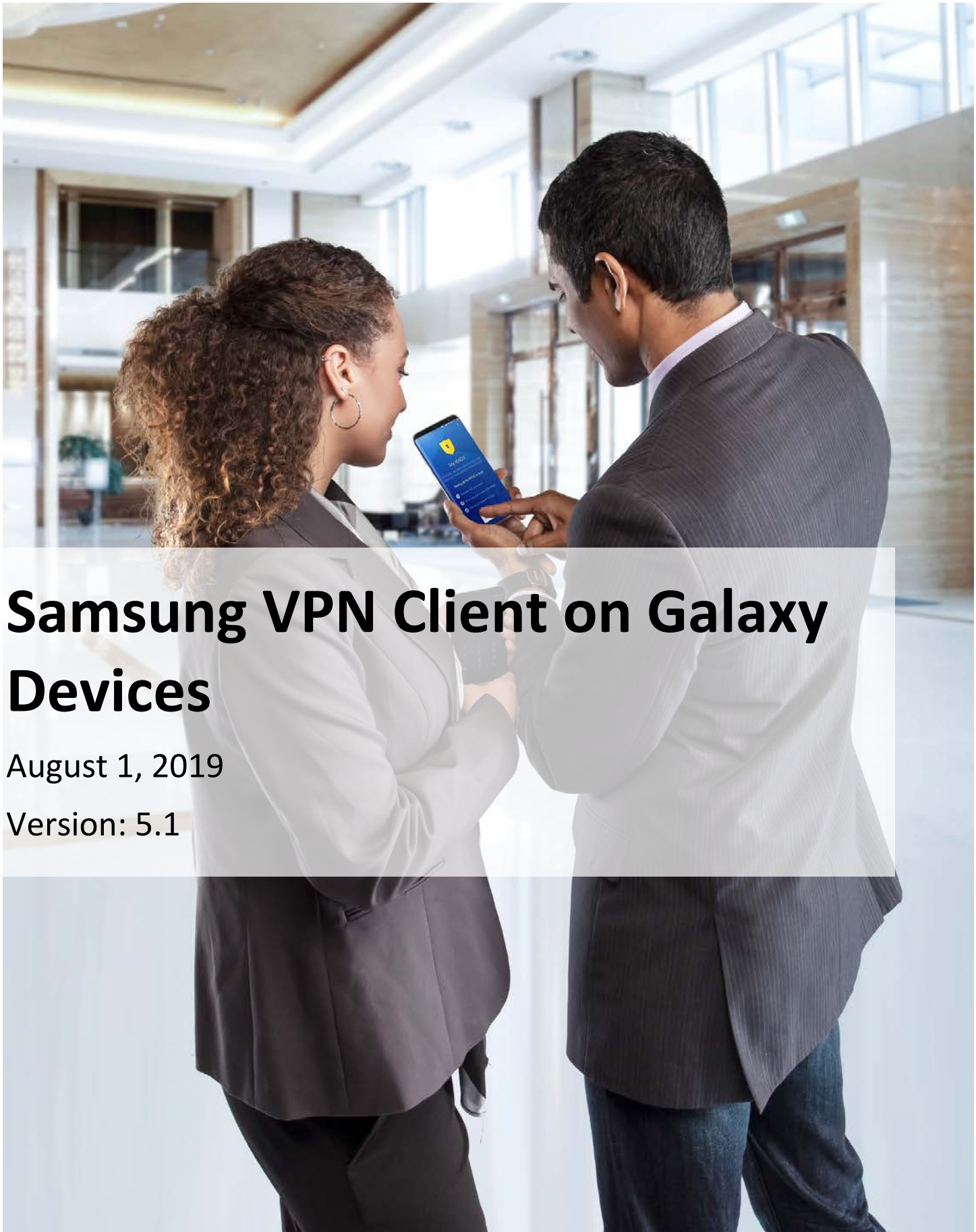
SAMSUNG

Administrator Guide



Samsung VPN Client on Galaxy Devices

August 1, 2019

Version: 5.1

Copyright Notice

Copyright © 2018 Samsung Electronics Co. Ltd. All rights reserved. Samsung is a registered trademark of Samsung Electronics Co. Ltd. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

About this document

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

Document Identification

Document ID	Samsung VPN Admin Guidance v5.1
Document Title	Samsung VPN Client on Galaxy Devices Administrator Guide

Revision History

Version	Date	Changes	Author
4.0	March 28, 2018	Android 8, new template	Brian Wood
4.1	September 11, 2018	Android 8.1, added new devices	Brian Wood
5.0	May 22, 2019	Android 9, Generic VPN	Brian Wood, Parashuram Chawan
5.1	August 1, 2019	Added new devices	Brian Wood

Contents

1 Introduction

1.1 Scope of Document

This document is intended as a guide for administrators deploying Samsung devices using the built-in Samsung VPN client in the enterprise. The guidance provided here focuses on how to configure devices to be in an approved configuration based on the PP-Module for Virtual Private Network (VPN) Clients v2.1 for the Samsung devices specified here.

