Samsung VPN Client on Galaxy Devices

VPN User Guidance Documentation

Version 3.1

November 13, 2017

Document management

Document identification

Document ID	Samsung VPN User Guidance Documentation 3.1.
Document title	Samsung VPN Client on Galaxy Devices VPN User Guidance Documentation
Release authority	

Document history

Version	Date	Description	Author
0.1	April 2, 2014	Initial version	Brian Wood
0.2	April 4, 2014	Updated based on info about server cert field	Brian Wood
0.3	April 7, 2014	Updated supported devices list	Brian Wood
0.4	April 21, 2014	Updated based on evaluation feedback	Brian Wood
0.5	May 13, 2014	Updated device list	Brian Wood
0.6	June 6, 2014	Modified device list table	Brian Wood
0.7	September 15, 2014	Updated device list	Brian Wood
0.8	September 19, 2014	Updated device list	Brian Wood
1.0	October 7, 2014	Edited versions and CC Mode access	Brian Wood
1.1	October 28, 2014	Updated device list	Brian Wood
2.0	December 17, 2014	Edited for Android 5	Brian Wood
2.1	April 10, 2015	Updated device list	Brian Wood
2.2	September 10, 2015	Updated device list, added support for IKEv1	Brian Wood
2.3	March 23, 2016	Updated device list	Brian Wood

2.4	July 13, 2016	Updated device list	Brian Wood
3.0	April 18, 2017	Updated for Android 7	Brian Wood
3.1	November 13, 2017	Updated device list	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*** and ***Settings/About device/Software information***. The following are version information that 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 VPN evaluation for the mobile device, this will show:

VPN v**ABC** Release **XYZ**

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

3 Secure VPN 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 configure the VPN.

Several of the steps here explain how to enroll the device into an MDM or to enable Common Criteria Mode. One of these steps is necessary to place the VPN into the validated configuration.

Note: While the VPN configuration is related to the Mobile Device Fundamentals evaluation, it is not required to completely configure the device into the MDF evaluated configuration. The directions here focus on the VPN configuration only.

The validated configuration only supports IKEv1 Xauth and IKEv2 VPN configurations. While other types of VPN configurations may be available, only IKEv1 Xauth and IKEv2 tunnels are part of the validated configuration.

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 may need to enable Unknown Sources for applications if the Agent will not be installed from the Google Play Store. This can be achieved by going to ***Settings/Lock screen and 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. If your MDM is available through the Play Store this is not necessary.

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, which is required for the VPN to be in the 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.

For full instructions on configuring the device into the CC Mode, review the Common Criteria User Guidance Documentation for the device that can be found at the same website.

3.2.1 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/Software Information/Software Security Version***.

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

Note: For the VPN it is only necessary for the CC Mode status to be Enforced. When used in combination with the MDF configuration, CC Mode must be Enabled.

3.2.2 VPN Requirements/Configurations

When CC Mode is first turned on, it changes the status from Disabled to Enforced. In addition to this setting, the VPN requires the user set a PIN or password to protect the configuration. While either authentication method can be used, it is recommended to use a password to match the MDF configuration.

See the following sections on how to set the PIN/password and to configure the VPN.

3.3 Setting a PIN/Password

The first thing to do (if it hasn't already been done) is to set a PIN or password for the device. These are set under ***Settings/Lock screen and security***.

To enable a PIN/Password:

1. Select ***Screen lock type***
2. Select ***PIN*** or ***Password***
3. Enter the ***PIN*** or ***Password*** and then enter it twice to confirm.
4. Click ***OK***

You will now be required to enter the PIN or Password to unlock the device.

3.4 Creating a VPN Tunnel

Samsung provides a VPN client on the validated devices that can support IKEv1 Xauth or IKEv2 tunnels. This tunnel is accessed through the normal VPN user interface and then selecting the appropriate options for the type of connection.

Access to the VPN interface is through ***Settings/Connections/More connection settings/VPN***.

Note: On some devices (dependent on the Carrier), there may be two further selections under **VPN**. Choose the ***Basic VPN*** to access the validated VPN client.

Note: Many fields are marked with **Not used**. Entries can be made in these fields but normally they would be left blank. The VPN admin would specify any information for these fields.

