SAMSUNG

Administrator Guide

Samsung File Encryption 1.6.0

March 1, 2024

Version: 1.6

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 File Encryption Admin Guidance v1.6.0
Document Title	Samsung File Encryption 1.6.0 Administrator Guide

Contents

1 Introduction

1.1 Scope of Document

This document is intended as a guide for administrators deploying Samsung File Encryption in the enterprise. The guidance provided here focuses on how to configure devices to be in an approved configuration based on the PP-Module for File Encryption 1.0 (and the Protection Profile for Application Software Version 1.4) for the functionality specified here.

The document is evolutionary. It will cover all devices evaluated with a common major version of the Knox File Encryption software.

1.1.1 End-User Guidance

This guidance document is focused on the deployment of Knox File Encryption. Guidance related to user functions on a device, such as managing Bluetooth connections or setting authentication credentials are outside the scope of this documentation as they are part of the device configuration on which Knox File Encryption relies. 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 and the software bundled with them 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 Knox File Encryption 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
API	Application Programming Interface
BYOD	Bring Your Own Device

Evaluated Device	Processor
COPE	Corporately-Owned, Personally Enabled
EDM MDM	Enterprise Device Management Mobile Device Management NOTE: EDM will be used for consistency
FOTA	Firmware Over-the-Air
KPE	Knox Platform for Enterprise
SDK	Software Development Kit

Table 1 - Acronyms

1.4 Evaluated Devices & Software

The Common Criteria evaluation was performed on a set of devices covering a range of processors.

The evaluation was performed on the following devices;

Device Name	Model Number	Chipset Vendor	CPU	Android Version	TEE OS	Knox Version	DualDAR Version	Evaluation
Galaxy S24 Ultra 5G	SM-S928	Qualcomm	Snapdragon 8 Gen 3 (SM8650)	14	QSEE 6.1	3.10	1.6.0	Spring 2024
Galaxy S24 Ultra 5G	SM-S928	Samsung	Exynos 2300	14	TEEGRIS 5.0.0	3.10	1.6.0	Spring 2024
Galaxy S23 Ultra 5G	SM-S918U	Qualcomm	Snapdragon 8 Gen 2 Mobile Platform	14	QSEE 5.24	3.10	1.6.0	Spring 2024
Galaxy S22 Ultra 5G	SM-S908B	Samsung	Exynos 2200	14	TEEGRIS 4.2.1	3.10	1.6.0	Spring 2024
Galaxy S22 5G	SM-S908U	Qualcomm	Snapdragon 8 Gen 1 Mobile Platform	14	QSEE 5.16	3.10	1.6.0	Spring 2024
Galaxy S21 Ultra 5G	SM-G998B	Samsung	Exynos 2100	14	TEEGRIS 4.2	3.10	1.6.0	Spring 2024
Galaxy S21 Ultra 5G	SM-G998U	Qualcomm	Snapdragon 888	14	QSEE 5.11	3.10	1.6.0	Spring 2024
Galaxy XCover6 Pro	SM-G736	Qualcomm	Snapdragon 778G(SM7325)	14	QSEE 5.11	3.10	1.6.0	Spring 2024
Galaxy Tab Active5	SM-X300	Samsung	Exynos1380	14	TEEGRIS 5.0.0	3.10	1.6.0	Spring 2024

1.4.1 Application Version Details

The following table shows the Security software versions on devices supporting Knox File Encryption.

Device SoC	Version
Android Version	14
Knox Version	3.10
DualDAR Version	1.6.0

Table 2 - Security Software Versions

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://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/common-criteria-mode.htm
Samsung Knox SDK	Samsung Knox developer guides including EDM APIs	https://docs.samsungknox.com/dev/knox-sdk/index.htm
Samsung Knox MDM SDK	Samsung Knox guides for managing File Encryption	https://docs.samsungknox.com/devref/knox-sdk/reference/com/samsung/android/knox/ddar/package-summary.html
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
Knox Work Profile Guide	DualDAR with work profiles	https://docs.samsungknox.com/admin/knox-platform-for-enterprise/dualdar-for-wpc.htm?Highlight=dualdar
	DualDAR Encryption white paper	https://docs.samsungknox.com/admin/whitepaper/kpe/DualDAR.htm?Highlight=dualdar
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 SP 800-63B	NIST SP 800-63B Digital Identity Guidelines	https://pages.nist.gov/800-63-3/sp800-63b.html

Table 3 – Reference Websites

2 Samsung Knox File Encryption Deployment

2.1 Overview

Samsung Knox File Encryption is a software service designed to provide a second layer of encryption to files stored on the device independent of the default file encryption for the device. Depending on how Knox File Encryption is enabled, it can encrypt all files on the device or only those contained within the work profile.

The Knox File Encryption service runs in the background and utilizes the Samsung Android cryptographic modules included in the platform to provide file encryption services. The service is designed to run without any user intervention and all files (as determined by the configuration) will be encrypted automatically. It is an integrated component of the device image, and is not a separately installed app.

Knox File Encryption supports defining the set of files to be encrypted in two configurations: work profile or whole device. Note in the current evaluation, all devices use the work profile. When configured for the work profile, all files stored inside the work profile will be automatically encrypted. When configured for the whole device, all user files will be automatically encrypted (some Android and critical service files are not encrypted to allow the device to work, but these files do not contain user data).

