Samsung Android 7 on Galaxy Devices

User Guidance Documentation

Version 3.1

November 13, 2017

Document management

Document identification

Document ID	Samsung User Guidance Documentation 3.1.
Document title	Samsung Android 7 on Galaxy Devices User Guidance Documentation
Release authority	

Document history

Version	Date	Description	Author
0.1	14-October-2013	Initial draft for review.	
0.2	16-October-2013	Released to Samsung for review.	
0.3	20-December-2013	Released to Samsung for review.	
0.5	January 27, 2014	Update for Android 4.4	Brian Wood
0.6	January 31, 2014	Updates based on Admin Guide	Brian Wood
0.7	February 10, 2014	Updated based on feedback from CC evaluator	Brian Wood
0.7a	February 11, 2014	Added device list	Brian Wood
0.8	February 11, 2014	Added Crypto API	Ed Morris
0.9	February 12, 2014	Added Crypto API reference links	Brian Wood
0.10	February 13, 2014	Updates CC Mode app settings	Brian Wood
0.11	February 20, 2014	Added versioning information	Ed Morris
1.1	March 31, 2014	Updated for Galaxy S5/Note 10.1	Brian Wood
1.2	April 29, 2014	Updated to have VPN release number shown	Brian Wood
1.2a	May 2, 2014	Updated device list	Brian Wood
1.2b	June 6, 2014	Modified device list table	Brian Wood

Version	Date	Description	Author
1.3	September 7, 2014	Updated for new devices and options and KNOX usage	Brian Wood Sung Whan Moon
1.4	September 19, 2014	Updated device list	Brian Wood
1.5	October 7, 2014	Edited versions and CC Mode access	Brian Wood
1.6	October 20, 2014	Edited CC mode access	Brian Wood
1.7	October 28, 2014	Updated device list	Brian Wood
2.0	January 29, 2015	Edited for Android 5	Brian Wood
2.1	April 9, 2015	Edited for new devices	Brian Wood
2.2	July 31, 2015	Updated for new devices	Brian Wood
2.3	October 1, 2015	Updated for new device	Brian Wood
2.4	March 23, 2016	Updated device list & features	Brian Wood
2.5	October 5, 2016	Updated device list & features	Brian Wood
3.0	April 18, 2017	Edited for Android 7	Brian Wood
3.1	November 13, 2017	Updated device list & references	Brian Wood

Table of Contents

1 Document Introduction

This document contains enterprise guidance for the deployment of Samsung devices in accordance with the Common Criteria configuration.

1.1 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 7 (Nougat).

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 Note 8 (Fall 2017)
  - Galaxy S7 Edge (Spring 2017)
- Qualcomm Snapdragon
  - Galaxy S8 + (Spring 2017)
  - Galaxy Tab S3 (Spring 2017)
- Samsung Exynos
  - Tab Active2 (Fall 2017)
  - Galaxy S8 (Spring 2017)
  - Galaxy S6 Edge (Spring 2017)

The following table shows the devices for which equivalence is being claimed from each evaluated device.

Evaluated Device	Processor	Equivalent Devices	Differences
Galaxy S8 + (Qualcomm)	Snapdragon 835	Galaxy S8 (Qualcomm)	S8 + is larger
		Galaxy S8 Active	S8 + is larger S8 Active has a IP68 & MIL-STD-810G certified body
Galaxy S8 (Samsung)	Exynos 8895	Galaxy S8 + (Samsung)	S8 + is larger
Galaxy Tab S3 (T825Y)	Snapdragon 820	Galaxy Tab S3	T825 & T827 models have LTE T820 models only have Wi-Fi

Evaluated Device	Processor	Equivalent Devices	Differences
Galaxy Tab Active2 (T395)	Exynos 7870	Galaxy Tab Active2	T390 models only have Wi-Fi T395N & T397 models have LTE
Galaxy S7 Edge (Qualcomm)	Snapdragon 820	Galaxy S7 (Qualcomm)	Curved screen vs. Flat screen
		Galaxy S7 Active	Curved screen vs. Flat screen S7 Active has a IP68 & MIL-STD-810G certified body No fingerprint sensor
Galaxy S7 Edge (Samsung)	Exynos 8890	Galaxy S7 (Samsung)	Curved screen vs. Flat screen
Galaxy S6 Edge	Exynos 7420	Galaxy S6	Curved screen vs. Flat screen
		Galaxy S6 Edge+	Curved screen vs. Flat screen
		Galaxy Note 5	Curved screen vs. Flat screen Note 5 is larger Note 5 includes stylus & functionality to take advantage of it for input (not security related)
		Galaxy S6 Active	Curved screen vs. Flat screen S6 Active has a IP68 & MIL-STD-810G certified body No fingerprint sensor

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.

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 Note 8 (Qualcomm)	SM-N950	7.1	4.4.21	NMF26X	U, J, D
Galaxy Note 8 (Samsung)	SM-N950	7.1	4.4.13	NMF26X	N, F
Galaxy S8 (Qualcomm)	SM-G950	7.0	4.4.16	NRD90M	U
Galaxy S8 (Samsung)	SM-G950	7.0	4.4.13	NRD90M	N, F
Galaxy S8 + (Qualcomm)	SM-G955	7.0	4.4.16	NRD90M	U
Galaxy S8 + (Samsung)	SM-G955	7.0	4.4.13	NRD90M	N, F
Galaxy S8 Active	SM-G892	7.0	4.4.16	NRD90M	A, U, None
Galaxy Tab S3	SM-T820	7.0	3.18.31	NRD90M	None
	SM-T825	7.0	3.18.31	NRD90M	N, Y, None
	SM-T827	7.0	3.18.31	NRD90M	V, A, R4
Galaxy Tab Active2	SM-T390	7.1	3.18.14	NMF26X	None
	SM-T395	7.1	3.18.14	NMF26X	N, None
	SM-T397	7.1	3.18.14	NMF26X	None

Device Name	Base Model Number	Android Version	Kernel Version	Build Number	Carrier Models
Galaxy S7 (Qualcomm)	SM-G930	7.0	3.18.31	NRD90M	T, P, R4, V, A
Galaxy S7 (Samsung)	SM-G930	7.0	3.18.14	NRD90M	F, S, K, L
Galaxy S7 Edge (Qualcomm)	SM-G935	7.0	3.18.31	NRD90M	A, T, P, R4, V
Galaxy S7 Edge (Samsung)	SM-G935	7.0	3.18.14	NRD90M	F, S, K, L
Galaxy S7 Active	SM-G891	7.0	3.18.31	NRD90M	A, None
Galaxy S6 Edge+	SM-G928	7.0	3.10.61	NRD90M	F, I, A, T, P, R4, V, S, K, L
Galaxy Note 5	SM-N920	7.0	3.10.61	NRD90M	I, A, T, P, R4, V, S, K, L
Galaxy S6	SM-G920	7.0	3.10.61	NRD90M	F, I, A, T, P, R4, V, S, K, L
Galaxy S6 Edge	SM-G925	7.0	3.10.61	NRD90M	F, I, A, T, P, R4, V, S, K, L
Galaxy S6 Active	SM-G890	7.0	3.10.61	NRD90M	A, None

The Carrier Models column specifies the specific versions of the devices which have the validated configuration. These additional letters/numbers denote carrier specific models (such as V = Verizon Wireless). Only models with the suffixes listed in the table can be placed into the validated configuration.

