Mobile Security in Government Configuration Guide

Version 1.0

August 2020

Automated MDM Enrollment Configuration Guide

Overview

This document provides you with a baseline set of MDM policies, guidelines and configurations for government devices that could be used at above OFFICIAL. The following is an example using a Samsung Galaxy S8 running Knox 3.0 and using the latest VMWare AirWatch EMM version.

12 Principles for Securing Devices

Security Principle	Recommendation and Explanation
Assured data-in-transit protection	Samsung provide a Knox compatible VPN client that should be used to route data via the VPN. This client gives three options for its VPN: Knox workspace only VPN Whole device VPN (excluding Knox workspace) Whole device VPN (including Knox workspace) One of these should be chosen and should have the VPN set to "Per-App" and to include "All Packages", ensuring all application data within the desired scope is routed through the VPN. Choosing the container-only VPN allows less-trusted application data to be separated from the application data within the Knox Workspace - which could be treated as a security boundary for more sensitive information.
Assured data-at-rest protection	Data stored within the Knox Workspace is encrypted by default. Ensure Android's native data encryption is also enabled to protect data outside the Knox Workspace. The Knox native email client has been enabled to use the Sensitive Data Protection (SDP) feature. Third party applications can take advantage of the SDP-protected "Chamber" folder to protect data while locked as well as when the device is turned off. Samsung also provide an SDK to enable applications to treat files as "sensitive", meaning they are protected by the SDP mechanism.
Authentication	The user should be required to authenticate to the device in line with your organisational policy (see Authentication Policy). Your organisation's services should be configured to use X.509 client certificate authentication where possible. Devices should be provisioned with user-specific client certificates. The native mail client and browser can use these for authentication. The authentication mechanisms chosen can be in the form of passwords, biometrics, swipe pattern, or PIN. Each credential should be unique.

Secure boot	No configuration is required.
Platform integrity and application sandboxing	Knox 2.8 has several security features to verify the integrity of the phone software and hardware. Configure the MDM software to enable “Remote Attestation” to verify the integrity of the platform before creating the Knox Workspace. The MDM client application is not verified by the Knox platform. A social engineering attack could result in a compromised MDM client being installed. To prevent this, device enrollment should only be performed by an administrator and users should not be permitted to re-enrol.
Application Whitelisting	Samsung Knox-enabled devices allow a server to fully control applications both inside and outside the Knox Workspace, including maintaining an application installation whitelist. Optionally, the administrator can allow the user to move applications installed on the personal side of the device into the Knox Workspace, or enable the use of Google Play in the Knox Workspace. If either option is enabled, the administrator can still control installation via whitelisting. All enterprise applications should be deployed within the Knox Workspace. Some MDM servers allow an enterprise application catalogue to be established, permitting users access to an approved list of applications via the MDM client. If the Play Store or Samsung Store is enabled, an MDM should be used to control and monitor which applications a user can install.
Malicious code detection and prevention	Where possible, an enterprise application catalogue can be used which should only contain vetted applications. If the Google Play or Samsung Store is enabled, a whitelist should be used to control which applications may be downloaded. Content-based attacks can be filtered by scanning capabilities in the enterprise. Applications hosted in the Google Play Store are scanned for potentially harmful or malicious activity prior to being made available for download. Each application is protected by its own sandbox which is enhanced by controls such as SELinux and SECCOMP. Therefore, there is little additional value to be gained from any third-party anti-malware products in the platform.
Security policy enforcement	MDM software can be used to enforce security policies on both the device and Knox Workspace and prevent the user from altering security-related settings. Not all MDM products support the full range of Knox and Android settings. Choose an MDM provider which supports the required configuration settings for your particular deployment to ensure they are applied securely. Please see Samsung's list of supported MDM vendors for details on which MDM supports which policy.
External interface protection	Wi-Fi, NFC, Bluetooth, SD cards, and the use of USB interfaces can all be disabled if not required. At a minimum, USB debugging should be disabled via policy.
Device Update Policy	MDM software can be used to audit which apps and OS versions are installed on a device. Some MDM servers may provide an application, OS, and Firmware update policy to ensure that apps are updated.

	The user is responsible for installing Over-The-Air (OTA) updates, but the administrator can prevent OTA updates and view what OS version a user has installed via MDM. Enterprises can also use FOTA (Firmware Over-The-Air) to control how and when firmware updates are performed on devices.
Event collection for enterprise analysis	The MDM server can be used to retrieve information from the device such as, installed applications, the last time the device has been seen by the MDM, policy compliance, and location information. The extent of the available event collection will depend on the MDM in use. Additionally, some MDM servers support the additional Audit and Logging features which Samsung Knox adds to the Android platform. Logs created on the device, including failed unlock attempts, can be retrieved using an MDM which supports this feature.
Incident Response	Samsung Knox Workspace enabled devices support remote wipe when used in conjunction with a suitable MDM. This can be configured to selectively wipe the Knox Workspace, the device, or both, and uninstall the entire Knox Workspace. The SD card may also be wiped if configured in policy. In addition to this, Samsung Knox Workspace enabled devices offer a device attestation mechanism, enabling the device to attest its integrity to the MDM, or include tamper incident logs which can be responded to. Access to the enterprise network can be prevented by revoking the VPN client certificate associated with a lost or stolen device. Additionally, the client certificates for any other enterprise servers (such as email) that are stored on the device should be revoked.

