SAMSUNG

Administrator Guide

Samsung Android 9 on Galaxy Devices

October 16, 2019

Version: 5.3

Copyright Notice

About this document

This document describes the enterprise guidance for the deployment of Samsung devices in accordance with the Common Criteria-validated configuration. The document is intended for mobile device administrators deploying Samsung devices.

Document Identification

Document ID	Samsung MDF Admin Guidance v5.3
Document Title	Samsung Android 9 on Galaxy Devices Administrator Guide

Revision History

Version	Date	Changes	Author
4.0	May 15, 2018	Android 8, new template	Brian Wood
4.1	November 16, 2018	Android 8.1, added new devices	Brian Wood
5.0	July 19, 2019	Android 9 update	Brian Wood
5.1	August 1, 2019	Added new devices	Brian Wood
5.2	September 3, 2019	Added new devices for Fall 2019 eval	Brian Wood
5.3	October 16, 2019	Added new device	Brian Wood

Contents

1 Introduction

1.1 Scope of Document

This document is intended as a guide for administrators deploying Samsung devices in the enterprise. The guidance provided here focuses on how to configure devices to be in an approved configuration based on the Protection Profile for Mobile Device Fundamentals v3.1 for the Samsung devices specified here.

The document is evolutionary. It will cover all devices evaluated with a common major version of Android.

1.1.1 End-User Guidance

This guidance document is focused on the central management of Samsung mobile devices. Guidance related to user functions on a device, such as managing Bluetooth connections or setting authentication credentials are outside the scope of this documentation. End-user guidance can be found both on the device (most functions are guided through the user interface with descriptions and help) or from the Samsung support website. Links to online guidance can be found in section 1.5 References.

1.2 Overview of Document

Samsung mobile devices are designed to maintain a secure mobile environment. To successfully deploy and maintain such an environment requires coordination with multiple parties including:

- Enterprise/Mobile Device Management (EDM/MDM) software
- Carriers
- Mobile Device Administrators
- Users

This document is designed for the Mobile Device Administrators, to provide guidance in how to configure and deploy Samsung mobile devices within an enterprise environment. This includes information about API controls that can be used within the EDM/MDM software to achieve this configuration.

1.3 Terminology & Glossary

Evaluated Device	Processor
ADB	Android Debug Tool
ADT	Android Development Tools
API	Application Programming Interface
BYOD	Bring Your Own Device

Evaluated Device	Processor
CA	Certificate Authority
COPE	Corporately-Owned, Personally Enabled
EDM MDM	Enterprise Device Management Mobile Device Management NOTE: EDM will be used for consistency
FBE	File-Based Encryption
FOTA	Firmware Over-the-Air
KPE	Knox Platform for Enterprise
MDF MDFPP	Mobile Device Fundamentals Mobile Device Fundamentals Protection Profile
ODE	On-Device Encryption
SDK	Software Development Kit
TLS	Transport Layer Security
VPN	Virtual Private Network

Table 1 - Acronyms

1.4 Evaluated Devices

The Common Criteria evaluation was performed on a set of devices covering a range of processors. These devices were chosen based on the commonality of their hardware across several different devices that are also claimed through equivalency. All device models are evaluated with Samsung Android 9 (Pie).

The evaluation was performed on the following devices (note that the evaluation period is listed in parenthesis for each device):

- Samsung Exynos and Qualcomm Snapdragon
  - Galaxy S9+ (Spring 2019)
  - Galaxy Note8 (Spring 2019)
- Samsung Exynos
  - Galaxy Note10+ 5G (Fall 2019)
  - Galaxy Tab Active2 (Fall 2019)
  - Galaxy S10e (Spring 2019)
- Qualcomm Snapdragon
  - Galaxy Tab S3 (Fall 2019)

- Galaxy S10+ (Spring 2019)

1.4.1 Device Equivalency Claims

Many Samsung devices share common capabilities in different form factors, and Samsung provides common capabilities, including support for the configurations necessary for the evaluation on these devices. The following table shows the devices for which equivalence is being claimed from a device that is explicitly evaluated.

