Guidance

End User Devices Security Guidance: Samsung devices with Knox 2.x

Updated 28 July 2015

Contents

This guidance was developed following testing performed on a Samsung Galaxy S5 device and is applicable to Samsung KNOX Workspace enabled devices running Android 5.0 and higher with KNOX 2.4 and higher.

1. Usage scenario

The KNOX Workspace enabled devices will be used remotely over 3G, 4G and non-captive Wi-Fi networks to enable a variety of remote working approaches such as accessing OFFICIAL email; reviewing and commenting on OFFICIAL documents, and accessing the internet and other web resources.

The KNOX Workspace provides additional security features over the underlying Android platform. Users can store all or some of their enterprise data in the KNOX Workspace container, providing enhanced protection.

To support these scenarios, the following architectural choices are recommended:

- For users working primarily with sensitive data, the majority of their work will be within the KNOX Workspace container. The Android platform outside the KNOX Workspace

container is used for non-sensitive work.

- Users who only access sensitive data occasionally can use the KNOX Workspace container when they are required to work with that sensitive data, doing the non-sensitive majority of their work outside the container.
- All data-in-transit to and from the device should be routed over a secure enterprise VPN to ensure the confidentiality and integrity of the traffic, and to allow the devices and data on them to be protected by enterprise protective monitoring solutions.
- Arbitrary third-party application installation by users is not permitted on the device. An enterprise application catalogue should be used to whitelist and distribute approved applications to devices.
- Enterprise applications and data should be kept within the KNOX Workspace container where possible. Unnecessary applications outside the container should be removed or managed using an appropriate whitelist.

2. Summary of platform security

Samsung KNOX Workspace enabled devices were assessed against each of the 12 security recommendations. The results of the assessment are shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the platform can best satisfy the security recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	The KNOX-compatible VPN has not been independently assured to Foundation Grade.
2. Assured data-at-rest protection	
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	
7. Malicious code detection and prevention	
8. Security policy enforcement	

9. External interface protection
10. Device update policy
11. Event collection for enterprise analysis
12. Incident response

2.1 Significant risks

The following significant risks have been identified:

- The KNOX compatible VPN has not been independently assured to Foundation Grade. Without assurance of the VPN, there is a risk that data transiting from the device could be compromised.

3. How the platform can best satisfy the security recommendations

This section details the platform security mechanisms that best address each of the security recommendations.

3.1 Assured data-in-transit protection

Use a compatible KNOX VPN client until a Foundation Grade VPN client for this platform becomes available. VPN authentication should be certificate-based.

To route all data via the VPN, the ‘Per-App’ VPN should be configured for all applications on the device, both inside and outside the KNOX Workspace container. Using the per-app VPN in this configuration ensures that traffic from all applications is routed through the VPN. Applications will not have internet access until the VPN has connected.

Organisations may wish to set up two VPN profiles, one for all applications on the device, and a second for all applications within the KNOX Workspace container. This setup would allow traffic from less-trusted applications to be separated from the applications in the KNOX Workspace container that handle OFFICIAL material.

3.2 Assured data-at-rest protection

The KNOX Workspace container is encrypted by default, so applications and data relating to OFFICIAL material should be kept within it. Outside the KNOX Workspace use the device's native data encryption. The KNOX native email client has been enabled to use the Sensitive Data Protection (SDP) feature and applications can take advantage of the SDP-protected "Chamber" folder to protect data while locked as well as when the device is turned off.

Only the Galaxy S6 and S6 Edge devices have Foundation-grade approval of their encryption.

3.3 Authentication

Devise a scheme which requires a strong password to access sensitive data. For example:

- a numeric PIN to access the device, then a strong password to access the KNOX Workspace container
- a strong password to access the device, then a shorter password or token to access the KNOX Workspace container

The scheme selected should be based on the usage model of the device; if the user keeps most of their sensitive data in the KNOX Workspace container, and would like easier access to non-sensitive applications and data outside the container then follow the first scheme above. Conversely, if the user does nearly all their work outside the container then the device password must be stronger; the second scheme should be followed.

Whichever scheme is selected, the strong password must be complex, with a length of at least 9 characters including uppercase, lowercase and symbols. The KNOX password must be enforced with a complexity to meet the business need. Configure the device to self-wipe, and the KNOX Workspace container to be disabled, after a number of incorrect password attempts.

KNOX Workspace makes use of ARM TrustZone-based components together with the user's credentials to protect cryptographic material and strengthen the protection of data contained within it.

