Australian Government
Australian Signals Directorate

Security Configuration Guide: Samsung Galaxy S10, S20 and Note 20 Devices

Using Samsung Knox version 3.6+ and Android 10.0+

First published: February 2021
Last updated: October 2021

Table of contents

Introduction

The Australian Signals Directorate (ASD) has developed this guide to assist Australian's to understand the risks when deploying Samsung Galaxy S10 and S20 devices. It details the security requirements that allow Samsung Galaxy platforms to handle classified data. This security configuration guide does not replace the *Information Security Manual* (ISM). However, where a technical conflict arises organisations should asses their risk using both documents.

Audience

This guide is for users and administrators of Samsung Galaxy platform. These devices include S10, S20 and Note 20 mobile device series, procured within the Australian market. Note that the above models have relied on prior ASD Cryptographic Evaluation (ACE) program results to assess risks.

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 reference product features that will require the deployment of additional networking equipment or Mobile Device Management (MDM) software. 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 their vendor when planning their system implementation. Note, mention of third-party products is not an 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 be implemented by experienced systems administrators and should be used in conjunction with thorough testing.

Purpose

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

This guide provides a summary of features and associated risks for the Samsung Galaxy S10, S20 and Note 20. Throughout this guide, devices and combinations of software are collectively referred to as the 'Samsung Galaxy platform'.

The advice in this guide has been written for the use of the Galaxy platform within Australia and its territories. Organisations and individuals seeking to use devices outside Australia should also refer to the *Travelling With Mobile Devices* publication.

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 residual risks. Refer to the *applying a risk-based approach to cyber security* section of the 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 the Exynos mobile processor and run Samsung Knox 3.6 or higher and Android 10.0 or higher.

Series	S10e	S10	S10+	S20	S20+	S20 Ultra	Note 20	Note 20 Ultra	S20 FE
4G	SM-G970F	SM-G973F	SM-G975F	SM-G980F	SM-G985F	N/A	N/A	N/A	G780F

5G	N/A	SM-G977B	N/A	SM-G981B	SM-G986B	SM-G988B	SM-N980B	SM-N986B	G781B

Evaluation status

Since April 2014, ASD 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. Earlier versions of Samsung Galaxy platform have been evaluated against MDFPP and completed an ASD Cryptographic Evaluation (ACE) in 2018.

This guide is based on the findings of ASD and provides guidance that must be enforced for **OFFICIAL: Sensitive** and **PROTECTED** deployments. Guidance in this publication will also assist organisations to comply with existing policies when deploying devices at lower classifications.

Samsung also has additional security information for their devices.

General advice

When new versions of Samsung Galaxy platform Operating System (OS) are released, there is potential for the introduction of changes that can have security implications. Authorising officers should seek additional guidance, if required, when considering new versions. In the absence of additional guidance, ASD provides the following advice.

- Upgrade to the latest version of the Samsung Galaxy platform OS as new versions provide security enhancements and address known vulnerabilities. This is consistent with ASD advice to install the latest versions of software and to patch operating system vulnerabilities as communicated in the ISM and the *Strategies to Mitigate Cyber Security Incidents*.

Samsung and Google provide release notes regarding the content of Android security updates. This information can help organisations quantify the risks if they do not update.

Introduction to mobile device security

In this guide, mobile device security advice centres on the three security tenets of:

- device integrity
- data at rest
- data in transit.

ASD evaluates cryptographic implementations to determine the configurations necessary to reduce the handling requirements of devices used for processing, storing or communicating classified data. Each organisation is responsible for configuring their devices according to ASD guidance, and ensure that available cryptographic protections are appropriately configured.

Configuration advice regarding device integrity aims to provide a level of protection suitable for classified mobile devices. It assumes malicious actors have physical access to mobile devices while powered on and in a locked state. Configuration advice draws upon an assessment of:

- key hierarchy and architecture
- cryptographic implementation
- operating system architecture
- configuration under typical deployment scenarios.

Configuration advice regarding the protection of data at rest aims to provide a level of protection suitable for classified data stored on a Samsung Galaxy platform. This advice assumes malicious actors have physical access to devices while they are powered on and in a locked state. Configuration advice draws upon configuration assessments and details of application implementations, including availability of security features.

Configuration advice regarding the protection of data in transit aims to provide a suitable level of protection for classified data traversing a network. It assumes malicious actors are able to intercept this traffic. Each organisation is responsible for configuring their devices according to ASD guidance and maintaining appropriate Virtual Private Network (VPN) infrastructure to support VPN tunnels. Noting such supporting infrastructure is out of scope for this guide.

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 devices at a hardware and software level.