Note: Where Carrier Models specifies “None” that means a device without a suffix is also a device which can be placed into a validated configuration.

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

Device Name	MDF Version	MDF Release	WLAN v1.0 Release	VPN v1.4 Release	KNOX Release
Galaxy S6, S6 Edge, S6 Active, Note 5	3.0	2	2	8.1	2.7
Galaxy S7, S7 Edge, S7 Active, Tab S3	3.0	2	2	8.1	2.7
Galaxy S8, S8+, S8 Active	3.0	2	2	8.1	2.8
Galaxy Note 8, Tab Active2	3.1	2	2	8.2	2.9

The MDF version number is broken into two parts as the claimed MDFPP has been updated in the latest devices. For example, the Galaxy S8 would show “MDF v3.0 Release 2”.

2 How to use your device securely

As a mobile enterprise user it is your responsibility to assist the enterprise in maintaining the security of your Samsung device. Some important aspects of device security are reliant on your actions and you are required to be aware of your responsibilities and take appropriate steps to help ensure device security. In particular, you are responsible for:

- Setting and protecting a sufficiently complex password;
- Being aware of your surrounding environment when operating the device;
- Reporting suspicious activity or security incidents;
- Taking caution when installing applications;
- Using the device in accordance with enterprise policy;
- Assisting the enterprise to enrol a device into the evaluated configuration (apply security to the device); and
- Protecting the mobile device when not in use.

2.1 Password management

Users will be required to set a password when the device is first configured to protect the key that will encrypt the data on the device, and to protect against unauthorised access to device functions. It is critical that you select an appropriate password and that your password is never made available to anyone.

2.1.1 Setting passwords

The acceptable complexity of a password will be set by your administrator and will consist of the following:

- Minimum letters required in password (a-z, A-Z);
- Minimum lowercase letters required in password (a-z);
- Minimum non-letter characters required in password (0-9 and special characters +=%_@#$/^&*()‘-”:!;?,`.~\|<>{}[]);

- Minimum numerical digits required in password (0-9);
- Minimum symbols required in password (+=%_@#$/^&*()‘-”:!;?,`.~\|<>{}[]); and
- Minimum uppercase letters required in password (A-Z).

It is important that you understand the requirements stated within your organisation’s Information Security Policy and/or Mobile Device Policy.

When setting a password, you should be careful **not** to:

- Use known information about yourself (e.g. address, birthday, pets names, your name or any information recoverable from the public domain);
- Include your username or company name within your password;
- Set a password which is similar to previous passwords (adding a ‘1’ or “!” to the end of the password is not sufficient); or
- Use simple dictionary words (Welcome1!).

A good method of creating passwords is to think of a long passphrase and simply use the first characters of each word. For example:

I really want to set a very secure password with 16 characters! Irwtsavspw16c!

Note: Please do not use this password.

2.1.2 Password use

Your administrator will set an expiration date for your password which will require you to change it once that time has elapsed (e.g. 90 days). It is important that you choose a unique password each time and do not use previous passwords, including derivatives.

It is also your responsibility not to disclose your password to anyone. This includes:

- Writing your password down and placing it in an area that other people can access (this includes on your computer or in online resources);
- Re-using the same password for other accounts (e.g. email, twitter or Facebook); and

- Providing the password to others, including family members, so that they can use the device. It is important to note that your organisation will never ask you for your password as they have no use for it.

2.2 Be aware of your environment

Due to the nature of mobile enterprise access, users can find themselves in situations where unauthorised parties may be able to view a password or business critical information being entered or viewed on the device. This could be achieved through “shoulder surfing” or other surveillance techniques such as security cameras and recording devices.

Because of this, it is very important that you are aware of your surroundings when using your device and take proper precautions to prevent data disclosure.

If you would like to further understand your level of risk in remote locations, speak to your Enterprise Security Team.

2.3 Physical security of the device

It is important that at all times you maintain control of the device to reduce the risk of tampering by unauthorised parties. When not in use, the device should be stored in an appropriately secure location. If you are unsure of what is considered appropriately secure, refer to the Mobile Device Policy or contact your Enterprise Security Team.

2.4 Application control

As part of the device configuration, your enterprise administrator may choose to restrict, or apply levels of restriction, to applications on the device. Make sure that you are aware of the Enterprise Mobile Acceptable Use Policy including any guidance or limitations on the applications you are allowed to download and install.

2.5 Reporting suspicious activity and security incidents

It is very important that you report any suspicious activity or security incidents as they could result in negative consequences for the enterprise. Suspicious activity could include situations in which:

- The device is operating abnormally (e.g. performance issues, unusual applications or messages); and

- Outside parties take an unusual interest in the device.

Security incidents might include situations in which:

- The device has been left unattended for significant periods of time;
- The device is confiscated or out of your control for significant periods of time (e.g. Border Control in a foreign country); and
- You notice visible tampering with the device.

Note: It is extremely important, especially when travelling overseas, that you are aware of the methods to report suspicious activity and security incidents.

If you are unsure whether a situation constitutes either suspicious activity or a security incident, report it just in case.

2.6 Wiping the data on a device

To protect the confidentiality and integrity of information on your device, the device is configured to be able to be wiped. In the event the device is wiped, the encryption key on the device will be wiped and a soft wipe will occur on all user data. This means that all user data will be inaccessible with no options for recovery. The device will then reboot and reset to the factory default settings.

The device may be wiped under the following conditions:

- You manually initiate a wipe (Settings/Backup and reset/Factory data reset);
- You, or a third party, exceed the number of incorrect login attempts allowed by the local device wipe threshold (set by your enterprise administrator);
- 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 you are leaving the organisation.

Warning: Make sure you regularly backup any personal data on the device as this will be destroyed as part of a wipe.

2.6.1 Re-enrolling a device

In the event that your device is wiped and you still have access to the device, you may be asked to re-enrol (re-connect) the device to the Enterprise Device Management Solution. Make sure you follow the guidance of the Enterprise Administrator to get the device back into a secure state. The device should not be used to receive, store or process enterprise information prior to being placed in a secure state.