3.4.1 IPSec IKEv2 Pre-Shared Key Tunnel

To setup an IKEv2 VPN tunnel using a Pre-Shared Key (PSK), tap the **+** in the upper right-hand corner to add a new VPN tunnel. Enter the following information:

- **Name** – specify a name for the VPN
- **Type** – select ***IPSec IKEv2 PSK***

- **Server address** – enter the IP address or Fully Qualified Domain Name of the VPN gateway
- **IPSec identifier** – enter the IPSec ID for the connection. This may not be used and would be provided by the VPN admin
- **IPSec pre-shared key** – enter the PSK provided by the VPN admin for the connection
    - The PSK can be either ASCII or HEX. To enter a HEX PSK start the entry with "0x"
- **Always-on VPN** – select this to require all connectivity to be forced to go through this VPN

Tap ***SAVE*** to save the VPN configuration.

3.4.2 IPSec IKEv2 Certificate Tunnel

To setup and IKEv2 VPN tunnel using certificates, tap the **+** in the upper right-hand corner to add a new VPN tunnel. Enter the following information:

- **Name** – specify a name for the VPN
- **Type** – select ***IPSec IKEv2 RSA***
- **Server address** – enter the IP address or Fully Qualified Domain Name of the VPN gateway
- **IPSec user certificate** – select the user certificate from the drop down list that will be used to authenticate the device to the VPN gateway
- **IPSec CA certificate** – select the CA certificate used to validate the VPN gateway certificate from the drop down list
- **IPSec server certificate** – this certificate can be used to override the downloaded certificate from the gateway. If loaded, this certificate will always be used for the VPN tunnel.

Note: The **IPSec server certificate** can only be loaded through the user interface and cannot be specified through the MDM.

The server certificate must be loaded into Credential Storage separately from any other certificate (i.e. it cannot be bundled with a client or CA certificate in the same P12 file). It should be loaded from its own DER file.

- **Always-on VPN** – select this to require all connectivity to be forced to go through this VPN

See the section below about Certificate Management for more information about loading certificates onto the device for use in the VPN configuration.

3.4.2.1 Valid Certificate Types

While the menu selection for the type of tunnel states ***IPSec IKEv2 RSA*** it is possible to utilize both RSA and ECC certificates for the tunnel. As long as the certificates are valid (not expired, properly formatted, etc) they can be used for the VPN configuration.

3.4.2.2 Advanced Options - OCSP

When any VPN tunnel is configured there are certain advanced options that may be configured. These are not required but can be used. Of these, one is potentially important for the VPN evaluation, the OCSP web address.

For organizations using OCSP to validate certificates, it may be necessary to specify the OCSP server to be used for validation (this may also be specified as part of the CA Certificate, but not always). To configure this option:

- Check the ***Show advanced options*** box
- Enter the URL for the OCSP server in the ***OCSP Web address*** field

Note: The **OCSP Web address** field is only shown when CC Mode has been turned on.

3.4.3 IPSec Xauth IKEv1 Pre-Shared Key Tunnel

To setup an IKEv1 Xauth VPN tunnel using a Pre-Shared Key (PSK), tap the **+** in the upper right-hand corner to add a new VPN tunnel. Enter the following information:

- **Name** – specify a name for the VPN
- **Type** – select ***IPSec Xauth PSK***
- **Server address** – enter the IP address or Fully Qualified Domain Name of the VPN gateway
- **IPSec identifier** – enter the IPSec ID for the connection. This may not be used and would be provided by the VPN admin
- **IPSec pre-shared key** – enter the PSK provided by the VPN admin for the connection
    - The PSK can be either ASCII or HEX. To enter a HEX PSK start the entry with “0x”

- **Always-on VPN** – select this to require all connectivity to be forced to go through this VPN

Tap ***SAVE*** to save the VPN configuration.

3.4.4 IPSec Xauth IKEv1 Certificate Tunnel

To setup and IKEv1 Xauth VPN tunnel using certificates, tap the **+** in the upper right-hand corner to add a new VPN tunnel. Enter the following information:

- **Name** – specify a name for the VPN
- **Type** – select ***IPSec Xauth RSA***
- **Server address** – enter the IP address or Fully Qualified Domain Name of the VPN gateway
- **IPSec user certificate** – select the user certificate from the drop down list that will be used to authenticate the device to the VPN gateway
- **IPSec CA certificate** – select the CA certificate used to validate the VPN gateway certificate from the drop down list
- **IPSec server certificate** – this certificate can be used to override the downloaded certificate from the gateway. If loaded, this certificate will always be used for the VPN tunnel.

Note: The **IPSec server certificate** can only be loaded through the user interface and cannot be specified through the MDM.