Samsung Galaxy platform leverage hardware features coupled with Knox software to verify that the device boot chain is not compromised and tampering has not occurred. Samsung Galaxy S20 and Note 20 devices provide additional security through a ‘secure element’ chip which further extends the ability of Knox to perform hardware verification and provide secure data storage.

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

Further information can be accessed from the *Samsung Knox Platform for Enterprise (KPE) guide*.

Data protection

The Samsung Galaxy platform supports Samsung's On-Device Encryption and Sensitive Data Protection (SDP), which provide hardware backed encryption for data-at-rest. Two levels of protection; 'Protected Data' and 'Sensitive Data' are provided by the system. This is not to be confused with the **PROTECTED** or **OFFICIAL: Sensitive** classification levels:

- **Protected Data:** This is the default level of protection for every file inside the work profile. Cryptographic keys are not evicted from memory at work profile lock; they stay in memory until the device is powered off.
- **Sensitive Data:** Applications must specifically mark files as Knox Sensitive Data, or place the files into the *Chamber* directory which encrypts the contents with SDP. Cryptographic keys are evicted from memory at work profile lock, and data is only accessible when the work profile is unlocked.

Additional information is available from the *Samsung Knox Platform for Enterprise (KPE) guide* and the *Sensitive Data Protection* whitepapers.

The encryption deployed by the Samsung Galaxy platform is optionally DualDAR, which means the data is encrypted in two layers when Android Enterprise Work Profiles are enabled. The inner layer allows a third-party cryptographic module to be installed and deployed. The default setting is a FIPS 140-2 certified cryptographic module. The outer layer uses AES 256 XTS encryption and file encryption keys are encrypted through AES-GCM 256. Additional information is available from the KPE white paper's section on DualDAR.

Organisations deploying Samsung Galaxy platforms that handle **PROTECTED** level classified data, must ensure it is stored as 'Knox Sensitive Data'. SDP provides a sufficient mechanism for **PROTECTED** level classified data and is a key requirement supporting the ability to reduce the handling requirements.

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 stored within the SDP area.

Application Container

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

The Android Enterprise Work Profile creates a secure container on the device using encryption. When applications are running inside the work profile, they are cryptographically separated from the base device storage. Applications running inside the Android Enterprise work profile are separate instances to ones outside of the work profile.

KPE also has a storage area inside the work profile called '*Chamber*', which marks all files with SDP that are 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*.

MDM enrolled devices

ASD guidance advises that devices handling classified data (**OFFICIAL: Sensitive** and above) be MDM enrolled. MDM enrolment manages KPE, as outlined later in this guide. MDM enrolment of devices handling classified data is necessary to ensure that the correct policies and configurations are applied throughout the lifecycle of devices. Organisations will need to register their devices with Samsung to access KPE. For high-risk implementations, and cases where registering with Samsung is neither desirable nor technically feasible, advice may be sought from ASD.

Individuals wishing to utilise Bring Your Own Device (BYOD) must consider the need for enrolment with an organisations MDM. MDM enrolment provides control and remote wipe functionality of devices within their organisation. Therefore, a detailed discussion about the need for BYOD should be held between the user and authorising officer, with appropriate policy developed to support this requirement.

Samsung Knox Premium licence

In order to securely configure Samsung Galaxy platform in accordance with this guide, organisations will be required to purchase a KPE Premium licence from a Samsung Knox reseller. Once obtained, the KPE Premium licence must be loaded into an MDM, and enable KPE functionality.

Advice to authorising officers

ASD has developed the *Strategies to Mitigate Cyber Security Incidents* to help organisations and their authorising officers mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies are known as the Essential Eight. While the strategies were developed for workstations and servers, much of this is applicable to modern smartphones.

Samsung Galaxy platform and the Essential Eight

Application control

- When configured in accordance with ASD guidance, the Samsung Galaxy platform only implement application controls that are enforced via an application's package name.
- The Samsung Galaxy platform offers no granular configuration, such that applications can be controlled based on specific versions or via package hashes (a unique cryptographic fingerprint for an application version). This level of control must be provided through a managed app store.
- Therefore it is not advisable to allow the Samsung Galaxy platform that have access to **PROTECTED** information to interact with unmanaged rich application ecosystems, such as the Google Play Store or Samsung Galaxy App Store, or permit configuration such that applications can be installed from unknown sources. For environments where apps that are not part of the platform are required, a managed app store should be utilised to control the apps available on the device with the needed granular control. These conditions ensure that only approved applications are allowed to run on the devices.