2.7 Checking the version of a device

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*** or ***Settings/About device/Software information***. The following version information can be found:

- ***Model number*** – this is the hardware model (this is carrier specific, so for example a Samsung Galaxy S4 on Verizon Wireless has a different model number than on AT&T)
- ***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 for the mobile device, this will show:

MDF v**ABC** Release **XYZ**

Where **ABC** is the version of the MDFPP and **XYZ** is the version number of the software that has been validated.

2.7.1 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 (see section 3.2 for information about accessing the website) and select the device you are using. This will provide a complete list of the software installed on the evaluated device.

2.7.1.1 Software Versions on Device

To verify the versions of any software on the device (compared to the list from the website), open ***Settings*** and either ***Apps*** or ***Application***. Under the heading ***All apps***, 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.

3 Secure Device Configuration

The device may be configured securely either as a stand-alone device or in connection to an Enterprise. Depending on the type of management there are different options available to a user related to the configuration and how to secure the device.

3.1 Enrolling a Device with a Mobile Device Management Service

If your device will be managed by an Enterprise via an MDM (Mobile Device Management) service, you will need to enroll your device into the service. This is done through the installation of the MDM Agent application provided by your Enterprise administrator. Before installing the MDM Agent, you must enable Unknown Sources for applications as the Agent will not be installed from the Google Play Store. This can be achieved by going to ***Settings/Security/Unknown sources***. Checking this box will prompt to confirm the enabling of Unknown sources due to the possibility of vulnerabilities in being able to install apps from outside of the Play Store.

See your Enterprise administrator about obtaining and installing the MDM agent.

3.2 Enabling Common Criteria Mode (CC Mode)

Samsung provides a setting to enable services to bring the device into the Common Criteria-evaluated configuration. This is called CC Mode. If you are enrolled in an MDM, this will be handled by your Enterprise administrator.

The CCMode.apk can be downloaded from Samsung here. In addition to the APK, you can download the latest guidance documentation and the list of applications provided with each validated device.

From this page you can see the list of applications provided with each validated device as well as the CC Mode application at the top.

3.2.1 Installing the CC Mode App

Before installing the CC Mode app, you must enable Unknown Sources for applications as the app will not be installed from the Google Play Store. There are two ways this can be handled:

- Going to ***Settings/Security/Unknown sources*** and changing this to allow.

- Allowing the app install process to prompt you to allow Unknown Sources. This will prompt you to allow the installation of this app from an Unknown Source as a one-time authorization (you can select to also enable it completely at the prompt). Choosing the default selection will not enable Unknown Sources for any app, only for the CC Mode app being installed immediately.

Choosing to enable Unknown Sources carries a risk due to the possibility of vulnerabilities in being able to install apps from outside of the Play Store. By default the Play Store will still scan installed apps for known vulnerabilities, but it is recommended to not leave this enabled.

Note: Once the CC Mode app is installed, Unknown Sources can be disabled if they were enabled.

3.2.2 CC Mode Prerequisites

Before the activation of CC Mode can be completed, it is necessary to set a password on the device; until the password is configured, it is not possible to complete the activation. The password may be set before starting the activation of CC Mode or it can be done during it (by exiting the app and setting the password), but it is simpler to do it first.

The password must contain be at least 4 characters including at least 1 letter.

3.2.2.1 Setting the Password on Galaxy S6 Variants & Galaxy Note 5

Note: These instructions assume no authentication method has been set on the device.

To set the password for these devices:

1. Open ***Settings/Lock screen and security*** and select ***Screen lock type***
2. Select ***Password*** from the ***Lock type*** menu
3. Enter and confirm your new password
4. Choose whether to show notifications when the device is locked and select ***Done***
5. Select ***Later*** when prompted to enter fingerprints (these will not be allowed in the CC Mode configuration)

3.2.3 Activating CC Mode

Note: To complete activation the device must have an Internet connection, such as Cellular or W-Fi.

The devices can be grouped based on their similarities of features and processors. Due to the differences between the groups, the steps to get a device into CC Mode are slightly different for each one, and as such are laid out separately here.

Note: Once a device has been placed into CC Mode, the only way to disable it is to perform a factory reset or to connect to an MDM which can disable it.

3.2.3.1 Activation on Galaxy S7 & S8 Variants

Note: If your environment requires generation of the ODE key to be done during the setup process (or post factory load), a factory reset of the phone prior to starting the enrolment process will force the generation of a new ODE key after the factory reset has been completed.

To activate CC Mode on Galaxy S7 devices:

1. Set the device password
2. Open ***Settings/Lock screen and security*** and select ***Secure startup***
3. Select ***Require password when device turns on*** and select ***OK***
4. Enter your password
5. Launch the CCMode app
6. Accept the CCMode license and select ***Confirm***
7. Select ***Activate***
8. Select ***Activate License***
9. Choose ***Samsung KNOX***

Note: For customers using an on premise license server, you can select ***onprem*** and enter license information from your server. See your server admin for more information about this option.

10. Agree to the KLMS License and select ***Confirm***
11. Select ***Turn On CCMODE***
12. On the Turn on CCMode popup, select ***Agree***
13. Select ***OK*** to restart the phone

At this point the device will restart, you will need to enter the password and CC Mode will be Enabled.

Once CC Mode is enabled, the device will be configured such that 5 unsuccessful login attempts will force a factory reset on the device wiping all data. This can be changed via MDM.

3.2.3.1.1 CC Mode and SD Cards on Galaxy S7 & S8 Variants

For devices that have slots available for SD Cards, the encryption must be enabled for the SD Card as well. The setting was enabled as part of activating CC Mode.

When an SD Card is inserted (if one wasn't present initially), you will be prompted to encrypt the SD Card. If you do not follow the prompts and enter the device password to encrypt the SD Card, it will not be mounted and you will not be able to access it.

Note: If you do not enter the password for encrypting the SD Card when prompted, the only way to re-prompt is to remove and reinsert the SD Card.

3.2.3.2 Activation on Galaxy S6 Variants and Note 5

To activate CC Mode on Galaxy S6 and Note 5 devices:

1. Set the device password
2. Open ***Settings/Lock screen and security*** and select ***Encrypt Device***
3. Select ***Encrypt Device***
4. Enter your password
5. Select ***Encrypt Device***

The device will now restart and start the encryption process.

6. Launch the CCMode app
7. Accept the CCMode license and select ***Confirm***
8. Select ***Activate***
9. Select ***Activate License***
10. Choose ***Samsung KNOX***

Note: For customers using an on premise license server, you can select ***onprem*** and enter license information from your server. See your server admin for more information about this option.

11. Agree to the KLMS License and select ***Confirm***
12. Select ***Turn On CCMODE***
13. On the Turn on CCMode popup, select ***Agree***
14. Select ***OK*** to restart the phone

At this point the device will restart, you will need to enter the password and CC Mode will be Enabled.