Knox File Encryption is designed as a framework which can be used for the Knox work profile or the whole device. Through this service, all files (per the configuration) that are read or written when Knox File Encryption is enabled will be filtered and encrypted/decrypted automatically. The service does not require the user or any apps to be aware of the service, only that Knox File Encryption to be enabled for the work profile or device. The service provides the ability to fully clear and close all open apps after a defined timeout period.

The Knox File Encryption service relies on the Android EDM APIs to provide management.

The Knox File Encryption service is built on the Samsung Software Development Kit (SDK). It is possible for a third party to utilize this SDK to integrate into the File Encryption service to provide separate cryptographic modules used to protect the files encrypted by the service. Installation and management of these third party integrations are handled by the developer of the add-on component.

2.2 Deployment

The deployment of Knox File Encryption is tied to the deployment of a device. When creating a Knox work profile, the administrator must select the DualDAR option to enable Knox File Encryption. When configuring the whole device, it must be enabled during the initial device configuration. Note in the current evaluation, all devices use the work profile. This is the only step necessary to activate Knox File Encryption on a supported Samsung device.

The specific details of the EDM solution and options are outside the scope of this document, the EDM guidance will provide specific information about configuring a Knox work profile.

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

2.2.1 EDM Solution Selection

To manage Knox File Encryption, an EDM must be deployed. This EDM should support the Samsung Knox APIs to enable the capabilities documented in this guide.

Once Knox File Encryption has been enabled on a device by the EDM, the user must follow any further steps (such as setting a password) to complete the configuration. Knox File Encryption Configuration

This section of the guide will list the configuration settings that are reviewed as part of the Common Criteria evaluation.

2.3 File Encryption Settings

This section specifies the settings that must be configured to enable Knox File Encryption. This flag is set when the device management is configured. If the work profile will be created, then the Intent to create a managed profile must be this constant specified. If the device will be fully managed, then the Intent to set the device configuration must have this constant specified. In either case, this must be done during the initial configuration, it cannot be added later.

All settings here are based on the Class com.samsung.android.knox.ddar.DualDARPolicy.

Setting	Value	Description	Method() or Constant
Enable File Encryption	Enable	When this is set, the work profile will be created with File Encryption enabled	KEY_DUAL_DAR_CONFIG

Table 4 - Mandatory File Encryption Settings

Note: The configuration to enable File Encryption can only be set during the creation of the Knox work profile. Once a work profile has been created, the File Encryption setting is fixed (either on or off).

2.3.1 Optional Configuration Settings

In addition to the mandatory configuration to enable File Encryption, the administrator can also configure the following optional settings.

Setting	Value	Description	Method() or Constant
Data Lock Timeout	1 or 5 min	Specifies how long after the device has been locked to enter the Data Lock state (where all File Encryption keys are cleared) Note: For Managed Profiles -Admin can configure a timeout from 1 minute to infinity (-1 for infinity). For Managed Devices-Admin can configure a timeout from 5 minutes to infinity (-1 for infinity). .	KEY_CONFIG_DATA_LOCK_TIMEOUT

Table 5 - Optional File Encryption Settings

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.

2.3.2 Whole Device Password Settings

In the whole device configuration (not used on any devices listed in 1.4), the File Encryption password settings use the device password settings, so the type of password and any restrictions on it, will be matched for the File Encryption password. The administrator can configure a different minimum length for the File Encryption.

In addition to setting a different minimum password length, the administrator may also set a reset token that can be used to reset the File Encryption password (with administrator assistance). By default, the password reset token is disabled and must be specifically set to be enabled.

Setting	Value	Description	Method() or Constant
Change password		Forces the user to change their password immediately	resetPasswordWithTokenForInner()
Password length	4 to 256	Specifies how long the File Encryption password must be	setPasswordMinimumLengthForInner()
Password reset token	String	Specifies a string that may be used to reset the File Encryption password by the administrator	setResetPasswordTokenForInner()
Clear password reset token		Specifies to delete the reset token (will disable the administrator reset)	clearResetPasswordTokenForInner()

Table 6 - Password Settings

2.4 End User Procedures

While the administrator can configure the software, 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.

The user does not directly interact with the File Encryption service. The user interacts with the Knox work profile, which then automatically encrypts all data stored within the work profile boundary.

2.4.1 User Authentication

The user must configure a password for the Knox work profile. Detailed instructions for configuring these methods can be found under “Change unlock method” in the Knox work profile Guide.

2.4.1.1 Setting Passwords

Passwords are available for use to prevent unauthorized access to the work profile, and hence the information protected by Knox File Encryption. 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 Software Updates

3.1 Secure Updates

The Knox File Encryption software is bundled as part of the operating system on Samsung devices. Updates to the software are bundled as part of the FOTA updates that are provided by Samsung. 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 S24 on Verizon will not have an update signed with the same key as a Galaxy S24 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. This signature covers the entirety of the update, including any updates for Knox File Encryption.

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.

The device management capabilities allow the administrator to control the ability to install these updates. See the EDM guidance for the device for more information about these capabilities.

3.2 Software Version

As the Knox File Encryption software is bundled with the Knox work profile as part of the overall Android operating system, the version information can be found in the Setting/About device/Software information page. Under Knox version information is shows the DDAR version.

For the Common Criteria evaluation version information see section 1.4.1 Application Version Details.

4 Operational Security

4.1 Wiping File Encryption Data

Samsung Android devices provide administrators with the ability to wipe the device or the work profile. These capabilities are not part of the Knox File Encryption software but are built into the underlying platform.

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

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

The administrator should refer to the EDM guidance for more information about how to specify the settings to wipe the work profile (or the entire device) according to the needs of the organization.

4.2 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.