Symantec™ Mobile Management for Configuration Manager 7.2

Scalable, Secure, and Integrated Device Management

Data Sheet: Endpoint Management and Mobility

Overview

The rapid proliferation of mobile devices in the workplace is outpacing that of any previous technology and enterprises are moving quickly to address this trend. IT departments are dealing with an explosion of mobile data, application costs, data privacy, and IP protection. As with previous technologies, this new wave of technology must be enabled, secured, and managed to maximize business agility and employee productivity.

Symantec™ Mobile Management for Configuration Manager 7.2 (previously called Athena™ Mobile Device Management from Symantec™) helps enterprises to confidently enable new 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™, Windows® Phone 7, and Windows® Mobile.

What's New

Mobile Management adds advanced security and mobile device management (MDM) capabilities for Android and Windows Phone 7 devices, and continues pre-existing support for Apple® iOS and Windows Mobile devices.

Core Functionality

Mobile Management addresses the three core areas of functionality that should be integral to any comprehensive mobile management solution, in a process that is simple and efficient for both IT managers and mobile users:

1. **Enable** the device for use in the corporate environment. This includes providing access to key corporate assets including email, calendars, critical mobile applications, documents, and media content.
2. **Secure** the device and the data that is stored on it or passes through it. This includes activating appropriate password and access controls, and maintaining separation of corporate data from personal data.
3. **Manage** all diverse mobile devices from a central location, with real-time access to inventory, configuration, and help desk functions. This includes integration with Microsoft® System Center Configuration Manager to provide a unified and efficient endpoint management solution.

Enable

- **Enterprise Activation** is a user-friendly self-service provisioning process that helps users to connect their mobile devices to the enterprise network in an approved and secure way. Instead of blocking devices and encouraging rogue IT, administrators can leverage this seamless process to authenticate and authorize users' devices to email and network services. Users can be directed to download the Mobile Management device agent from the public app store or private servers. Administrators can enforce customized end-user license agreements as part of the enrollment process.
- **Enterprise App and Content Library** is an organization-specific app and content repository. It can be used to distribute internally developed applications or to provide recommendations for approved applications from the public app stores such as Apple AppStore or Google Play. It can also be used to distribute documents, multimedia, and web content to end-user devices. With group-based and over-the-air distribution capabilities, Mobile Management allows administrators to efficiently and securely distribute applications and content.

Enterprise App and Content Library

- **Secure Email Client (Optional Component)** provides enterprises with a dedicated corporate email client on Android devices. Powered by Nitrodesk, TouchDown™ is a Microsoft® Exchange ActiveSync® client that can be used for syncing and

storage of email, contacts, calendar, and tasks on Android devices, and works with email servers such as Exchange, Lotus, and Microsoft® Office 365, etc. in the backend. Mobile Management is integrated with TouchDown to provide seamless configuration, security, and management of enterprise email.

- **Configuration Management** allows automated configuration of email, VPN, Wi-Fi, and other settings on iOS devices. It eliminates user errors and enables large scale mobile deployments without IT hand-holding. While this process provides standardized configuration and connection settings for all devices, it also reduces the costs associated with mobile deployments and maximizes efficiency for enterprise IT (applies to iOS devices only).

Secure

- **Advanced Security Settings** enables enterprises to secure mobile devices regardless of ownership. With Mobile Management administrators can set, deploy, and update security settings such as passwords, remote lock and wipe, application, resource and content restrictions, over-the air in near real-time without user intervention. Policy settings can be targeted to an individual user/device, groups from the directory systems, or custom groups from the console. All settings are automatically applied and are enforced on devices at all times.
- **Selective Secure Wipe** is used to decommission a personal device in the enterprise. With this command, Mobile Management leaves the user's personal data intact and securely wipes the corporate data (email, contacts, calendar, attachments, and Mobile Content Library). This enables enterprises to apply appropriate security policies to corporate data while leaving personal data untouched.
- **Compliance Enforcement** enables enterprises to allow only devices that meet the security and corporate requirements around encryption, jailbreak, and policy updates. This periodic health check enables administrators to meet auditing requirements and specify granular device hardware, software, policy, and user controls.
- **Certificate Distribution** allows integration with certificate authorities and extends seamless strong authentication to iOS devices. By enabling certificate-based authentication, organizations can provide secure access to corporate email, VPN, and Wi-Fi and prevent unauthorized devices from connecting to corporate resources (applies to iOS devices only).

