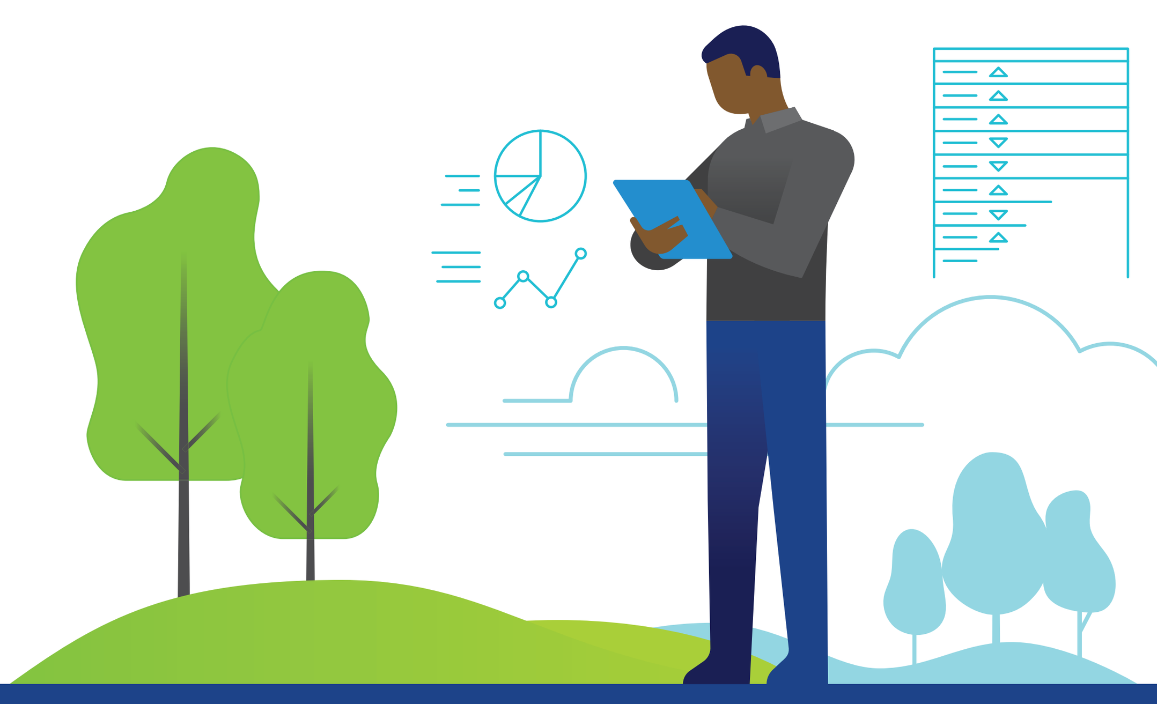
vmware

How VMware and Google Make Android Devices Ready for the Enterprise

Today's users are accustomed to a consumer-like experience that is simple and convenient, and they expect to be able to work from anywhere, anytime, and from any device.



With more than 2 billion active endpoints worldwide, Android offers a wide range of devices fit for many enterprise price points and use-case scenarios. To enable device management, Google unveiled device administrator APIs in 2010.

However, enterprise needs have evolved, sparking the development of Android Enterprise.

DEVICE ADMINISTRATOR "DEPRECATION"

Android devices running Android 10 or later do not have certain device administrator APIs required for many management capabilities. Given the deprecation of device administrator, organizations must be ready to adopt Android Enterprise. VMware can help make migration from legacy deployments as seamless as possible.

In order to support today's enterprise requirements, Google has introduced Android Enterprise, a modern management approach with three management modes:

WORK PROFILE MODE

for personally owned devices.

- Designed for personal or bring-your-own (BYO) devices.
- Enables IT to manage a work profile on a personal device.
- Corporate policies restricted to the work profile keeping company info secure and separate from personal data

FULLY MANAGED DEVICE MODE

for corporate owned devices.

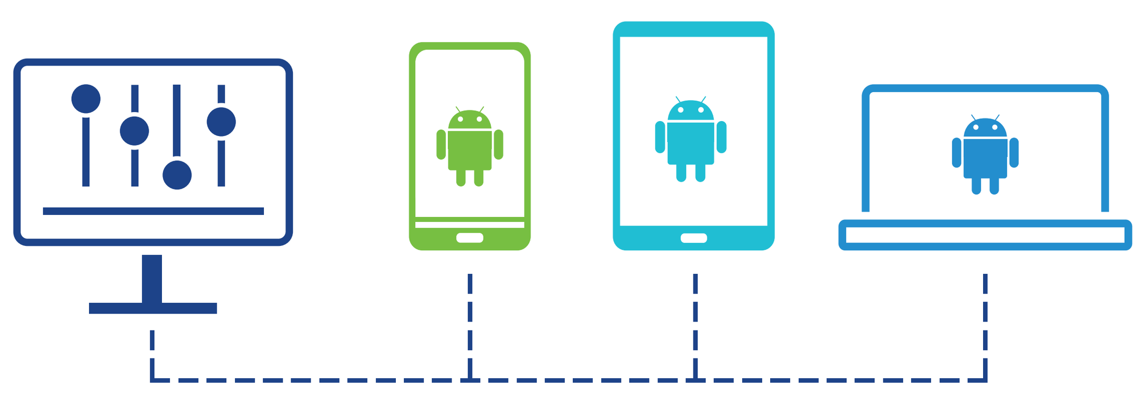
- Designed for corporate-owned and dedicated device use cases.
- Enables IT to manage the entire device enforcing an extended range of policy controls.
- Can be further locked down to restrict settings and the apps that can be installed.

CORPORATE-OWNED PERSONALLY ENABLED (COPE) MODE

a hybrid of work profile and fully managed device modes.

- Designed for corporate-owned devices that are used both for work and personal purposes.
- Allows a work profile to be set up to separate work from personal apps and data.
- Enables IT to secure or wipe the entire device in cases of loss or theft.

The modern management approach for enterprises using Android offers flexible integration options to suit a wide variety of use cases while maintaining a consistent native experience for end users, regardless of the device manufacturer.



THE ROLE OF VMWARE WORKSPACE ONE UEM

With the proliferation of various endpoints in the enterprise, organizations have begun to demand a single management tool and process. A unified endpoint management (UEM) approach is a holistic management framework that enables organizations to manage any endpoint to create a fully connected and secure IT environment.

VMware Workspace ONE® provides a simple yet robust solution for managing and supporting any device—from smartphones and laptops to rugged devices and wearables—from one central console. Workspace ONE combines UEM with apps and identity management to enable a complete digital workspace.

Workspace ONE is fully integrated with Android Enterprise, providing scalable, comprehensive support for work profile mode, fully managed device mode, dedicated devices, and corporate-owned personally enabled (COPE) mode.

It enables IT to save time and resources with low-touch enrollment and configuration, protect corporate data with device controls and policies, and give workers access to mission-critical apps that drive business operations.

To learn more, visit

www.vmware.com/products/workspace-one.html.

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com