Evaluated Device	Processor	Equivalent Devices	Differences
Galaxy Note10+ 5G (Samsung)	Exynos 9825	Galaxy Note10+ (Samsung) Galaxy Note10 5G (Samsung) Galaxy Note10 (Samsung)	• Note10+ devices have larger screen • 5G devices had different cellular modem
Galaxy S10e (Samsung)	Exynos 9820	Galaxy S10 (Samsung) Galaxy S10+ (Samsung) Galaxy S10 5G (Samsung)	• S10 & S10+ have ultrasonic fingerprint sensor • S10 & S10+ have larger screen sizes • S10 5G has different cellular modem
Galaxy S10+ (Qualcomm)	SM8150	Galaxy S10e (Qualcomm) Galaxy S10 (Qualcomm) Galaxy S10 5G (Qualcomm) Galaxy Fold (Qualcomm) Galaxy Note10 (Qualcomm) Galaxy Note 10+ (Qualcomm) Galaxy Note10+ 5G (Qualcomm) Galaxy Tab S6	• S10e & Fold has side image fingerprint sensor • S10 & S10e have smaller screen sizes • Fold has 2 screens • Note10 & Note10+ have larger screen sizes • S10 & Note10+ 5G has different cellular modem • Note10 devices include S Pen & functionality to take advantage of it for input (not security related) • Tab S6 (T86x) is tablet form factor (no voice calling) with S Pen • T865 & T867 tablets have LTE • T860 tablets only have Wi-Fi
Galaxy S9+ (Samsung)	Exynos 9810	Galaxy S9 (Samsung) Galaxy Note9 (Samsung) Galaxy XCover FieldPro	• S9 has smaller screen • Note9 includes S Pen & functionality to take advantage of it for input (not security related) • XCover FieldPro is smaller, has hardened shell, removable battery, Push-to-Talk button

Evaluated Device	Processor	Equivalent Devices	Differences
Galaxy S9+ (Qualcomm)	SDM845	Galaxy S9 (Qualcomm) Galaxy Note9 (Qualcomm)	• S9 has smaller screen • Note9 includes S Pen & functionality to take advantage of it for input (not security related)
Galaxy Tab S4 (T837A)	Snapdragon 835	Galaxy Tab S4	• T835 & T837 models have LTE T830 models only have Wi-Fi
Galaxy Note8 (Samsung)	Exynos 8895	Galaxy S8 (Samsung) Galaxy S8+ (Samsung)	• S8 & S8+ do not include S Pen • S8 & S8+ are smaller
Galaxy Note8 (Qualcomm)	MSM8998	Galaxy S8 (Qualcomm) Galaxy S8+ (Qualcomm) Galaxy S8 Active (Qualcomm) Galaxy Tab S4 (All)	• S8, S8+ & S8 Active do not include S Pen • S8, S8+ & S8 Active are smaller • S8 Active has a IP68 & MIL-STD-810G certified body • Tab S4 (T83x) is tablet form factor (no voice calling) • T835 & T837 tablets have LTE • T830 tablets only have Wi-Fi
Galaxy Tab S3 (T825Y)	MSM8996	Galaxy Tab S3	• T835 & T837 models have LTE • T830 models only have Wi-Fi
Galaxy Tab Active2 (T397)	Exynos 7870	Galaxy Tab Active2	• T390 & T397 models have 32GB of storage, T395 has 16GB • T395 & T397 models have LTE

Table 2 - Device Equivalence

The differences between the evaluated devices and the equivalent ones do not relate to security claims in the evaluated configuration. The Wi-Fi chipsets are the same for each series of common devices.

1.4.2 Device Details

The model numbers and evaluated versions of the mobile devices being claimed are as follows:

Device Name	Base Model Number	Android Version	Kernel Version	Build Number	Carrier Models
Galaxy Note10+ 5G (Samsung)	SM-N976	9.0	4.14.113	PPR1.180610.011	B, N
Galaxy Note10+ 5G (Qualcomm)	SM-N976	9.0	4.14.85	PPR1.180610.011	U, V
Galaxy Note10+ (Samsung)	SM-N975	9.0	4.14.113	PPR1.180610.011	F
Galaxy Note10+ (Qualcomm)	SM-N975	9.0	4.14.85	PPR1.180610.011	C, U, SC-01M*, SCV45*
Galaxy Note10 5G (Samsung)	SM-N971	9.0	4.14.113	PPR1.180610.011	N
Galaxy Note10 (Samsung)	SM-N970	9.0	4.14.113	PPR1.180610.011	F
Galaxy Note10 (Qualcomm)	SM-N970	9.0	4.14.85	PPR1.180610.011	U

