



# Samsung File Encryption 1.0

October 14, 2019

Version: 1.0

## Copyright Notice

---

Copyright © 2019 Samsung Electronics Co. Ltd. All rights reserved. Samsung is a registered trademark of Samsung Electronics Co. Ltd. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

## 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

---

<b>Document ID</b>	Samsung File Encryption Admin Guidance v1.0
<b>Document Title</b>	Samsung File Encryption 1.0 Administrator Guide

## Revision History

---

Version	Date	Changes	Author
1.0	October 14, 2019	Initial version	Brian Wood

# Contents

---

1	Introduction.....	4
1.1	Scope of Document.....	4
1.1.1	End-User Guidance .....	4
1.2	Overview of Document .....	4
1.3	Terminology & Glossary .....	4
1.4	Evaluated Devices & Software .....	5
1.4.1	Application Version Details .....	5
1.5	References .....	5
2	Samsung Knox File Encryption Deployment .....	7
2.1	Overview .....	7
2.2	Deployment.....	7
2.2.1	EDM Solution Selection .....	7
3	Knox File Encryption Configuration.....	9
3.1	File Encryption Settings.....	9
3.1.1	Optional Configuration Settings .....	9
3.2	End User Procedures.....	10
3.2.1	User Authentication .....	10
4	Software Updates.....	11
4.1	Secure Updates .....	11
5	Operational Security.....	12
5.1	Wiping File Encryption Data.....	12
5.2	Additional Notes on Operational Security .....	12

# 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 Extended Package for Software File Encryption 1.0 (and the Protection Profile for Application Software Version 1.3) 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 (note that the evaluation period is listed in parenthesis for each device):

- Samsung Exynos
  - Galaxy S10e (Spring 2019)
- Qualcomm Snapdragon
  - Galaxy S10+ (Spring 2019)

### 1.4.1 Application Version Details

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

Device SoC	Android Version	Knox Version	DualDAR Version
Qualcomm Snapdragon	9	3.3	1.0.2
Samsung Exynos	9	3.3	1.0.3

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	<a href="https://support.samsungknox.com/hc/en-us/articles/115015195728">https://support.samsungknox.com/hc/en-us/articles/115015195728</a>

Site	Information	URL
Samsung Knox SDK	Samsung Knox developer guides including EDM APIs	<a href="https://seap.samsung.com/sdk/knox-android/developer-guides">https://seap.samsung.com/sdk/knox-android/developer-guides</a>
Samsung Knox MDM SDK	Samsung Knox guides for managing File Encryption	<a href="https://seap.samsung.com/api-references/android/reference/native/html/classddar_1_1abstract_crypto.html">https://seap.samsung.com/api-references/android/reference/native/html/classddar_1_1abstract_crypto.html</a>
Galaxy S Device Support	Manuals & User Guides for Galaxy S devices	<a href="https://www.samsung.com/us/support/mobile/phones/galaxy-s">https://www.samsung.com/us/support/mobile/phones/galaxy-s</a>
Galaxy Note Device Support	Manuals & User Guides for Galaxy Note devices	<a href="https://www.samsung.com/us/support/mobile/phones/galaxy-note">https://www.samsung.com/us/support/mobile/phones/galaxy-note</a>
Galaxy Tablet Device Support	Manuals & User Guides for Galaxy Tab devices	<a href="https://www.samsung.com/us/support/mobile/tablets/galaxy-tabs">https://www.samsung.com/us/support/mobile/tablets/galaxy-tabs</a>
Knox Workspace Guide	Guidance for accessing and using Knox Workspace	<a href="https://docs.samsungknox.com/knox-platform-for-enterprise/admin-guide/workspace-reset-unlock.htm">https://docs.samsungknox.com/knox-platform-for-enterprise/admin-guide/workspace-reset-unlock.htm</a>
NIAP	Product Compliant List for Samsung Electronics	<a href="https://www.niap-ccevs.org/Product/PCL.cfm?par303=Samsung%20Electronics%20Co%2E%2C%20Ltd%2E">https://www.niap-ccevs.org/Product/PCL.cfm?par303=Samsung%20Electronics%20Co%2E%2C%20Ltd%2E</a>
	Approved Protection Profiles	<a href="https://www.niap-ccevs.org/Profile/PP.cfm">https://www.niap-ccevs.org/Profile/PP.cfm</a>
NIST SP 800-63B	NIST SP 800-63B Digital Identity Guidelines	<a href="https://pages.nist.gov/800-63-3/sp800-63b.html">https://pages.nist.gov/800-63-3/sp800-63b.html</a>

Table 3 – Reference Websites

## 2 Samsung Knox File Encryption Deployment

### 2.1 Overview

---

Samsung Knox File Encryption is a software service available to the Knox Workspace container designed to provide a layer of encryption to everything stored in the Workspace container, independently from any other encryption on the device.

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 for the Knox Workspace container. The service is designed to run without any user intervention as all files in the Knox Workspace container will be encrypted automatically. It is an integrated component of the device image, and is not a separately installed app.

Knox File Encryption is designed as a framework for the Knox Workspace container. Through this service, all files that are read or written within a container with Knox File Encryption 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 the Knox Workspace container to have been created with File Encryption enabled. The service provides the ability to fully clear and close all apps opened within the Workspace container when the Workspace becomes locked, providing a data at rest encryption layer while the device is still in use.

The Knox File Encryption service relies on the Android EDM APIs to provide management (which is limited to enabling the service during the creation of a Workspace container).

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 Knox Workspace container. When creating a Knox Workspace container, the administrator must select the DualDAR option to enable Knox File Encryption. 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 Workspace container.

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

#### 2.2.1 EDM Solution Selection

To manage the Knox Workspace container, 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 in the Workspace container.

Once a Knox Workspace container has been deployed to a device by the EDM, the user must follow any further steps (such as setting a password) to complete the configuration.



## 3 Knox File Encryption Configuration

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

### 3.1 File Encryption Settings

This section specifies the settings that must be configured to enable Knox File Encryption when a Workspace container is created in this configuration.

All settings here are based on the Class [com.samsung.android.knox.ddar.DualDARPolicy](#).

Setting	Value	Description	Method() or Constant
File Encryption configuration		Method for configuring File Encryption settings	setConfig()
Enable File Encryption	Enable	When this is set, the container 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 Workspace container. Once a container has been created, the File Encryption setting is fixed (either on or off).

#### 3.1.1 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	0 to infinite (default 5 minutes)	Specifies how long after the device has been locked to enter the Data Lock state (where all File Encryption keys are cleared)	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.

## 3.2 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 Workspace container, which then automatically encrypts all data stored within the container boundary.

### 3.2.1 User Authentication

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

#### 3.2.1.1 *Setting Passwords*

Passwords are available for use to prevent unauthorized access to the Workspace container, 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](#).

## 4 Software Updates

### 4.1 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 S10 on Verizon will not have an update signed with the same key as a Galaxy S10 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.

### 4.2 Software Version

---

As the Knox File Encryption software is bundled with the Knox Workspace 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.

# 5 Operational Security

## 5.1 Wiping File Encryption Data

---

Samsung Android devices provide administrators with the ability to wipe the device or the Workspace container. 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 Workspace container, 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 Workspace container (or the entire device) according to the needs of the organization.

## 5.2 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.