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

1.1.1 End-User Guidance

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

1.2 Overview of Document

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

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

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

1.3 Terminology & Glossary

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

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

Table 1 - Acronyms

1.4 Evaluated Devices

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

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

- Samsung Exynos and Qualcomm Snapdragon
  - Galaxy S9+ (Spring 2019)
  - Galaxy Note8 (Spring 2019)
- Samsung Exynos
  - Galaxy S10e (Spring 2019)
- Qualcomm Snapdragon
  - Galaxy S10+ (Spring 2019)

1.4.1 Device Equivalency Claims

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

Evaluated Device	Processor	Equivalent Devices	Differences
Galaxy S10e (Samsung)	Exynos 9820	Galaxy S10 (Samsung) Galaxy S10+ (Samsung) Galaxy S10 5G (Samsung)	• S10 & S10+ have ultrasonic fingerprint sensor • S10 & S10+ have larger screen sizes • S10 5G has different cellular modem
Galaxy S10+ (Qualcomm)	SM8150	Galaxy S10e (Qualcomm) Galaxy S10 (Qualcomm) Galaxy S10 5G (Qualcomm) Galaxy Fold (Qualcomm) Galaxy Note10 (Qualcomm) Galaxy Note 10+ (Qualcomm) Galaxy Note10+ 5G (Qualcomm) Galaxy Tab S6	• S10e & Fold has side image fingerprint sensor • S10 & S10e have smaller screen sizes • Fold has 2 screens • Note10 & Note10+ have larger screen sizes • S10 & Note10+ 5G has different cellular modem • Note10 devices include S Pen & functionality to take advantage of it for input (not security related) • Tab S6 (T86x) is tablet form factor (no voice calling) with S Pen • T865 & T867 tablets have LTE • T860 tablets only have Wi-Fi
Galaxy S9+ (Samsung)	Exynos 9810	Galaxy S9 (Samsung) Galaxy Note9 (Samsung)	• S9 has smaller screen • Note9 includes S Pen & functionality to take advantage of it for input (not security related)
Galaxy S9+ (Qualcomm)	SDM845	Galaxy S9 (Qualcomm) Galaxy Note9 (Qualcomm)	• S9 has smaller screen • Note9 includes S Pen & functionality to take advantage of it for input (not security related)
Galaxy Tab S4 (T837A)	Snapdragon 835	Galaxy Tab S4	• T835 & T837 models have LTE T830 models only have Wi-Fi
Galaxy Note8 (Samsung)	Exynos 8895	Galaxy S8 (Samsung) Galaxy S8+ (Samsung)	• S8 & S8+ do not include S Pen • S8 & S8+ are smaller
Galaxy Note8 (Qualcomm)	MSM8998	Galaxy S8 (Qualcomm) Galaxy S8+ (Qualcomm) Galaxy S8 Active (Qualcomm) Galaxy Tab S4 (All)	• S8, S8+ & S8 Active do not include S Pen • S8, S8+ & S8 Active are smaller • S8 Active has a IP68 & MIL-STD-810G certified body • Tab S4 (T83x) is tablet form factor (no voice calling) • T835 & T837 tablets have LTE • T830 tablets only have Wi-Fi

Table 2 - Device Equivalence

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

1.4.2 Device Details

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

Device Name	Base Model Number	Android Version	Kernel Version	Build Number	Carrier Models
Galaxy Note10+ 5G (Qualcomm)	SM-N976	9.0	4.14.85	PPR1.180610.011	U, V
Galaxy Note10+ (Qualcomm)	SM-N975	9.0	4.14.85	PPR1.180610.011	C, U, SC-01M*, SCV45*
Galaxy Note10 (Qualcomm)	SM-N970	9.0	4.14.85	PPR1.180610.011	U
Galaxy Tab S6	SM-T867	9.0	4.14.85	PPR1.180610.011	R4, U, V
	SM-T865	9.0	4.14.85	PPR1.180610.011	N, None
	SM-T860	9.0	4.14.85	PPR1.180610.011	None
Galaxy S10 5G (Samsung)	SM-G977	9.0	4.14.85	PPR1.180610.011	B, N
Galaxy S10 5G (Qualcomm)	SM-G977	9.0	4.14.78	PPR1.180610.011	P, T, U
Galaxy S10+ (Samsung)	SM-G975	9.0	4.14.85	PPR1.180610.011	F, N
Galaxy S10+ (Qualcomm)	SM-G975	9.0	4.14.78	PPR1.180610.011	U, SC-04L*, SCV42*
Galaxy S10 (Samsung)	SM-G973	9.0	4.14.85	PPR1.180610.011	F, N
Galaxy S10 (Qualcomm)	SM-G973	9.0	4.14.78	PPR1.180610.011	U, SC-03L*, SCV41*
Galaxy S10e (Samsung)	SM-G970	9.0	4.14.85	PPR1.180610.011	F, N
Galaxy S10e (Qualcomm)	SM-G970	9.0	4.14.78	PPR1.180610.011	U
Galaxy Fold	SM-F900	9.0	4.14.78	PPR1.180610.011	F, N, U, SC-06L*, SCV44*
Galaxy Note9 (Samsung)	SM-N960	9.0	4.9.59	PPR1.180610.011	F, N
Galaxy Note9 (Qualcomm)	SM-N960	9.0	4.9.112	PPR1.180610.011	U, SC-01L*, SCV40*
Galaxy Tab S4	SM-T830	9.0	4.4.153	PPR1.180610.011	None
	SM-T835	9.0	4.4.153	PPR1.180610.011	N, None
	SM-T837	9.0	4.4.153	PPR1.180610.011	A, R4, P, V, T
Galaxy S9+ (Samsung)	SM-G965	9.0	4.9.59	PPR1.180610.011	F, N