Once CC Mode is enabled, the device will be configured such that 5 unsuccessful login attempts will force a factory reset on the device wiping all data. This can be changed via MDM.

3.2.4 Removing the CC Mode App

Once CC Mode has been enabled, the app can be removed from the device. To remove the app from the device, you must first disable it as a Device Administrator. This can be done through ***Settings/Lock screen and security/Other security settings/Device Administrators***. Unselect the CC Mode app and choose Deactivate. The app can now be removed through the Application Manager.

3.2.5 CC Mode Status

CC Mode has the following statuses:

Status	Description
Ready (blank)	CC Mode has not been turned on
Enforced	CC Mode has been turned on but some of the required settings or configurations have not been set
Enabled	CC Mode has been turned on and all required settings and configurations have been set
Disabled	CC Mode has been turned on but an integrity check or self-test has failed (such as a FIPS 140-2 self-test)

The CC Mode status can be seen by going to ***Settings/About device*** or ***Settings/About device/Software information*** and then ***Software Security Version***. This will show the current status.

Note: The Ready state does not have any indicator. Only Enforced, Enabled and Disabled actually show a specific status

3.3 Other Password and Lock screen Settings

There are a few other password and lock screen settings which can use useful to configure to your needs.

- Screen timeout - ***Settings/Display/Screen timeout***
    - This setting will control how long the display stays on before turning off when it is not being touched (or not controlled by an individual app). Setting this high can increase the drain on your battery.
- Lock with Power Button –***Settings/Lock screen and security/Secure lock settings/Lock instantly with power key*** or ***Settings/Lock screen and security/Secure lock settings/Secured lock time/Instantly with the power key…***
    - This setting will cause the device to lock immediately when you press the power button. When unchecked pressing the power button only turns off the display, waiting for the lock timeout before locking the device.
- Lock automatically after timeout –***Settings/Lock screen and security/Secure lock settings/Lock automatically*** or ***Settings/Lock screen and security/Secure lock settings/Secured lock time***
    - This setting will control how quickly the device will lock after the screen has timed out (turned off). The longer the time the longer you will be able to wake the device up without needing to enter a password. This should be set to a low time to prevent a left device being unlocked without a password needing to be entered.
- Make passwords visible – ***Settings/Security/Make passwords visible*** or ***Settings/Lock screen and security/Other security settings/Make passwords visible***
    - This setting will allow the entered password to be seen on the display as it is entered. This should be set to disabled (or off) to ensure that someone cannot see your password by “shoulder-surfing”.

3.4 Biometric Enrollment

Samsung devices support the use of biometric authentication to unlock the device. Note that a biometric cannot be used after a device restart, your password must be entered both at the ODE lock screen and the Android lock screen before a biometric can be used.

The KNOX container can also support biometric authentication in a hybrid method where-in you must enter both a password and the biometric before gaining access to the container. In the CC Mode configuration, the KNOX container does not support biometric-only authentication.

The available modes of biometric authentication can vary between devices.

3.4.1 Activation of Fingerprint on Galaxy S8/Note 8 Variants

To enroll a fingerprint on Galaxy S8/Note 8 devices:

1. Open ***Settings/Lock Screen and Security*** and select ***Fingerprint Scanner***
2. Select ***Continue***
3. Enter your password (or enter and confirm if you have not created one when enrolling)
4. Follow the prompts to scan your finger until the process is complete

Multiple fingers can be added. It is recommended to add at least 2 fingerprints.

3.4.2 Activation of Iris on Galaxy S8/Note 8 Variants

To enroll a fingerprint on Galaxy S/ Note 8 devices:

1. Open ***Settings/Lock Screen and Security*** and select ***Iris Scanner***
2. Select ***Continue***
3. Enter your password (or enter and confirm if you have not created one when enrolling)
4. Accept the disclaimer
5. Follow the prompts to scan your iris until the process is complete
6. Review the tips for using the iris scanner

It is possible to use only one iris instead of the default of two. This does not provide the ability to register two separate iris scans (as is possible with fingerprints).

3.4.3 Activation on Galaxy S7/S6 Variants, Galaxy Note 5 & Tab S3/Tab Active2

To enroll a fingerprint on Galaxy S7/S6/Note5/Tab S3/Tab Active2 devices:

1. Open ***Settings/Lock Screen and Security*** and select ***Fingerprints***
2. Select ***Password***
3. Enter your password (or enter and confirm if you have not created one when enrolling)
4. Follow the prompts to scan your finger until the process is complete

Multiple fingers can be added. It is recommended to add at least 2 fingerprints.

3.5 Settings that can be controlled

There are many settings that can be controlled by the user. The following is a list of specific functions which are claimed as available for users when in CC Mode.

3.5.1 Radio Control

The following list of radios can be controlled from the ***Settings*** menu under the heading of ***Connections***:

- Wi-Fi
    - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***
- Bluetooth
    - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***
    - The Bluetooth friendly name can be edited from the ***Settings/About device/Device name***
- Cellular (Airplane mode)
    - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***
    - This will disable all radios though other radios can then be re-enabled individually.
- NFC
    - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***
    - When NFC is enabled, Android Beam can be switched between ***On*** and ***Off*** by ***selecting*** NFC and payment

- Mobile Hotspot and Tethering
    - Mobile Hotspot
        - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***.
        - Under ***Settings/Configure Mobile hotspot***, it is possible to configure the settings of the Mobile Hotspot
            - Network SSID – the name of the wireless network
            - Hide my device – whether or not to broadcast the network name
            - Security – the security of the wireless network
            - Password – the password for the chosen network security
            - Advanced options
                - Broadcast channel – specify whether to use 2.4 or 5 GHz and the frequency channels
    - Bluetooth tethering (not available on all devices)
        - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***.
    - USB Tethering
        - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***.
- GPS (Location)
    - This can be enabled or disabled by sliding the switch between ***On*** and ***Off***
        - There may be multiple location sources, but all are controlled by the Location Services switch.

3.5.2 Notification Control

Notifications for the Calendar and Messaging applications can be disabled, which will prevent notifications to be displayed for these applications during a locked state. Note that the disabling is complete, not just for the locked state, and so these applications will not show notifications at any time. Notifications inside and outside of a KNOX container are separate, so it is possible to disable

notifications in one while leaving them available in another (for example you could turn off Calendar notifications inside the KNOX container tied to a corporate account while leaving notifications for personal accounts outside the KNOX container enabled).

These only work for the provided Calendar and Messaging apps. Third party apps, such as Google Calendar or Handcent (SMS) will not follow these settings though they have their own means for disabling notifications.

3.5.2.1 Calendar Notifications

Open the Calendar application and access ***Menu/Settings***. Set ***Notification*** to ***Off*** to disable notifications. Other options will enable notifications based on the chosen settings.