Device Name	Base Model Number	Android Version	Kernel Version	Build Number	Carrier Models
Galaxy Tab S6	SM-T867	9.0	4.14.85	PPR1.180610.011	R4, U, V
	SM-T865	9.0	4.14.85	PPR1.180610.011	N, None
	SM-T860	9.0	4.14.85	PPR1.180610.011	None
Galaxy S10 5G (Samsung)	SM-G977	9.0	4.14.85	PPR1.180610.011	B, N
Galaxy S10 5G (Qualcomm)	SM-G977	9.0	4.14.78	PPR1.180610.011	P, T, U
Galaxy S10+ (Samsung)	SM-G975	9.0	4.14.85	PPR1.180610.011	F, N
Galaxy S10+ (Qualcomm)	SM-G975	9.0	4.14.78	PPR1.180610.011	U, SC-04L*, SCV42*
Galaxy S10 (Samsung)	SM-G973	9.0	4.14.85	PPR1.180610.011	F, N
Galaxy S10 (Qualcomm)	SM-G973	9.0	4.14.78	PPR1.180610.011	U, SC-03L*, SCV41*
Galaxy S10e (Samsung)	SM-G970	9.0	4.14.85	PPR1.180610.011	F, N
Galaxy S10e (Qualcomm)	SM-G970	9.0	4.14.78	PPR1.180610.011	U
Galaxy Fold	SM-F900	9.0	4.14.78	PPR1.180610.011	F, N, U, SC-06L*, SCV44*
Galaxy Note9 (Samsung)	SM-N960	9.0	4.9.59	PPR1.180610.011	F, N
Galaxy Note9 (Qualcomm)	SM-N960	9.0	4.9.112	PPR1.180610.011	U, SC-01L*, SCV40*
Galaxy XCover FieldPro	SM-G889	9.0	4.9.59	PPR1.180610.011	A
Galaxy Tab S4	SM-T830	9.0	4.4.153	PPR1.180610.011	None
	SM-T835	9.0	4.4.153	PPR1.180610.011	N, None
	SM-T837	9.0	4.4.153	PPR1.180610.011	A, R4, P, V, T
Galaxy S9+ (Samsung)	SM-G965	9.0	4.9.59	PPR1.180610.011	F, N
Galaxy S9+ (Qualcomm)	SM-G965	9.0	4.9.112	PPR1.180610.011	U, SC-03K*, SCV39*
Galaxy S9 (Samsung)	SM-G960	9.0	4.9.59	PPR1.180610.011	F, N
Galaxy S9 (Qualcomm)	SM-G960	9.0	4.9.112	PPR1.180610.011	U, SC-02K*, SCV38*
Galaxy Note8 (Samsung)	SM-N950	9.0	4.4.111	PPR1.180610.011	F, N
Galaxy Note8 (Qualcomm)	SM-N950	9.0	4.4.153	PPR1.180610.011	U, SC-01K*, SCV37*

Device Name	Base Model Number	Android Version	Kernel Version	Build Number	Carrier Models
Galaxy S8+ (Samsung)	SM-G955	9.0	4.4.111	PPR1.180610.011	F, N
Galaxy S8+ (Qualcomm)	SM-G955	9.0	4.4.153	PPR1.180610.011	U
Galaxy S8 (Samsung)	SM-G950	9.0	4.4.111	PPR1.180610.011	F, N
Galaxy S8 (Qualcomm)	SM-G950	9.0	4.4.153	PPR1.180610.011	U
Galaxy S8 Active	SM-G892	9.0	4.4.153	PPR1.180610.011	A, U
Galaxy Tab S3	SM-T827	9.0	3.18.31	PPR1.180610.011	V, A, R4
	SM-T825	9.0	3.18.31	PPR1.180610.011	N, Y, None
	SM-T820	9.0	3.18.31	PPR1.180610.011	None
Galaxy Tab Active2	SM-T397	9.0	3.18.14	PPR1.180610.011	U
	SM-T395	9.0	3.18.14	PPR1.180610.011	N, None
	SM-T390	9.0	3.18.14	PPR1.180610.011	None

Table 3 - Device Details

The Carrier Models column specifies the specific versions of the devices that have the validated configuration. These additional letters/numbers denote carrier specific models (such as U = US Carrier unified build). Only models with the suffixes listed in the table can be placed into the validated configuration. The carrier models marked by * are explicit model numbers for those carriers and do not follow the standard specified for other models.

The following table shows the Security software versions for each device.

Device Name	MDF Version	MDF Release	WLAN v1.0 Release	VPN PP-MOD v2.1 Release	Knox Release
Note10+ 5G, Note10+, Note10 5G, Note10, Tab S6	3.1	4	2	2.0	3.4
S10 5G, S10+, S10, S10e, Fold, Tab S4	3.1	4	2	2.0	3.3
Note9, XCover FieldPro, S9+, S9, Note8, S8+, S8, S8 Active, Tab S3, Tab Active2	3.1	4	2	2.0	3.2.1

Table 4 - 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 S10 would show “MDF v3.1 Release 4”.

The following table shows the biometric modalities supported on each type of device. All versions of a device will have the same supported modalities.

Device	Fingerprint	Iris
Galaxy Note10 (all versions)	X	
Galaxy S10 (all versions)	X	
Galaxy Tab S6	X	
Galaxy Fold	X	
Galaxy Note9	X	X
Galaxy XCover FieldPro	X	
Galaxy Tab S4		X
Galaxy S9 (all versions)	X	X
Galaxy Note8	X	X
Galaxy S8 (all versions)	X	X
Galaxy S8 Active	X	X
Galaxy Tab S3	X	
Galaxy Tab Active2	X	

Table 5 - Supported Biometrics

1.4.3 Android 9 Encryption Changes

The Galaxy S10 5G/S10+/S10/S10e/Fold/Note10+ 5G/Note10+/Note10 5G/Note10/Tab S6 devices support Direct Boot and File-Based Encryption (FBE) instead of On-Device Encryption (ODE) as supported on earlier devices. FBE and Direct Boot allows an encrypted device to boot straight to the Android lock screen where it is possible to receive calls and for FBE-aware apps can provide notifications prior to authentication.