Manage

- **Centralized Management** capabilities of Mobile Management provide comprehensive visibility and control over devices, users, and applications in near real-time and enable efficient IT operations including help desk. Mobile Management leverages the native reporting capabilities of Microsoft™ Configuration Manager, SQL reporting services, and includes predefined and customizable reports.
- **Mail Server Agnostic** nature of Mobile Management allows management and security of mobile devices in a variety of enterprise environments, supporting all of the popular mail servers, including Microsoft® Exchange 2003/2007/2010, Lotus Notes®, and Gmail™.
- **Massive Scalability** is achieved by leveraging the native capabilities of Configuration Manager. Each Mobile Management instance can support 20,000+ devices and provides future proofing against projected mobile adoption rates.
- **Unified Endpoint Management** provides native integration with Microsoft Systems Center Configuration Manager, enabling a single console to manage all enterprise computing devices: smartphones, tablets, laptops, and desktops. Mobile Management integration with corporate infrastructure elements such as Active Directory®, firewalls, and certificate authorities allows efficient enterprise deployments with minimal changes.

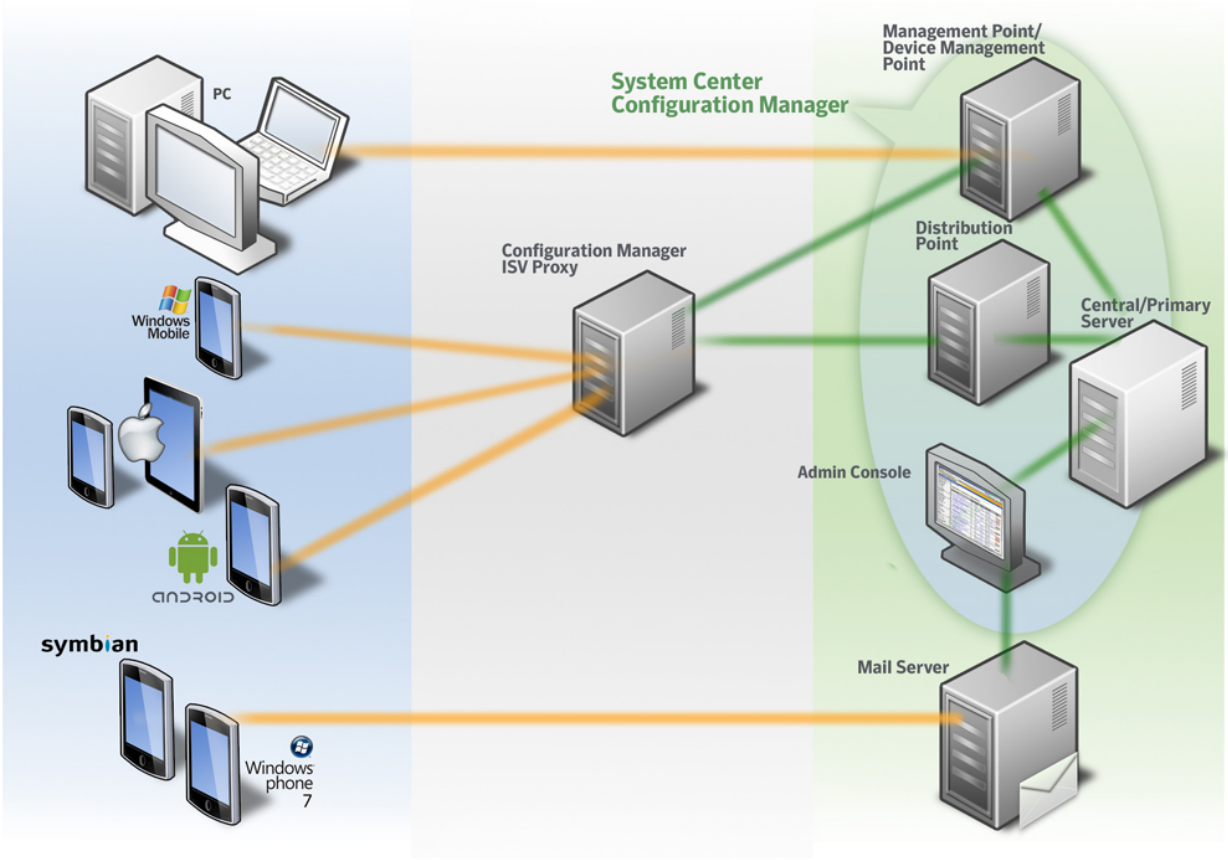
Multi-platform Support

Mobile Management adds in-depth security and management capabilities for Android and Windows Phone 7 devices, and continues pre-existing support for iOS and Windows Mobile devices.

Comprehensive Enterprise Mobility from Symantec

In addition to Mobile Management, Symantec solves broader enterprise mobility needs around application management and security, information protection, and strong authentication with the following products:

- **Mobile Device Management**
  Symantec™ Mobile Management allows enterprises to enable, secure, and manage mobile devices either as a standalone or as part of Symantec™ IT Management Suite. It has an identical feature set as the Symantec Mobile Management for Configuration Manager product and provides MDM capabilities for iOS, Android, and Windows Phone 7 devices.
- **Mobile Application Management**
  Nukona App Center™ is a scalable solution for securing, deploying, and managing applications and content on mobile devices. Nukona provides clear separation of corporate and personal data with targeted management of corporate applications on iOS and Android - without source code changes or SDK embedding.
