SAMSUNG

Security Configuration Guide Samsung Galaxy Mobile and Tablet Devices

Using Samsung Knox version 3.9+ and Android13.0+

SAMSUNG

Table of contents

Introduction 5

Audience 5

Purpose 5

Evaluation 7

Samsung Knox advice 7

Samsung Knox Platform for Enterprise 7

Samsung Knox Premium licence 13

Samsung Galaxy platform feature summary and risk considerations 13

Knox work profile 13

Knox work profile for BYOD 14

Knox work profile passcode 14

Device passcode 14

Non-native applications inside the Knox work profile 14

Non-native applications outside the Knox work profile 15

Mobile Device Management 15

Mobile Application Management 15

Virtual Private Network 15

Unknown software sources 16

SDP-aware email applications running inside Knox work profile 16

Non-SDP aware email application running inside Knox work profile 16

Email applications running outside Knox work profile 16

Document preview running inside Knox work profile 16

External storage 17

Application control 17
Backups 17
Microsoft Office for Android 17
Mobile device administration 18
Managing mobile device security 18
Purchasing and enrolling devices 20
Secure Device Delivery 20
Secure Updates 22
Operational Security 22
Revoking use, device sanitisation, end of life and device disposal 24
Self-assessment of non-native applications 24
Topics to guide user behaviour 25
Peripherals and other connectivity 25
Recommended device settings 29
Knox work profile settings 29
Non-work profile device settings 34
Audit Records 42
Types of Audit Events 42
Audit Collection Filter Settings 42
Audit Record Fields 43
Audit Events 43
Developer References 43
Cryptographic APIs 43
Bluetooth APIs 44
TLS/HTTPS APIs 44

Certificate Pinning 44

IPsec VPN APIs 44

Glossary of cyber security terms 44

Further information 46

Contact details 46

SAMSUNG

Introduction

This guide has been produced by Samsung Electronics to assist Australian government and industry partners when deploying Samsung Galaxy Mobile and Tablet devices at **OFFICIAL: Sensitive** and **PROTECTED** deployments and the security requirements that need to be met to allow Samsung Galaxy devices to handle Australian government data. This security configuration guide does not replace the ***Australian Government Information Security Manual*** (ISM). However, where a technical conflict arises agencies should asses their risk using both documents.

The current version of the ISM can be found here: https://www.cyber.gov.au/acsc/view-all-content/ism.
The ISM guidance on enterprise mobility covering Mobile Device Management (MDM) and Mobile Device Usage can be located here: *https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-enterprise-mobility*.

Audience

This guide is for Australian Government users and administrators of Samsung Galaxy mobile and Tablet devices procured within the Australian market.

To use this guide, readers should be familiar with basic networking concepts, be an experienced mobile device system administrator and be or have access to an experienced network administrator.

Parts of this guide will make reference to product features that will require the engagement of other software, networking equipment or Mobile Device Management (MDM) vendors. While every effort has been made to ensure content involving any third-party vendor products is correct at the time of writing, organisations should always check with these vendors when planning their system implementation. Note, mention of third-party products is not a specific endorsement of that vendor over another and has been used to illustrate desirable features.

Some security configuration instructions within this guide are complex, and if implemented incorrectly could reduce the security of devices, networks or an organisation's overall security posture. These instructions should only be implemented by experienced systems administrators and should be used in conjunction with thorough testing.

Purpose

This guide provides information for Australian Government organisations on the security of Samsung Galaxy devices sold in Australia, and their risks, which should be considered before they are introduced into an organisation's mobile fleet.

This guide provides a summary of features and associated risks for the Samsung mobile and tablet devices. Throughout this guide, the combinations of devices and software are referred to as the 'Samsung Galaxy platform'.

The advice in this guide has been written for the use of the Samsung Galaxy platform within Australia. Organisations and individuals seeking to use devices overseas should also refer to the ACSC's ***Travelling Overseas with Mobile Devices*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/travelling-overseas-electronic-devices.

Implementing the settings provided in this guide can significantly impact system functionality and user experience. Authorising officers are encouraged to consider the balance of user requirements and security, as not all advice may be appropriate for every user, environment or deployment.

Organisations should seek approval from their authorising officer to allow for the formal acceptance of the risks. Refer to the 'applying a risk-based approach to cyber security' section of the ***Australian Government Information Security Manual*** (ISM) for more information.

Finally, this guide reflects the ISM. Although, not all ISM requirements can be implemented on the Samsung Galaxy platform. In these cases, risk mitigation measures are provided in the *Advice to authorising officers* section.

The Security Configuration Guide contains feature summaries and risk considerations of the Samsung Galaxy platform as listed in Table 1. These devices use Samsung Knox 3.9 or higher and Android13.0 or higher.

Series	4G	5G	Wi-Fi Only	Chipset Vendor	Evaluated under Common Criteria
S23	SM-S911B	SM-S911B	N/A	Qualcomm	Yes
S23+	SM-S916B	SM-S916B	N/A	Qualcomm	Yes
S23 Ultra	SM-S918B	SM-S918B	N/A	Qualcomm	Yes
S22	SM-S901E	SM-S901E	N/A	Qualcomm	Yes
S22+	SM-S906E	SM-S906E	N/A	Qualcomm	Yes
S22 Ultra	SM-S908E	SM-S908E	N/A	Qualcomm	Yes
Tab S8	SM-X706B	SM-X706B	N/A	Qualcomm	Yes
Tab S8 Plus	SM-X806B	SM-X806B	N/A	Qualcomm	Yes
Tab S8 Ultra	SM-X906B	SM-X906B	N/A	Qualcomm	Yes
S21	N/A	SM-G991B	N/A	Samsung	Yes
S21+	N/A	SM-G996B	N/A	Samsung	Yes
S21 Ultra	N/A	SM-G998B	N/A	Samsung	Yes
Z Flip4	SM-F721B	SM-F721B	N/A	Qualcomm	Yes
Z Fold4	SM-F936B	SM-F936B	N/A	Qualcomm	Yes
Xcover6 Pro	SM-G736B	SM-G736B	N/A	Qualcomm	Yes
Tab Active4 Pro	SM-T636B	SM-T636B	N/A	Qualcomm	Yes
Tab Active4 Pro Wi-Fi	N/A	N/A	SM-T630	Qualcomm	Yes
A53 5G	SM-A536E	SM-A536E	N/A	Qualcomm	Yes

Table 1 - Model numbers of the Samsung Galaxy phone, Note, and Tablet models covered in this guide

Evaluation

Since April 2014, ASD has endorsed the ***Mobile Device Fundamentals Protection Profile*** (MDFPP) with specified additional mitigations as a key component in all mobile device evaluations. The MDFPP, as defined by the United States National Information Assurance Partnership (NIAP), outlines the security requirements for a mobile device for use in an enterprise. The following table shows the Security software versions for each device.

MDFPP v3.2	BT v1.0	WLAN v1.0	VPN PP-MOD v2.3	Knox
1	1	2	1.1	3.9

Table 2 - Security Software Versions

The version number is broken into two parts showing the Protection Profile or Extended Package version as well as the software version that is certified. For example, the Galaxy S22 would show "MDF v3.2 Release 1".

This guide provides guidance for consideration by the authorising officer for **OFFICIAL: Sensitive** and **PROTECTED** deployments. The principles in this document will also assist organisations to comply with existing requirements when deploying devices at lower classifications under a risk based model.

More information may be obtained from the NIAP Common Criteria portal at:

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11342

Samsung also has additional security information for their devices at: https://www.samsung.com/au/security.

Samsung Knox advice

Samsung Knox Platform for Enterprise

Extending the security of the native Android operating system, Samsung Knox Platform for Enterprise (KPE) provides additional security features to Samsung Galaxy platform at a hardware and software level.

The Samsung Galaxy platform uses hardware features with Knox to verify the device is not compromised and has not been tampered with. Samsung Galaxy and Tab S8 devices provide additional security through a secure element which further extends the ability of Knox to perform hardware verification and provide secure data storage.

Samsung Galaxy devices with KPE use software to ensure compliance checks, provide encryption, and isolation of applications.

The mobile device is intended for use as part of an enterprise messaging solution providing mobile staff with enterprise connectivity. With a focus on enterprise security, the mobile device also provides support for both IKEv1 and IKEv2 VPN tunnels using both Pre-Shared Keys as well as certificates, providing flexibility based on the environment.

The mobile device combines with an EDM solution to enable the enterprise to watch, control and administer all deployed mobile devices, across multiple service providers as well as facilitate secure communications through a VPN tunnel. This provides a secure mobile environment that can be managed and controlled by the environment and reduce the risks that can be introduced when enabling mobility in the enterprise, whether through a Bring-Your-Own-Device (BYOD) or a Corporate-Owned deployment.

The Samsung Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration of options to over 600 configurable policies and including additional security functionality such as application blacklisting. The ability to set these policies is based on the capabilities of the EDM.

Samsung provide a comprehensive **Knox white paper** detailing the available features:
https://docs.samsungknox.com/admin/whitepaper/kpe/samsung-knox.htm

Further information can be accessed from the ***Samsung Knox Platform for Enterprise (KPE) admin guide***:
https://docs.samsungknox.com/admin/knox-platform-for-enterprise/welcome.htm

MDFPP Evaluated Device Capabilities

Security Feature	Description	ASD Application Note
Device data protection. The mobile device provides security functionality to help protect data at rest	**File-Based Encryption (FBE)**. The mobile device automatically encrypts data on the internal flash media of the device using hardware-backed AES256. Protected Data (**see application note**): This is the default level of protection for every file inside the Knox work profile. Keys are not evicted from memory at Knox work profile lock, they stay in memory until the device is powered off.	This is not to be confused with the *Australian Government Security Classification System (AGSCS)* **PROTECTED** or **OFFICIAL: Sensitive** levels, which are based on the *Protective Security Policy Framework (PSPF).* Please see here for the PSPF: https://www.protectivesecurity.gov.au/ Organisations deploying Samsung Galaxy platforms that handle **PROTECTED** classified information, must ensure it is stored as 'Knox Sensitive Data'. SDP provides sufficient protection for the classified information and is a key requirement supporting the ability to reduce the handling requirements for the device. Applications that specifically opt-in to Knox SDP are authorised to store information classified as **PROTECTED**. When selecting applications to run in the KPE at **PROTECTED**, the organisation must have assurance that all **PROTECTED** information is written to storage encrypted with SDP.
	DualDAR. The Samsung Galaxy platform also provides an optional configuration that provides two independent layers of data encryption when a Knox work profile is enabled. This additional configuration is called DualDAR, and more information is available from the KPE white paper section on DualDAR: https://docs.samsungknox.com/admin/whitepaper/kpe/DualDAR.htm. In this configuration, all data inside the Knox work profile is encrypted once before being provided to the normal device encryption layer. By default, the Knox work profile data is encrypted by a Samsung-provided FIPS 140-2 validated cryptographic module, but a third-party cryptographic module can also be installed and used. The inner layer is encrypted using AES-CBC while the outer layer of encryption uses XTS-AES (all encryption keys are encrypted using AES-GCM). The DualDAR configuration also provides support for clearing all Knox work profile encryption keys based on the locking of the work profile.	
	Removable storage encryption. The mobile device can encrypt all files placed onto, or already residing on, removable storage attached to the device (not all devices support removable media).	
	Sensitive data protection (SDP). The mobile device has the ability to securely store incoming data that is considered sensitive such that it can't be decrypted without the user logging in.	