1.5 References

The following websites provide up to date information about Samsung device certifications.

Site	Information	URL
Samsung Knox Portal	Common Criteria documentation, Application Version List, Tools	https://support.samsungknox.com/hc/en-us/articles/115015195728
Samsung Knox SDK	Samsung Knox developer guides including EDM APIs	https://seap.samsung.com/sdk/knox-android/developer-guides
Galaxy S Device Support	Manuals & User Guides for Galaxy S devices	https://www.samsung.com/us/support/mobile/phones/galaxy-s
Galaxy Note Device Support	Manuals & User Guides for Galaxy Note devices	https://www.samsung.com/us/support/mobile/phones/galaxy-note
Galaxy Tablet Device Support	Manuals & User Guides for Galaxy Tab devices	https://www.samsung.com/us/support/mobile/tablets/galaxy-tabs
Galaxy Tab Active2 Support	Manuals & User Guides for Galaxy Tab Active2 devices (downloads)	https://www.samsung.com/us/business/support/mobile/tablets/galaxy-tab-active2/
NIAP	Product Compliant List for Samsung Electronics	https://www.niap-ccevs.org/Product/PCL.cfm?par303=Samsung%20Electronics%20Co%2E%2C%20Ltd%2E
	Approved Protection Profiles	https://www.niap-ccevs.org/Profile/PP.cfm
NIST CMVP	Validated Cryptographic Modules (search for Samsung)	https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search
NIST CAVP	Validated Cryptographic Algorithms	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program
NIST SP 800-63B	NIST SP 800-63B Digital Identity Guidelines	https://pages.nist.gov/800-63-3/sp800-63b.html

Table 6 – Reference Websites

2 Mobile Device Deployment

2.1 Device Overview

The TOE is a mobile operating system based on Android with modifications made to increase the level of security provided to end users and enterprises. The TOE is intended for use as part of an enterprise messaging solution providing mobile staff with enterprise connectivity.

The TOE combines with an EDM solution that enables the enterprise to watch, control and administer all deployed mobile devices, across multiple mobile service providers as well as facilitate secure communications through a VPN. This partnership 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.

2.2 Evaluated Device Capabilities

The product provides a significant amount of security capabilities with the core capabilities being included within the common criteria evaluation including:

Security Feature	Description
Device data protection. The TOE provides security functionality to protect data at rest.	**File-Based Encryption (FBE) and On-Device Encryption (ODE).** The TOE has the ability to encrypt data on the device using AES 256.
	Removable storage encryption. The TOE can encrypt all file placed onto, or already reside on, removable storage attached to the device.
	Sensitive data protection. The TOE has the ability to securely store incoming data that is considered sensitive such that it can't be decrypted without the user logging in.
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 TOE can be configured to lock automatically after a defined period of inactivity (1 to 60 minutes) limiting access to device functions accept those that are explicitly authorized such as emergency calls.
	Local wipe. The TOE has the ability to wipe encryption keys/data on a device after a defined number of authentication attempts are surpassed.
	Credential complexity. The TOE can enforce enterprise password policies forcing users to use a defined level of complexity in device passwords.
	Biometrics Use. The TOE can provide biometric authentication for access to the device complementary to password policies, restricting access based on failed attempts.

Security Feature	Description
	Privileged access. The TOE can be configured to restrict mobile user's access to privileged functions such as device configurations.
	Hotspot Control. The TOE can be configured to act as a hotspot for sharing Internet access to other devices.
	Wireless network settings. The wireless network configuration of the TOE 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 TOE to wipe all local storage and the SD card.
	Security policy. The TOE can be configured by an EDM solution that supports the Samsung Enterprise SDK.
	Auditing. The TOE can monitor and generate records related to security-relevant events within the device.

Table 7 – Device Security Features

2.3 Deployment Architecture

The first step in deploying Samsung devices is to decide on both an EDM solution and an appropriate architecture. These selections are beyond the scope of this guidance. There are many approaches to how the management infrastructure can be configured, from on premise servers to cloud to hybrid approaches combining the two. The specifics of the architecture should be discussed with the EDM solution vendor.

Ideally, the deployed EDM solution should be evaluated to the requirements of the Protection Profile for Mobile Device Management (MDMPP).

2.3.1 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 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.