Patch applications

- When configured in accordance with this guidance, the Samsung Galaxy platform receives patches to applications as soon as they are available.
- It is recommended that user education is provided so that users understand the necessity to update applications when prompted by the device.
- Organisations can leverage their MDM to measure compliance with this control.

Configure Microsoft Office macro settings

- Currently, Microsoft Office for Android does not support high-risk features such as Microsoft Office macros.
- New versions of Microsoft Office for Android may introduce macro functionality. Authorising officers will need to reassess of their exposure to this risk.

User application hardening

- When configured in accordance with ASD guidance, the Samsung Galaxy platform do not display or run Adobe Flash content. Samsung Galaxy platform is configured to not allow Java to execute or to allow pop-ups; however, these settings can be manually disabled by the user.

Restrict administrative privileges

- When configured in accordance with this guidance, the Samsung Galaxy platform is managed by an MDM solution and performs self-attestation checks to ensure the correct permissions are set and enforced.
- Authorising officers are encouraged to ensure that the MDM fully supports the security features recommended in this guide.

Patch operating systems

- Samsung have recently announced that the Samsung Galaxy platform will receive Android operating system updates for 'up-to' three generations of flagship devices.

- The Samsung Galaxy platform is an Android-based ecosystem; consequently, there are many stakeholders involved in the patching lifecycle for the OS. These include: Google's Android Open Source Project (AOSP), Samsung and Australian telecommunications network providers. Organisations shall ensure that users are advised to apply operating system software updates when prompted.
- Organisations can leverage their MDM to measure compliance with this control.

Multi-factor authentication

- When configured in accordance with this guidance, the user is initially authenticated locally on the Samsung Galaxy platform, and then mutual authentication is then performed through Remote Server infrastructure (e.g. MDM, VPN) using usernames, passwords and certificates. While this is not a traditional model for multi-factor authentication, the useability and security considerations are appropriately satisfied for the intent of the mitigation strategy.

Daily backups

- When configured in accordance with ASD guidance, the Samsung Galaxy platform does not allow for backup of government information.
- If the mobile device is only used to access corporate data hosted on remote servers such as email, the requirement to backup handset data is reduced to the configuration required to rebuild the device, such as those hosted in an MDM.
- Organisations considering the use of third party or custom backup applications should investigate the risk to government information.

Samsung Galaxy platform feature summary and risk considerations

Work profile

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

The work profile is the only logical storage area that meets the requirements to handle **OFFICIAL: Sensitive** or **PROTECTED** data. The 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 classified data.

When using applications inside the 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 classified data, the work profile must be locked. Set the work profile lock to the device lock screen in order to appropriately clear ephemeral keys from device memory.

Work profile passcode

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Required

Risks

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

The biometric mechanisms of the Samsung Galaxy platform have not undergone an ACE, and the security claims of the feature are difficult to assess. The use of biometrics to protect classified 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 two unique passwords be used to unlock the handset and 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 requirement 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.

Device passcode

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Required

Risks

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

It is recommended to use a unique password or passphrase to unlock the device. PIN codes, pattern/swipe codes and built-in biometric sensors should not be used. The biometric mechanisms of the Samsung Galaxy platform have not undergone an ACE, and the security claims of the feature are difficult to assess. The use of biometrics to protect classified 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 work profile

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

Applications that do not handle classified data appropriately or afford a suitable level of encryption are at risk of disclosing or mishandling classified 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 classified data is appropriately handled within the 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 classified data stored inside the work profile. Applications should be assessed in detail before being allowed to run inside a work profile that contains classified data. Applications should not be installed inside the work profile without a genuine need for access to classified data.

Additional information can be found under the 'Application hardening' section in the ISM.

Non-native applications outside the work profile

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not recommended

Risks

Android applications may contain functionality that contravenes an organisations 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 work profile provides appropriate protections, when configured in accordance with this guide, to defend against applications from outside the work profile. While it is possible to install non-native applications outside of the 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 work profile, the application must never handle **PROTECTED** data or interact with applications within the work profile.

Non-native applications should not be 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 in the ISM.

Mobile Device Management

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

Without an MDM, devices may not 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 classified 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.

Mobile Application Management

OFFICIAL: Sensitive	PROTECTED
Recommended	Required

Risks

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. For deployments that do not require non-native applications, there is no requirement for a MAM solution.

Additional information can be found under the ‘Mobile Device Management’ topic in the ISM.

Bring Your Own Device

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not permitted

Risks

BYODs have a higher risk of inadvertently introducing risk into an organisation’s mobile deployment. They are at higher risk of infection with malicious applications or software before MDM configuration is applied to make them suitable for handling classified data. Organisations should perform a risk assessment before allowing privately-owned devices onto their networks.