	Sensitive Data (**see application note**): Applications must specifically mark files as Knox Sensitive Data, or place the files into the Chamber directory which encrypts the contents with SDP. Keys are evicted from memory at Knox work profile lock, and data is only accessible when the Knox work profile is unlocked. Additional information is available from the *Samsung Knox Platform for Enterprise (KPE) admin guide* and a ***Sensitive Data Protection*** whitepaper: https://docs.samsungknox.com/admin/whitepaper/kpe/sensitive-data-protection.htm
Application Management. The device provides a number of security functions to manage device software.	**Application resource restrictions**. All applications are run within a controlled environment that limits applications to only accessing only authorized data and resources.
Access Control. The device can implement access control that reduces mobile user permissions and assists in reducing unauthorized access.	**Device lock.** The mobile device can be configured to lock automatically after a defined period of inactivity (1 to 60 minutes) limiting access to device functions those that are explicitly authorized such as emergency calls.
	Local wipe. The mobile device has the ability to wipe encryption keys/data on a device after a defined number of authentication attempts are surpassed.
	Credential complexity. The mobile device can enforce enterprise password policies forcing users to use a defined level of complexity in device passwords.
	Biometrics Use. The mobile device can provide biometric authentication for access to the device complementary to password policies, restricting access based on failed attempts.
	Privileged access. The mobile device can be configured to restrict mobile user's access to privileged functions such as device configurations.
	Hotspot Control. The mobile device can be configured to act as a hotspot for sharing Internet access to other devices.
	Wireless network settings. The wireless network configuration of the mobile device

	can be specified, providing requirements or pre-loaded networks.
Enterprise device management. Enterprise administrators can control and audit mobile endpoint configurations and wipe device if needed.	**Remote wipe.** An enterprise administrator can send a message to the mobile device to wipe all local storage and the SD card.
	Security policy. The mobile device and VPN can be configured by an EDM solution that supports the Samsung Enterprise SDK.
	Auditing. The mobile device can monitor and generate records related to security-relevant events within the device.
Secure Channel. Enterprise devices can securely connect to the enterprise network.	**VPN.** The mobile device provides a secure communications channel to the VPN Gateway.

Table 3 - Mobile Device Security Features

Cryptography

Part of the Common Criteria-evaluated configuration is the availability of approved cryptographic engines for use by the system and applications. Samsung has chosen to utilize NIST-validated cryptographic algorithms within the cryptographic modules on its devices for the Common Criteria configuration. These algorithms are made available for use by applications installed on the device through the normal Android Framework APIs.

Samsung provides the following cryptographic modules with NIST-validated algorithms on all the evaluated devices:

- Samsung BoringSSL Cryptographic Module
- Samsung Kernel Cryptographic Module
- Samsung SCrypto Cryptographic Module

In addition, the following cryptographic modules with NIST-validated algorithms are available, depending on the CPU:

- Samsung Flash Memory Protector (on devices with Samsung Exynos processors)
- QTI Inline Crypto Engine (on devices with Qualcomm Snapdragon processors)

All modules always run in a FIPS-validated mode. BoringSSL, for compatibility reasons, provides access to non-FIPS algorithms. Developers should not utilize non-FIPS algorithms in a validated configuration (but these are necessary to ensure functionality with many commercial services). Samsung integrates the cryptographic modules directly into Android so they can be accessed by any app using the native Android APIs. The APIs providing access to FIPS-validated algorithms are detailed in the Developer References section. Wi-Fi connections can utilize both FIPS and non-FIPS algorithms for compatibility reasons. To ensure the use of FIPS-validated algorithms in Wi-Fi connections the Wi-Fi Access Point should be configured to specify the proper cipher suites.

Note: It is possible that some applications will implement their own cryptography instead of relying on the modules provided with the device. It is the responsibility of those vendors to validate their own cryptography. Samsung recommends that developers utilize the cryptographic functions provided with the device using the native Android APIs.

Enabling CC Mode

The Samsung devices listed in this document support a Common Criteria (CC) Mode. This CC Mode provides feedback on whether or not the device meets the minimum required configuration according to the MDF requirements.

While there are two methods for enabling CC Mode on a device, only the EDM-managed method will be explained here.

NOTE: The CC Mode app is for testing and not intended as a deployment tool.

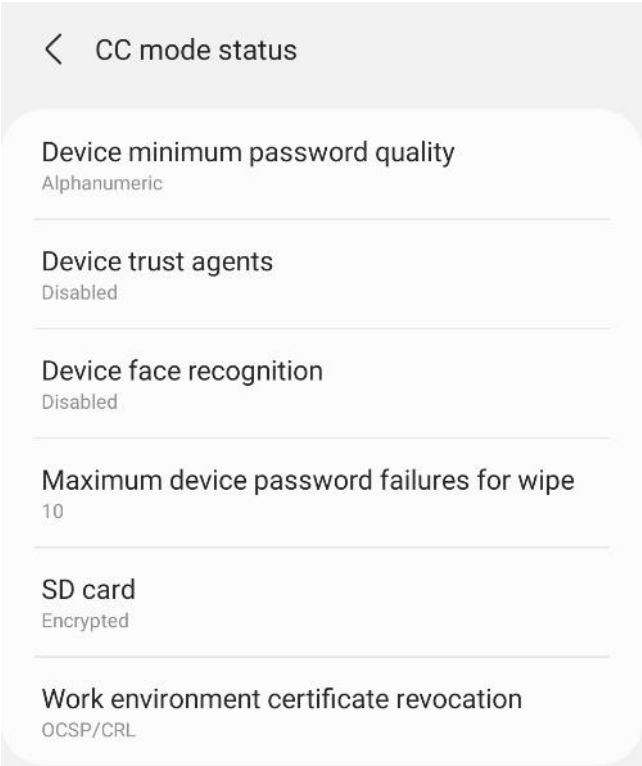
CC Mode Status

CC Mode has two possible states:

Status	Description
Enabled	CC Mode has been turned on
Disabled	CC Mode has been turned on but an integrity check or self-test has failed (such as a FIPS 140-2 self-test)

Table 4 – CC Mode Status

The status of the CC Mode check is entered into the audit log through a series of entries about each of the conditions necessary for CC Mode. The CC Mode status can be seen by a user in ***Settings/About phone/Software Security Version*** under ***CC mode status***. This will only appear when CC Mode has been enabled on the device. Tapping on the status will show the current settings related to meeting the evaluated configuration, the same settings recorded in the audit log.



The following settings are listed:

Setting	Possible Values	Description
Device minimum password quality	Unspecified Something Numeric Numeric Complex Alphabetic Alphanumeric Complex Biometric	The specified level of the password requirements (recommended minimum is alphanumeric)
Device trust agents	Enabled/Disabled	Status of Smart Lock function
Device face recognition	Enabled/Disabled	Status of face biometric
Maximum device password failures for wipe	30 or less	The number of failed authentication attempts before the device will be wiped
SDCard Encryption	Encrypted/Decrypted	Status of whether SD Card encryption is set
Work environment certificate revocation	None/CRL/OCSP	None = no revocation checking CRL = CRL checking enabled OCSP/CRL = OCSP as primary and CRL as secondary is enabled Work environment – this means that the setting is applied to the work profile

Table 5 - CC mode status Page

Note: It is unlikely a user will see the Disabled state as the failures necessary to meet this condition are such that the device is unlikely to boot.

Common Criteria Minimal Configuration

To configure the device into the minimal evaluated configuration, all settings marked as Always and Mandatory must be set. Once these have been set, the device configuration can be verified by reviewing the audit records from the device boot.

The optional configuration settings can be used to meet the deployment needs of the organization. These settings have been covered in the evaluation, but the specific settings of those items does not affect the evaluated configuration.

The following settings must be configured via the EDM after CC Mode has been enabled:

- Set Password Quality
- Enable the Maximum Password Failure Wipe Policy
- Disable Smart Lock
- Enable SD Card Encryption

NOTE: SD Card encryption is only needed on devices that support inserting removable media.

- Enable Revocation Checking

NOTE: The administrator can choose either CRL or OCSP revocation checking.

If biometrics are enabled, the following setting must be configured:

- Disable Face Lock

To ensure overall control of the Common Criteria configuration, CC Mode cannot be disabled by an end user except by performing a factory reset. It is possible to change the CC Mode status through the EDM.

Application Isolation

Applications and associated data can be securely isolated using the ***Android Enterprise work profile***:

https://docs.samsungknox.com/admin/whitepaper/kpe/sensitive-data-protection.htm

The Android Enterprise work profile creates a secure container on the device using platform-level separation of work apps and data. When applications are running inside the work profile, they have a level of separation from the base device. Applications running inside the Android Enterprise work profile are separate instances to ones outside of the work profile.

