MobileIron UEM for Android

MobileIron is the mobile-centric security platform for the Everywhere Enterprise. Our comprehensive unified endpoint management (UEM) platform is purpose-built to secure Android environments with innovative device lifecycle management, application management and content 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 over 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 rugged devices for frontline workers, single-use, dedicated use cases to kiosk mode and 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.

Flexibility to fit your organization

MobileIron UEM 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 features not only simplify IT management, they also reduce Android fragmentation by enabling more consistent app distribution and security.

Challenge

- Secure sensitive data on Android devices while maintaining user privacy
- Ensure the right applications are available to users
- Lack of technical expertise within an organization to onboard/scale Android deployments
- Identify the right deployment modes to deliver critical business value with superior user experience
- Consistent management across Android devices from different manufacturers such as Samsung, Pixel, Zebra and more at scale

Solution

- MobileIron UEM for Android

Capabilities

- Broaden multi-device support by securely enabling Android devices and apps
- Streamline onboarding by integrating with Samsung Knox Mobility Enrollment and Google Zero Touch Provisioning
- 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 such as a Kiosk device

A secure foundation for Android in the enterprise

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

Device Security

- Work profile on company owned devices for better user privacy
- 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

- MobileIron Sentry acts as an email and content in-line gateway that manages, encrypts and secures traffic between the Android device and back-end enterprise systems.
- MobileIron Tunnel is a multi-OS app VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction

Key use cases

- **Ensure privacy and compliance** in organizations primarily concerned about protecting sensitive data: Secure business data on any endpoint and separate business and personal data on various endpoints including Android devices
- **Enable multi-device, multi-OS, multi-app management from a single console:** The organization has a mixed device environment with Android based devices (Samsung, Google, Pixel, Zebra, Oculus, Honeywell, etc) iOS, macOS and Win 10 laptops. Unified management of these devices with different OSs and apps is top priority.
- **Empower Android frontline workers:** Support the field, fleet, and mobile workers in Healthcare, Transportation, Manufacturing, and other industries who use rugged devices or devices in Kiosk mode.
- **Provide a superior end user choice and delightful user experience:** When user choice and end user experience matters, MobileIron UEM provides the simplest Android onboarding and superior on device experience which improves user productivity
- **Industry security certifications for UEM:** Gain industry-standard security certifications such as FIPS 140-2 Validated Container, Common Criteria MDM PP V3.0 , DISA STIG, FedRAMP, and National Cryptologic Center – Assurance High
- **Provide security automation for device compliance:** Automated compliance: deletes all business data on compromised device without any manual IT actions
- **Multi-app, multi-cloud, support:** Connect securely to hybrid resources. Connect to SaaS based solutions with MobileIron Access and connect to on-premises resources with MobileIron Tunnel.
- **Flexible deployment models:** Cloud and on-premises based on your needs

Complete Device Lifecycle Management

Onboarding a fleet of Android devices manually can be challenging for any organization given that there are many vendors of Android devices available today such as Google, HTC, LG, Samsung, Zebra, Honeywell and more. Zero touch enrollment along with Mobileiron UEM is the process of automating the onboarding, user provisioning, configuration, application deployment and security and control of Android endpoints for users including remote workers. With zero touch enrollment you can also:

- Seamlessly and quickly onboard remote users on Android endpoints
- Provision the devices in specific modes based on the privacy/security requirements

You can expedite user provisioning for corporate owned Android devices with native user experience. With UEM and zero touch enrollment you can:

- Automate user provisioning when users log into device
- Supports provisioning of corporate-owned, kiosk or single App mode, and shared device use cases across your organization
- Centrally configure and push user email, Wi-Fi, and VPN settings
- Set device-security standards
- Track device inventory and details
- Seamlessly install business applications to the device
- Automate application and Android updates
- Wipe corporate data off a device at the end of the device lifecycle, employee termination or loss of equipment.