Component	Description
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 to the 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 8 – Enterprise Deployment Component Services

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

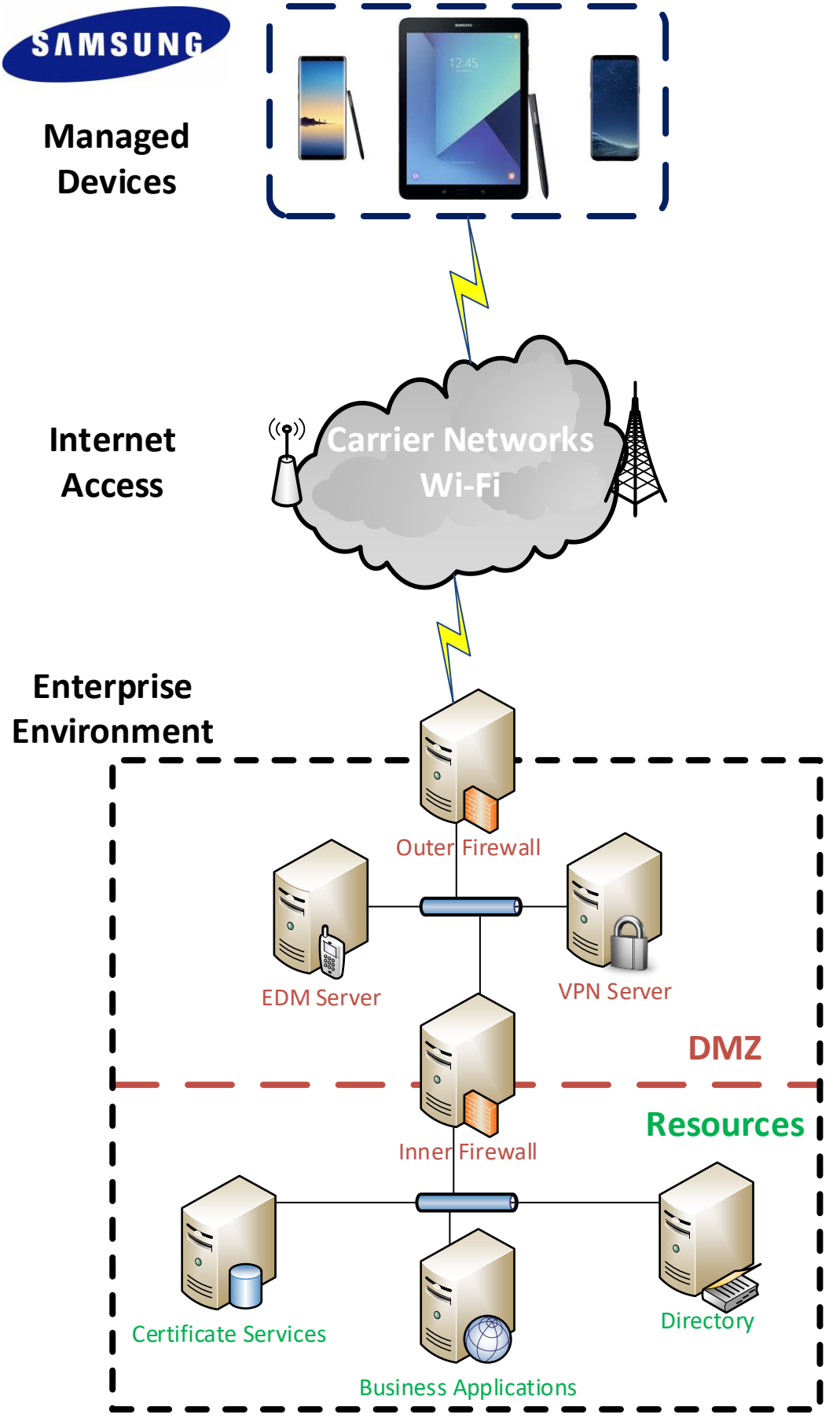

Figure 1 - Example Enterprise Architecture

2.3.2 EDM Solution Selection

To manage the mobile devices, an EDM must be deployed. This EDM should support the Samsung Knox APIs to enable the capabilities documented in this guide. The more complete the EDM vendor support, the more capabilities can be controlled on the device.

To enable capabilities such as remote wipe of a device, the EDM must be placed within the Enterprise environment such that it can communicate over the internet. This communication can be enabled with or without a VPN, though it is normally recommended to have EDM traffic outside the VPN to ensure access is most widely available to the device.

When selecting an EDM solution, care should be taken to ensure the ability to configure the Common Criteria configuration. The Common Criteria Configuration section provides the specific information about the Knox APIs that are necessary to support this configuration and can be used to check the compatibility of the EDM solution with the needs of the Enterprise.

2.4 Provisioning of Samsung Devices

As noted above, the secure deployment of enterprise devices is reliant on many components beyond the mobile device itself. It is expected that within the Enterprise environment the EDM solution and other required services are securely installed and configured according to the security requirements of the organization.

Once the EDM is installed and available, it is possible to begin provisioning end user devices. The provisioning process will prepare the devices for a policy configuration to be deployed, enabling the device to be placed into a Common Criteria configuration.

The mobile device must be enrolled with the EDM server to enable administration via the EDM. Enrollment is accomplished by installing the EDM Agent application onto the device. There many methods and configurations for doing this depending on the deployment scenario. The EDM documentation for deployment should be followed.

