android

Company-owned Android devices: **flexible and secure**

Android offers a management option for any deployment, from strictly locked-down devices to personally-enabled and dedicated scenarios

The challenge

When it comes to company-owned devices, there is no one-size fits all. Work-only devices remain critical for regulated and high security situations. Increasingly, employees expect to only carry one device for work and personal use. Dedicated devices such as kiosks or shared task-worker devices are increasingly transforming workflows, offering real-time customer service at lower total cost, but they need to be maintained remotely. And in all cases, corporate data must remain protected.

The Android difference

Android provides a consistent managed device mode and app ecosystem across a diverse range of over 400 manufacturers, from affordable smartphones for communication, to ruggedized tablets for the most demanding of environments. You can use the same Enterprise Mobility Management provider (EMM) across your whole device fleet.

Android fully managed device mode

From Android 6.0 Marshmallow and later, Android devices support a comprehensive OS-level managed device mode for corporate-owned devices, bringing consistency across device manufacturers, and allowing every app on the Google Play store to be used out of the box. Fully managed device mode gives critical capabilities for corporate-owned devices:

- **Theft protection** - Ensure devices cannot be reset, used for another purpose, or resold.
- **Whole device management** - Apply management controls to everything that happens on the device, from lock screen to encryption, VPN to app install.
- **Remote diagnostics and forensics** - Remotely audit activity on devices or debug issues for users.

Depending on your use case, Android offers three deployment types

Work-only device

Prevent users from adding personal accounts to devices, and maintain the device as only for work purposes.

Dedicated device

Lock an app to the screen for devices that are dedicated to a specific app, such as kiosks or task worker devices.

IT can also hide system navigation and settings to avoid distracting users. Apps are managed entirely remotely, with no browsable app store made available.

Personally-enabled device[1]

Enable Android's OS-level container, called a work profile, on a managed device to allow users to use personal applications and data, while ensuring that corporate applications and data remain separate.

The work and personal 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.

All while IT retains overall control of the device.

[1]Android 8.0 Oreo and above

android

Securing work data

The lifecycle and policies of an Android managed device are available through a comprehensive range of EMM providers. Many policies can be enforced, including the following critical elements for preventing data loss:

- **Screen lock** - Enforce minimum complexity on the whole device or for solely the work profile.
- **Encryption** - Storage encryption is on by default and enforceable by policy.
- **App whitelisting** - Use managed Google Play to curate your enterprise app store. You explicitly authorize which apps can be installed on a managed device to get access to corporate data.
- **VPN** - Secure app traffic on the network through a variety of VPN options, including the ability to ensure only apps in the work profile can use the VPN, or device-wide VPN to secure all communications.

Additionally in the work profile, you can enforce:

- **Data separation** - Enforce separation between a user's personal and work data at the OS kernel, ensuring partitioning of corporate data down to the process, memory and storage level.
- **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 sharing entirely.

Enrollment

Managed devices must be enrolled from an out-of-box or factory-reset state for security reasons. A number of enrollment options are available depending on your use case:

- **Zero-touch enrollment**[2] - Pre-configure devices with management settings before they're unboxed.
- **NFC** - User taps their device to a programming device. Great for admin mass-enrolling devices.
- **EMM token** - User enters a code. Easy to send by email, or SMS.
- **QR code** - User scans a QR code. Easier than typing, and can be sent by email.

Work-life balance (personally-enabled only)

An important part of a successful device rollout 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 devices

With such a broad range of devices available with Android, how do you choose?

Start with the Android Enterprise device catalog[3] to browse and filter devices based on their specs.

Specify the Android version that meets your needs. If you want to personally-enable corporate devices and/or use zero-touch enrollment, you'll need 8.0+.

If you want to use NFC enrollment then you'll need an NFC-capable device.

Consider whether the manufacturer, and your mobile carrier, offer OS security patch updates.

[2]Android 8.0 Oreo and above
[3]android.com/enterprise/device-catalog

Conclusion

Android fully managed devices provide comprehensive and consistent device management, with features for personal enablement or dedicated device deployments, allowing you to cover every use case.

Android's managed device mode is the best way to deploy corporate-owned Android devices in the enterprise.

Call your EMM today to get started deploying Android managed devices.