KPE also has a file system inside the work profile called '*Chamber*', which marks all files with SDP stored within the directory. SDP offers stronger security when compared to the default Samsung Protected Data encryption. Further details are available from the ***Chamber*** section in the Samsung admin guide:

https://docs.samsungknox.com/admin/whitepaper/kpe/sensitive-data-protection.htm

KPE also offers another application isolation technology - Knox Separated Apps. Separated Apps is focused solely on providing a highly segmented application group with no ability to share anything across the group boundary. Instead of a full environment (as in a work profile), Knox Separated Apps provides the administrator with the ability to allow or block apps from being placed into the application group, and only these apps will be available. Knox Separated Apps does not require any separate authentication, providing seamless access to the isolated apps to the end user.

Background Network Communications

Samsung Android devices are usually configured by default to send anonymous usage data (including location, device ID etc.) to Google and Samsung servers. This can be disabled through device settings and will need to be enforced through procedural controls.

Samsung Android devices do not need to be associated with a Google account to operate as required within the enterprise. For example, it is still possible to receive push notifications through Google Cloud Messaging. Knox EDM APIs can be used to prevent users from signing in to these services.

Samsung Knox Premium licence

In order to securely configure the Samsung Galaxy platform, organisations will be required to purchase a KPE Premium licence from a Samsung Knox reseller. Once obtained, the KPE Premium licence must be input into an MDM, which will enable Knox functionality. More information can be found at ***Knox License Keys*** area of the Samsung website:

https://docs.samsungknox.com/admin/fundamentals/license-knox-products.htm

Samsung Galaxy platform feature summary and risk considerations

Knox work profile

The Knox work profile can provide suitable encryption and key management. Users must be trained in how to store information inside the *Chamber* appropriately, data stored outside the *Chamber* or without SDP does not have the suitable key management or encryption required to handle Australian government data.

When using applications inside the Knox work profile, organisations should assess the Android Package capabilities against the Knox SDK to ensure that required functionality is supported by the application.

In order to downgrade the handling requirements of Samsung Galaxy platform containing Australian government data, the Knox work profile must be locked. Set the Knox work profile lock to the device lock screen in order to appropriately clear ephemeral[1] keys from device memory.

[1] Ephemeral keys are implemented on the device to ensure data is encrypted at all times.

Knox work profile for BYOD

Depending upon approval of authorising officer of an organisation, user may be allowed to use a personal device for work called BYOD scenario. ACSC provides guidance that organisations will need to consider when allowing BYOD access into the enterprise system (https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/remote-working-and-secure-mobility/secure-mobility/bring-your-own-device-executives).

To Support BYOD scenario a personal device is equipped with an MDM agent that creates a work profile where work-specific apps/data are subject to security policies. On Samsung Galaxy Android devices, the work profile is managed by a Profile Owner (PO) that can apply configurations to the Work Profile only, with the exception of very few policies that can be applied to the device. The non-work profile (personal profile) is almost free from any restrictions. This implies that certain features such as disabling Bluetooth/Wi-Fi sharing are not present as this would inhibit the personal side of the device as well respecting the user's privacy. The lack of some restrictions shall be covered with necessary user guidance based mitigations to minimise the risk.

Knox work profile passcode

The security of the Knox work profile is limited by the strength of the Samsung Galaxy platform and Knox work profile passcodes. If these passcodes can be guessed or brute-forced, all information stored on the device could be viewed or modified.

The use of biometrics to protect Australian government data is an organisation risk decision for **OFFICIAL: Sensitive** deployments, however, must not be used when the device handles **PROTECTED** data.

It is recommended that a unique password or passphrase should be used to unlock both the Samsung Galaxy handset and Knox work profile. Personal Identification Number (PIN) codes, pattern/swipe codes and built-in biometric sensors should not be used. Deployments of Samsung Galaxy platform using biometrics should consider the practicality and privacy of users, and tailor advice surrounding these features to best suit the deployment scenario. Authorising officers should seek ASD guidance where a tangible practical demand for biometrics is identified.

The organisation should set and enforce policies in accordance with the ISM. Additional information can be found under the **Single-factor authentication** topic in the ISM: https://www.cyber.gov.au/acsc/view-all-content/guidance/authentication-hardening

Device passcode

The security of the device is limited by the strength of the device passcode. If this passcode can be guessed or brute-forced, all information stored on the device could be decrypted.

It is recommended that a unique password or passphrase be used to unlock the device. PIN codes, pattern/swipe codes and built-in biometric sensors should not be used. The use of biometrics to protect Australian government data is an organisation risk decision for **OFFICIAL: Sensitive** deployments. Biometrics must not be used when the device handles **PROTECTED** data.

The organisation should set and enforce policies in accordance with the ISM. Additional information can be found under the **Single-factor authentication** topic in the ISM.

Non-native applications inside the Knox work profile

Applications that do not handle Australian government data appropriately or afford a suitable level of encryption are at risk of disclosing or mishandling Australian government data.

Native applications are applications that come pre-installed on the device. Non-native applications can be third-party or applications developed in-house within an organisation.

In approving an application for use within KPE, organisations should conduct a rigorous assessment of that application. This should include determining whether Australian government data is appropriately handled within the Knox work profile and *Chamber*, such that SDP is appropriately applied in line with ASD guidance.

Not allowing applications other than approved applications prevents compromise of Australian government information stored inside the Knox work profile. Applications should be assessed in detail before being allowed to run inside a Knox work profile that contains Australian government information. Applications should not be installed inside the Knox work profile without a genuine need for access to Australian government information.

Additional information can be found under the **Application hardening** section of the ISM: https://www.cyber.gov.au/acsc/view-all-content/guidance/application-hardening

Non-native applications outside the Knox work profile

Android applications may contain functionality that contravenes an organisation's policy. Functionality may be hidden and able to be remotely updated causing impacts to user privacy, experience and security. The Android security model does not provide sufficiently granular control of applications to provide assurance that an application is trusted and unmodified.

The Knox work profile provides appropriate protections, when configured in accordance with this guide, to defend against applications from outside the Know work profile. While it is possible to install non-native applications outside of the Knox work profile this can inadvertently introduce additional risks.

For **PROTECTED** deployments, where the authorising officer has accepted use of non-native applications outside of the Knox work profile, the application must never handle **PROTECTED** data or interact with applications within the Knox work profile.

It is recommended that non-native applications are not installed on devices handling **PROTECTED** data and in cases where the application has not been approved by the organisations authorising officer.

Additional information can be found under the **Application hardening** section of the ISM: https://www.cyber.gov.au/acsc/view-all-content/guidance/application-hardening

Mobile Device Management

Without an MDM, devices may not always comply with an organisation's approved configuration and/or audit requirements.

MDM solutions are important configuration and deployment tools for mobile devices, providing security features, management and logging functionality. Devices that handle Australian government data, whether BYOD or provided by the organisation, must enrol in an MDM that is configured in line with ASD guidance and allow the MDM to be a device administrator.

A core functionality of an MDM is the ability to remotely disable and/or wipe lost or stolen devices, and perform fleet-wide compliance checks against required controls.

Organisations operating in higher risk situations are encouraged to engage with ASD when developing and implementing their MDM solution.

Additional information can be found under the **Mobile Device Management** topic in the ISM: https://www.cyber.gov.au/acsc/view-all-content/guidance/mobile-device-management

Mobile Application Management

Using Mobile Application Management (MAM) allows an organisation to vet and deploy applications without needing to enable high risk installation processes such as by unknown sources and public app stores. MAM also provides a platform for organisations to deploy application updates without requiring access to public app stores.

MAM servers (usually as part of an MDM solution) are important tools for deploying privately developed applications to devices.

If organisations have permitted non-native applications on a **PROTECTED** device a MAM is required however, deployments without non-native applications do not require a MAM.

Additional information can be found under the **Mobile Device Management** topic in the ISM: https://www.cyber.gov.au/acsc/view-all-content/guidance/mobile-device-management

Virtual Private Network

A Virtual Private Network (VPN) can provide data-in-transit protection between organisations devices and a trusted gateway.

Samsung Galaxy platform implementation of VPN permits some data to transit outside of the VPN. ASD has observed some plain-text (unencrypted) device identifying information outside of the VPN, even in an Always On configuration. This may introduce additional risk is some deployment scenarios.

All data communications for the Samsung Galaxy platform handling Australian government data must be through the Always On IKEv2 VPN. The Samsung Galaxy platform offers two types of VPN client – OpenVPN (which must be downloaded) and strongSwan (which is the built-in IKEv2 client). The strongSwan client is enforced via the kernel and therefore offers a stronger security claim for the VPN tunnel.

Addition information can be found under the **Connecting mobile devices to the internet** topic in the ISM.

Unknown software sources

Samsung Galaxy platform deployments that allow unknown sources have less control over the applications that are present this introduces additional risk to the platform.

The use of a MDM and/or a MAM can allow the controlled installation of privately developed applications without the requirement to enable unknown sources.

Refer to the ***Self-assessment of non-native applications*** *section in this guide*, in addition, refer to the ISM sections **Application hardening**, and **Mobile device management**.

SDP-aware email applications running inside Knox work profile

SDP aware email applications can offer appropriate protections for the encryption and handling of Australian government information up to **PROTECTED**. Mail client applications should be considered on a case-by-case basis.

If an email client does not support the application of protective markings to emails, organisations should consider configuring email servers to allow for manual protective marking of emails by users. Organisations should consider whether to allow attachments to or from the Samsung Galaxy platform devices based upon the risks surrounding the storage and handling of Australian government data on the devices.

For SDP-aware email applications that run inside a Knox work profile, such as the Samsung Mail Client, email headers may not be handled in accordance with protective markings or appropriate encryption. Email clients may not apply protective markings appropriately introducing the risk that users may store them without appropriate protections. Due to performance considerations, some email clients encrypt header information with the Samsung Protected Data mechanism; as opposed to the Knox SDP.

Organisations should carefully consider the risks associated with the header information, and any potential impact this would have on Australian government information.

Authorising officers should be aware that the handling of attachments on mobile devices introduces risk. Risk includes aggregation and the potential loss of control of the information, similar in risk to when Australian Government data is printed in hardcopy.

Organisations must deliver a high level of user training to ensure that users understand that any attachments moved outside of the application must be stored inside the *Chamber* directory, as the files are not encrypted by SDP when stored in other locations.

Additional information can be found under the **Email usage** section in the ISM.

Non-SDP aware email application running inside Knox work profile

The use of non-SDP aware email applications introduces a high degree of risk for Australian government data due to the lack of appropriate encryption.