Once a device has been enrolled to the EDM, other optional configurations may be set, depending on the organization security policy. These are not required to place the device into a Common Criteria configuration, but are best practices for mobile devices.

NOTE: Configurations that are included as part of the controls for the Common Criteria configuration are not included here.

The following list provides some of the most common additional configuration items that may be done on a mobile device:

- Install applications required for enterprise productivity
- Provision client certificates by either:
    - Using the EDM server;
    - Using the Android Development Tools (ADT) to manually push certificates to each device via USB
        - Using the Android Debug Tool (ADB) required USB debugging to be enabled on the device for provisioning of the certificates (it can be disabled once this operation is complete)

    - Placing the certificates on a microSD card and import using the device user interface
    - The certificates commonly deployed are:
        - Enterprise CA certificate (used to validate the server certificates presented by the VPN endpoint and reverse proxy)
        - Wi-Fi client certificate (for authentication to an EAP-TLS Wi-Fi AP)
        - VPN client certificate (for authentication to the enterprise VPN endpoint)
        - SSL client certificate (for authentication to the reverse proxy for intranet services)
- Configure the VPN client to connect to the enterprise VPN endpoint
    - Enable 'Always-On' VPN
- Configure the email client to connect to the enterprise server

2.4.1 Knox Workspace Configurations

Through the Knox Platform, Samsung devices include an integrated capability to configure the device for an enterprise environment with Knox Workspace. A Knox Workspace can be configured for a whole device or with a Knox Workspace container. When a Knox Workspace container is configured, it provides a segmented area on the device that can have its own apps and data that is not accessible from the "normal" area (sometimes called the "personal" side of the device). The Knox Workspace container can be used to separate different apps and data, such as in a BYOD scenario where an enterprise could manage their own data in a separate Workspace container on the user's device.

A Samsung device can be placed into an evaluated configuration both with and without a Knox Workspace container being configured on the device. For organizations that do not need to segment the device, a configuration can be used without creating a Knox Workspace container. For organizations that have a need for data separation, a Knox Workspace can be created and still be in an evaluated configuration.

3 Common Criteria Configuration

This section of the guide will list the configuration settings that are reviewed as part of the Common Criteria evaluation. Some of these settings are required for the device to be placed into a validated configuration while others are optional and can be used at the discretion of the organization and the attendant security policies.

3.1 Approved 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 Kernel Cryptographic Module
- Samsung BoringSSL 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 section 5 Developer References.

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.

3.2 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.

3.2.1 CC Mode Status

CC Mode has three possible states:

Status	Description
Ready	The conditions for CC Mode have not been met
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 9 – 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***. The only status mark shown here is Disabled (an error has occurred); there is no shown status for any other state.

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.

3.3 Common Criteria Settings

This section will lay out all the settings which are mandatory as part of the MDF-validated configuration.

The settings have been grouped into categories as well as marked with applicability based on the following table.

Applicability	Description
Device	These APIs are only applied to the device as a whole and cannot be applied to the Knox Workspace
All	These APIs can be applied to both the device or the Knox Workspace
Workspace	These APIs are only applicable to the Knox Workspace
Knox	These APIs are applicable to the Knox Platform for Enterprise (KPE) and can be applied to the device or Workspace depending on the configuration

Table 10 – API Applicability

A Knox Workspace implements many of the same APIs as are available to the device (such as hardware state configurations). Policies in Knox Workspace are tied specifically to the Workspace as part of the Knox

Platform API configuration. All Knox APIs specified are part of the Knox Platform for Enterprise (KPE) set of APIs and require a Knox Platform for Enterprise license to be used.

Note: While most of the APIs listed here are part of the Knox SDK, some APIs come from the Android Device Management set. The APIs from native Android are *italicized*.

The settings have also been marked as mandatory or objective (or in the case of CC Mode, Always).

All the settings are included in the attached spreadsheet.


Settings Table.xlsx

3.3.1 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:

1. Set Password Quality
2. Enable the Maximum Password Failure Wipe Policy
3. Enable SD Card Encryption
4. Enable CRL Checking
5. Disable Password History

If a Microsoft Exchange ActiveSync account will be deployed and configured for client management:

1. Password Recovery must be disabled (or not configured)

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

1. Disable Face Lock

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

1. Set a Password
2. Enable Secure Startup (not applicable on S10 5G/S10+/S10/S10e/Fold/Note10+ 5g/Note10+/Note10 devices)
3. Enroll biometrics (if enabled)

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; a user can only turn off CC Mode by choosing to perform a factory reset.

3.3.1.1 Microsoft® Exchange ActiveSync Settings

Many environments use Microsoft® Exchange Server and along with that use ActiveSync to manage policies related to access to the Exchange Server. For environments using ActiveSync (EAS) policies to perform some device management, the Password Recovery setting must be disabled (set to False) or not configured.

