VMWARE AIRWATCH SAMSUNG KNOX MANAGEMENT
Start with the Hardware: Trust and Security with Samsung Knox

OVERVIEW
VMware AirWatch® Enterprise Mobility Management (EMM) platform provides comprehensive support of Samsung Knox for Workspace management and security.

KEY BENEFITS
• Advanced security and government certifications for use in the most secure deployments
• Comprehensive device and application management for the device and Knox Workspace for additional security and ease of use
• Separation of work and personal data for BYOD deployments

Why VMware AirWatch for Samsung Knox
Samsung Knox is a defense-grade, hardware level mobile security platform built into Samsung devices to provide data protection, management and deployment options. This framework introduces additional levels of security to meet varying enterprise use cases. Create a dual persona with Knox Workspace to keep work apps and data in a separate container. Knox can also be configured in Container Only Mode, fully locking the device into Knox Workspace with no personal side, ideal for corporate-liable devices.

The AirWatch Enterprise Mobility Management (EMM) platform provides comprehensive management for Samsung Knox devices through native capabilities supported by the platform and Samsung-specific APIs:
• Knox Workspace management
• App security and management
• Multi-layered security and compliance

Knox Workspace Management
Easily deploy and manage the Knox Workspace from the AirWatch console to fit organization requirements for both dual persona and container-only use cases. AirWatch and Samsung Knox blend a native user experience with the security features IT requires, while providing users with a familiar Android experience and the ability to seamlessly switch between work and personal personas.

AirWatch device enrollment for Samsung Knox is simple with Knox Mobile Enrollment, enabling IT to bulk enroll devices simultaneously. Within the AirWatch console, easily setup MDM profiles and assign to devices. Separately, the Samsung Knox Portal identifies the device by serial number or IMEI to be registered into AirWatch and the policies are deployed to the devices. When a device is initially powered on and connected to Wi-Fi, the profiles and settings are automatically configured, along with the Knox Workspace container. Once a device is enrolled with Knox Mobile Enrollment, the device will automatically re-enroll even if the device is reset.

With AirWatch, configure automatic access to corporate resources such as Wi-Fi and VPN. Deploy secure native email with additional security policies such as SSL encryption and digital certificate signatures.
App Security and Management

With AirWatch, easily manage and secure enterprise apps within the Knox Workspace. Install internal applications automatically and enable secure single sign-on (SSO). Enable Google Mobile Services applications such as Google Chrome, Google Play Store, Google Maps and more inside the Knox Workspace. For dual persona devices, maintain separate versions of common apps inside and outside the Workspace.

Create app policies, including whitelists, blacklists, and required applications using app groups so only approved applications are on the device. Per-app VPN provides a secure connection to internal data from apps within the Knox Workspace. App containerization provides separation of work and personal data to prevent data from being shared from the work side to the personal side. Detailed app reporting makes it easy to view app inventory, manage app versions and track app compliance.

Multi-layered Security

Enterprise data in the Knox Workspace is secured with a hardware-rooted trusted environment that ensures that operations can only occur when the device is proven to be in a non-compromised and approved state. Multi-layered device level protection is built into each flagship Samsung device along with configurable two-factor authentication based on enterprise requirements. Configure both device level and Workspace container passcodes, and multifactor authentication to require a pattern, PIN or passcode in addition to a fingerprint. Data within the Knox Workspace is secured with 256-bit AES encryption. Enable advanced security features such as enabling Common Criteria mode, enabling TIMA KeyStore, SmartCard authentication, ODE Trusted Boot verification, and more.

Fully lock corporate liable devices into Container Only Mode where the entire device is restricted to the Knox Workspace to isolate, encrypt and protect work data. In Container Only Mode there is no access to a dual persona, maintaining a high level of security.

Manage devices remotely with commands such as clear passcode and enterprise wipe and have these actions only apply to the Knox Workspace. Detect rooted devices automatically and configure actions and escalations to remediate device compliance. Set audit logs to monitor if any errors occur during the creation of the Knox Workspace.