A deployment can include BYOD when the devices are enrolled in an MDM and appropriately configured for handling **OFFICIAL: Sensitive**. It is not permitted to use BYOD for **PROTECTED** deployments.

Additional information can be found under the 'Privately-owned mobile devices' topic in the ISM and the *Risk Management of Enterprise Mobility (Including Bring Your Own Device)* publication.

Virtual Private Network

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

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 certain deployment scenarios.

All data communications for the Samsung Galaxy platform handling classified data must be through the Always On 'StrongSwan' VPN. The Samsung Galaxy platform offers two versions of VPN client – OpenVPN and StrongSwan. 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

OFFICIAL: Sensitive	PROTECTED
Not recommended	Not permitted

Risks

Samsung Galaxy platform deployments that allow unknown sources have less control over the applications that can be loaded, 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 'Application hardening' and 'Mobile device management' sections in the ISM.

SDP-aware email applications running inside work profile

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Required

Risks

SDP aware email applications offer appropriate protections for the encryption and handling of classified data 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 security 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 based upon the risks surrounding the storage and handling of classified data on the devices.

For SDP-aware email applications that run inside a 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 email header information 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 classified data.

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 classified data is printed in hardcopy form.

Organisations must deliver user training to ensure that users understand that 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 work profile

OFFICIAL: Sensitive	PROTECTED
Not recommended	Not permitted

Risks

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

It is not recommended for **OFFICIAL: Sensitive** deployments and not permitted for **PROTECTED** deployments.

Email applications running outside work profile

OFFICIAL: Sensitive	PROTECTED
Not recommended	Not permitted

Risks

The use of email applications running outside of the work profile introduces a high degree of risk for classified data.

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

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

Document preview running inside work profile

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

Classified 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 mail client. There is no guarantee 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 classified data using document preview applications.

If organisations allow the use of document preview applications for classified 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 encrypted with SDP would assist in reducing risk.

External storage

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not permitted

Risks

Any data stored or accessed on external or adoptable media will not be encrypted with SDP, and therefore such external storage media is not suitable for classified 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

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

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 allow or deny applications through Mobile Application Management (MAM).

Note, application control via developer certificate allows all applications signed with an approved developer's certificate to be installed.

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

Backups

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

Without regular backups, classified data may be irrecoverable should only a local copy of the data exist and become inaccessible. However, with unapproved backup solutions, classified 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 classified data that is only held on the device. Currently there is not an Android or Samsung implementation of automated backup from within the 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

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

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 classified data, as provided by SDP.

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

Mobile device administration

Managing mobile device security

MDM and MAM solutions are an integral part of implementing any smartphone solution for an organisation. Any smartphone device that handles classified data will require an appropriate MDM and MAM solution to satisfy the security requirements outlined in this guide and the ISM. 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 contains.

In order to deploy core Samsung security features, such as work profiles, 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.

Purchasing and enrolling devices

It is important that organisations purchase smartphone 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 smartphone 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 includes BYOD deployment scenarios. Rooting allows complete access to the underlying mobile operating system and removes important controls.

Each MDM solution has its own way of enrolling devices, however the general theme for the Samsung Galaxy platform is for a client application to be installed manually and configured to enrol the device into the MDM and associate the device with a user. 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 classified data. Devices should be enrolled into the MDM from within an organisation's trusted network. MDM client applications will need to be given the 'Device Administrator' permission. 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.

Revoking use, 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 at end of life and are to be disposed of, or stop being used by an individual.

Classified data

When devices are at the end of life and are to be disposed of, multiple decommissioning steps are required. When classified data has been stored on the device in accordance with the settings specified in the device summary of this guide, for its entire life, un-enrolling from the MDM will result in the associated work profile automatically being destroyed and the data deleted. A factory reset is still required to ensure all classified data is removed as per guidance in the ISM.

Revoking 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 performing 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 assessment, is deployed on devices.
- **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.
- **Carefully consider applications that contain integration into file-sharing, cloud and social media platforms:** Fully understand the applications in terms of how they handle classified data.
- **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

Data spill

When classified data has not been stored and handled in accordance with the guidelines specified in the device summary section, it is deemed a data spill. Users must report the incident to their system manager at their earliest opportunity. On device remedial action must satisfy the ISM control for sanitisation of non-volatile flash memory. Consideration of subsequent sanitisation requirements to be determined by the system manager with regard to connected remote services.

Peripherals and other connectivity

An organisation may wish to consider the following to aid developing user policy on the use of peripherals and other connectivity features present in the Samsung Galaxy platform.

