

Symantec™ Mobile Management

MDM for iOS, Android and Windows Phone Devices

Data Sheet: Mobile Security and Management

Overview

Symantec™ Mobile Management 7.2 helps enterprises confidently enable mobile productivity by facilitating scalable, secure, and integrated Smartphone and tablet deployments. Mobile Management provides comprehensive visibility and control over all the popular mobile devices such as iPhone®, iPad®, Android™, and Windows® Phone.

Core Functionality

Symantec Mobile Management addresses the three core areas of functionality that should be integral to any mobility solution:

- **Enable** devices for use in a corporate environment. This includes providing access to key corporate assets, such as email, calendars, critical mobile applications, documents, and media content.
- **Secure** devices and data on all devices. This includes activating appropriate password and access controls as well as maintaining separation of corporate data and personal data.
- **Manage** all devices in the enterprise from a single, centralized solution. This includes visibility and control over all phases of device lifecycle with needed administrative and helpdesk options.



Three core areas of mobile device management

Enable

Enterprise Enrollment: Symantec Mobile Management helps prevent unauthorized shadow enrollments and provides a standard and automated provisioning process. Features include authorization based on group, minimum OS, authentication with LDAP, and jailbreak/rooted status.

Self-service Activation: Symantec Mobile Management helps reduce IT handholding and provides an easy end-user driven activation process. Features include automated configuration of device settings with native agents for iOS, Android and Windows Phone.

Business Email: Symantec Mobile Management solves the popular requirement of providing access to corporate email. Features include automatic configuration for native and third party email clients that connect to mail servers like Microsoft® Exchange, Office 365, Gmail™ and Lotus Notes®.

Enterprise Apps: Symantec Mobile Management helps realize new business models that leverage enterprise mobile applications. Features include an in-house app store with the ability to distribute internal or public apps. Provides control over managed apps with lifecycle management features.

Corporate Content: Symantec Mobile Management enables mobile collaboration by making content available on the end user device of choice. Distribute documents, videos, and media files by targeting specific groups, users, languages, operating system, compliance or any device attribute. Update and revoke content seamlessly.

Network Access: Symantec Mobile Management enables access to corporate network resources like Wi-Fi and VPN. Supports all protocols and authentication methods and automates configuration settings.

Secure

Policy Management: Symantec Mobile Management ensures corporate compliance by enabling advanced security settings on devices. All policy options including passwords, remote

wipe, and resource and app restrictions are available and can be targeted to a specific user/device/OS/group.

Strong Authentication: Symantec Mobile Management extends enterprise identity requirements to devices with automated provisioning and processing of certificates. Can be used for authentication requirements on email, Wi-Fi and VPN, and integrates with Symantec™ MPKI and Microsoft CAs.

Secure Email Access: Symantec Mobile Management enforces access control policies for mobile email. Enables advanced allow/restrict rules based on groups, device compliance or device attributes in Exchange 2010 or F5 environments. In F5 environments, the restriction policy can also limit email access to specific apps: native or 3rd party (Ex: Android TouchDown™).

Secure Email App: Symantec Mobile Management allows advanced email security policies by leveraging Nitrodesk TouchDown, a dedicated 3rd party email app. Initially for Android, this app enables advanced security policies like authentication, encryption and copy paste restrictions.

Compliance & Remediation: Symantec Mobile Management enables administrators to allow only compliant devices. Define compliance using device status (jailbreak, encryption), user status (group membership), or app status (required apps, blacklisted apps), and get remediation details for any non-compliant devices.

Data Separation: Symantec Mobile Management limits data loss & privacy concerns by separating corporate and personal data. Remove only corporate data upon employee departure, without touching personal data. Identifies corporate email, apps, docs, and any other content.

Manage

Centralized Management: Symantec Mobile Management allows IT to use a single solution to manage all mobile devices. Allows enterprise grade management with a scalable and mail server agnostic architecture. Supports distributed deployments with role based access control.

Integrated Management: Symantec Mobile Management enables efficient management of all the computing devices in the enterprise with a unified solution for managing Macs, PCs, iPhones and Androids in the same console either with Symantec™ IT Management Suite or Microsoft System Center Configuration Manager.

App Management: Symantec Mobile Management allows management of all enterprise apps through the lifecycle phases with over-the-air (OTA) control. Distribute and update apps with group based management and leverage integration with Apple® Volume Purchase Programs and B2B Plans.

App Curation: Symantec Mobile Management keeps enterprise mobile ecosystem safe with policy driven blacklisting. In addition to preventing unauthorized backup of corporate apps, policy options also allow blocking and revocation of blacklisted apps and corresponding devices from the enterprise.

Dashboards & Reports: Symantec Mobile Management provides exact details of enterprise mobile assets at all times by leveraging built-in dashboards, reports and alerts. Comprehensive user, device, app, and profile details are available for additional custom reports as well.

Automated Actions: Symantec Mobile Management makes mobility management efficient by automating administrative and operational tasks. In addition to built-in automated processes, management console includes an intuitive drag and drop user interface for creation of custom actions.

Key Benefits

- **Enables mobility** in the enterprise by providing a security and management solution for all popular devices, both corporate and personally owned. Enterprise grade architecture that supports 20,000+ devices from a single instance.
- **Secures corporate data** with enterprise grade policy management and clear separation of corporate and personal data. Integrates with Symantec's trusted Managed PKI, Data Loss Prevention and Endpoint Protection technologies.

- **Optimizes operational costs** by allowing standardization - one platform for managing ALL endpoints and applications in the enterprise. Integrates with Microsoft SCCM and Symantec IT Management Suite products to provide unified endpoint management.

Packaging Options & System Requirements

Symantec Mobile Management is available in two versions, with similar feature functionality:

- **Symantec Mobile Management:** This version of the product can be installed either standalone or in combination with Symantec IT Management Suite. Requires Windows® Server 2008 and SQL Server 2005/2008
- **Symantec Mobile Management for Configuration Manager:** This version of the product is integrated with Microsoft SCCM. Requires Microsoft SCCM.

Devices Supported:

- Apple: iOS 4.0, 5.0, 6.0
- Google: Android 2.2 and above
- Microsoft: Windows Phone 7-7.5, Windows Mobile 6-6.5

More Information

Visit our website

<http://go.symantec.com/mobile>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.