Therefore, it is not recommended for **OFFICIAL: Sensitive** deployments and not permitted for **PROTECTED** deployments.

Email applications running outside Knox work profile

The use of email applications running outside of the Knox work profile introduces a high degree of risk for Australian government information.

Email clients that run outside of Knox lack suitable encryption and key management attributes for attachments that may be moved outside of the application.

Additional information can be found under the **Email usage** section in the ISM.

Document preview running inside Knox work profile

Australian government data may be stored inappropriately after files are opened in a document preview application.

Viewing documents opens the file outside of the parent application, for example, outside the file explorer or email client. There are no guarantees of correct file handling, classification markings and encryption if these document preview applications are used to save or edit files. While open, the Knox model still protects the file in memory; however, there is considerable risk associated with saving or editing Australian government data using document preview applications.

If organisations allow the use of document preview applications for Australian government data, user training should be provided to reduce the risk of inappropriate storage. Educating users in how to save files to *Chamber* where they are appropriately encrypted with SDP would assist in reducing this risk.

External storage

Any data stored or accessed on external or adoptable media will not be encrypted with SDP, and therefore such external storage media are not suitable for Australian government data. External media such as microSD cards should be treated the same as external media, such as unapproved Universal Serial Bus (USB) storage, in a traditional desktop computing environment.

Application control

Applications are only compared against a list of approved applications at installation time. Therefore, applications could be modified for malicious purposes after the list of approved applications has been checked.

With Android, a list of approved applications is defined via an MDM and enforces control of the installation of these applications. Current Android versions control applications via package name or developer certificate, with most common MDMs offering package name only control of applications. Knox has a capability to whitelist or blacklist applications through Mobile Application Management (MAM).

It should be noted that application control via developer certificate allows all applications signed with an approved developer's certificate to be installed.

For most MDM solutions, Android application control first requires a list of unapproved applications to be explicitly configured to prevent the installation of all applications. Approved applications can subsequently be allowed on an exception basis.

Additional information can be found under the **Application hardening** and **Mobile Device Management** sections of the ISM.

Backups

Without regular backups, Australian government data may be irrecoverable should only a local copy of the data exist and become inaccessible. However, with unapproved backup solutions, Australian government data may be extracted and then stored on, or transit over, systems that are not suitable for the sensitivity or classification of the data.

Daily backups are recommended for all Australian government data that is only held on the device. Currently there is not an Android or Samsung implementation of automated backup from within the Knox work profile. A backup process would need to be manual or enabled by a non-native application.

If data of organisational value is being created on devices, careful application selection or development can negate the need for organisational data to require backup explicitly from devices, because it is synchronised to servers implicitly (such as using a Content Management System that has a client with a File Sharing Extension).

Additional information can be found under the **Data backup and restoration** section in the ISM.

Microsoft Office for Android

Android devices do not currently run Microsoft Office macros and therefore many of the risks associated with handling Office documents are not relevant at this time. As this is a feature of a third-party vendor, continual monitoring of this risk will need to be undertaken. The ability for Office for Android to expose the enterprise to macros should also be considered when implementing mail gateway architectures Additionally, users will require training in saving and marking files appropriately for the *Chamber* in order to make use of the appropriate encryption for Australian government data, as provided by SDP.

Organisations looking to implement Microsoft Office for Android should refer to the **Application hardening** section of the ISM, and are encouraged to contact ASD to assess risks and deployment scenarios.

SAMSUNG

Mobile device administration

Managing mobile device security

MDM and MAM solutions are an integral part of implementing any smartphone solution for an organisation. Any mobile device that handles classified Australian government data will require an appropriate MDM and MAM solution to satisfy the security requirements outlined in this guide and the ISM. MDM and MAM solutions should be hosted by an organisation inside their trusted network (known as an On-Premise MDM solution) as opposed to a cloud solution being implemented. An organisation's authorising officer, system manager and risk owner should work together to select the best MDM and MAM solution for the organisation's implementation, while giving careful consideration to the functionality of the solution and its ability to meet the requirements outlined in this guide and the ISM. Samsung publishes a list of MDM vendors that integrate with the Samsung Galaxy platform, and the features that each MDM is compatible with.

In order to deploy core Samsung security features, such as the Knox work profile, organisations will require a KPE Premium key. This key is distributed to Samsung Galaxy platform devices via an MDM, and allows an organisation to access and implement the Samsung security features outlined in this guide. Samsung publish a list of resellers for the KPE premium key on their website.

Deployment Environment

The enterprise environment must provide all of the services required to operate and manage devices. The basic components of this model include:

Component	Description
Enterprise/Mobile Device Management (EDM) Solution	The EDM Solution secures, monitors, manages and supports mobile devices deployed across the organization. Controlling and protecting the data and configuration settings for all mobile devices in the network reduces security risks. As part of the EDM solution, an app (usually called an Agent) is installed onto the mobile device. This Agent implements the policies from the EDM and can communicate back to the server, sending status information and logs for review.
Secure Tunnel Termination	A secure VPN tunnel should be initialized between the managed Android devices and the Enterprise Environment to prevent unauthorized access to enterprise resources. The connection should be based on certificates deployed on the Android user devices. Ideally, mutual authentication is deployed, meaning that both the Android user devices authenticate themselves with a certificate but also the gateway to the enterprise environment. Mutual authentication serves to prevent Android user devices to login into an unauthorized enterprise network and on the other hand prevents the unauthorized login of untrusted devices into the enterprise environment. For services that do not require a VPN, TLS should always be used to encrypt access to the site. Similar to the VPN, mutual authentication between the client and server is recommended. Note that EDM access between the device and server does not need to be through a VPN but is expected to have its own secure channel for communications.
Directory Services	The directory services should be set up to store, organize and provide access to information in a directory.

Business Applications	Business applications allow enterprise users to fulfill or access certain business tasks pertinent to requirements. This may include management tools, accounting utilities and contact management software/solutions.
Certificate Services	Certificate services must be implemented to manage all certificate needs throughout the enterprise environment. This includes issuing new Android device user certificates that are needed to facilitate secure communications through a VPN or TLS connection. It is possible that the certificate services could be provided by a third party instead of a stand-alone internal service for the organization.

Table 6 – Enterprise Deployment Component Services

Figure 1 shows an example of a high-level design of an enterprise-based environment.

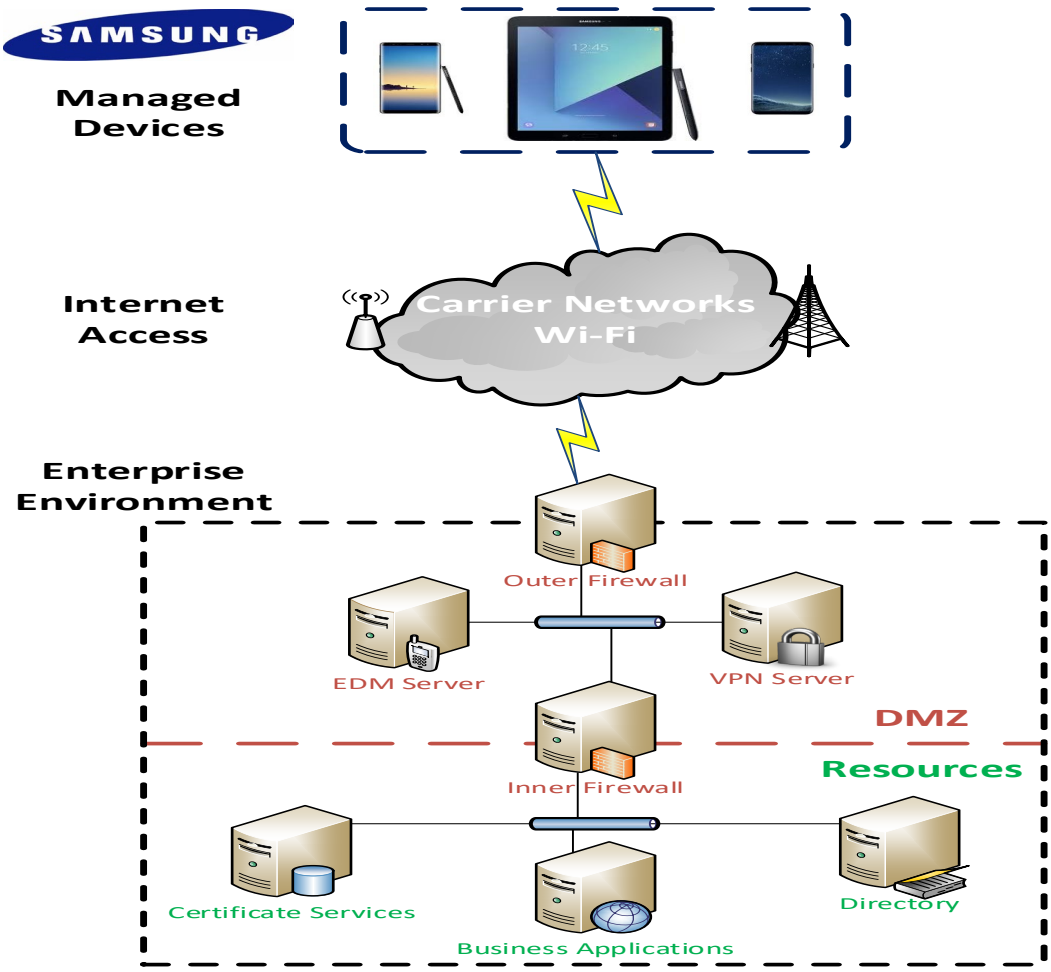


Figure 1 - Example Enterprise Architecture

Purchasing and enrolling devices

It is important that organisations purchase mobile devices within Australia, and only allow BYOD devices that were purchased within Australia. Devices from other regions and/or with different model numbers have hardware, firmware and software differences. These differences mean that the advice in this guide may not be directly applicable, and may present risks not considered in this guide.

It is recommended to avoid purchasing second hand mobile devices for enrolment in enterprise deployments. Purchasing new will reduce the risk of obtaining a device which fails attestation.

Do not attempt to enrol devices which have been 'rooted', this including BYOD deployment scenarios. Rooting allows complete access to the underlying Android Operating System and removes important security controls.