3.5.2.2 Messaging Notifications

Open the Messaging application and access ***Menu/Settings***. Set ***Notification*** to ***Off*** to disable notifications.

3.5.3 Other Controls

3.5.3.1 Developer Mode (USB debugging)

In some circumstances it may be necessary to ensure that developer access is not allowed on the device. It should be noted that by default developer mode is hidden (and hence disabled) on Android devices. In the ***Settings*** list, if there is no ***Developer options*** item shown, then developer mode is disabled.

To access the ***Developer options*** menu, open the ***About device*** option. Then find the ***Build number*** item (this may be under ***Software information***). Click this item 7 times and the ***Developer options*** will be enabled.

To disable the developer mode, open the now-visible ***Developer Options*** menu. Under ***Debugging***, ensure that ***USB debugging*** is not selected.

3.5.3.2 Date/Time Control

It is important to have a trusted source of time on your device. Normally a device utilized the network-provided time from the cellular carrier as the trusted time source, and except under unusual circumstances this should always be used. This can be controlled through the ***Menu/Settings*** menu. Under ***General management/Date and time*** the setting ***Automatic date and time*** should be selected to use an external trusted time source.

3.5.3.3 Google Remote Backup Control

Google provides a remote backup service for Android devices that can back up some application data, Wi-Fi settings, and similar data to make setting up a new device quicker. This only works when a Google account is linked to the device. This feature can be disabled in ***Setting/Cloud and Accounts/Backup and restore*** by unchecking ***Back up my data*** for the Google Account.

3.6 Certificate Management

Many secure services require the use of certificates, such as to trust secure servers or to authenticate your device to those same servers. Certificates can only be installed on a device which is protected by a login (in this case a password).

3.6.1 Managing the Trust Anchor Database

The Trust Anchor Database (TAD) is a list of all trusted Certificate Authorities. In most cases these certificates are pre-loaded by Samsung and Google (similar to browser certificates) though further ones may be loaded either via MDM or by you. The built-in certificates cannot be deleted but they can be disabled.

To disable a built-in certificate, go to ***Settings/Lock screen and security/Other security settings*** and then ***View security certificates***. Under the System tab you will see all the pre-loaded certificates. To disable a certificate select it from the list, and then in the Security certificate pop-up window, scroll down and select ***Turn off***. Then click OK. This will disable the selected certificate.

3.6.2 Importing New Certificates

To import your own certificates into your device you must have a way to download the certificate. This could come in many forms, such as through a USB connection from a PC where it is copied to the device from the PC, or downloaded from a web server via a browser on the device.

3.6.2.1 Browser Import Example

This is an example of loading a certificate through a browser. It is possible other applications may perform the same service. It is assumed you already know where the certificate is stored and have accessed the page.

1. Select the certificate to be installed from the web page
2. Enter the password protecting the certificate (may not always be present)
3. Once the certificate is downloaded you will be prompted to ***Name the certificate***

4. Enter a name for the certificate and select the use (VPN and apps or Wi-Fi)
    a. Be sure you know the intended purpose of the certificate as you cannot change this after installation, you will need to remove and reload the certificate if this is wrong
5. Click OK to import the certificate

3.6.2.2 Direct Import Example

To load a certificate directly it must be stored on the internal storage of the device. If you save the certificate to an SD Card it will be ignored for the import process. To load a certificate directly:

1. In the ***Settings/Lock screen and security/Other security settings*** menu select ***Install from device storage***
2. If there is more than one certificate available, select the desired certificate to install
    a. If there is only one, this will step will be skipped
3. Enter the password protecting the certificate (may not always be present)
4. You will be prompted to ***Name the certificate***
5. Enter a name for the certificate and select the use (VPN and apps or Wi-Fi)
    a. Be sure you know the intended purpose of the certificate as you cannot change this after installation, you will need to remove and reload the certificate if this is wrong
6. Click OK to import the certificate

3.6.3 Removing Certificates

Periodically it may be necessary to remove certificates that you have imported. This is similar to disabling TAD certificates.

To disable an imported certificate, go to ***Settings/Lock screen and security/Other security settings*** and then ***View security certificates***. Under the User tab you will see all the certificates you have imported. To remove a certificate select it from the list, and then in the Security certificate pop-up window, scroll down and select ***Remove***. Then click OK. This will remove the selected certificate.

3.6.3.1 Clear credentials

In the case where you need to clear all the certificates you have imported at once, it is possible to clear all at once. This is done from the ***Settings/Lock screen and security/Other security settings*** menu by selecting ***Clear credentials***. Selecting and confirming this option will erase all imported certificates, regardless of type.

3.7 Configure Wireless Networks

It is possible to utilize many different methods for accessing Wi-Fi networks, including open access points, WEP encrypted, WPA2 PSK encrypted and 802.1x EAP-TLS protected networks. The settings for each access point are stored separately so credentials for one network are not used for another. For any network that is not open, the specific configuration needed to access the network must be provided by the administrator of the specific access point.

Under the ***Settings/Connections*** menu is a selection for ***Wi-Fi***. A selection can be used to enable/disable all Wi-Fi connectivity here. For further configuration select the ***Wi-Fi*** item instead of the on/off switch. When enabled, it is possible to connect to any visible network from the list of Access Points displayed on below the configuration. This list includes both visible but not configured networks (i.e. ones you have not connected to before), visible networks you have a made connections to, and saved network configurations that are not currently in range. If you are connected, that network will show at the top of the list as Connected.

At the bottom of the listed access points (assuming Wi-Fi is enabled), is an option the ***Add network***. From this selection you can configure a network which may be hidden (i.e. the SSID is not being broadcast) or one that is out of range.

Using the information provided by the access point administrator, fill out the information in the ***Add network*** pop-up menu.

Note: In CC Mode some modes of 802.1x EAP are disabled (such as LEAP & PEAP).

3.7.1 Configuring EAP-TLS Connections

To setup a connection using EAP-TLS, start by choosing the option to ***Add network*** and enter the following information:

- **Network name –** the SSID for the wireless network
- **Security -** select ***802.1x EAP*** from the list
- **EAP method –** select ***TLS*** from the list
- **CA certificate –** select the CA certificate used to validate the Access Point certificate from the drop down list
- **User certificate –** select the user certificate from the drop down list that will be used to authenticate the device to the Access Point

- **Identity –** the identity for the device/user (provided by the access point administrator)

The following advanced options can also be configured:

- **Proxy –** you can specify a proxy server (none, manual or auto-config)
- **IP settings –** specify whether DHCP or static IP address will be used on the connection
- **Key Management –** if available on your access point, this is Fast Roaming key management.
    - **FT –** 802.11r Fast Roaming
    - **CCKM –** Cisco Centralized Key Management

Note: The Key Management functions are listed for completeness in the configuration; they are not included as part of the tested configuration and so should be left empty.