3.3.1.2 Application White/Black Listing Settings

White/Black listing is done using the full name of the application (such as com.android.testingapp).

The application removal process will automatically clear data associated with the application stored in the application directories. Data created or stored outside the application directories (such as photos by a camera application or documents created by a word processor) will not be removed when the application is uninstalled.

The method for configuring these lists is highly dependent on the EDM solution chosen. Please refer to the EDM specific guidance on exactly how to set these policies.

Note: The Application White/Black lists will not have any impact on apps that are part of the system image. Built-in apps can instead be Disabled.

3.4 End User Procedures

While the administrator can configure the device, the end user of the device will interact with the resulting configuration. Specific instructions about procedures for an end user can be found in the support links in section 1.5 References. There the user can specifically select their device and have tailored usage instructions.

3.4.1 User Authentication

When allowed, a user will be able to enroll fingerprint or iris biometrics for use at the lock screen as an alternative to entering a password. Detailed instructions for configuring these methods can be found under the “Secure” or “Security” section of the guide for the specific device. Information about setting up the Screen Lock, fingerprint and iris will be listed separately.

3.4.1.1 Setting Passwords

Passwords and biometrics are available (depending on the configuration) for use to prevent unauthorized access to the device. A user must always have a password set for authentication, and this password should never be shared with anyone. Recommendations for setting strong passwords can be found in NIST SP 800-63B, section 5.1.1, Memorized Secrets.

3.4.1.2 Two-step Verification

When the Workspace is configured for Two-step verification (also called multi-factor or hybrid authentication), the user must provide both a biometric and password to login successfully. The user will see a new option in the Screen Lock Type that will allow the user to configure both components of the authentication credentials.

When the Two-step verification is selected, the user will be prompted to choose the first lock type, which will be a Password. Once the password has been entered, the user will be prompted to enter a biometric from those available for use (fingerprint or iris). If the biometric has not yet been registered, the user will be prompted to re-enter the password before continuing to register the biometric.

The process for entering the password or registering a biometric in the same manner as when used individually (specified in 3.4.1 User Authentication). The Two-step verification process provides a wizard to register both components at once.

3.4.2 Wi-Fi Connectivity

While the administrator may pre-configure some Wi-Fi networks via the EDM, the user has local control over the Wi-Fi connectivity of the device, including the ability to enable/disable Wi-Fi and to connect/reconnect to networks. Detailed instructions for connecting to Wi-Fi networks can be found under the “Connections” section of the guide for the specific device.

Wi-Fi connections can sometimes be dropped (such as when moving out of range). Generally, the device will automatically reconnect to the network once in range, but when this does not happen, following the steps used to establish a new connection by selecting the available network would start the reconnection. This process will not require re-entry of any configuration information but will start the connection using the configuration already stored.

3.4.3 Bluetooth Connectivity

When connecting your device to various other Bluetooth devices it is important to be sure they are properly paired. Some peripherals have no interface for pairing (such as headphones or mice) while others do (such as another smart device or your car). A key difference between these types of devices is whether information can be transferred to them. For example, while you can talk or listen through a Bluetooth headset, it does not store data. Connections to devices that support data transfer capabilities must always be paired explicitly before any use of functionality between them.

Detailed instructions for pairing Bluetooth devices can be found under the “Connections” section of the user guide for the specific device or in the Interactive Guide under “Connections -> Connect to Bluetooth Devices”.

3.4.4 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 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 new 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.

3.4.5 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.

3.5 VPN Client Configurations

Samsung devices includes a built-in VPN client and can support third-party VPN clients.

3.5.1 VPN Configuration (Device)

The built-in Samsung VPN client can be configured for use by the whole device. More information about the specific management APIs can be found in the Samsung VPN Client on Galaxy Devices Guidance Documentation v5.0.

3.5.2 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.

3.5.3 Knox VPN Services (All)

Samsung Knox provides 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 Workspace, depending on where the VPN client is installed (inside or outside the Workspace).

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 11 – 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://seap.samsung.com/api-references/android-premium/reference/com/sec/enterprise/knox/profile_creation.pdf.

With the Knox Platform for Enterprise, VPN configurations can be created for individual apps, groups of apps or Workspace containers. It is possible to set multiple VPN configurations in parallel for different apps or groups of apps. It is also possible to configure dual layer VPN tunnels by using one VPN outside the Workspace paired with a Knox containerized VPN. These Methods are all part of the GenericVpnPolicy Class.

