MobileIron for Android™

The largest companies in the world trust MobileIron as the foundation for their secure Mobile First organizations. Our comprehensive unified endpoint management (UEM) platform is purpose-built to secure multi-OS environments with innovative mobile application management, content management, and device management capabilities. Our global partner network also ensures customers can access our UEM technology and integration services around the world.

Our highly scalable UEM platform and global expertise is why more organizations are looking to MobileIron to help accelerate their Android adoption. With two billion monthly active devices, Android has become the number-one mobile platform for consumers. For enterprises, Android powers the widest range of deployments from single-use dedicated use cases to high-end knowledge worker productivity tools.

As the first provider to deliver an enterprise app storefront, BYOD privacy controls, and certificate based identity management for Android, MobileIron is also one of the first UEM providers to support the Android enterprise platform.

Challenge

- Secure sensitive data on Android
- Secure and configure Android apps
- Enrolling corporate-owned devices requires user technical expertise
- Deploy Android BYOD and corporate-owned devices
- Consistent IT management across devices from different manufacturers at scale

Solution

- MobileIron for Android

Capabilities

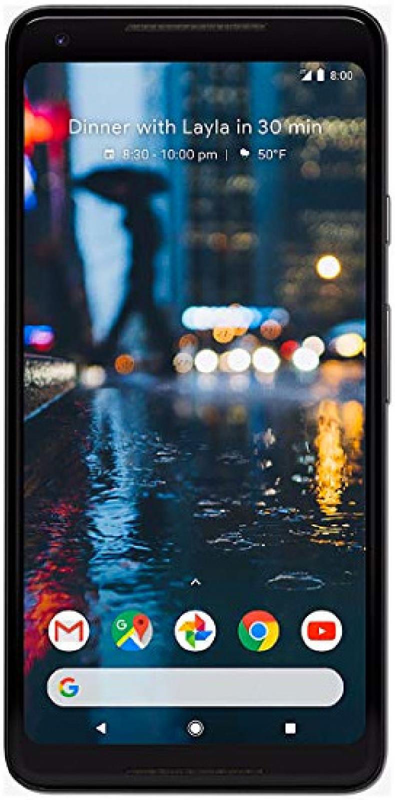
- Broaden multi-device support by securely enabling Android devices and apps
- Zero-touch mobile enrollment support for corporate devices
- Separate work and personal data on the device
- Enforce security and privacy policies
- Protect data-at-rest through encryption and DLP controls
- Preserve the native device experience and keep employees happy
- Maintain granular app-level control over the entire lifecycle
- Secure and protect dedicated Android devices as a Kiosk device

Flexibility to fit your organization

MobileIron for Android supports a broad range of use case scenarios to best fit your organization. With use cases, you can segment your users by role and by device ownership, either company-owned or personally-owned. Android device use cases range from knowledge-worker consumer devices (such as BYOD) to task-worker dedicated devices. With MobileIron for Android, enterprises can extend employee productivity with the right tools and the right devices to achieve your secure mobile transformation.

Consistent IT management across disparate devices at scale

Android enterprise delivers a deeper and more consistent security model to enterprise customers — a model that is supported by MobileIron. Using MobileIron's UEM console IT can securely distribute enterprise apps and push configurations to Android enterprise devices. These new features not only simplify IT management, they also reduce Android fragmentation by enabling more consistent app distribution and security.



A secure foundation for Android in the enterprise

MobileIron for Android addresses enterprise security concerns by enabling a containerized enterprise persona that separates personal and professional apps and content while preserving the native user experience. Whether the device is corporate-owned or employee-owned as part of a BYOD program, IT has full control over the enterprise container. The administrator can set and manage app and data-level policies and perform selective or complete wipes of the container.

MobileIron for Android gives IT the data security controls it requires while maintaining a consistent user experience across devices. Features include:

Device Security

- Secure Android devices with passcode policies, including managing biometric access options
- Protect unauthorized access by locking down hardware access
- Kiosk mode lockdowns, with support for shared devices

Data Security

- Separate app data encryption
- Certificate-based security for email, Wi-Fi, and VPN
- Secure single sign-on
- Selective wipe of business apps

Data Loss Prevention (DLP)

- Encrypted attachment control
- Screen capture control
- Copy/paste control

Secure Network Access

- App tunneling
- Enterprise Wi-Fi configuration
- Enterprise VPN configuration

Productivity Advanced app management for Android

MobileIron offers the most complete platform for mobile application management on Android to enable a productive mobile experience with apps on mobile devices. MobileIron supports managed Google Play or Apps@Work for app distribution and discovery, data security with native enterprise containers or AppConnect and AppConfig for an industry standard means of delivery secure configurations to enterprise apps.

With MobileIron for Android, business apps are inside a secure container whose data is encrypted, protected from unauthorized access, and wipeable. A single container passcode secures access to business apps, and users can easily access and share data between those apps. All containerized apps are managed with the MobileIron platform for centralized policy management, which supports native Android workflows and a productive mobile experience for the user. Productivity features include:

Secure PIM

MobileIron for Android offers a choice of solutions that provide secure access to personal information management (PIM) apps. Using the MobileIron platform, IT can easily configure and distribute containerized apps including email, contacts, calendar, and tasks. With Android enterprise, public apps can even be silently installed and removed.

	MobileIron Email+ for Android	Gmail
IT-Configured	✓	✓
Email	✓	✓
Calendar	✓	✓
Contacts	✓	✓

Secure content management

MobileIron Docs@Work allows users to connect securely and easily to a variety of content repositories. They can download content and view, annotate, and edit remote files and folders from their mobile devices as well as save back changes. Docs@Work allows IT administrators to centrally provision access to content repositories, pre-populate user names and directory paths, and allow devices outside a trusted network to access internal content repositories through MobileIron Sentry. Docs@Work provides a secure connection to numerous disparate content servers. (For more information, please refer to the Docs@Work data sheet.)

Secure browsing

Web@Work, MobileIron's secure browsing solution, delivers browser-specific tunneling to access corporate web resources without the need for a device-wide VPN. Android enterprise will also offer Google Chrome as a secure containerized browser, and both can be managed by the MobileIron platform.

MobileIron

MobileIron provides the secure foundation for modern work to companies of all sizes around the world.
For additional information,visit www.mobileiron.com/android or contact your MobileIron sales representative.

android enterprise recommended

Android Enterprise Recommended, a Google-led program, validates Enterprise Mobility Management (EMM) product offerings built with advanced Android Enterprise features by partners that can deliver trusted guidance and enterprise support.