3.8 Bluetooth Pairing

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, you can't transfer files or store data on the headset. Connections to devices which support these capabilities must always be paired explicitly before any use of functionality between them.

3.8.1 Initiating a Pairing from Your Device

To setup a secure pairing from your device, follow these steps:

1. Enable Bluetooth (either through ***Settings/Connections*** or Quick Settings)
2. Open ***Settings/Connections/Bluetooth***

From the other device, make the device discoverable.

3. When you open the Bluetooth settings your device will automatically scan for other devices. If the device has not been found, press ***SCAN*** and it will again scan for other devices
4. Tap the name of the device

5. In the dialog **Bluetooth pairing request** verify that the PIN shown matches on both devices. This is a 6-digit number and will change every time you attempt to pair two devices (even the same ones)

6. If the PIN matches on each device, tap **OK** to accept the pairing

The devices are now paired.

3.8.2 Accepting a Pairing from Your Device

To setup a secure pairing that has been initiated from another device connecting to yours, follow these steps:

1. Enable Bluetooth (either through ***Settings/Connections*** or Quick Settings)

2. Open ***Settings/Connections/Bluetooth***. This will automatically make your device visible until this screen is closed

From the other device, scan and find your device and select to pair it.

3. In the dialog **Bluetooth pairing request** verify that the PIN shown matches on both devices. This is a 6 digit number and will change every time you attempt to pair two devices (even the same ones)

4. If the PIN matches on each device, tap **OK** to accept the pairing

The devices are now paired.

4 General usage

The following sections will provide some basic information for using your device and additional information on the functionality available.

4.1 Using your device

The Samsung Galaxy series are running Android 7 overlaid with the Samsung TouchWiz interface. An example of this is provided in the following image:

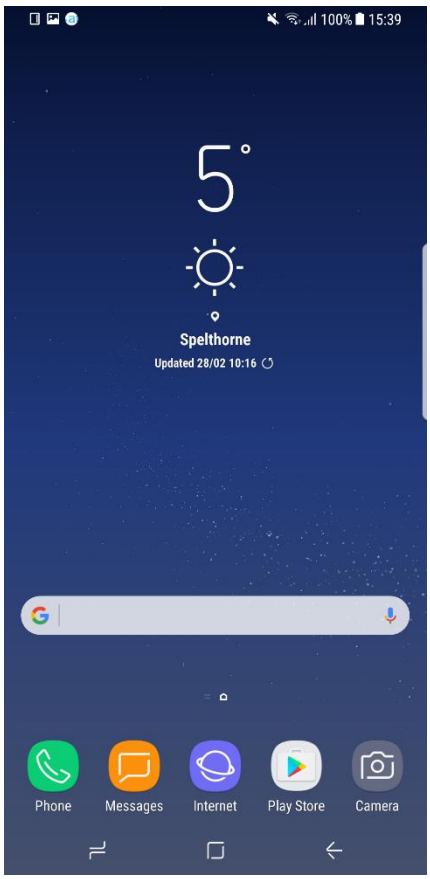

Figure 1 – Galaxy TouchWiz interface

You will interact with the TouchWiz interface via your device touchscreen. When required to enter information, a keyboard will be displayed on the screen for you to interact with the device. Further information on both Android and TouchWiz is available online.

4.1.1 Authenticating to your Device

Once the device has been configured and encryption enabled, you will be required to authenticate to the device every time it starts and every time it becomes locked. A password screen with a keyboard will appear and you will need to enter the password you selected.

Note: When you restart the device you will authenticate twice, once to unlock the ODE encryption and a second time to access Android. This only occurs when the device has been powered off or power cycled.

There are two ways to access the KNOX Container, Launcher Style and Folder Style. To switch between styles, access the ***KNOX settings/KNOX style***. Select the preferred style and select ***DONE***.

Launcher style presents a new Launcher Home which looks like the normal Home, but with only the KNOX container apps available. It looks like a second workspace. The Folder style presents the KNOX apps in a special KNOX folder, but otherwise they look and act like any other app on the device, providing a more integrated view of the device. In this style the user only sees the apps, is prompted for authentication when needed, but sees it all as one interface.

4.1.1.1 Authenticating to the KNOX Container – Launcher Style

If the KNOX container has been turned on, then access to the container will also require authentication to access any apps or data within the container. The login to the KNOX container is accessed by tapping on the KNOX icon in the notification bar (Figure 2) or in the application menu (Figure 3).

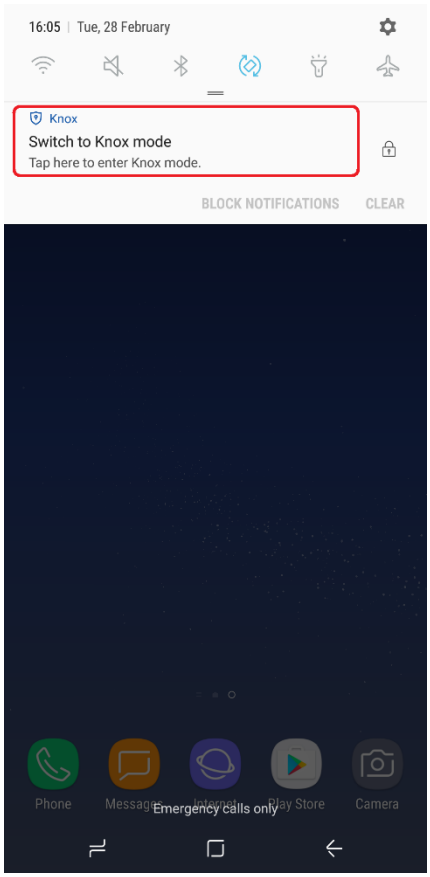
16:05 | Tue, 28 February
Knox
Switch to Knox mode
Tap here to enter Knox mode.
BLOCK NOTIFICATIONS
CLEAR
Phone
Messages
Internet
Play Store
Camera
Emergency calls only

Figure 2

Figure 3

4.1.1.2 Authenticating to the KNOX Container – Folder Style

If the KNOX container has been turned on, then access to the container will also require authentication to access any apps or data within the container. The login to the KNOX container is accessed by tapping on the KNOX icon in the notification bar (Figure 4) and then by selecting the application you want to launch (Figure 5). Once you have authenticated for one app, you can access any KNOX app until the container is locked (either by inactivity timeout or manually).