Each MDM solution has its own way of enrolling devices. The default for Samsung Galaxy platform devices, is the MDM client application is installed and configured with the Knox Enrolment solution for a seamless experience. This will enrol the device into the MDM and associate the device with a user. Depending on the usage scenario, Samsung can provide additional services for automated enrolment. It is recommended that this enrolment process is undertaken before the devices are provided to an end user, or in the case of BYODs, that enrolment is verified before the device is allowed to handle Australian government data. Devices should be enrolled into the MDM from within an organisation's trusted network. Once enrolled, the device will undergo self-attestation and make changes in accordance with the organisation's policies and settings pushed via the MDM, with any non-compliant devices reported through the MDM Administrator Console.

Secure Device Delivery

While a Samsung device requires initial configuration before it can be added to the enterprise environment, it is also critical to ensure that the device is received prior to configuration in a secure manner, free from tampering or modification.

It is very important that the devices to be deployed into the enterprise are obtained from reputable carriers to reduce the likelihood that tampering of devices may occur.

Upon receipt, the boxes containing the device should have both a tracking label and two labels placed at either end of the box to indicate whether the box has been opened prior to delivery. If these seals are broken, do not accept the device and return it to your supplier.

The tracking label should look similar to Figure 2 - Tracking Label, while the two tamper labels should appear similar to Figure 3 - Security Seal (Black) or Figure 4 - Security Seal (White).

Figure 2 - Tracking Label

Figure 3 - Security Seal (Black)

Figure 4 - Security Seal (White)

MDFPP Evaluation Version

There are a number of components determining the device that is being used and the components on that device (such as the operating system version, the build version, etc.). These are all contained under Settings/About device. The following are version information that can be found:

- ***Model number*** – this is the hardware model
- ***Android version*** – this is the Android OS version
- ***Build number*** – this is the specific binary image version for the device
- ***Security Software Version*** – this shows the Common Criteria evaluations and the version of the software components related to those evaluations on the device

For the Common Criteria evaluation version information see Table 2 - Security Software Versions

Pre-packaged Software Versions

Samsung Android devices come with large amounts of software apps to provide the full breadth of functionality expected by the customer. Some of the apps come from Google, some from Samsung, and others from the cellular carrier.

Software Versions on Device

To verify the versions of any software on the device (compared to the list from the website), open ***Settings/Application manager***. Under the heading ***All***, you will see every application on the device (both those that are pre-installed and any you have installed). Selecting an application will display its properties. The version number is shown at the top under the name.

Note: Using adb (USB debugging must be enabled to use adb) it is possible to extract all package version information at once.

Secure Updates

Once a device has been deployed, it may be desirable to accept updates to the software on the device to take advantage of the latest and greatest features of Samsung Android. Updates are provided for devices as determined by Samsung and the carriers based on many factors.

When updates are made available, they are signed by Samsung with a private key that is unique to the device/carrier combination (i.e. a Galaxy S22 on Telstra will not have an update signed with the same key as a Galaxy S22 on Optus). The public key is embedded in the bootloader image, and is used to verify the integrity and validity of the update package.

When updates are made available for a specific device (they are generally rolled out in phases across a carrier network), the user will be prompted to download and install the update (see the User Guide for more information about checking for, downloading and installing the update). The update package is checked automatically for integrity and validity by the software on the device. If the check fails, the user is informed that there were errors in the update and the update will not be installed.

Allowed Update Methods

When CC Mode is enabled, only FOTA updates can be installed on the device. Other methods for installing updates (such as Recovery Mode or Samsung KIES) are blocked and cannot be used to update the firmware. This provides insurance against local, physical attacks that could change the software unknowingly.

Blocking Updates

It is possible to block FOTA updates on a device by setting **allowOTAUpgrade** to be false via the EDM. This can be used either to freeze the software installed or to allow an organization time to test the update before letting it roll out to the user community.

Operational Security

Modes of Operation

The mobile device can be operated in four different modes, depending on the role of the user accessing the device:

- Administrator mode;
- User mode;
- Error mode; and
- Recovery mode

A device is considered to be in Administrator mode before it is delivered to the user. The device is prepared and configured for deployment in the enterprise environment via the Samsung Enterprise SDK. The mobile device administrators are trusted to follow and apply all administrator guidance in a trusted manner. An unprivileged user will not have access to this mode of operation.

If an error or operational failure occurs during the transition from Administrator mode (causing the device to enter the Error mode of operation) to User mode, the administrator should follow the guidance for the EDM in case of the failure and restore the device to normal operational abilities. If it is not possible to adequately eliminate the error or operational failure, the device is not to be delivered to an end user and should be returned to the supplier.

After the device is configured in accordance with the Common Criteria evaluated settings, the device is ready for deployment to a user. When the user receives the device, only the TouchWiz user interface will be visible and no further changes to the security configuration are possible. Once deployed to a user, the device will be operating in User Mode. Within User Mode, the only security relevant functions accessible for the user are 'lock screen password protection', 'change of password' and 'local device wipe'. Typically, an administrator will not access the device in this mode of operation.

The mobile device may also be placed into Recovery mode, bypassing the standard boot process and allowing configuration changes to be made to the installation of Android. However, since this requires the boot loader for the device to be unlocked and is therefore considered out of scope for this environment.

Wiping Data

The evaluated security configurations provide the ability to both locally or remotely wipe data work profile level or both.

An enterprise initiated remote wipe command (for either the device or just the work profile, depending on the configuration) occurs under the following conditions:

- The enterprise sends a remote wipe command to the device:
    - when the device has been lost or stolen;
    - in response to a reported incident;
    - in an effort to resolve current mobile issues; and
    - for other procedural reasons such as when an Android device end user leaves the organization.

Wiping the Device

The evaluated security configuration provides for a local and a remote wiping process of Android user devices. This type of wipe works at the storage level and will wipe all data on the device. In a work profile configuration, this will wipe all data including the work profile (as well as everything not in the work profile). This type of wipe is available in all configurations.

The local wipe is manually initiated by the Android device user or after an exceeded number of incorrect login attempts. The remote wipe process is in general remotely initiated by the Enterprise Device Administrator via a remote wipe command.

Wiping the Work Profile

When a Work Profile has been created, it is also possible to wipe only the data stored in the work profile. A wipe of the work profile data will remove the work profile, including apps and data, but it will not remove anything outside the work profile. This process must be initiated remotely by the Enterprise Device Administrator via a remote wipe work profile command.

The only way for a user to wipe the work profile is to un-enrol the device from the control of the EDM. When this is done the work profile, all data and apps as well as the EDM Agent will all be removed from the device.

Additional Notes on Operational Security

Common Criteria Part 3 does require operational user guidance for the following:

- User-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
- Secure usage of available interfaces.
- Security parameters of interfaces and functions under the control of the user and their secure values.
- Each type of security-relevant event relative to the user-accessible functions.

Administrators and users are considered to use a Samsung Enterprise device. As described in previous sections of this document, the administrator is responsible for configuration and installation of the device. The end user receives the device in an operational state where

no further security configuration is possible. The only user accessible user functions are 'lock screen password protection', 'change of password' and 'local device wipe'.

The user is responsible to obey the provided user guidance and to not actively working against the protection of the device data.

The mobile device Administrators are trusted to follow and apply all administrator guidance, including the EDM guidance in a trusted manner.

Revoking use, device sanitisation, end of life and device disposal

An organisation may wish to consider the following to aid the development of processes and procedures when devices are to be re-issued, at end of life and are to be disposed of, or cease to be used by an individual.

Australian government data

Multiple steps are required when organisation owned devices are either re-issued or are at the end of life and are to be disposed. When Australian government data has been stored on the device in accordance with the settings specified in the device summary of this guide, for its entire life removing or un-enrolling from the MDM will result in the associated Knox work profile automatically being destroyed and the data deleted. A factory reset is still required to ensure all Australian government information is removed as per the ISM.

Australian government access

Credentials must be revoked from both the handset and the organisation's remote infrastructure such as VPN server infrastructure. Should a user be reinstated, new credentials must be generated.

All remaining UNOFFICIAL data and accesses

When devices are at the end of life and are to be disposed of a factory data reset is required. **UNOFFICIAL** data, including personal data, contacts and accesses, may be removed before a reset. Additional utilities may aid in further sanitisation of the device, at the organisation's discretion.

Self-assessment of non-native applications

An organisation may wish to consider the following non-exhaustive list of issues to aid in a self-assessment of non-native applications:

- Trusted developer: A developer with a history of producing quality and widely used applications is less likely to have malicious components in their applications that would impact the security of the data that the application handles.
- Trusted source: Large reputable application stores, are more likely to host unmodified applications without bloatware or malware. Where possible, applications should be sourced directly from the trusted developer.
- Application signed correctly: Applications should be verified to be signed by the trusted developer to ensure that they are unmodified and do not contain additional software packages or components that may be malicious.
- Review code and libraries: Applications may be developed specifically for an organisation's use or are uncommon or bespoke. Organisations should review the software libraries contained in the application to ensure that they are up-to-date and do not contain known vulnerabilities. Commercially available tools can be used to determine the software libraries used by Android applications.
- Distribute applications via Mobile Application Manager (MAM): Applications should be deployed via a MAM. This is typically a component of a Mobile Device Manager (MDM). This allows system managers to ensure that the chosen version of the chosen application, that has undergone organisation assessment, is being deployed on devices.
- Any self-assessment should carefully consider the features and function of the application under review. An application should only have the minimal set of features required for it to perform its intended function.
- Applications that contain integration into file-sharing, cloud and social media platforms should be carefully considered and fully understood in terms of how they handle Australian government information.
- Review application updates and changes before pushing the updated application to an MDM: While ASD advice is to update to the most recent version of an application, system managers should conduct the above checks on updated applications before deploying them to the organisation's fleet of devices.

Topics to guide user behaviour

.

Peripherals and other connectivity

Android Debug Bridge, USB debugging and developer mode

Android devices can allow some low-level access to a device, such as via Android Debug Bridge (ADB), USB debugging or Android's developer mode. To reduce the attack surface presented by the Samsung Galaxy platform, these in-built functionalities should be disabled for maximum security. This may not be available in all MDMs.

Samsung specific Wi-Fi features

As these features have not been assessed, any Samsung or Android features that enable sharing media, data or device information should not be allowed, due to the unmitigated security risks.