Charging

It is recommended that only the issued charger be used by the users. Users should not use public charging stations or shared public charging cables and not use gifted chargers and/or battery power banks. Users should not be charging from other devices, for example, personal computers, televisions or power banks not issued by the supplier or organisation.

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.

Direct Memory Access

Mobile devices can be susceptible to Direct Memory Access, even with modern preventative measures. Mobile devices should not be left unlocked and unattended, or be connected to unapproved or non-Australian Government owned devices.

USB mass storage, MTP and P2P

If a mobile device is unlocked and connected to a non-approved or malicious system then files or applications may be transferred to the device via USB. Examples of potentially malicious connections include to printers, USB flash media and computers. These may compromise the security of the data that the device holds and compromise the security of future communications. Risk owners should give consideration to disabling USB functionality via MDM controls.

Bluetooth

Disabling Bluetooth when not required, and by using it only when necessary reduces the attack surface. The ISM has additional guidance on how to best approach the use of Bluetooth peripherals on Australian Government deployments applicable to the Samsung Galaxy platform.

Connecting to vehicles, Android Auto, headsets and speakers

Bluetooth pairing typically allows access to messages and contacts on the device. In vehicles, there may be the ability to interact with applications. Bluetooth peripherals may retain a copy of private correspondence and **OFFICIAL** contact details. This may present a risk, particularly when using rental vehicles. The ISM has additional guidance on how to best approach the use of Bluetooth peripherals on Australian Government deployments applicable to the Samsung Galaxy platform.

Wi-Fi

Avoid connecting electronic devices to any open or untrusted Wi-Fi networks. Examples of such networks include airport lounges, in-flight facilities, public libraries and shopping centre networks. Use an approved VPN connection to encrypt all internet traffic. Alternatively, use per-application VPNs for all web browsing, email and instant messaging applications. The ISM has additional guidance on how to best approach the use of Wi-Fi on Australian Government deployments relevant to the Samsung Galaxy platform.

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 unassessed security risks.

Personal assistants

Personal assistant applications generally carry out the user's command by voice input. These should be disabled by MDM policy. These applications may process conversation taking place around the devices at any time. Should these applications be used, there is a risk that classified conversations will be transmitted for additional processing in the cloud, and the data could then be stored and processed by the voice assistant servers with insufficient protection of classified data.

Display output or casting

Samsung Galaxy platforms have various wired and wireless methods to share the device display with other displays. These casting and sharing methods have not been assessed, and present the opportunity for classified data, if stored on or accessed by the device, to be viewed or modified when sharing. Therefore, devices holding classified data should not be used for casting or sharing the display.

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 classified data 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 Workspace settings

Knox Workspace passcode

Setting	Recommendation
Fingerprint Authentication	Disallow
Multifactor Authentication	Disable
Minimum Passcode Length	14
Maximum Number of Failed Attempts	5
Passcode Content	Complex
Maximum Passcode Age	Less than 12 months
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 Workspace 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 Workspace VPN

Organisations should implement a Non-Workspace (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 Workspace VPN in addition to the Device Wide VPN to separate organisation specific application traffic.

Knox Workspace 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 Workspace Exchange ActiveSync

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 Workspace credentials

When uploading credentials, enable the option to have them stored in the device's TIMA Keystore.

Knox Workspace application control

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

Knox Workspace 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 Container	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 Container Keyguard	Enable
Prevent New Admin Activation	Enable
Set Common Criteria CC Mode	Enable
Enable Application Move	Disable

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 Container	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 Container on Reboot	Disable

Non-Workspace device settings

Non-Workspace (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	StrongSwan 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 approved cryptography.

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 Container VPN implementation)	Select the assignment level as All Container 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: ▪ 'Container application – sec_container_1.airwatchEmailClient'. ▪ 'Application outside the container – 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-Workspace passcode

Setting	Recommendation
Minimum Passcode Length	14
Passcode Content	Complex
Maximum Number of Failed Attempt	5

Maximum Passcode Age	Less than 12 months
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
Require SD Card Encryption	Require

Non-Workspace 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-Workspace 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-Workspace 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-Workspace 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-Workspace tethering restrictions

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

Non-Workspace 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-Workspace 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-Workspace 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

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.
ASD Cryptographic Evaluation (ACE)	The rigorous investigation, analysis, verification and validation of cryptographic software and equipment by ASD against a stringent security standard.
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 IT equipment evaluations.
cryptographic software	Software designed to perform cryptographic functions.
cyber security	Measures used to protect systems and information processed, stored or communicated on such 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.
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.
IT equipment	Any device that can process, store or communicate electronic information.
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 vulnerabilities, or improve the usability or performance of software and IT 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 *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).