Examples of Zero touch Enrollment for Android vendors

- Google Zero Touch Provisioning (ZTP): Enables an IT administrator to mass deploy configured, managed, corporate owned devices
- Samsung Knox Mobile Enrollment (KME): Provides automated enrollment of Samsung Galaxy devices capable of Android Enterprise (AE)

Application Management

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 delivering 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.

- Secure, identity-based delivery of in-house and App Store apps through the Apps@Work private app storefront
- Improve productivity by using secure user apps such as MobileIron Email+ for containerized corporate email, calendar, contacts; Docs@Work for secure document storage; Help@Work to provide remote access for faster helpdesk resolution of issues
- Selective wipe of business apps and apps data on the Android devices
- Blacklist/whitelist of apps to protect against inappropriate access
- Containerization and dynamic policy to protect data-at-rest and enable compelling app-based user experiences through AppConnect

MobileIron unified endpoint management (UEM)	Secure UEM	Secure UEM Premium
Device management and security		
Security and management - Secure and manage endpoints running Apple's iOS, macOS, iPadOS, Google's Android, and Microsoft's Windows 10 operating systems. Available on-premises and as a cloud service.	✓	✓
Mobile application management (MAM) - Secure business apps with MobileIron AppStation on contractor and employee devices without requiring device management.	✓	✓
Easy on-boarding - Leverage services such as Apple Business Manager (ABM), Google Zero-Touch Enrollment and Windows AutoPilot to provide users with automated device enrollment.	✓	✓
Secure email gateway - MobileIron Sentry, an in-line gateway that manages, encrypts, and secures traffic between the mobile endpoint and back-end enterprise systems.	✓	✓
App distribution and configuration - Apps@Work, an enterprise app storefront, combined with Apple Volume Purchase Program (VPP) facilitates the secure distribution of mobile apps. In addition, capabilities such as iOS Managed Apps and Android Enterprise allow for easy configuration of app-level settings and security policies.	✓	✓

Continued on next page...

Scale IT operations		
Helpdesk tools - Help@Work lets IT remotely view and control a users' screen, with the user's permission, to help troubleshoot and solve issues efficiently.	✓	✓
Reporting - Gain in-depth visibility and control across all managed devices via custom reports and automated remediation actions.	✓	✓
Secure productivity		
Secure email and personal information management (PIM) app - MobileIron Email+ is a cross-platform, secure PIM application for iOS and Android. Security controls include government-grade encryption, certificate based authentication, S/MIME, application-level encryption, and passcode enforcement.		✓
Secure web browsing - Web@Work enables secure web browsing by protecting both data-in-motion and data-at-rest. Custom bookmarks and secure tunneling ensure that users have quick and safe access to business information.		✓
Secure content collaboration - Docs@Work allows users to access, create, edit, markup, and share content securely from repositories such as SharePoint, Box, Google Drive and more.		✓
Mobile app containerization – Deploy the AppConnect SDK or app wrapper to provide an additional layer of security for your in-house mobile apps or choose from our ecosystem of AppConnect integrated apps.		✓
Derived Credentials – Support two-factor authentication using common access cards (CAC) and personal identity verification (PIV).		✓
Secure connectivity		
Per app VPN – MobileIron Tunnel is a multi-OS VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.		✓
Conditional access		
Trust Engine – Combine various signals such as user, device, app, network, geographic region, and more to provide adaptive access control.		✓
Passwordless user authentication – Passwordless multi-factor authentication using device-as-identity for a single cloud or on-premises application.		✓

Note: Availability of certain features and functionality is dependent on the deployment type – on-premises vs SaaS. Availability might vary based on operating system and device type

About MobileIron

MobileIron is the mobile-centric security platform for the Everywhere Enterprise, enabling a secure workforce through a zero trust approach. MobileIron's platform combines award-winning UEM capabilities with passwordless MFA (zero sign-on) and mobile threat defense (MTD) to validate the device, establish user context, verify the network, and detect and remediate threats to ensure that only authorized users, devices, apps, and services can access business resources in a "work from everywhere" world.

MobileIron establishes the data loss prevention (DLP), privacy, and access control protections Mobile IT needs to be able to adopt iOS and IPadOS across the organization.