

MobileIron UEM for iOS and iPadOS devices



The demand for iOS-based devices such as iPhones and iPads among enterprise users has exploded. Employees want to use their iOS devices for accessing both corporate resources as well as personal data and are putting more pressure on IT to support them. By combining the MobileIron mobile-centric security platform with Apple's expanding ecosystem of endpoints and apps, IT admins can now securely deliver the full value of iOS mobility to end users. MobileIron provides a seamless and native end-user experience during device enrollment, and the unified console enables organizations to reduce the complexity and costs of managing a fleet of iOS devices.

The largest companies in the world trust MobileIron as their endpoint management solution. Available as a highly scalable cloud or on-premises solution, MobileIron Unified Endpoint Management (UEM) was purpose-built to secure and manage corporate apps and data across any device. MobileIron was the pioneer of iOS in the enterprise, delivering the platform's first private app storefront, BYOD privacy controls, and certificate-based identity management.

Comprehensive App Management

MobileIron UEM was designed for iOS app management and distribution that includes in-house apps, App Store apps, and web apps: By using a single console for app and OS distribution and updates, UEM improves user productivity.

- Secure, identity-based delivery of in-house and App Store apps through the Apps@Work private enterprise
- Improve productivity by using secure user apps such as MobileIron Email+ for containerized corporate email, calendar, contacts; Docs@Work for secure document storage; Web@Work for secure browsing into your intranet.
- Enable DLP through selective wipe of business apps and apps data on the iOS and iPadOS 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

Challenge

- Enable iOS app distribution and management
- Support BYOD initiatives
- Protect corporate data and user privacy
- Preserve native iOS experience
- Unified console for management of iOS and iPadOS fleet deployments

Solution

- MobileIron UEM for iOS and iPadOS

Benefits

- Complete app management – secure delivery, data containerization, tunneling
- App download without network latency
- Data loss prevention (DLP) for iOS email
- Privacy protection and data separation
- Identity-based security through certificates
- Multi-user configuration for shared devices
- Secure productivity apps on the go
- Enterprise integration thru extensible APIs
- Scales to fit your device growth needs
- Multi-tier management for delegation
- Flexible deployment options: cloud and on-premises

Enhanced Security

Mobile IT is responsible for the protection of corporate data. MobileIron provides security across the data lifecycle while preserving end-user privacy:

- Separate business and personal data using AppConnect to maintain compliance with corporate and regulatory requirements
- The ability to prevent flow of sensitive enterprise data from managed to unmanaged apps and services via Shortcuts
- Automatic provisioning and enforcement of security and configuration settings for Exchange, FaceTime, iCloud, iMessage, SCEP, screen capture, Siri, VPN, Wi-Fi, Office365, Outlook, Slack and SFDC
- Set password policies and deploy certificates to secure the device
- Seamlessly activate eSIM (virtual SIM) through a provider using automated device enrollment
- Protect data at rest by encrypting business data using FIPS 140-2 cryptographic modules
- Enable granular app-level access control using a secure access gateway
- Protect data in motion using a per-app VPN that provides a secure tunnel to backend resources
- Set up automated policy violation responses to free IT from daily administrative tasks.
- Supports tiered compliance - providing IT capability to launch responses automatically over a period of time
- Combine various signals such as user, device, app, network, geographic region, and more to provide conditional access to devices to various on-prem sources and SaaS applications

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.

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 Apple devices
- Enable multi-device, multi-OS, multi-app management from a single console: The organization has a mixed device environment with iPhones, iPads, Macs, Android based devices, Win 10 laptops and PCs, Zebra, Oculus, etc. Unified management of these devices with different OSs and apps is top priority.
- Empower Apple frontline workers Support the field 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 Apple 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 (On-premises/Cloud) based on your needs

Complete Endpoint Lifecycle Management

MobileIron UEM provides complete device lifecycle management from onboarding and provisioning to retirement.

- Provides a unified console to onboard and manage your iPhone, iPad, macOS, Apple TV and Apple Watch endpoints
- Supports provisioning of corporate-owned, BYOD, kiosk or single App mode, and shared device use cases across your organization
- Supports a new way to roll-out BYO using Managed Apple IDs for maximum user privacy - called User Enrollment
- Leverages Apple Business Manager (ABM) and Apple School Manager (ASM) for out-of-the-box configurations
- Wipe corporate data off a device at the end of the device lifecycle, employee termination, or loss of equipment.

MobileIron tightly integrates iOS into Microsoft environments with Office 365, Azure Active Directory, SharePoint, Exchange, Certificate Authority and SCCM.

Customer Perspective

"From day one, MobileIron has helped us with clinical care decision making. This includes decision making that saves lives. Now that we've deployed 3,000 iPads and established a way to secure and manage them through MobileIron, the sky's the limit for our mobile strategy," says Walker. "There's almost no limit to the ways we can deliver apps that boost clinician effectiveness and enable better patient outcomes. This is exactly what we hoped our mobile initiative would be."

- **Mark Walker,**
Head of IT, Oxford Health NHS Foundation Trust

"The iPad secured by MobileIron is an excellent tool for ad hoc meetings because we can access secure business files immediately, in any location. This allows us to have productive, in-person meetings with customers or colleagues anywhere. It's especially important while traveling because it supports all of our daily business needs."

- **René Degros,**
European Sales Director at Canon Medical Systems Europe.

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.	✓	✓
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.	✓	✓

Continued on next page...

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.