The server certificate must be loaded into Credential Storage separately from any other certificate (i.e. it cannot be bundled with a client or CA certificate in the same P12 file). It should be loaded from its own DER file.

- **Always-on VPN** – select this to require all connectivity to be forced to go through this VPN

See the section below about Certificate Management for more information about loading certificates onto the device for use in the VPN configuration.

3.4.4.1 Valid Certificate Types

The ***IPSec Xauth RSA*** setting only accepts RSA (unlike the IKEv2 which can accept both RSA and ECDSA) certificates for the tunnel. As long as the certificates are valid (not expired, properly formatted, etc) they can be used for the VPN configuration.

Note: It is possible to specify an ECDSA certificate that has been loaded into the system, but it cannot be used to establish a connection.

3.4.4.2 Advanced Options - OCSP

When any VPN tunnel is configured there are certain advanced options that may be configured. These are not required but can be used. Of these, one is potentially important for the VPN evaluation, the OCSP web address.

For organizations using OCSP to validate certificates, it may be necessary to specify the OCSP server to be used for validation (this may also be specified as part of the CA Certificate, but not always). To configure this option:

- Check the ***Show advanced options*** box
- Enter the URL for the OCSP server in the ***OCSP Web address*** field

3.4.5 Always-on VPN

In many cases it may be desired (or required) to have a VPN tunnel attempt to auto-reconnect to the gateway after a loss or change in network connectivity. This can be done by specifying the tunnel for Always-on VPN. When a VPN tunnel is specified as Always-on the device will not be allowed to connect to the network without a VPN tunnel, so if the VPN disconnects the device will no connect to the Internet directly but will attempt to reconnect to the VPN gateway automatically.

The choice for Always-on can be made in the VPN profile at the bottom of each profile configuration.

Note: In general you should only set a single VPN tunnel to be Always-on. More advanced configurations can be made by the admin using an MDM.

3.5 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.

3.5.1 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.

Note: To setup a VPN connection using certificates the CA Certificate must be loaded for the VPN gateway (if it is not a trusted CA).

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*** and then under ***Other security settings*** select ***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.

3.5.2 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.

3.5.2.1 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

3.5.2.2 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

3.5.3 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*** and then under ***Other security settings*** select ***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.

3.5.3.1 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.

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:

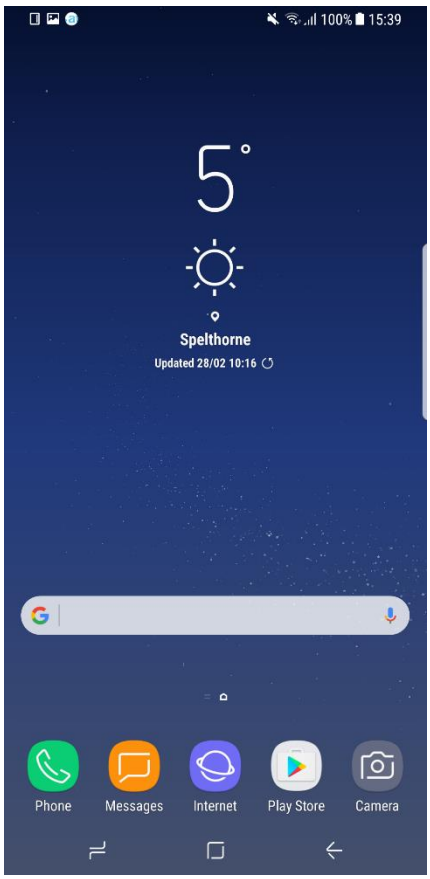

Figure 1 – Galaxy TouchWiz interface

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.

4.1.2 Changing your Password

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

4.1.3 Connecting to the VPN

If you have not enabled a VPN connection for Always-on VPN, you must manually connect to the VPN when needed. This is done by going to ***Settings/Connections/More connection settings/VPN*** and tapping the desired VPN connection. This will bring up a dialog box asking to connect to the VPN.

4.1.4 Editing a VPN Tunnel

To edit a VPN tunnel after it has been created, go to ***Settings/Connections/More connection settings/VPN***. Click the settings gear for the VPN you need to edit or delete. The settings can be edited and then clicking ***Save*** to update the configuration. Clicking ***Delete*** will remove the VPN configuration.

4.1.5 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*** and select ***Download updates manually***. This will prompt you to confirm the check for a new update and then contact the appropriate update server to see 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.

4.2 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. Your device will unlock after a period of time (set by your enterprise security team) and will be ready for use.

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.