Android Enterprise vs Device Admin Management

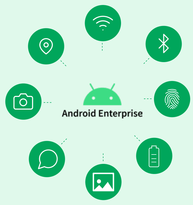
hexnode

Why should enterprises migrate?

With the announcement of **Android 12**, the legacy management style for Android devices is being pushed further into obscurity. The evolution of enterprise requirements over the years has played a significant role in the deprecation of the device admin mode of management. Most of the new-age businesses are using Android Enterprise for device management but there are businesses that are still resorting to the legacy method.

Android Enterprise Management

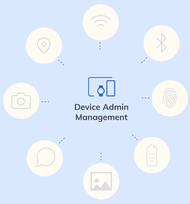
Feature Rich



The provision to enable and disable the camera, safe mode, screen orientation, screen timeout, Wi-Fi, Bluetooth, microphone, screen capture, USB debugging, factory reset, verify apps, configure VPN, and location sharing are some of the plethora of features that AE brings to the table.

Device Admin Management

Bare Minimum



The deprecation of several device policies like camera, password, and keyguard features on devices running Android 10 and above is a dealbreaker for enterprises that use the latest device versions. More deprecations in future updates will make DA unusable.

Application Management

- Silently install and uninstall apps
- Private apps via Managed Google Play
- Pre-configure app configuration and permissions
- OEMConfig management, especially for rugged devices

- User action to install and uninstall apps
- Multiple device admin apps can cause conflicts in device functionality
- Blacklisted apps won't be hidden from the user
- Lack of custom play store and app approval

Bring Your Own Device

- Separation of personal and work profiles via containerization
- Restrictions and management will be limited to the work profile
- Data sharing between the two profiles can be blocked
- OEMConfig management, especially for rugged devices

- Work and personal data remain mixed
- A single password for the whole device lowers security
- Data sharing between the two profiles can be blocked
- Same apps used for personal and work requirements

And More

- Zero-touch enrollment for all devices running Android 8.0 and above
- Schedule OS updates to keep up with security improvements
- Advanced restrictions beyond what the device admin management offers
- Kiosk management is seamless and efficient with device enrolled in device owner mode
- Customize playstore layout with app clusters and pages

- Tedious enrollment methods that make deployment difficult for large enterprises
- The lack of factory reset protection allows users to overcome device management
- Lack of mandatory device encryption and limited restrictions make it difficult to achieve compliance
- OS updates and patch delivery can take up to 180 days when compared to 90 days in AE

mdm-support@hexnode.com
partners@hexnode.com