Setting	Value	Description	Class or Method
Create VPN Profile	VPN Vendor, json file	Specifies the VPN client vendor and the json configuration file	createVpnProfile()
Active VPN Profile	Enable/ Disable Profile	Specifies to activate or deactivate VPN profile	activateVpnProfile()
Remove VPN Profile	VPN profile	Deletes VPN profile	removeVpnProfile()
Add Apps to VPN	Package names	Adds apps to VPN profile such that these apps must use this VPN profile for connectivity	addPackagesToVpn() addAllPackagesToVpn()
Add Apps to Workspace VPN	Package names	Adds apps to Workspace VPN profile such that these apps must use this VPN profile for connectivity	addContainerPackagesToVpn() addAllContainerPackagesToVpn()
Remove Apps to VPN	Package names	Removes apps from VPN profile	removePackagesFromVpn() removeAllPackagesFromVpn()
Remove Apps to Workspace VPN	Package names	Removes apps from Workspace VPN profile	removeContainerPackagesFromVpn() removeAllContainerPackagesFromVpn()

Table 12 – Knox VPN Service Settings

Note: When adding packages to a VPN profile, use User0 for the whole device and User100 for the Knox Workspace.

3.6 Additional Common Criteria Features

3.6.1 Sensitive Data Protection

Samsung has added capabilities for Sensitive Data Protection. This feature is designed to allow applications that run in the background and receive information to protect that information upon receipt. This feature is provided as part of the device, but its use is dependent on applications having been written to the APIs providing the capability. It is expected that this list will grow over time, but is currently limited to the Samsung Email application contained within the Knox Workspace.

The API for Sensitive Data Protection exists for different Knox Platform configurations, but unless an application has been written to the API, it will not take advantage of the Sensitive Data Protection function.

3.6.2 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 (see EDM guidance).

4 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 unenrollment process, so any events created between the last review/upload and the unenrollment will be lost.

4.1 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.

4.2 Audit Collection Settings

All methods are in the class com.samsung.android.knox.log.

Setting	Value	Description	Class or Method
Enable Auditing	-	Enables audit collection	enableAuditLog()
Disable Auditing	-	Disables audit collection	disableAuditLog()
Configure Logging Filters	See Filter Settings table	Configures what events to be captured (see Filter table)	setAuditLogRules()
Enable IP Tables Auditing	-	Enables the collection of IP Tables	enableIPTablesLogging()
Disable IP Tables Auditing	-	Disables the collection of IP Tables	disableIPTablesLogging()

Table 13 – Audit Settings

4.2.1 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 Knox Workspace (inside the Workspace the EDM can only see the Workspace user). System events (UID 2) are always logged regardless of any specific selections made by the administrator.

Table 14 – Audit Collection Filter Settings

4.3 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 100-102 is for Workspace users (multiple Workspaces can be defined)
Component	String representing the facility/Software Component name

Setting	Description
Message	Free-form message description of the event (generally a human-readable message)

Table 15 – Audit Fields

4.4 Audit Events

The list of audit records that are produced related to the functionality claimed in the MDFPP are listed in the attached spreadsheet. The Event column shows what the audit record that is generated, where the information in the <> may vary (such as the status of the setting being measured, or the value being reported). The Description column describes the audit record and may provide additional information about fields that may be displayed.

Audit Event Table.xlsx

The events categorized with Common Criteria Status are generated when CC Mode is first enabled and on every device boot sequence thereafter. These events will not be generated again if CC Mode is called, but will only occur during the boot sequence. If the check being made passes, the status will be OK. Otherwise, the message will show corrective actions to be taken.

Most of the management functions for the Workspace (such as password management or camera access) generate the same messages as outside the Workspace. The messages inside the Workspace will be marked with the container ID (usually 10 or 100 depending on the device).

5 Developer References

5.1 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
Key Import, Use, Destruction	javax.crypto.KeyGenerator java.security.KeyPairGenerator java.security.KeyStore android.security.KeyChain	developer.android.com developer.android.com

Table 16 – 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).

5.2 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.

5.3 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.

5.4 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.

5.5 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 Enterprise Alliance Program (SEAP).

6 Device Delivery and Updates

6.1 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)

6.1.1 Evaluation Version

There are a number of components to 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 section 1.4.2 Device Details.

6.1.2 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. For a list of the apps and their versions contained on a specific device, visit the website where you can download the CC Mode app and select the device you are using. This will provide a complete list of the software installed on the evaluated device.

6.1.2.1 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.

6.2 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 S9 on Verizon will not have an update signed with the same key as a Galaxy S9 on AT&T). 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.

6.2.1 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.

6.2.2 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.

7 Operational Security

7.1 Modes of Operation

The TOE 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 TOE 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 he 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 TOE 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.

7.2 Wiping Data

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

An enterprise initiated remote wipe command (for either the device or just the Knox Workspace, 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.

7.2.1 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 Knox Workspace configuration, this will wipe all data including the Knox Workspace (as well as everything not in the Workspace). 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.

7.2.2 Wiping the Knox Workspace

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

The only way for a user to wipe the Knox Workspace is to unenroll the device from the control of the EDM. When this is done the Knox Workspace, all data and apps as well as the EDM Agent will all be removed from the device.

7.3 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 TOE Administrators are trusted to follow and apply all administrator guidance, including the EDM guidance in a trusted manner.