Guidance

End User Devices Security Guidance: Samsung devices with KNOX

Published 14 May 2014

Contents

This guidance is applicable to Samsung devices with KNOX running Android 4.3. This guidance was developed following testing performed on a Samsung Galaxy S4 device running Android 4.3 and KNOX version 1.0.

1. Usage scenario

Samsung devices with KNOX 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 container provides additional security features over the underlying Android platform. Users can store all or some of their enterprise data in the KNOX 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 container. The Android platform outside the container is used for non-sensitive work.
- Users who require only periodic access to sensitive data can use the Android platform outside the container for the majority of their work, and open the KNOX container when they are required to use sensitive data.
- 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 container where possible. Unnecessary applications outside the container should be removed or managed using an appropriate whitelist.

2. Summary of platform security

This platform has been assessed against each of the twelve security recommendations, and that assessment is 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	No KNOX-compatible VPN has been independently assured to Foundation Grade.
2. Assured data-at-rest protection	Android data encryption has not been independently assured to Foundation Grade. The KNOX data encryption has not been independently assured to Foundation Grade. Keys for data protected under both KNOX and Android encryption remain in memory when the device is locked.
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:

- No KNOX-compatible VPN has been independently assured to Foundation Grade, and none currently supports all of the mandatory requirements expected from assured VPNs. Without assurance in the VPN there is a risk that data transiting from the device could be compromised.
- Neither the KNOX container data encryption nor Android's device encryption have been independently assured to Foundation Grade, and do not support some of the mandatory requirements expected from assured full disk encryption products. Without assurance there is a risk that data stored on the device could be compromised.
- Encryption keys protecting sensitive data remain in device memory when the device is locked. This means that if the device is attacked while powered on and locked, keys and data on the device may be compromised without the attacker knowing the password.

3. How the platform can best satisfy the security recommendations

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

3.1 Assured data-in-transit protection

Use a KNOX-compatible IPsec VPN client until a Foundation Grade VPN client for this platform becomes available.

To effectively ensure that all data is routed via the VPN, the per-app VPN should be configured for all applications on the device, both inside and outside the KNOX container.

3.2 Assured data-at-rest protection

Data in the KNOX container is encrypted by default. Use the device's native data encryption outside the KNOX container. The data is protected when powered off, but it is not protected when the device is locked.

To encourage use of the KNOX container, enterprise applications outside the container should be disabled or removed.

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 container
- a strong password to access the device, then a shorter password or token to access the KNOX 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 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 a complex, with a length of at least 8 characters including uppercase, lowercase and symbols. The Mobile Device Management server (MDM) should be used to set and enforce the password complexity rules.

The KNOX container 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. Only data stored in the KNOX container will be protected using this technology.

3.4 Secure boot

This requirement is met by the platform without additional configuration.

3.5 Platform integrity and application sandboxing

This requirement is met by the platform without additional configuration.

3.6 Application whitelisting

In KNOX 1.0, only KNOX-wrapped applications may run within the KNOX container. All enterprise applications which will process sensitive data should be deployed within the KNOX container; applications outside the KNOX 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 server 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.

Google Play scans applications outside the KNOX container for potentially harmful or malicious activity prior to making them available for download.

3.8 Security policy enforcement

Security policy is enforced via MDM configuration via the Samsung KNOX standard (formerly SAFE) and Samsung KNOX Premium APIs. It provides a number of additional controls over and above the standard Android set of controls.

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.

3.10 Device update policy

MDM software can be used to audit which applications and OS versions are installed on a device. Some MDM servers may provide an application update policy to ensure that applications are updated.

3.11 Event collection for enterprise analysis

Some MDM servers support the additional Audit and Logging features which Samsung KNOX adds to the Android platform. Logs created on the device include failed unlock attempts, can be retrieved using an MDM which supports this feature.

Additionally, the MDM server can be used to retrieve information from the device such as installed applications, last time device has been seen by the MDM, policy compliance and location information.