Figure 4

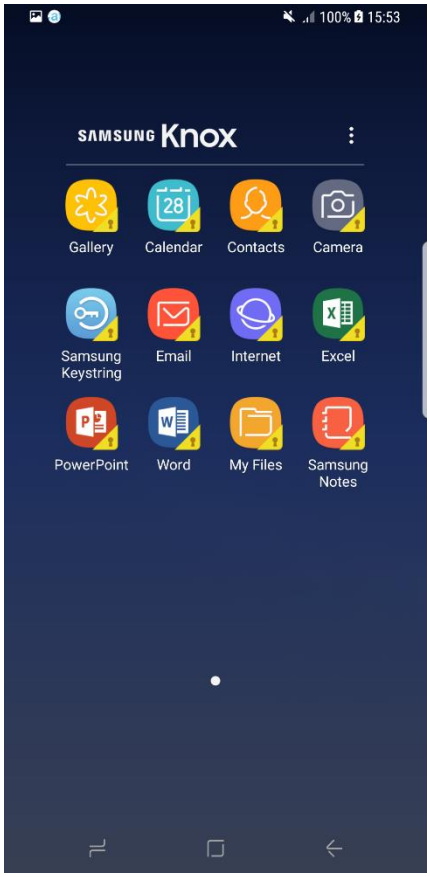

Figure 5

4.1.1.3 Leaving the KNOX Container – Launcher Style

To leave the KNOX container and return to the personal side of the device, tap the PERSONAL icon in the notification bar (Figure 6) or in the container application menu (Figure 7). This will close the KNOX container and return to the normal world of the device.

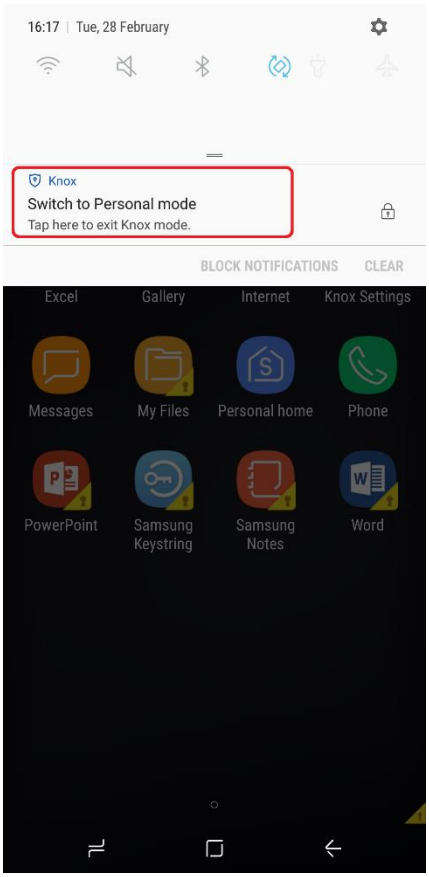
16:17 | Tue, 28 February
Knox
Switch to Personal mode
Tap here to exit Knox mode.
BLOCK NOTIFICATIONS
CLEAR
Excel
Gallery
Internet
Knox Settings
Messages
My Files
Personal home
Phone
PowerPoint
Samsung Keystring
Samsung Notes
Word

Figure 6

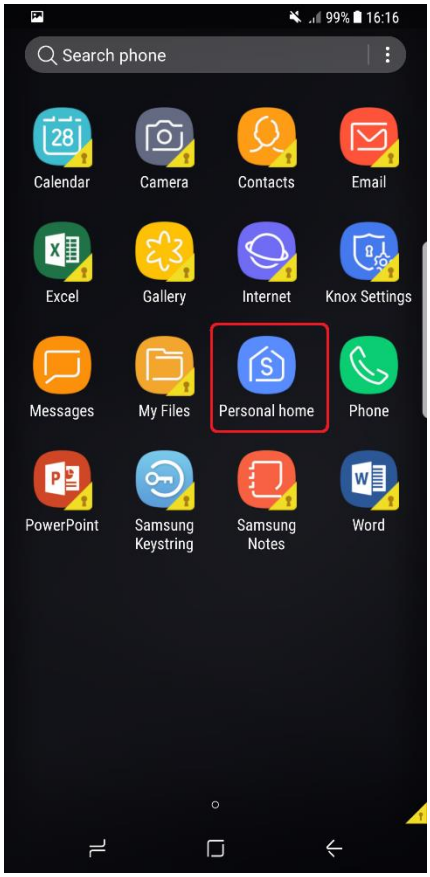

Figure 7

4.1.1.4 Leaving the KNOX Container – Folder Style

To leave the KNOX container and return to the personal side of the device just exit the app normally, for example by pressing the **HOME** button on the device. This will return you to the personal side automatically.

4.1.1.5 Manually locking the KNOX Container – Launcher Style

To manually lock and leave the KNOX container and return to the personal side of the device, tap the lock icon in the notification bar (Figure 8).

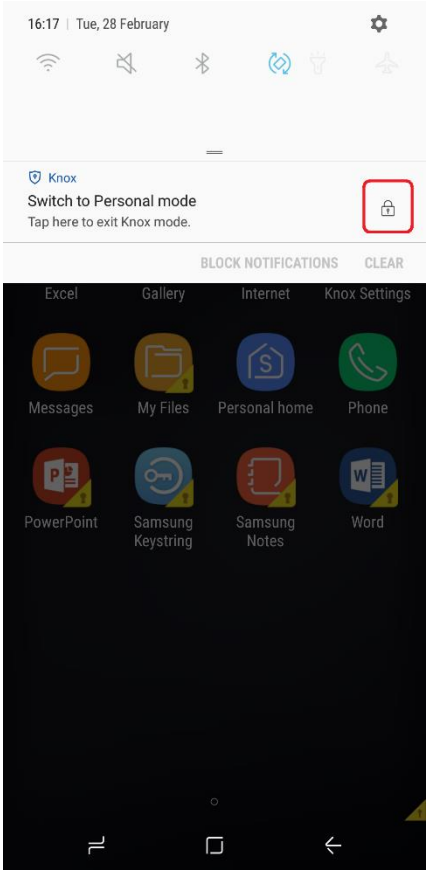

Figure 8

4.1.1.6 Manually locking the KNOX Container – Folder Style

To manually lock the KNOX container, tap the menu icon in the upper-right corner of the KNOX folder and tap **Lock** (Figure 9).