Recommended Policies and Settings

Automatic Provisioning

Automated provisioning of a Samsung device can only be achieved using Knox Mobile Enrollment (KME). This service is designed to assist in the deployment of devices and is able to provision devices in bulk.

Knox Mobile Enrollment also performs an Attestation check of a device prior to enrollment, to ensure the device has not been compromised. If integrity cannot be assured, the mobile enrollment process will and the user will be exited to the home screen.

Knox Workspace Policies

Configuration Rule	Recommended Setting
Allow applications to be moved into the Workspace **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Restrictions Profile -> Enable Application Move**	Enabled. Applications that can be moved into the container are restricted by the whitelist.
Whitelist Applications **Devices -> Compliance Policies -> App Groups** **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Application Control**	Whitelist essential applications for accessing and manipulating corporate data only. e.g. email client, browser, secure communications and productivity suite. If the Managed Google Play Store is permitted, allow only applications in the whitelist to be installed.
Browser	Enabled by default.
VPN **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> VPN**	Apply the Per-App VPN to all applications in the Knox Workspace, including background services and widgets.
Email **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Exchange ActiveSync**	Configure the native email client to connect to the email server using client certificate or credential authentication.
Email account addition	Disabled.
HTTP Proxy **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> VPN**	Set the enterprise proxy as both the device and Knox proxy. This will prevent network traffic which is not configured to use the VPN reaching the Internet.
Password **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Passcode**	The authentication mechanisms chosen can be in the form of passwords, biometrics, swipe pattern, or PINs and should adhere to the model of having the user authenticate once to the device, and then again to access the sensitive data within Knox. Each authentication method should be unique.
Credentials **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Credentials**	Some certificates can be installed via policy, VPN, email, etc. However, other certificates need to be sent to the device then manually moved to the Knox area.

Permit moving files into the Knox Workspace **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Restrictions Profile**	Disabled.
Permit moving files out of the Knox Workspace **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Restrictions Profile**	Disabled.
Knox Workspace data synchronisation **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Restrictions Profile**	The following settings should be set to 'disallow' to prevent data being moved into and out of the Knox Workspace: - Preview Knox notifications - Export contacts to personal mode - Export calendar items to personal mode
Biometrics **Devices -> Profiles & Resources -> Profiles -> Android -> Container -> Passcode**	Samsung's S8 devices are required to perform biometric checking within a Trusted Execution Environment (TEE). This means that a physical attack on a locked device should not result in compromise of data. Fingerprint readers are required to have less than 0.002% false acceptance rate, but the performance of individual sensors can vary within that range. You should consider these limitations when devising an authentication policy which permits the use of biometrics.
Secure Communications **Apps & Books -> Applications -> Native**	Secure Communications apps are possible to use inside the Knox Workspace container. Some Samsung Partners have also integrated their Secure Communications app with TrustZone on the device for enhanced security. You should consider these integrations when choosing a secure communications application.

Knox Enabled Device Policies (Device Side)

Configuration Rule	Recommended Setting
App Stores **Devices -> Profiles & Resources -> Profiles -> Android -> Restrictions Profile**	Disable or remove the Google Play and Samsung App store, and prevent the installation of applications from unknown sources.
Whitelist Applications **Devices -> Compliance Policies -> App Groups**	Disable or remove unnecessary applications. If the Google Play or Samsung App stores are permitted, allow only applications in the whitelist to be installed.

Devices -> Profiles & Resources -> Profiles -> Android -> Application Control	
Developer Mode **Devices -> Profiles & Resources -> Profiles -> Android -> Restrictions Profile**	Prevent all developer mode settings, including USB debugging and USB storage mode.
Encrypted Storage	Enforced internal encryption. Encrypted by default on Android 7.0 and above.
SD Card **Devices -> Profiles & Resources -> Profiles -> Android -> Restrictions Profile**	Disable access to the SD card.
HTTP Proxy **Devices -> Profiles & Resources -> Profiles -> Android -> Global Proxy**	Set the enterprise proxy as both the device and Knox proxy. This will prevent network traffic which is not configured to use the VPN reaching the Internet.
Password **Devices -> Profiles & Resources -> Profiles -> Android -> Passcode Profile**	The authentication mechanisms chosen can be in the form of passwords, biometrics, swipe pattern, or PINs and should adhere to the model of having the user authenticate once to the device, and then again to access the sensitive data within Knox. Each authentication method should be unique.
Lock Timeout **Devices -> Profiles & Resources -> Profiles -> Android -> Passcode Profile**	10 minutes.
VPN **Devices -> Profiles & Resources -> Profiles -> Android -> VPN**	Apply the Per-App VPN to all applications outside the Knox Workspace, including background services and widgets.
Certificates **Devices -> Profiles & Resources -> Profiles -> Android -> Credentials**	Enable certificate validation at install. Install enterprise certificates (including VPN certificates and organisation CA certificates).
Interfaces **Devices -> Profiles & Resources -> Profiles -> Android -> Restrictions Profile**	Disable unnecessary interfaces, e.g. USB interface, Bluetooth, NFC as required.

Attestation	Verification of Knox attestation status should be required.