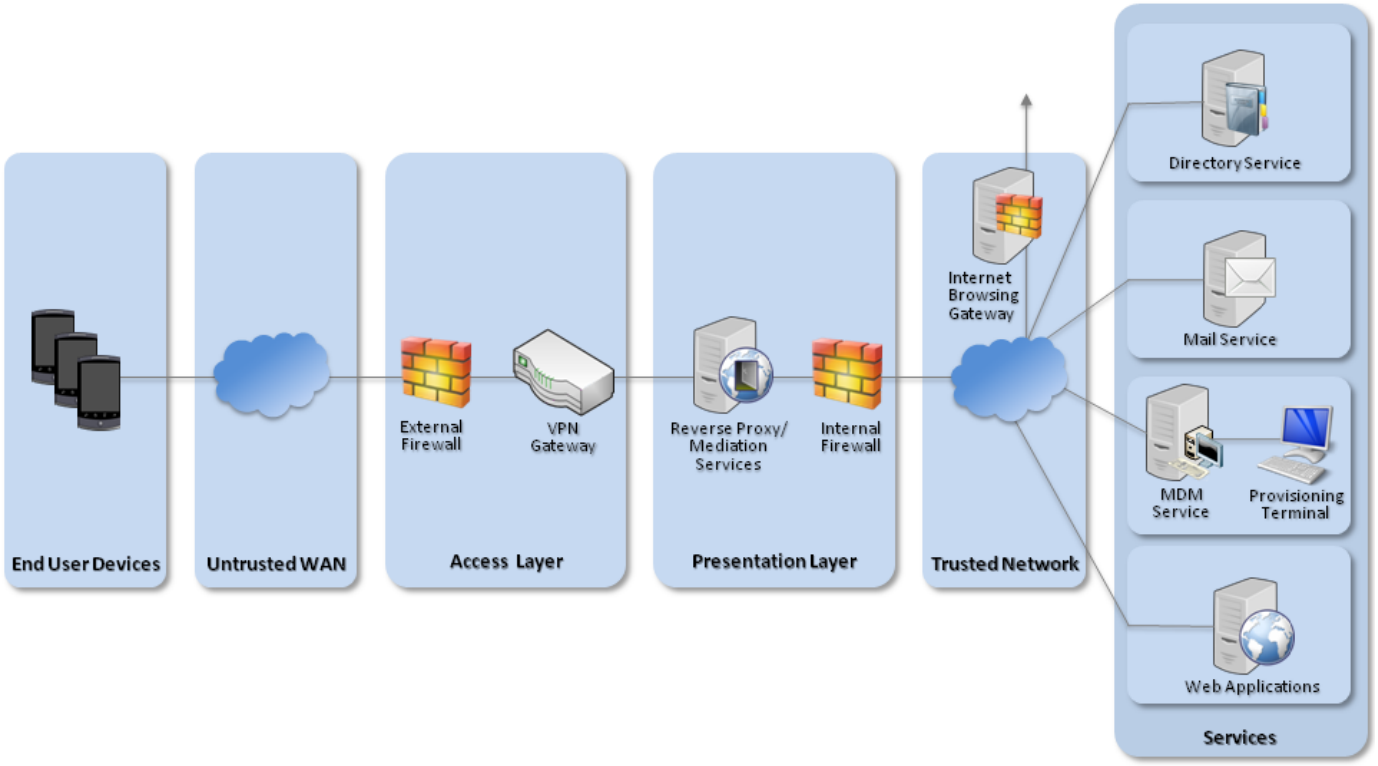
3.12 Incident response

The KNOX container supports remote wipe when used in conjunction with a suitable MDM, which can be configured to selectively wipe the KNOX container, the device, external memory cards or a combination of these, and uninstall the entire KNOX container.

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.



Recommended network architecture for deployments of Samsung devices with KNOX

5. Deployment process

For an enterprise deployment of Samsung KNOX-enabled Android devices, 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 the KNOX container and is able to enforce all the settings given in the Policy Recommendations section below.
3. Create MDM security profiles for the KNOX 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 end user device onto the enterprise network to prepare it for distribution to end users.