- **Mobile Information Protection**
  Symantec™ Data Loss Prevention for Mobile is the first comprehensive data loss prevention (DLP) solution for the monitoring and protection of sensitive information on mobile devices. Available first for the iOS devices, Data Loss Prevention for Mobile provides context-aware protection, without effecting end user productivity and experience.
- **Mobile Threat Protection**
  Symantec™ Mobile Security offers enterprise grade protection for Android, Windows Mobile, and Symbian® smartphones against malicious threats with award-winning antivirus technology, an advanced firewall, and SMS antispam features.
- **Mobile Strong Authentication**
  Symantec™ Managed PKI is the industry-leading PKI certificate management and authentication service that runs on Symantec's proven, globally managed, and highly reliable infrastructure.
  Symantec™ VIP Access for Mobile turns a mobile phone into a two-factor authentication security device using a native agent or an integrable SDK. It helps companies mitigate risk and maintain compliance with a scalable, reliable two-factor authentication platform.



Mobile Management Infrastructure

Why Symantec

Mobile Management offers compelling advantages to IT administrators:

- Symantec enables all device management functions for iOS, Android, and Windows Phone devices from the Microsoft System Center Configuration Manager (SCCM) native console. This extends the systems management functionality of SCCM and turns it into a true single console for lifecycle management of enterprise and mobile resources - from policy management to helpdesk and reporting.
- Symantec leverages the SCCM platform's native infrastructure to provide a highly scalable, reliable mobile solution. By supporting 20,000+ devices from a single server, and multiple more from a clustered architecture, Symantec can serve the mobility needs of organizations of any size.

System Requirements

Mobile Management for is available as an add-on to Microsoft Systems Center Configuration Manager 2007.

Devices Supported:

- Apple: iOS 4.1 and above
- Google: Android 2.2 and above (with Nitrodesk Touchdown as an optional component)
- Microsoft: Windows Phone 7, Windows Mobile 6.1, 6.5

More Information

Visit our website

http://go.symantec.com/mobile

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

Call 585-214-2409 Ext. 120

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

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

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.