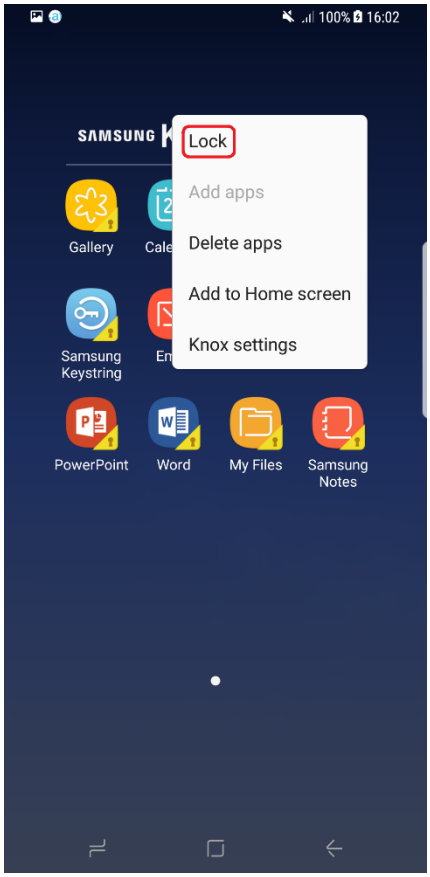

Figure 9

4.1.2 Changing your Password

4.1.2.1 Password change in the Personal Space

To change your password at any time you follow the same steps as setting it. To change your password:

1. Open ***Settings/Lock screen and security*** and select ***Screen lock (type)***
2. Enter your current password
3. Select ***Password*** from the ***Select screen lock*** menu
4. Enter and confirm your new password

4.1.2.2 Password change in the Knox Container

Password changes for both the device and the KNOX container are done in the same way, but to change the KNOX container password you must already be inside the KNOX container before following these steps.

1. Select ***KNOX Settings*** from the container applications
2. Select ***KNOX unlock method***
3. Depending on the minimum password complexity configured by your administrator, some options will not be available to the end user.

4.1.3 Check for a Software Update

While you will be notified when a software update is available, due to carrier rollout schedules it may be possible to access an update before you are notified. To check for a software update, go to ***Settings /Software update***. Selecting ***Download updates manually*** to check if a new update is available.

If an update is available, you will be prompted to download and install the update at this time. The integrity and validity of the update are automatically checked by the phone using embedded keys before installing the update.

Note: When the device is configured in CC Mode over the air updates are the only method allowed for updating the operating system and firmware.

4.1.4 Managing Applications

Over time you will want to remove apps that have been installed on your device (this may be managed by an MDM if you have enrolled the device to be managed). While this can be done through the Play Store, the best place is the Application Manager. This can be found under ***Settings/Apps*** or ***Application***. From here you can see a list of all apps that have been installed regardless of the source (i.e. from here you can see apps that have been "sideloaded" or installed from an alternative App Store such as Amazon along with any Play Store apps). Selecting an all and then Uninstall will remove the app and associated data from your device.

4.1.4.1 Application Access to Privileged Services

Any time an application is installed you will be prompted to accept its request to access various privileges on the system. For example, an application could request access to the Location services during the installation process. At that time, you can choose to allow access to the requested privilege/service or refuse to allow the application to be installed. You must accept all the requested privileges. There isn't any way to selectively authorize the requested permissions.

4.1.5 Wipe/Erase the Device

It is possible to erase all data on the device and reset it to the factory defaults. This is available under ***Settings/General management/Reset***. Selecting ***Factory data reset*** will erase all the data stored on the internal storage device. Upon restarting the device, it will wipe all the existing data and the device will prompt to be setup as on the first startup.

4.1.6 Wipe/Erase SD Card

To erase the data on the SD Card you must format the SD Card. This is available under ***Settings/Device maintenance/Storage***. Select the menu option ***Storage settings*** and then select the ***SD card***. Select ***Format*** to reformat the card and all data will be deleted.

4.1.7 Sensitive Data Protection

Samsung has added capabilities for Sensitive Data Protection. This feature is designed to allow applications which 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 Email application within KNOX.

The API exists both for the whole device and KNOX, but unless an application has been written to the API, it will not take advantage of the Sensitive Data Protection function.

4.1.8 Using Google Backup

Google provides the ability to back up some critical information from your device to the cloud so it can be restored later if the device is wiped. This can include information such as the Wi-Fi configuration, the apps installed, Google application settings, and some other local settings (like the user dictionary). While this can make moving to new devices much easier, it is possible that storing some of this information could violate your company policies and so you should verify whether this is allowed with your Administrator.

This can be managed through ***Setting/Cloud and Accounts/Backup and restore*** and enabling or disabling the ***Back up my data*** setting for the appropriate service. A Google account associated with the device will be used for the backup.

Note: Any data backed up to Google is not covered by any security functions on the device.

4.2 Access rights and policy

Your access to applications and device functions will be dependent on your enterprise security settings and policies – you may be able to install applications from the Samsung Apps or Google Play stores, or you may be restricted to a set of pre-installed applications. Contact your enterprise security team for more information on your security settings and mobile policy.

At a minimum, you should be able to do the following with your device:

- Send/receive phone calls (applicable devices only);
- Send/receive text messages (applicable devices only);
- Browse the internet;
- View system information via the Setting menu;
- Access default applications; and
- Change certain settings (lock screen password, initiate local wipe, etc.)

4.3 Modes of operation

Your device is designed to operate in a single mode, which is the standard operational mode (i.e., your device is turned on and is operating normally). If an error occurs, your system may enter error mode and will provide you with feedback regarding the error or fault that has occurred.

If an error occurs, if the device allows, clear the error and continue to use the device as normal. If the device does not let you continue use, or you are concerned about the cause of the fault, contact your technical support department or phone distributor for technical assistance.

4.4 Errors

When using the device, you may encounter a number of security-relevant errors. This section will provide an overview of these errors and their causes.

Incorrect Password/PIN: The password or PIN number to access your device has been entered incorrectly. Entering the correct authentication data will allow you to access the device.

Password Length/Complexity: Your enterprise security settings will place certain requirements when setting a password for your device regarding length, complexity and types of characters used. If you receive this error, ensure that your proposed password meets the requirements.

Error Encrypting/Decrypting Storage: An error has occurred within the Android OS that has caused the device to fail when encrypting or decrypting your devices internal or external (SD card) storage. This may be caused by a temporary fault within the device (such as a cryptographic module error) or may indicate a hardware issue.

Access/Permissions Denied: Your current enterprise settings do not permit you to access a particular function or application. If you feel this is in error, contact your enterprise security team.

Invalid Application Signature: All applications installed on your device must have a verifiable digital signature, applied by the developer. If this error occurs, an application you have chosen to install is either missing or has an invalid signature. You may contact the application developer or Google Play support to resolve this.

Device Lockout: Your device has received too many invalid authentication attempts in a preset time period and is locked from use. At this point your whole device will be wiped with all data and apps being deleted.

KNOX Container Lockout: Your KNOX container has received too many invalid authentication attempts in a preset time period and is locked from use. At this point the KNOX Container contents will be wiped (but content outside the KNOX Container will be preserved).

Note: If you are unsure as to why an error has occurred or feel it has occurred unexpectedly, please contact your technical support department for assistance.

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 sources for 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	developer.android.com

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.