android

Empower **User Privacy** on Company-Owned, Personally Enabled Devices

With the work profile in Android 11, IT organizations can balance enterprise data security with consistent employee privacy protections.

The challenge

Employees demand privacy over their personal data and apps, and are concerned about IT monitoring their activity, even on their corporate-owned devices. As a result, 38 percent of corporate-owned devices go unmanaged due to push back from employees, according to IDC.

For IT and security admins tasked with preserving data security on corporate-owned, personally enabled (COPE) devices, the challenge is ensuring device and data protection without intruding on employee privacy.

The Android difference

Android 11 brings the work profile to company-owned devices, enabling IT and security teams to keep full control over the device, including personal and work apps and work data without any visibility into personal apps and data. On company-owned devices, the work profile offers the same privacy employees expect on their personal devices so they can feel confident that their personal usage is private. But the work profile also offers additional controls over personal usage to keep devices compliant with IT policy along with asset management tools to ensure device and management consistency.

The work profile is built on Android's multi-layered security protections -- including sandboxing, Google security services, and Android management APIs.

With Android 11, organizations can achieve a successful COPE deployment that:

- Protects corporate data with strong device security
- Preserves employee privacy
- Enforces asset compliance with corporate policy

Protect corporate data with strong device security

IT shouldn't put corporate data at risk for the sake of mobile enablement and productivity. With the work profile, IT admins can still keep a tight security grip over corporate data without jeopardizing consistent personal privacy. Data separation implementations -- such as sandboxing and isolation -- enable IT to fully manage work data through the separation of application data from other apps at every layer.

Android 11 extends work profile's best-in-class data security to company-owned devices, without sacrificing the device-wide management capabilities expected when managing corporate assets.

Device security remains enforced through:

- Key platform technologies that protect enterprise data
- Secure management framework that enables enterprise-grade controls for data sharing, notifications, password requirements and more
- Google Play Protect and SafetyNet attestation services

android

Preserve employee privacy

When it comes to the use of mobile devices, users expect privacy over their personal data and apps, even if the company owns their device. With the work profile, protecting and preserving a user's privacy does not impact a device's overall security but rather prevents an admin from viewing potentially sensitive information. In turn, IT can reduce the potential risk of liability from viewing private employee data.

In Android 11, all employees have consistent privacy protections on both company and employee-owned devices. Employees can be assured of privacy around:

- Apps they have installed
- Websites they have visited
- Network activity outside the work profile

Exclusive to the Android Management API, Android 11's strong personal privacy protections will be available for older Android devices, as far back as Android 8. Organizations will be able to gain the benefits of Android 11 across many of the Android devices and versions they need to manage.

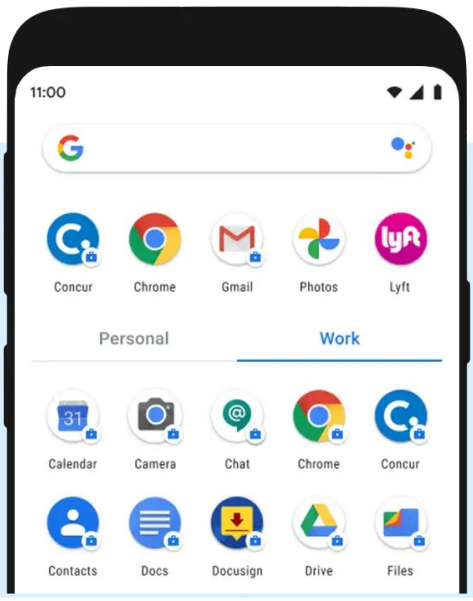
Enforce personal usage policies and asset compliance

Even without visibility into personal data and apps, on company-owned devices, the work profile offers IT asset management controls to ensure corporate policy and compliance standards are enforced on company-owned devices. For instance, just as is the case with fully managed devices, IT and security teams can allow or block apps that employees can use with additional granular control over which apps can be used for work and which apps can be used for personal use. Admins can also retain full control of asset behavior and ownership through factory reset protection management.

Additional features IT can leverage include:

- Restrict access to hardware features like Bluetooth, camera, and removable storage
- Personal app allow or block list
- Asset management protections (even if devices are lost or stolen)

With this level of control, IT teams can ensure that personal and overall device usage stays in compliance with corporate policies.



Conclusion

As your organization deploys company-owned, personally enabled devices, Android Enterprise is ready to keep your company data secure and enforce corporate asset requirements, all while safeguarding employee privacy.

To set up the work profile for company-owned, personally enabled devices, contact an enterprise mobility management (EMM) provider today.