3.4 Secure boot

This requirement is met by the platform without additional configuration.

3.5 Platform integrity and application sandboxing

KNOX 2.x 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 container.

The MDM client application is not verified by the KNOX platform as being unmodified. A social engineering attack could result in a compromised MDM client being installed. To prevent this, device enrolment should only be performed by an administrator and users should not be permitted to re-enrol.

3.6 Application whitelisting

Samsung KNOX enabled devices allow an MDM to fully control applications both inside and outside the KNOX Workspace container including maintaining an application installation whitelist.

Optionally, the administrator can allow the user to install applications installed on the personal side of the device into the KNOX Workspace container, or enable the use of Google Play in the KNOX Workspace container. If either option is enabled, the administrator can still control installation via whitelisting.

All enterprise applications should be deployed within the KNOX Workspace container; enterprise applications outside the KNOX Workspace container should be limited.

Some MDM servers allow an enterprise application catalogue to be established to permit users access to an approved list of applications via the MDM client. If the Play Store or KNOX Store is enabled, an MDM should be used to control and monitor which applications a user can install.

3.7 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 KNOX store is enabled, a whitelist should be used to control what applications may be downloaded. Content-based attacks can be filtered by scanning capabilities in the enterprise.

Several third-party anti-malware products exist which attempt to detect malicious code for this platform and can be used if desired.

Applications hosted in the Google Play marketplace are scanned for potentially harmful or malicious activity prior to being made available for download.

3.8 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.

3.9 External interface protection

Wi-Fi, NFC, Bluetooth and the use of USB interfaces can all be disabled. At a minimum, USB debugging should be disabled via policy.

3.10 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 update policy to ensure that apps are updated.

The user is responsible for installing OTA updates, but the administrator can prevent OTA updates and view what OS version a user has installed via MDM.

3.11 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.

3.12 Incident response

Samsung KNOX Workspace enabled devices support remote wipe when used in conjunction with a suitable MDM, which can be configured to selectively wipe the KNOX Workspace container, the device, or both, and uninstall the entire KNOX Workspace container. The SD card may also be wiped if configured in policy.

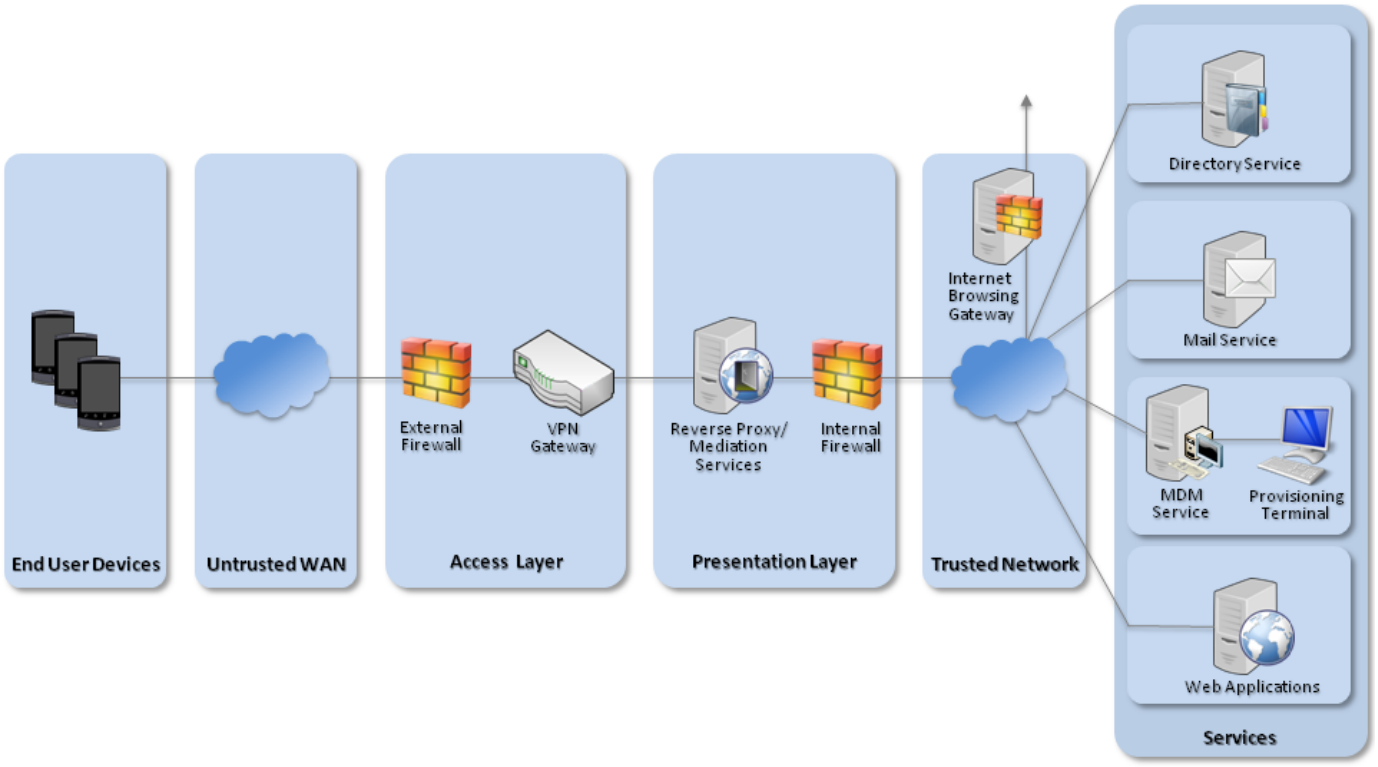
In addition to this, Samsung KNOX Workspace enabled devices offer a device attestation mechanism, enabling the device to attest its integrity to the MDM, or include tamper incident logs which can be responded to.