VPN Client Settings

The device also includes an evaluated VPN client. There are two ways to configure the built-in VPN client, depending on the needs of the organization, via the Standard APIs or via the Knox Generic VPN APIs.

The Standard APIs provide a basic set of functionality for a VPN client that is configured for the entire device (all traffic would pass through this VPN profile).

The Knox Generic VPN APIs provide a highly flexible method for configuring VPNs that can include the ability to control access to applications or groups of applications to specific tunnels. The Knox VPN framework can be used to control tunnels both inside and outside the work profile, depending on where the VPN client is installed (inside or outside the work profile). The Knox VPN framework can be used with the built-in Samsung VPN client or with third-party VPN client vendors, depending on the needs of the organization.

The settings for configuring a VPN client profile can be found in Knox work profile VPN, and Non-work profile (device wide) VPN sections of this document.

VPN Profile Settings (All)

Valid Certificate Types for IKEv1

The IPsec Xauth RSA setting only accepts RSA certificates for the tunnel. As long as the certificates are valid (not expired, properly formatted, etc.) they can be used for the VPN configuration.

Note: It is possible to specify an ECDSA certificate that has been loaded into the system, but it cannot be used to establish a connection to the gateway using IKEv1.

Valid Certificate Types for IKEv2

While the menu selection for the type of tunnel states IPsec IKEv2 RSA it is possible to utilize both RSA and ECDSA certificates for the tunnel. As long as the certificates are valid (not expired, properly formatted, etc.) they can be used for the VPN configuration.

Specifying a Strong Pre-Shared Key

A PSK (Pre-shared key) is like a password, a fixed string used to authenticate the VPN client to the VPN gateway. Since the PSK does not change (or at least does not change often), a strong string should be selected to protect against unauthorized access to the VPN by unknown clients.

The PSK can be entered in two forms: ASCII or HEX. All ASCII characters are supported. HEX keys must start with "0x" as the first two characters entered. If those are the first two characters, the remaining entry will be read as a HEX key. The maximum key size is 64 characters entered.

The PSK will be provided by the organization for entry (since this is something that must match the value on the VPN Gateway). The PSK is recommended to be at least 22 characters long and if not HEX, a mix of letters numbers and symbols.

VPN Profile Settings (Standard APIs)

Server Certificate for the Gateway

It is possible to specify a Server Certificate for the Gateway in the configuration of a VPN tunnel. This certificate will override any certificate provided by the Gateway during the negotiation of the tunnel.

This certificate may be loaded through the UI or EDM. See the device User manual for more information about loading certificates manually.

Knox VPN Profile Settings (Knox Generic APIs)

Configuring the VPN via Knox Generic VPN APIs has the benefit of allowing per-app routing to the VPN client. For example, all container packages can be forced to go through one tunnel, while personal applications are routed through another, or not at all.

The Knox VPN framework can be used with the built-in Samsung VPN client or with third-party VPN client vendors, depending on the needs of the organization.

To use the Knox VPN framework, the following is needed:

Setting	Value	Description
VPN Installer(s)	APKs from vendor	Installation package(s) from the VPN client vendor for installation on the device. Generally (though not always) this would include 2 files.
VPN profile(s)	JSON files	The VPN profile(s) to be deployed on the device
"vpn" folder	JSON files and vendor.ini	The full set of configurations (including Knox configuration) needed for deployment of the VPN profile

Table 7 – Knox VPN Framework Components

The VPN client vendor would provide the files above though the JSON configuration would have to be edited by the Administrator. More information about the JSON configuration can be found here: https://docs.samsungknox.com/dev/knox-sdk/VPN-json.htm.

Samsung VPN Client Configuration for Knox VPN Profile

Using Knox Generic APIs requires installation of the Samsung Proxy APK on the device, which translates configuration received through these APIs onto the underlying Samsung VPN client. The use of other Proxy APKs could be used to support non-Samsung VPN clients (that is not covered here).

Note: Using the Samsung VPN APK will configure the Knox VPN Profile to point to the evaluated VPN client.

Provided the profile configuration string has been created as per the next section, the API flow for creating and starting a VPN connection will be createVpnProfile() -> addPackagesToVpn() -> activateVpnProfile() API.

The API flow for removing a VPN profile will be activateVpnProfile() (De-activate it) -> removeVpnProfile() API.

Note: When adding packages to a VPN profile, use User0 for the whole device and User10 or User100 (depending on the device) for the work profile.

JSON Configuration String

This is an example JSON file for the Knox VPN Client Profile.

```
{
  "KNOX_VPN_PARAMETERS": {
    "profile_attribute": {
      "profileName": "ss1",
      "host": "",
      "isUserAuthEnabled": true,
      "vpn_type": "ipsec",
      "vpn_route_type": 1
    },
    "knox": {
      "connectionType": "keepon",
      "chaining_enabled": "-1",
      "uidpid_search_enabled": "0"
    },
    "vendor": {
      "basic": {
        "autoretry": "1",
        "username": "sampleu",
        "password": "samplepw",
        "authentication_type": "type",
        "host": "111.111.111.111"
      },
      "ipsec_xauth_psk": {
        "identifier": "test@sta.com",
        "pre_shared_key": "example",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ]
      },
      "ipsec_xauth_rsa": {
        "user_cert_alias": "",
        "ca_cert_alias": "",
        "server_cert_alias": "",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ]
      },
      "ipsec_ike2_psk": {
        "identifier": "test@sta.com",
        "pre_shared_key": "example",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ]
      },
      "ipsec_ike2_rsa": {
        "user_cert_alias": "",
        "ca_cert_alias": "",
        "server_cert_alias": "",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ],
        "ocsp_url": ""
      }
    }
  }
}
```

Example Xauth-PSK JSON (Other configurations in gray)

Server Certificate for the Gateway

It is possible to specify a Server Certificate for the Gateway in the configuration of a VPN tunnel, by providing the server_cert_alias string corresponding to a certificate previously installed into the keystore. This certificate will override any certificate provided by the Gateway during the negotiation of the tunnel.

This certificate may be loaded through the UI or EDM. See the device User manual for more information about loading certificates manually.

VPN Gateway Configuration Control

There are many configuration options for a VPN tunnel that only be configured from the gateway. The VPN client will utilize these settings from the gateway configuration to construct the secure tunnel. The following is a list of the settings that must be configured through the gateway:

- Encryption settings – while the VPN client will use FIPS validated encryption, the gateway will specify which algorithms should be used.
- IKE Protocols & Authentication – the gateway specifies which IKE protocols authentication techniques are required for establishing the connection. This includes requiring Main mode when IKEv1 is being used.
- IPsec Session Key cryptoperiod – the gateway specifies the session key cryptoperiod and can be used to configure periods under 1 hour in duration.

Third-Party VPN Clients (Device)

While Samsung devices come with a Common Criteria-certified VPN client, Enterprise customers may also use a VPN client from a third party vendor. Android provides the public class android.net.VpnService for third party vendors to build VPN clients that can be installed within Android.

These clients may contain additional capabilities beyond those provided by the built-in Android or Samsung clients. VPN client software built using this interface may provide their own management interface outside of that provided by Samsung.

Always-on Tunnel

When the device has a tunnel configured for Always-on VPN, all traffic will automatically go through this tunnel, and if for some reason a connection for the tunnel cannot be made, no traffic will be allowed to communicate off the device.

"Normal" VPN Tunnels

When VPN tunnels are configured and no tunnel is specified as Always-on, then the user must select the tunnel to be used. The user will select the tunnel from those available at ***Settings/Connections/More connection settings/VPN***.

Cellular/Mobile Network Configuration

There may be times when it is necessary to limit the type of Cellular network(s) to which a device should be allowed to connect. The device can be configured to connect to specific combinations of network modes such as 5G, LTE, 3G and 2G. The specific options may be limited by a combination of the SIM and the carrier the phone is connected to at any time (such as when roaming).

To change the network modes used to connect to the cellular network, the user can search for "Mobile Networks" in the user guide. Inside the Mobile Networks settings, the user can select "Network Mode" and choose from the available modes. In many cases the selections will have 2 or more modes with (auto connect) specified; this means the device will connect to any of the listed modes to provide the best cellular connection.

Certificate Management

While generally certificates would be managed through the EDM, it may be necessary for a user to update the Trust Anchor database locally. A user is not able to change settings managed by the EDM, but is able to add, remove or disable certificates outside the restrictions an EDM may enforce. Detailed instructions for managing certificates locally can be found under the "Credential Storage" section of the user guide for the specific device.

A work profile has an independent Trust Anchor database that is managed separately through the EDM or locally. Managing certificates locally within the work profile will follow the same steps as outside the work profile, but require the user to be authenticated to the work profile to access the settings.

Application Permissions

Applications may request access to system services, such as location, to support the functionality of the application. When an application is run for the first time, the user will be prompted to allow (or deny) access to the service for the application. Some services may also have an option for allowing access only when the application is running (preventing access when the application is not active on the screen). Unless a choice is made to allow access one time only, the selection made by the user will be remembered across application restarts.

These permissions can be managed on the device later in the Permission manager available at ***Settings|Privacy|Permission manager***. Here the permissions for each application can be checked and modified as desired.

Recommended device settings

The following list contains settings that you typically find in an MDM. This is not an exhaustive list of settings available via an MDM solution, rather indicative of settings that are relevant to the security of the device and its ability to handle Australian government information appropriately.

The recommended settings listed are considered suitable for Australian government owned devices carrying data at **PROTECTED** level; however, these settings should be thoroughly reviewed for risks as they apply to the organisations deployment scenario and accepted by an organisation's authorising officer and their system manager.

