MobileIron for Samsung KNOX Android

With one billion devices running Android, and 1.5 million device activations every day, Android currently dominates the market as the number-one mobile platform for consumers. By contrast, enterprises have been much slower to embrace these devices due to long-held concerns about Android security and fragmentation. But that's all about to change, because organizations can no longer ignore the market dominance of Android smartphones and tablets and employee demands to use them for work.

To securely enable Android in the enterprise, IT must be able to enforce security and compliance requirements on any device without putting personal apps and data at risk. Meeting these complex requirements demands an IT platform that is purpose-built to secure content, apps, and devices across multi-OS environments so IT can protect corporate data while delivering the choice and flexibility users expect.

MobileIron and Samsung: Accelerating Samsung Android Adoption in the Enterprise

To help secure Android in the enterprise, MobileIron and Samsung are working together to provide the most secure and powerful mobility solutions for both employee-owned and corporate-provided rollouts of Samsung Android devices.

MobileIron has long been a champion of Android adoption in the enterprise, and was the first provider to deliver an enterprise app storefront, BYOD privacy controls, and certificate-based identity management for Android. MobileIron's comprehensive enterprise mobility management (EMM) platform also fully supports the Samsung KNOX platform, which helps to strengthen IT security controls for Android.

Samsung KNOX devices provide the underlying device and operating system services that MobileIron leverages to meet enterprise requirements for email, Wi-Fi, and VPN access. Samsung KNOX also provides hardware-integrated, defense-grade security and data isolation between work and personal data on Android devices. Together, MobileIron and Samsung deliver a complete solution for Android device and application security that can meet the unique requirements of any IT organization.

Device Security with Samsung KNOX

Samsung KNOX is an Android security framework specifically developed for the enterprise. KNOX provides hardware and software security capabilities that help IT securely deploy Android as a primary computing platform. Key features include:

- Enhanced OS tampering/root detection via Trusted Boot and hardware-based security mechanisms like the TrustZone-based Integrity Measurement Architecture (TIMA) to prevent compromised devices from accessing corporate data.
- Hardware-based TIMA key store protects encryption keys that can only be accessed if a device is compliant and running trusted software verified through special attestation technologies.

Challenge

- Secure sensitive data on Android
- Support Android app initiatives
- Support Android BYOD initiatives
- Migrate from BlackBerry

Solution

- MobileIron for Samsung KNOX Android

Benefits

- Secure mobile app lifecycle
- Configure all core services
- Establish security and privacy controls
- Protect data-at-rest through data loss prevention (DLP) and encryption controls
- Manage app lifecycle
- Deploy at scale

Recent Recognition

- Gartner: MobileIron positioned in the 2014 Leaders Quadrant for the Enterprise Mobility Management (EMM) Suites for the fourth consecutive year.

MobileIron - 415 East Middlefield Road - Mountain View, CA 94043 USA - Tel. +1.650.919.8100 - Fax +1.650.919.8006 - info@mobileiron.com

- Data separation for applications and systems services through enhancements to SE for Android and an SE for Android Management (SEAMS) API used to secure application containers.

Application Security: Two Containerization Solutions

The enhanced Android security features listed above focus on monitoring software integrity and securing the device. To protect applications, Samsung KNOX and MobileIron provide two options: The Samsung KNOX Workspace and MobileIron AppConnect for KNOX. Each of these options provides varying levels of granular control and security depending on the needs of the organization.

Option 1: Samsung KNOX Workspace

The Samsung KNOX Workspace is a security container that forms a protective barrier around the applications and data that reside within it so they can't be accessed by applications outside of the container. For example, documents stored in the KNOX Workspace cannot be viewed in editing apps that are not inside the container.

The KNOX Workspace includes a rich set of policies for authentication, data security, per-app VPN, email, application distribution, and control over information exchange between the container and the rest of the device. All of these processes are managed through the MobileIron EMM platform.

The KNOX Workspace is best suited for customers that:

- Maintain standardized mobile deployments on KNOX-enabled Samsung devices.
- Deploy both third-party and custom containerized apps that don't require app-specific configurations.
- Operate in highly regulated industries with specific compliance and regulatory requirements.

The KNOX Workspace is ideal for managing:

High-security deployments: Information flow must be tightly managed, and data loss prevention (DLP) controls are fundamental to the protection of data. The Samsung KNOX platform provides defense-grade encryption and authentication features such as FIPS-validated encryption and support for CAC card authentication.

Option 2: MobileIron AppConnect for KNOX

MobileIron AppConnect for Samsung KNOX containerizes apps to protect app data-at-rest without touching personal data. Each app becomes a secure container whose data is encrypted, protected from unauthorized access, and removable. Because each user has multiple business apps, each app container is also connected to other secure app containers. This allows the sharing of policies like app single sign-on (SSO) and the sharing of data, such as documents. All individual app containers are connected to MobileIron for policy management.

With AppConnect for Samsung KNOX, customers have the opportunity to leverage the cross-platform AppConnect containerization solution in combination with the enhanced security capabilities of Samsung KNOX.

AppConnect for Samsung KNOX is best suited for customers that:

- Maintain a multi-OS environment with a mix of mobile operating systems including iOS and different flavors of Android devices.
- Need to deploy wrapped apps with support for app SSO, app-level access control, and the ability to push app-specific configurations.
- Require apps that provide secure access and DLP enforcement for corporate intranet and file-sharing without requiring a VPN infrastructure.

AppConnect for Samsung KNOX is ideal for:

BYOD/COPE program management: IT supports both BYOD and corporate-owned, personally enabled (COPE) devices. In this environment, AppConnect for Samsung KNOX enables IT to create a separate enterprise persona that keeps enterprise data and apps separate from personal data while preserving the native device experience.

Granular App Management: The combination of MobileIron's comprehensive EMM platform and Samsung's enterprise-class Android devices allows organizations to securely and confidently enable Android. With the MobileIron for Samsung Android solution, enterprises can deploy apps at scale while automating app configurations and settings. This is ideal for organizations that need to deploy wrapped apps with support for app SSO, app-level access control, and app-specific configurations. It also enables secure access through DLP enforcement for corporate intranet and file-sharing without requiring a VPN.

Take the Next Step

To learn more about the MobileIron for Samsung Android solution, please visit www.mobileiron.com.

MobileIron and Samsung provide advanced security and app management that allows organizations to adopt Android broadly as a mobile computing standard.

Gartner, Inc., Leaders Quadrant for Enterprise Mobility Management, 2014. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

MobileIron - 415 East Middlefield Road - Mountain View, CA 94043 USA - Tel. +1.650.919.8100 - Fax +1.650.919.8006 - info@mobileiron.com