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.

4. Network architecture

It is recommended that all remote or mobile working scenarios use a typical remote access architecture based on the Walled Garden Architectural Pattern.

Configure the Samsung KNOX Workspace enabled device's global HTTP proxy so that it is used for both the device and the KNOX Workspace container.



Recommended network architecture for deployments of Samsung devices with KNOX 2.x

5. Deployment process

For an enterprise deployment of Samsung KNOX Workspace enabled Android devices that is suitable for organisations working with OFFICIAL data, administrators should:

1. Deploy and configure the requisite network components as described above.
2. Procure and set up an MDM server that is compatible with KNOX and is able to enforce the settings given in the Policy Recommendations section below.
3. Create MDM security profiles for the Samsung KNOX Workspace enabled devices in line with the guidance given in the Policy Recommendations section, and associate these profiles with the devices.

6. Provisioning steps

The following steps should be followed to provision each device onto the enterprise network to prepare it for distribution to end users.

1. Install the MDM client on the device, and enrol the device into the MDM. The enrolment process will vary according to the MDM in use.
2. Install the KNOX compatible VPN client; this should be done via the MDM if possible.
3. Push the MDM policy to the device. If the MDM does not allow configuration of any of the following via policy, it should be done manually. Dependent on the MDM, policies should be applied for the following configuration settings:
    1. Install and configure the KNOX Workspace container.
    2. Configure on-device security settings.
    3. Install required user, device and required trusted CA certificates for the organisation on the device. MDM software may automate this process.
    4. Ensure that only trusted apps are installed and enabled on the device (disable or delete unnecessary apps both inside and outside the KNOX Workspace container including Google Play and the KNOX Store).
    5. Ensure that all enterprise apps are installed inside the KNOX Workspace container. Apps outside the KNOX Workspace container should be restricted to basic functionality, and personal web browsing if desired.
    6. Configure a per-app VPN profile for all applications inside the KNOX Workspace container. This can be done with a single setting, and does not require each application to be set up individually to use the VPN.
    7. Configure a per-app VPN profile for all applications permitted outside the KNOX Workspace container. This can be done with a single setting, and does not require each application to be set up individually to use the VPN.
    8. Configure the KNOX email client to connect to the enterprise server using client certificate authentication.

9. Configure the device's global HTTP proxy so that it is used for both the device and the KNOX Workspace container.

7. Policy recommendations

The following settings should be applied from the MDM interface. As all MDMs vary, the text accompanying the setting may be slightly different to that shown below.

7.1 KNOX Workspace container policies

The following policy should be applied to KNOX Workspace container.