1. When powering on the device for the first time, choose not to send any data to the manufacturers as part of the setup process. This will prevent any services from leaking personal data via these channels.

2. 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.
3. Install a KNOX VPN client; this should be done via the MDM if possible.
4. The MDM policy should then be pushed to the device. Dependent on the MDM, policies should be applied for the following configuration settings. If the MDM does not allow configuration of any of the following via policy, it should be done manually.
    1. Install and configure the KNOX container.
    2. Configure on-device security settings.
    3. Ensure that only trusted applications are installed and enabled on the device (disable or delete unnecessary applications both inside and outside the KNOX container including Google Play and the KNOX Store).
    4. Ensure that all enterprise applications which will process sensitive data are installed inside the KNOX container, applications outside the KNOX container should be restricted to non-sensitive functionality such as personal web browsing if desired.
    5. Configure the per-app VPN for all applications inside the KNOX container.
    6. Configure the per-app VPN for all applications permitted outside the KNOX container.
    7. Configure the proxy settings for the device, both inside and outside the KNOX container.
    8. Configure the KNOX email client to connect to the enterprise server using client certificate authentication.

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 Policies for KNOX container

Policy Setting	Recommended Value
App stores	Disable or remove the Google Play and Samsung App store, and prevent the installation of applications from unknown sources.
Whitelist	Whitelist essential applications for accessing and manipulating corporate data only, e.g. mail client, browser, and office suite. If the KNOX Store is permitted allow only applications in the whitelist to be installed.
Browser	Enable.
VPN	Apply the per-app VPN to all applications in the KNOX container, including background services and widgets.
Email	Configure the email client to connect to the enterprise server using client certificate authentication.

Proxy	Set the enterprise proxy IP as the KNOX proxy. This will prevent network traffic which is not configured to use the VPN.
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.
Lock timeout	10 minutes.
Credentials	Required client certificates should be installed via policy.

*The choice of password complexity may be altered according to the organisational requirement. See the detail under the Authentication recommendation above for further discussion around this.

7.2 Policies for Android device

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	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.
Camera	Disabled (this forces the user to take and store photographs inside the KNOX container).
Encrypted storage	Enforced internal encryption.
SD card	Disable access to the SD card.
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
Lock timeout	10 minutes.
VPN	Apply the per-app VPN to all applications outside the KNOX container, including background services and widgets.
Proxy	Set the enterprise proxy IP to be the same as the KNOX proxy. This will prevent network traffic which is not configured to use the VPN.
Wi-Fi	Allow access to secure Wi-Fi only.
Credentials	Required VPN certificates should be installed via policy.
Interfaces	Disable unnecessary interfaces unless there is an overriding business need, e.g. USB interface, Bluetooth, NFC.

*The choice of password complexity may be altered according to the organisational requirement. See the detail under the Authentication recommendation above for further discussion around this.

7.3 VPN configuration

The KNOX VPN client should be configured with the PSN Interim IPsec Profile in the CPA Security Characteristic.

This VPN profile should be applied as a per-app VPN to all applications on the device; apply it to both applications inside the KNOX container and to applications outside the container.

8. Enterprise considerations

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

8.1 Choice of MDM provider

Not all MDM solutions are capable of interacting with all KNOX features. Is it 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.

8.2 Application management

To effectively ensure that all traffic routes over a secure enterprise VPN, the KNOX per-app VPN should be applied to all applications running on the device. This includes background services and widgets. Unnecessary applications should also be removed from the device.

Due to the number of applications running on a Samsung device, and the variation across platforms, it is advisable to maintain a software inventory. Such an inventory should record which applications are whitelisted, removed, disabled, or configured to use a per-app VPN. Additionally, because of the dependencies of applications and background services, care should be taken when removing applications and the device should be tested fully with the given configuration.

Legal Information