inter-app sharing** - Specify which work apps can share data with personal apps or block entirely.
- **App whitelisting** - Use managed Google Play to curate your enterprise app store. You explicitly authorize which apps can be installed in the work profile to get access to corporate data.
- **VPN** - Apps in the work profile may be secured on the network through a variety of VPN options, including the ability to ensure only apps in the work profile can use the VPN.

android

stratix

Enrollment

Enrolling a device with a work profile couldn't be simpler. The user downloads your EMM's app from the Google Play Store and signs in using their corporate credentials. The EMM app does the rest. After the work profile is created, many EMMs allow IT to specify a list of apps, configurations and certificates to be pushed to the work profile automatically, allowing users to be up and running within minutes.

Keeping personal data privates

In the personal profile, the employee is in control. They can continue to use the apps that they choose. Personal apps along with system-wide apps, such as the keyboard and the launcher, are controlled by the user, and may not be inspected by IT.

Furthermore, if IT needs to remotely wipe corporate apps and data, for example when the employee leaves the company, they can confidently wipe corporate data from the work profile, leaving the employee's personal data untouched.

Android gives IT admins controls to ensure device-wide integrity while preserving privacy, such as:

- Block app installs from unknown sources
- Require Google Play Protect anti-malware service to be switched on
- Define screen lock complexity

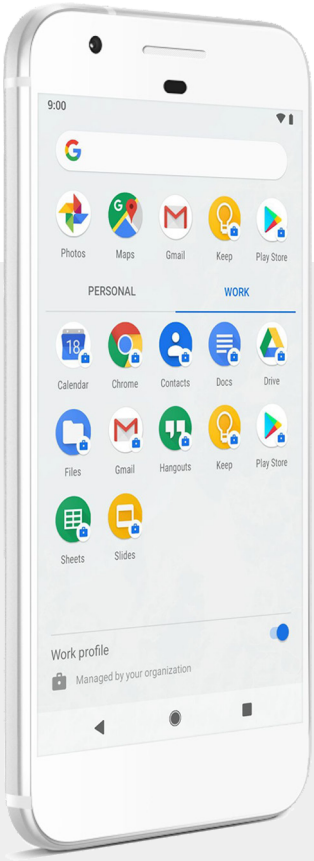
Work-life balance

An important part of a successful BYOD program is helping employees disconnect when they're away from work. In some countries, this is mandated by law. Android's work profile provides the best of both worlds – when employees want to disconnect from work, they can easily toggle off the device's work mode, or admins can toggle it by policy. Switching off work mode suspends the work profile, stopping all work apps from running, syncing in the background or presenting notifications.

Choosing what devices employees can bring

The stance you take on what devices to support will depend on your security posture. Google recommends the following best practices:

- Organizations should standardize on Android 6.0+ and use Android's work profile mode. Use our device catalog[1] to browse the wide range of devices available.
- If many employees have older Android devices, consider funding, or partially funding, employee purchases of new devices as an employment benefit, in exchange for them activating work apps on their device.
- For more controlled environments, set a policy through your EMM to put a device out of compliance, and therefore block data access, if a security patch hasn't been applied in the last 90 days.



Conclusion

Work profile on Android brings the best of both worlds to BYOD: security over corporate data and privacy over personal data. Android work profile is a must have for any company deploying BYOD.

Call your EMM today to get started deploying Android work profile. Need an EMM? Search the full list of EMMs and other partners that support work profile here[2].

[1] android.com/enterprise/device-catalog/
[2] https://androidbusinesspartners.withgoogle.com