Knox work profile settings

Knox work profile passcode

Setting	Recommendation
Multifactor Authentication	Organisation Decision
Fingerprint Authentication	Organisation Decision If allowed multifactor authentication will need to be enabled.
Minimum Passcode Length	Single factor authentication: 14 Multi factor authentication: 6
Maximum Number of Failed Attempts	5
Passcode Content	Complex
Maximum Passcode Age	90 days
Passcode History	8
Lock Timeout (in Seconds)	Immediately on Device Lock 60 second timeout from inactivity

Maximum Length of Numeric Sequences	5
Minimum Number of Characters Changed	4
Forbidden Strings	Organisation decision (Recommended list of common passwords and passcodes)
Password Visibility	Disabled

Knox work profile Samsung Browser

Setting	Recommendation
Allow Pop-Ups	Disallow
Allow Cookies	Allow
Allow Auto Fill	Allow
Allow JavaScript	Allow
Enable Show Security Warning	Enable
Enable SmartCard Authentication	Organisation decision

Knox work profile VPN

Organisations should implement a Non-work profile (device wide) VPN to ensure that all device traffic traverses the VPN, noting the exceptions identified in the *Advice to authorising officers* section. Organisations may decide to implement a Knox work profile VPN in addition to the Device Wide VPN to separate organisation specific application traffic.

Knox work profile Samsung Email

Setting	Recommendation
Incoming Mail	
Use SSL	Enable
Protocol	Set which server the email client uses to receive and send emails.
Username	Define the Username for the authentication credentials using lookup values.
Password	Leave the Password blank to allow end-users to set their own password.
Ignore SSL Errors	Disable
Outgoing Mail	
Use SSL	Enable
Protocol	Set which server the email client uses to receive and send emails.
Username	Define the Username for the authentication credentials using lookup values.

Password	Leave the Password blank to allow end-users to set their own password.
Ignore SSL Errors	Disable

Knox work profile Exchange Active Sync

Setting	Recommendation
Mail Client	Select the native email client to be used on the device from the drop-down menu.
Login Information	
Domain	Use lookup values to define the domain for authentication credentials.
User	Use lookup values to define the user for authentication credentials.
Email Address	Use lookup values to define the email address for authentication credentials.
Password	Leave this text box blank to allow end-users to create their own password.
Path Prefix	Enter your path prefix.
Identity Certificate	Select an Identity Certificate from the drop-down, if you require the end-user to pass a certificate to connect to the Exchange ActiveSync.
Settings	
Retrieval Size	Indicate the maximum email size that is automatically delivered to your device without having to download the message.
Period Calendar	Select frequency from the drop-down menu.
Accept Certificates	Enable to allow certificates for email authentication.
Enable HTML Email	Enable to allow HTML formatted emails.
Peak Days for Sync Schedule	
Use SSL	Enable
Default Account	Assign the EAS account as the default for sending email messages.

Knox work profile application control

Setting	Recommendation
Prevent Installation of Blacklisted Apps	Enable, Blacklist all
Only Allow installation of Whitelisted Apps	Enable
Prevent Un-installation of Required Apps	Enable

Knox work profile device restrictions

Setting	Recommendation
Allow Camera	Organisation decision
Allow Video Recording if Camera is Allowed	Organisation decision
Allow USB	Disable
Allow Microphone	Organisation decision
Allow Audio Recording if Microphone is Allowed	Organisation decision
Allow Display of Share Via List	Disable
Force Secure Keypad Usage	Enable
Allow Contact Info Outside the Work profile	Disable
Allow Account Addition	Disable
Allow Google Account Activation	Disable
Allow Screen Capture	Disable
Enable Allow Clipboard	Organisation decision
Allow Mock Locations	Disable
Allow Bluetooth	Disable
Security	
Enforce Work profile Keyguard	Enable
Prevent New Admin Activation	Enable

Set Common Criteria CC Mode	Enable
Enable File Move	Disable
Enable OCSP Check	Turn on to allow use of Online Certificate Status Protocol during certificate revocation for application SSL connections.
Application	
Allow Google Crash Report	Disable
Allow S Voice (Bixby)	Disable
Allow User to Stop System Signed Applications	Disable
Allow Google Mobile Services (GMS) Applications in Work profile	Disable
Sync and Storage	
Allow Google Accounts Auto Sync	Disable
Allow Change Data Sync Policy	Disable
Allow SD Card Move	Disable
Hardware	
Allow Settings Change	Disable
Allow Reset Work profile on Reboot	Disable

Non-work profile device settings

Non-work profile (device wide) VPN

Setting	Recommendation
Connection Info	
Client Type	Native Samsung Internet Protocol Security (IPsec) Client (com.samsung.sVpn)
Enforce Service Validation	Enable
Server Suffix	Designate the domain to which the authenticating server must belong.
Authentication	

User Authentication	Enable this text box to require user credentials for VPN access. The selected Client Type determines applicable text boxes displayed in this section. The following text boxes display upon selection: ▪ Username – Enter the username users are required to enter at setup. ▪ Password – Leave blank to allow Users to input their password.
Connection Type	VPN Certificates
Identity Certificate	Use the drop-down to select the credentials for authenticating the connection.
Root Certificate	Specify the trust certificate authority.
Advanced	
Enable Advanced Configurations	Select the check box to display more options to configurable your VPN profile based on the selected client type.
Backup Server Name	Enter the name of the server to connect to if the primary VPN gateway fails.
Default Route Enabled	Enable to ensure that all network traffic goes through the tunnel.
IKE Version	Internet Key Exchange (IKE) protocol version for setting up security association. Ensure either 'IPsec Xauth RSA' or 'IPsec IKEv2 RSA' are selected.
Dead Peer Detection	Enable dead peer detection to allow the KeyVPN client to detect a dead IKE peer.
PFS Exchange	To be enabled if the session key should be protected.
Suite B	Use Suite B cryptography for connecting to VPN for higher security.
Phase 1 Mode	Sets up a secure tunnel to authenticate and secure the IKE tunnel. If the MDM presents the option for 'Aggressive Mode' for IKEV1 this should be disabled.
DH Group	Sets the key strength used in phase 1 during key exchange. The higher the group number, the more secure the key exchange. Organisations should implement at minimum **group 14**. Organisations should refer to the ISM to ensure implementation of an ASD Approved Cryptographic Algorithm.
Split Tunnel Type	Disallow
Forward Routes	Enter an alternate destination for the split tunnel to be directed. This text box is only displayed if Split Tunnel Type is set to Manual.

Authentication Type	Certificate-based should be selected.
Proxy	
Proxy Type	Select whether the proxy connects by Static Proxy or Proxy Auto Configuration.
Server	Enter the Host name or IP address for the proxy server.
Port	Specify the target port for the proxy server.
Username	Enter user credentials.
Password	Enter user credentials.
Assignment Level	
Assignment (For consideration in Work profile VPN implementation)	Select the assignment level as All Work profile Applications or Individual Applications. For Individual Applications, enter the application package name (app identifier) for the Applications you want to have Application level VPN. Examples include: ▪ Work profile application – sec_container_1.airwatchEmailClient. ▪ Application outside the work profile – com.airwatch.androidagent.
Logs and Warnings	
Enable Debug Logging	Include more detailed information in the diagnostics reports for troubleshooting.
Show Warnings	Show message in case of connectivity problems or when server name cannot be resolved.

Non-work profile passcode

Setting	Recommendation
Minimum Passcode Length	14
Passcode Content	Complex
Maximum Number of Failed Attempt	5
Maximum Passcode Age (days)	90 days
Passcode History	5

Device Lock Timeout (in Seconds)	Immediately on Device Lock 60 second timeout from inactivity
Enable Passcode Visibility	Disable
Allow Fingerprint Unlock	Disallow
Require Storage Encryption	Require

Non-work profile device restrictions

Setting	Recommendation
Allow Camera	Organisation decision
Allow Microphone	Organisation decision
Allow Factory Reset	Disallow
Allow Screen Capture	Organisation decision
Allow Mock Locations	Disallow
Allow Clipboard	Organisation decision
Allow USB Media Player	Disallow
Allow NFC	Disallow
Allow NFC State Change	Disallow
Allow Email Account Addition	Organisation decision
Allow Email Account Removal	Organisation decision
Allow Google Account Addition	Organisation decision
Allow POP / IMAP Email	Organisation decision
Allow Notifications	Organisation decision
Allow Audio Recording if Microphone is Allowed	Organisation decision
Allow Video Recording of Camera is Allowed	Organisation decision
Allow Ending Activity When Left Idle	Organisation decision
Allow User to Set Background Process Limit	Disallow

Allow Headphones	Organisation decision
Allow All Local Services	Organisation decision
Allow Fingerprint Authentication	Disallow
Allow Deactivate Device Admin	Disallow

Non-work profile sync and storage restrictions

Setting	Recommendation
Allow USB Debugging	Disallow
Allow USB Mass Storage	Disallow
Allow Google Backup	Disallow
Allow Google Account Auto Sync	Disallow
Allow SD Card Access	Disallow
Allow OTA Upgrade	Allow
Allow SD Card Write	Disallow
Allow USB Host Storage	Disallow
Allow SD Card Move	Disallow

Non-work profile application restrictions

Setting	Recommendation
Allow Google Play	Disallow
Allow YouTube	Disallow
Allow Access to Device Settings	Allow
Allow Developer Options	Disallow
Allow Non-Market App Installation	Disallow
Allow Google Crash Report	Disallow
Allow Android Beam	Disallow
Allow S Beam	Disallow

Allow S Voice (Bixby)	Disallow
Allow Copy & Paste Between Applications	Organisation decision
Allow User to Stop System Signed Applications	Disallow

Non-work profile Bluetooth restrictions

Setting	Recommendation
Allow Bluetooth	Organisation decision
Allow Bluetooth Pairing	Organisation decision
Enable Bluetooth Device Restrictions	If Bluetooth enabled - Allow
Enable Bluetooth Secure Mode	Allow

Non-work profile tethering restrictions

Setting	Recommendation
Allow All Tethering	Disallow
Allow Wi-Fi Tethering	Disallow
Allow Bluetooth Tethering	Disallow
Allow USB Tethering	Disallow

Non-work profile browser restrictions

Setting	Recommendation
Allow Native Android Browser	Allow
Allow Pop-Ups	Disallow
Allow Cookies	Allow
Enable Autofill for Android	Allow
Enable JavaScript For Android	Allow
Force fraud warning	Enable

Device-wide location services restrictions

Setting	Recommendation
Allow GPS Location Services	Organisation decision
Allow Wireless Network Location Services	Organisation decision
Allow Passive Location Services	Organisation decision

Non-work profile security restrictions

Setting	Recommendation
Allow Activation Lock	Allow
Allow Firmware Recovery	Disallow
Allow Lock Screen Settings	Organisation decision
Allow User Creation (Requires Allow Multiple Users to be enabled)	Disallow
Allow User Removal (Requires Allow Multiple Users to be enabled)	Disallow
Allow Multiple User	Disallow
Allow Keyguard	Allow
Allow Trusted Agent	Disallow
Allow Camera on Keyguard Screen	Organisation decision
Allow Fingerprint on Keyguard Screen	Disallow
Allow Notifications on Keyguard Screen	Organisation decision, as long as redacted only.
Allow Un-redacted Notifications on Keyguard Screen	Disallow
Allow Fingerprint Unlock	Disallow

Non-work profile network restrictions

As these are device-wide, they apply to both the workspace and the rest of the device.

