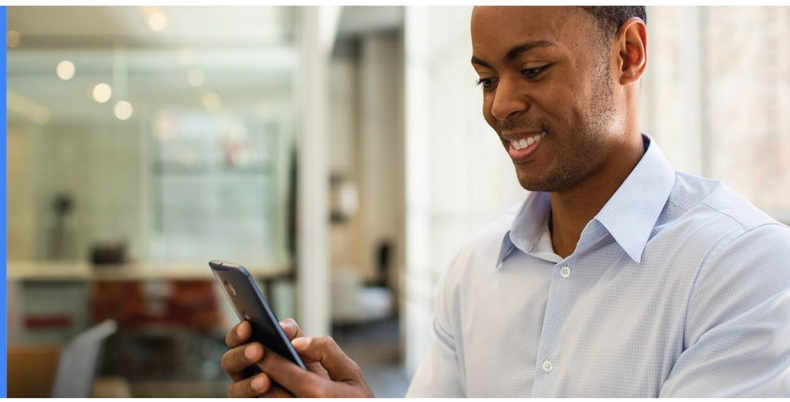
android

PARTNER LOGO HERE

Migrate from Device Admin to modern management with **Android Enterprise**



The deadline for the deprecation of Device Admin is approaching. Here's how to plan your migration to modern Android device management.

The challenge

The Device Admin API was originally introduced in Android 2.2 (2010) as a way to enable applications to enforce local policies on a device. It became the basis for many MDM solutions to manage enterprise devices. But its limitations, including an all-or-nothing approach, made it a less than ideal fit for modern deployments, forcing security compromises and introducing complexity.

Some of the challenges with Device Admin-based management solutions include:

- No ability to separate personal data on BYOD or mixed-use devices
- App management and distribution that relies on side loading of wrapped apps or the use of personal Gmail accounts
- Inconsistent management across devices from different OEMs
- Widely varying policy sets, unique to each EMM provider
- Limited features due to the inability to leverage Androids modern enterprise management and security APIs

Modern management with Android Enterprise

To create a modern approach to Android management, Google introduced a new, consistent framework for management built into the Android platform, starting in Android 5.0. Known as Android Enterprise, this framework provides a robust set of management APIs for a wide variety of use cases, a platform-based approach to separation of data for mixed-use devices and a modern, secure system for application deployment via Google Play.

Deprecating Device Admin

Now that Android Enterprise is mature and ready to replace the functionality of Device Admin, Google is moving forward with the deprecation of the Device Admin API. In Android 9 Pie, the APIs for password enforcement, disable camera and disable keyguard features will be marked as deprecated. With the next release of Android in 2019, those APIs will no longer be available. Google recommends that customers migrate from Device Admin-based management solutions to management deployments that leverage the more full-featured Android Enterprise framework via an EMM provider.

Standardized device management

- Extensive management controls
- Standardized management across OEMs
- Management solutions for BYOD, corporate-owned business-only, corporate-owned personally-enabled and dedicated device scenarios
- Modern enrollment methods including zero-touch enrollment, QR code, NFC and more

Robust security and privacy

- No reliance on unknown sources for application sideloading
- No manual downloads for enrollment
- Zero-touch enrollment to ensure devices remain managed
- Security APIs like ensure verify apps, block unknown sources and ADB controls
- More privacy for users
- More protection for user data

Modern application management

- Full app management, distribution of public and private apps via Google Play with silent install, whitelists and more
- No app wrapping needed
- No side loading of applications via third-party app stores
- No reliance on Gmail accounts to download public apps
- Managed app configurations for better app set up

Ongoing enterprise investment

- Device features won't break because of deprecation
- Devices stay current and capable of receiving the latest features
- Devices can receive support for new, upcoming features

Guidance for customers

Major mobility transitions are typically a large and important undertaking, when planning your migration we recommend following the steps below to successfully deploy Android Enterprise.

1. **Analysis** - analyze and document your legacy Android setup
2. **Requirements Mapping** - use documented legacy deployment to determine Android Enterprise feature requirements
3. **Proof of Concept** - setup a test instance to implement the required features and verify that they are working as intended.
4. **Walkthrough & Setup Documentation** - document user setup instructions with screenshots
5. **Deploy** - decide the type of rollout strategy that works best for your environment.

If you currently use device admin to manage your devices, there are two options available when moving to Android's current management solution: work profile and fully managed device mode.

To utilize these management modes you'll need an Enterprise Mobility Management (EMM) provider that supports them. Customers should choose the management mode which best suits their deployment. In some cases, both modes may be employed simultaneously*. Customers should then work with their EMM provider to build the necessary policies to enable these modes on their devices.

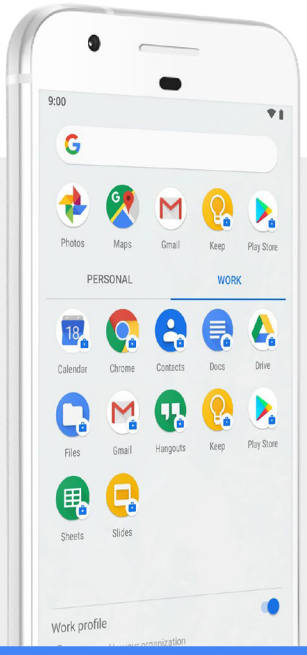
BYOD: Device admin to deployments of a work profile

We recommend work profiles be used for all personally-owned devices. Migration from legacy device admin to a work profile can be handled with minimal disruption. This can be handled either by pushing personal devices to install a work profile, or by having new devices enroll with a work profile as existing devices phase out of the fleet.

Company-owned devices: Device admin to fully managed device

We recommend that company-owned devices be set up as fully managed devices. Migrating a device from device admin to fully managed device mode requires a factory reset. Since this is more disruptive to users, we suggest a phased adoption, where new devices are enrolled as managed devices but existing devices are left on device admin.

*Setting up a fully managed device with a work profile requires Android 8.0 (Oreo). Please contact your EMM to confirm they support this mode.



Conclusion

We strongly recommend that businesses plan to move to work profile and managed device APIs. By sharing this update early, we aim to provide companies with sufficient time to migrate existing devices or start fresh as new ones are added to their fleet.

In order to avoid surprises we recommend starting early and reaching out to your EMM provider for specific implementation details and best practice guidance.

Get started today

[Add partner contact details]

For more information visit android.com/enterprise