CA Mobile Device Management
Enterprise Mobility Management Suite

At a Glance
CA Management Cloud for Mobility extends its leadership in enterprise management, security and scalability to solve challenges for managing mobile devices, apps, content, and email within the enterprise. As a fundamental component of CA Management Cloud for Mobility, enterprise mobility management features CA Mobile Device Management (CA MDM) as a marquee product.

CA MDM is a scalable, SaaS and on-premise solution that helps enterprises secure and manage mobile and desktop devices and deploy applications. As mobility rapidly evolves, CA MDM enables enterprises to face today’s Bring Your Own Device (BYOD) realities with a flexible and sustainable approach to unlocking and maximizing the value of mobility.

Key Benefits/Results

- **Deploy BYOD support.** As an on-premise or SaaS solution to address the needs of any enterprise.
- **Access corporate resources and email.** Quickly installs on a new mobile device within 90 seconds.
- **Quickly deploy enterprise and public apps.** Via CA MDM enterprise app store.
- **Secure corporate data.** At rest and in transit across all devices.
- **Monitoring and reporting.** Provides extended analytics and Telecom Expense Management (TEM).

Key Features

**Manage**
- **Device configuration management.** Policy-based enrollment of BYOD device to configure and access enterprise resources.
- **Enterprise app management.** Total enterprise app lifecycle management from enterprise app store.
- **Visibility, command and control.** Bring devices under management with virtually zero-touch IT.
- **Extended analytics.** Control costs with real-time analytics using Business Objects.

**Secure**
- **Security.** Locate, lock and selective/full wipe device capabilities through easy-to-use admin/self-service portal.
- **Enterprise integration.** Out-of-the-box support for key enterprise resource integration such as Exchange, AD and certification authority.
- **BYOD freedom.** Securely manage enterprise and personal apps, content and emails.

Business Challenges
While mobility increases convenience and improves productivity for enterprise end users, it also creates serious enterprise IT security challenges and risks.

**Personal Device Challenges.** The use of both personal and professional devices for work-related activity has been widely adopted by knowledge workers. Employees prefer to carry a single device for work and personal use. BYOD solutions allow enterprise productivity apps to reside on users’ personal devices. Consequently, sensitive corporate data resides on devices that are not fully under IT control and small form factors of these devices are prone to theft and loss.

**Security Challenges.** The onboarding of business applications that provide ease of access to corporate email on users’ devices also provides serious challenges to the enterprise in the case of device compromise. These devices are exposed to third-party apps as well as virus and malware threats. The risk of corporate data leakage on mobile devices has grown and now represents a bigger problem than malware. Organizations need a cost effective mobile device management solution that provides security and a delightful end-user experience while overcoming the challenges presented.

Solution Overview
CA MDM is built from the ground up as a highly scalable and available solution that manages various mobile platforms such as iOS, Android, BlackBerry and Windows desktop end points. It has a comprehensive policy framework for enrolling, configuring and onboarding enterprise applications. A broad range of enforcement allows IT to apply the right level of device, data and app security commensurate with a user’s role in the enterprise. Comprehensive usage analytics enables IT to track inventory, Telecom Expense Management, device trend analysis and security compliance. With on-premise and cloud offerings, IT has complete deployment flexibility.

The self-service portal streamlines enrollment and provisioning of a device. It allows users to remotely locate, lock and wipe a lost device; reset the passcode; remove enterprise controls; and unregister a device. With BYOD programs, users demand the flexibility of using their device for both work and personal use with the assurance that their enterprise information is secure and their personal content is untouched by the enterprise.
Critical Differentiators

**Smart Containerization™.** CA MDM is powered by Smart Containerization technology to dynamically control mobile device, application and email provisioning policies at a granular level.

**Leading enterprise IT management player.** CA Technologies is uniquely positioned to deliver thorough enterprise mobility management that integrates with multiple facets of enterprise IT stack.

**Best-in-class expense analytics.** Advanced querying and customer reporting.

**Device and app management beyond standard MDM through scripting capability.** Complex file and software distribution for desktop management, best-in-class remote management and diagnostics for Android™ devices, Linux®/Windows® client and server platform.

**Proven scalability and platform coverage.** Scalability through server farms and cluster landscape supports high SLAs, single pane of glass for managing both mobile and traditional Windows-based endpoints. Accommodates diverse mobility platforms and extended enterprise security support for Samsung and LG.

**Enterprise grade platform administration and security features.** Enterprise integration support, directory integration through LDAP, Active Directory and native NT domain. Relay server in DMZ enhances security for MDM infrastructure and ease of network deployment.

Related Products

- **CA Mobile Application Management (CA MAM)** – Helps convert unmanaged mobile applications into managed applications by embedding security, supportability and control within the applications.

- **CA Mobile Content Management (CA MCM)** – Enables secure access and collaboration across mobile devices regardless of where the content is located—the enterprise or the cloud.

- **CA Mobile Email Management (CA MEM)** – Lets users securely access their corporate email and ensure group and policy-based controls to protect sensitive email content.

- **CA Unified Endpoint Management (CA UEM)** – Provides comprehensive lifecycle automation capabilities across heterogeneous physical, virtual and mobile environments including servers, laptops, smartphones, tablets, POS, ATMs – any device with a supported operating system.

Supported Devices

- iOS 4/5/6/7/8 running on iPhone, iPad, iPad Mini, iPad Air

- Android 3/4 running on all popular vendors including Samsung, LG, HTC and Motorola

- Full support for Samsung SAFE and LG enterprise security APIs

- BlackBerry® devices running 5/6/7

- Windows 8 support with App management

- Windows XP/2003/2008 servers

- Windows XP/Vista/7 workstations

Language Support

Includes Brazilian Portuguese, French, German, Japanese, Spanish, Traditional Chinese, Simplified Chinese and Italian.

Deployment Options

CA MDM can be delivered as a cloud-based SaaS offering or deployed on-premises behind the firewall.

For more information, please visit [ca.com/mobility](http://ca.com/mobility)