Setting	Recommendation
Allow Wi-Fi	Organisation decision
Allow Cellular Data	Organisation decision
Allow Wi-Fi Profiles	Allow
Allow Wi-Fi Changes	Organisation decision
Allow Unsecure Wi-Fi	Organisation decision
Allow Auto Connection Wi-Fi	Organisation decision
Allow Prompt for Credentials	Allow
Minimum Wi-Fi Security Level	Organisation decision
Allow Only Secure VPN Connections	Allow
Block Wi-Fi Networks by SSID	Organisation decision
Allow Native VPN	Allow
Allow Wi-Fi Direct	Disallow
Set Global HTTP Proxy	Organisation decision

Audit Records

Auditing is enabled and events retrieved through the EDM. A Knox Platform for Enterprise license is required in order to enable the collection of audit records.

Audit records are stored in a compressed format to minimize space and maximize the amount of records that can be stored. When the allocated space is full, the oldest events will be overwritten so the most recent as always maintained (circular logging/buffering). Notifications are sent to the EDM based on the log space becoming full to warn before wrapping occurs.

The minimum amount of allocated space for audit storage is 10MB with a maximum of 50MB, depending on the available free space when activated. There must be at least 200MB of free space when Auditing is enabled (an error is returned to the EDM if not), and no more than 5% of free space will be used, up to the maximum of 50MB. The allocated space is not adjusted after it is initially set.

Within the logging, it is also possible to filter the events that are written to the log.

One important note about the audit capabilities is that they are tied to being enrolled to a management server (EDM). If the device is not enrolled there is no way to enable auditing, and when a device is unenrolled, the audit records are deleted as part of the un-enrolment process, so any events created between the last review/upload and the un-enrolment will be lost.

Types of Audit Events

There are three classes of audit events that can be logged, system and apps, kernel and IP tables. Each can be controlled individually, so you can log just select classes of events. Kernel and IP table logging generates a large amount of events, so care should be taken that the EDM collect the logs frequently if they are enabled or the circular logging function could cause events to be overwritten and lost.

Audit Collection Filter Settings

When configuring audit collection, it is possible to filter the events based on several selections using the AuditLogRulesInfo class. With the exception of the Groups and Users, the settings only accept a single value (i.e. you can specify only one of the options for the Outcome, only Failures, only Successes or All).

Setting	Value	Description
setSeverityRule(int severityRule)	Alert Critical Error Warning Notice	Specifies the minimum severity level to log. Everything with the specified number and lower will be logged.
setOutcomeRule(int outcomeRule)	Fail Success All	Specifies filtering based on the outcomes of each event
setGroupsRule(List<Integer> groupsRule)	Security System Network Events Application NULL = All	Specifies the groups of events to log. NULL will log events from all groups.
setKernelLogsEnabled(boolean enableKernel)	Enable Disable	Enables or disables Kernel logging
setUsersRule(List<Integer> usersRule)	List of UID	This allows logging only from specified UIDs in the list. This is only available to EDMs outside the work profile (inside the work profile the EDM can only see the work profile user). System events (UID 2) are always logged regardless of any specific selections made by the administrator.

Table 8 – Audit Collection Filter Settings

Audit Record Fields

The audit records have eight (8) fields as described in the following table.

Setting	Description
Timestamp	Long value that represents the UTC timestamp
Severity	Integer value representing the severity: 1 (alert), 2 (critical), 3 (error), 4 (warning), 5 (notice)
Group	Integer value representing the group code: 1 (security), 2 (system), 3 (network), 4 (events), 5 (application)
Outcome	Integer value representing the outcome of the event: 1 (success), 0 (failure)
PID	Integer value representing the process ID
USERID	Integer value representing the USERID for which the log was originated ID 0 is for a normal user ID -1 is for system events ID 10-12 or 100-102 is for work profile users (multiple work profiles can be defined, but only one is ever active at one time). IDs 100-102 are for legacy Knox profiles. Separated app profiles will be 10-12.
Component	String representing the facility/Software Component name
Message	Free-form message description of the event (generally a human-readable message)

Table 9 – Audit Fields

Audit Events

The list of audit records that are produced related to the functionality claimed in the MDFPP are beyond the scope of this document. For further information, refer to section 5.2 Audit Events of the MDFPP document "Samsung Android 13 on Galaxy Devices Administrator Guide (AGD)".

Developer References

Cryptographic APIs

This section provides information for developers to utilize the evaluated cryptographic APIs while writing their mobile applications. The Reference Link points to more information about the APIs for the specific cryptographic functions.

Cryptographic Function	Evaluated API	Reference Link
AES-CBC 128/256	javax.crypto.Cipher	developer.android.com
AES-GCM 128/256	javax.crypto.Cipher	developer.android.com
SHA-1/256/384/512	java.security.MessageDigest	developer.android.com
HMAC-SHA-1/256/384/512	javax.crypto.Mac	developer.android.com
RSA Key Generation	java.security.KeyPairGenerator java.security.KeyFactory	developer.android.com
ECDSA Key Generation	java.security.KeyPairGenerator	developer.android.com
RSA Signing/Verification	java.security.Signature	developer.android.com
RSA Encryption/Decryption	javax.crypto.Cipher	developer.android.com
ECDSA Signing/Verification	java.security.Signature	developer.android.com
ECDH Key Agreement	java.security.KeyPairGenerator javax.crypto.KeyAgreement	developer.android.com
RBG Random Generation	java.security.SecureRandom	developer.android.com
Certificate Verification	java.security.cert.CertPathValidator	developer.android.com

Cryptographic Function	Evaluated API	Reference Link
Key Import, Use, Destruction	javax.crypto.KeyGenerator java.security.KeyPairGenerator java.security.KeyStore android.security.KeyChain	 developer.android.com developer.android.com

Table 10 – Cryptographic API Reference

Developers can utilize with the KeyStore or the KeyChain to store their keys/credentials, depending on type of key (symmetric keys can only be stored in the KeyStore). Keys stored in the KeyStore can only be accessed (used or deleted) by the original app or by apps with a common developer with enforcement handled by the KeyStore. Keys stored in the KeyChain can be made globally available (with explicit approval by the user). When a key is imported/created it is assigned authorizations for use which cannot be changed later (i.e. what the key can be used for, how long the key can be available).

Bluetooth APIs

The device provides access to Bluetooth functions through a standard set of APIs. These can be found at developer.android.com under android.bluetooth and android.bluetooth.le.

TLS/HTTPS APIs

The device provides access to TLS & HTTPS functions through a standard set of APIs. These can be found at developer.android.com under javax.net.ssl.

Certificate Pinning

The device provides the ability for applications to utilize certificate pinning to lock the certificates accepted when accessing web services to only those that are specifically expected. This must be done by the app and is not something the user can set on their own. Information about configuring an app to utilize certificate pinning can be found at developer.android.com under Network Security Configuration.

IPsec VPN APIs

The device provides the ability to configure IPsec VPN tunnels through a standard set of APIs. These can be found at developer.android.com and at the Samsung Knox SDK API reference.

Glossary of cyber security terms

Term	Meaning
application control	An approach in which only an explicitly defined set of approved applications are permitted to execute on systems.
authorising officer	An executive with the authority to formally accept the security risks associated with the operation of a system and to authorise it to operate.
Classification	The categorisation of information or systems according to the business impact level associated with that information or system.
Common Criteria	An international standard for software and ICT equipment evaluations.
cryptographic software	Software designed to perform cryptographic functions.

cyber security	Measures used to protect systems and information processed, stored or communicated on ICT systems from compromise of confidentiality, integrity and availability.
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of systems or information.
data at rest	Information that resides on media or a system.
data in transit	Information communicated across a communication medium.
ephemeral keys	Cryptographic key that is generated for each new session.
ICT equipment	Any device that can process, store or communicate electronic information.
Integrity	The assurance that information has been created, amended or deleted only by authorised individuals.
Internet Protocol Security (IP Sec)	A suite of protocols for secure communications through authentication or encryption of Internet Protocol packets, as well as including protocols for cryptographic key establishment.
key management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.
Media	A generic term for hardware, often portable in nature, which stores information.
mobile device	A portable computing or communications device. For example, a laptop, mobile phone or tablet.
Passphrase	A sequence of words used for authentication.
Password	A sequence of characters used for authentication.
Patch	A piece of software designed to remedy security vulnerabilities, or improve the usability or performance of software and ICT equipment.
Product	A generic term used to describe software or hardware.
protective marking	An administrative label assigned to information that not only shows the value of the information but also defines the level of protection afforded to it.
Protection Profile	A document that stipulates the security functionality that must be included in Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to be undertaken to assess the security function of an evaluated product.

security risk	Any event that could result in the compromise, loss of integrity or unavailability of information or resources, or deliberate harm to people measured in terms of its likelihood and consequences.
Server	A computer that provides services to users or other systems. For example, a file server, email server or database server.
System	A related set of hardware and software used for the processing, storage or communication of information, and the governance framework in which it operates.
system manager	An individual to whom the system owner has delegated the day-to-day management and operation of a system.
system owner	The executive responsible for a system.
User	An individual who is authorised to access a system.
Virtual Private Network (VPN)	A private data network that maintains privacy through a tunnelling protocol and security procedures. VPNs may use encryption to protect traffic.
Workstation	A stand-alone or networked single-user computer.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at: https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

The ***Secure Mobility Guidance*** provides the advice and guides that can support system owners. It can be found at: https://www.cyber.gov.au/acsc/government/secure-mobility-guidance

Contact details

If you have any questions regarding this guidance you can contact:

Samsung Electronics Australia
Email: gov.support@samsung.com
Web: www.samsung.com.au