Symantec Mobility: Application Management

Protect and Manage Apps on Any Device

Data Sheet: Endpoint Management and Mobility

Overview: Deliver secure mobile apps that improve productivity

In the office or on the road, today's workforce expects easy access to mobile applications for collaborating and communicating with colleagues, accessing and interacting with enterprise resources, and improving their overall productivity regardless of time or location.

Symantec™ Mobility: Application Management, a module of Symantec Mobility: Suite, allows organizations to enable mobile workforce productivity by managing the lifecyle of securing, distributing and retiring apps. From one central console, IT can easily manage internally-developed apps, third party apps, native apps or web apps across personally-owned and corporate-managed devices. To safeguard apps and data, IT can apply granular application-level policies related to user authentication, data loss prevention and more.

Key Benefits

- **Manage apps without managing devices:** Application Management works with or without mobile device management (MDM), allowing you to focus on protecting apps and data, not just the device.
- **Expand mobility:** Application Management separates personal and corporate apps, giving organizations more flexibility to enable mobility in BYOD environments and the extended enterprise, without infringing on user privacy.
- **Add security in minutes:** Symantec's unique app wrapping technology applies a layer of security and policy management in minutes, without demanding a SDK or source code changes.

Key features

App wrapping

Application Management provides a simple and easy app wrapping mechanism that protects corporate apps and data while enabling a clear separation of enterprise and personal data on the device. Because Application Management does not require source code modifications or an SDK, anyone – IT administrators, project managers – can wrap an app in a matter of minutes, accelerating mobile deployments without compromising security or the user experience. Apps can be revoked quickly and securely when employees leave the organization or devices are no longer active—without impacting personal data.

App and data security

Centrally manage app protection and compliance policies. Implement granular control with comprehensive per-app policies including:

- User authentication, re-authentication, and single sign-on
- Data encryption (FIPS-certified algorithms)
- Local data storage control
- Enabling offline access
- Enabling document sharing, copy/paste, or other data loss policies
- Secure network communication
- Jailbreak/root detection

App-level policies work independent of device management, allowing you to manage enterprise apps and data without the additional overhead of managing devices not owned by the enterprise. Since all corporate app data written locally is managed by an app-level policy, an administrator can revoke both the app code and corporate data on demand, without affecting the user's personal data on the device, with or without MDM.

Authentication and single sign-on

Application Management delivers a simplified user experience with app-level single sign-on. IT can configure app authentication requirements where a wrapped app (e.g. any Symantec productivity app, a custom-built app, a web app, or a Sealed 3rd party ISV app) can act as an authentication proxy. This streamlines the user authentication process, as users no longer need to enter a password for every wrapped app. Instead, the user's first app login provides access to a mobile workspace consisting of multiple secured apps on the device. Application Management leverages popular authentication methods, such as Active Directory®, LDAP, and SAML.

Secure app connectivity

Application Management can enforce a secure SSL connection for wrapped apps and block the apps from going to unauthorized websites. This app wrap policy can mandate an SSL connection to ensure information security for HTTP data-in-transit. A secure app proxy protects data in transit with per-app SSL, FIPS 140-2 tunnels, separating corporate and personal traffic and simplifying compliance by controlling app communication without requiring a device-level VPN or firewall modifications.

Symantec productivity apps

Application Management includes Symantec™ Mobility: Workforce Apps to help you protect corporate data and keep employees productive anytime, anywhere with individually secured and protected apps for work.

Symantec Work Mail

Symantec™ Work Mail is a secure app that brings corporate email, calendar, contacts, notes, and tasks to the users. Email data at rest on the device is protected with FIPS-certified encryption that is independent of the device, helping to secure corporate data in the event the device passcode is compromised. IT administrators can configure security policies such as preventing copy/paste of content or limiting the apps in which email attachments can be opened. Work Mail supports a wide variety of mail servers, such as Microsoft® Exchange, Office 365™, Gmail™, and Lotus Notes® using Microsoft Exchange ActiveSync®. Work Mail can be delivered without mobile device management (MDM), so enterprises can deploy it with minimal impact on personal devices, while ensuring the security of corporate data. A secure email proxy provides end-to-end protection for email traffic, verifying device compliance before allowing connection to the network.

Symantec Work Web

Symantec™ Work Web is a secure Web browser, that provides safe access to internal Web-based applications and content. Employees gain mobile access to internal Web-based resources and apps. To protect data in transit, a secure app proxy serves as a virtual network gateway for incoming traffic. Administrators can apply data control policies, such as requiring internal URLs be opened with the Work Web app.

*Symantec Work File**

Symantec™ Work File is a secure file editor and content management application for accessing corporate data. With Work File, users benefit from a user-friendly tool for editing and collaborating on files, and IT benefits from a solution that protects confidential data by applying a layer of security and management policies, such as file expiration and removal, copy/paste and open-in restrictions, and DLP integration. Work File also leverages a secure app proxy to protect data in transit.

Symantec Work Hub

Application Management enables self-service distribution of apps to employees and other authorized users, such as contractors or partners with Symantec™ Work Hub. With a corporate-brandable, private enterprise app store, IT can provide a convenient, single place for your workforce to get the apps they need to get their jobs done. Distribute Workforce Apps custom-built or commercially available apps, wrapped (e.g. Symantec Sealed) or unwrapped apps, iOS, Android or HTML 5 apps.

Users can view only the apps they are authorized to use based upon their roles. They can also rate and review apps, while administrators can get reports on app downloads.

Symantec Sealed Program

The Symantec Sealed Program enables enterprises to confidently embrace third-party mobile apps while meeting data security requirements. The apps in the Sealed Program have been wrapped with a layer of security and management, allowing IT to define granular policies, such as encryption, authentication, and data-sharing restrictions. It delivers an ecosystem of trusted and secure third-party mobile apps, allowing you to provide a protected mobile workspace and fulfill the promise of mobile productivity.

Comprehensive Enterprise Mobility Management with Symantec Mobility: Suite

Mobility Suite simplifies mobility management, integrating mobile device management (MDM), mobile application management (MAM), mobile content management (MCM) and mobile threat protection into one comprehensive, single console solution. Whether your environment is standardized on corporate-owned devices, allows a choose your own device (CYOD) program, embraces bring your own device (BYOD), or manage a mix of these options, Mobility Suite makes it easier for enterprises to master security while maximizing productivity.

Minimum System Requirements

For an up-to-date list of system requirements visit www.symantec.com/mobility/products

*Planned for an upcoming release.

More Information

Visit our website

http://www.symantec.com/mobility/

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.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data-intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect 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

21333966 02/15