Configuration Rule	Recommended Setting
App stores	Disable the Samsung KNOX and Google Play app stores. Applications from these stores that are required may be installed using the out-of-Workspace store app, then installed inside the Workspace container using KNOX settings utility.
Allow applications to be moved into the Workspace	Enable. Applications that can be moved into the container are restricted by the whitelist.
Whitelist Applications	Whitelist essential applications for accessing and manipulating corporate data only, e.g. mail client, browser, and office suite. If the KNOX Store or Google Play stores are permitted, allow only applications in the whitelist to be installed.
Browser	Enable.
VPN	Apply the Per-App VPN to all applications in the KNOX Workspace container, including background services and widgets.
Email	Configure the email client to connect to the enterprise server using client certificate authentication.
Email account addition	Disable This prevents users adding additional email accounts within the Workspace.
HTTP Proxy	Set the enterprise proxy IP as both the device and KNOX proxy. This will prevent network traffic which is not configured to use the VPN reaching the Internet.
Password*	Enable KNOX Password Policy: True KNOX Timeout: 30 minutes Maximum failed attempts: 5 Minimum length: 8 characters Quality: Alphanumeric Password history: 8

	Maximum passcode age: 90 days Minimum character changes: Set to greater than 1 to prevent incremental password change.
Credentials	Required client certificates should be installed via policy.
Permit moving files into the KNOX Workspace container	False
Permit moving files out of the KNOX Workspace container	False
KNOX Workspace data synchronisation	The following settings should be set to 'disallow' to prevent data being moved into and out of the KNOX Workspace container: - Preview KNOX notifications - Export contacts to personal mode - Export calendar items to personal mode

*The choice of KNOX Workspace container password complexity may be altered according to the organisational requirement. Given assurance that the whole device is controlled by policy as per the guidelines, the complexity of the container password may be reduced as suggested here. However, the organisation may choose to enforce a greater level of complexity for the Workspace container password.

7.2 Samsung KNOX Workspace enabled device policies

The following policies should be applied outside the KNOX Workspace container. These settings will promote use of the KNOX Workspace container and secure residual data and activity outside the KNOX Workspace container.

Configuration Rule	**Recommended Setting**
App stores	Disable or remove the Google Play and Samsung App store, and prevent the installation of applications from unknown sources.
Whitelist Applications	Disable or remove unnecessary applications. If the Google Play store is permitted, allow only applications in the whitelist to be installed.
Developer Mode	Prevent all developer mode settings, including USB debugging and USB storage mode.

Common Criteria (CC) Mode	Enable CC mode
Encrypted storage	Enforced internal encryption.
SD card	Disable access to the SD card.
HTTP Proxy	Set the enterprise proxy IP as both the device and KNOX proxy. This will prevent network traffic which is not configured to use the VPN reaching the Internet.
Password*	Require Password: True Minimum length: 8 characters Maximum failed attempts: 5 Require complex password: True Password must contain uppercase, lowercase and symbols Passcode history: 8 Maximum passcode age: 90 days Wipe external storage during device wipe: True
Lock timeout	10 minutes.
VPN	Apply the Per-App VPN to all applications outside the KNOX Workspace container, including background services and widgets.
Certificates	Enable certificate validation at install. Install enterprise certificates (including VPN certificates and organisation CA certificates).
Interfaces	Disable unnecessary interfaces, e.g. USB interface, Bluetooth, NFC.
Attestation	Verification of KNOX attestation status should be required.
TIMA Key Store	Enable
ODE Trusted Boot Verification	Enable

*The choice of device password complexity may be altered according to the organisational requirement. If the whole device is controlled by policy as per the guidelines, the complexity of the container password may be reduced as suggested here. However, the organisation may choose to enforce a greater level of complexity for the container password.

7.3 VPN configuration

The KNOX compatible VPN client should be configured with the PSN Interim IPsec Profile in the CPA Security Characteristic. The configuration is dependent on the chosen MDM.

This VPN profile should be applied as a Per-App VPN to all applications on the device. A 'Per-App' profile does not require each app to be individually configured to work with the VPN; it causes the VPN to start automatically and all app traffic to be routed via the VPN tunnel.

8. Enterprise considerations

The following points are in addition to the common enterprise considerations, and contain specific issues for deployments of Samsung KNOX Workspace enabled devices.

8.1 Choice of MDM provider

Not all MDM solutions are capable of interacting with all KNOX APIs. It is essential that system architects evaluate which policies their MDM solution will enable them to set, and should note that currently no MDM solution can set all KNOX policy types. MDM solutions that cannot set the policies specified in section 8 should not be considered for use. Specifically, enabling CC mode requires either an MDM which supports the feature or installation of an Android application onto each device to enable the mode. Further details can be found in the "Samsung Android 5 on Galaxy Devices - Guidance documentation for CC and CPA" document.

Many MDM providers now offer cloud-based solutions. Organisations that wish to use cloud-based MDM products must take into consideration the risk of placing the security and control of their devices and data under a third party.

Legal information