Device Name	Base Model Number	Android Version	Kernel Version	Build Number	Carrier Models
Galaxy S9+ (Qualcomm)	SM-G965	9.0	4.9.112	PPR1.180610.011	U, SC-03K*, SCV39*
Galaxy S9 (Samsung)	SM-G960	9.0	4.9.59	PPR1.180610.011	F, N
Galaxy S9 (Qualcomm)	SM-G960	9.0	4.9.112	PPR1.180610.011	U, SC-02K*, SCV38*
Galaxy Note8 (Samsung)	SM-N950	9.0	4.4.111	PPR1.180610.011	F, N
Galaxy Note8 (Qualcomm)	SM-N950	9.0	4.4.153	PPR1.180610.011	U, SC-01K*, SCV37*
Galaxy S8+ (Samsung)	SM-G955	9.0	4.4.111	PPR1.180610.011	F, N
Galaxy S8+ (Qualcomm)	SM-G955	9.0	4.4.153	PPR1.180610.011	U
Galaxy S8 (Samsung)	SM-G950	9.0	4.4.111	PPR1.180610.011	F, N
Galaxy S8 (Qualcomm)	SM-G950	9.0	4.4.153	PPR1.180610.011	U
Galaxy S8 Active	SM-G892	9.0	4.4.153	PPR1.180610.011	A, U

Table 3 - Device Details

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

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

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

Table 4 - Security Software Versions

The version number is broken into two parts showing the Protection Profile or Extended Package version as well as the software version that is certified. For example, the Galaxy S10 would show “VPN PP-MOD v2.1 Release 2.0”.

1.5 References

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

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

Table 5 – Reference Websites

2 VPN Deployment

2.1 VPN Overview

The TOE is a VPN running on Android 9 with modifications made to increase the level of security provided to end users and enterprises. The TOE is intended for use as part of an enterprise mobility solution providing mobile staff with enterprise connectivity. With a focus on enterprise security, the TOE supports both IKEv1 and IKEv2 VPN tunnels using both Pre-Shared Keys as well as certificates, providing flexibility based on the environment.

The TOE combines with an EDM solution that enables the enterprise to manage VPN tunnels for mobile devices to facilitate secure communications back to the enterprise network. This partnership provides a secure mobile environment that can be managed and controlled by the environment and reduce the risks that can be introduced when enabling mobility in the enterprise, whether through a Bring-Your-Own-Device (BYOD) or a Corporate-Owned deployment.

The Samsung Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration of options to over 600 configurable policies and including additional security functionality such as application blacklisting. The ability to set these policies is based on the capabilities of the EDM.

2.2 Evaluated VPN Capabilities

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

Security Feature	Description
Secure Channel. Enterprise devices can securely connect to the enterprise network.	**VPN.** The TOE provides a secure communications channel to the VPN Gateway.
Enterprise Device Management. Enterprise administrators can control mobile endpoint configurations.	**Security policy.** The TOE can be configured by a Mobile Device Management solution that supports the Samsung Enterprise SDK.

Table 6 – VPN Security Features

2.3 Deployment Architecture

More information about deployment of Samsung mobile devices, review the document *Samsung Android 9 on Galaxy Devices Administrator Guide*, which can be downloaded at the Samsung Knox Portal link found in section 1.5 References.

3 Common Criteria Configuration

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

3.1 Approved Cryptography

Part of the Common Criteria-evaluated configuration is the availability of approved cryptographic engines for use by the system and applications. Samsung has chosen to utilize NIST-validated cryptographic algorithms within the cryptographic modules on its devices for the Common Criteria configuration. These algorithms are used by the VPN client to perform all cryptographic operations.

Samsung provides the following cryptographic modules with NIST-validated algorithms on all the evaluated devices:

- Samsung Kernel Cryptographic Module
- Samsung BoringSSL Cryptographic Module
- Samsung SCrypto Cryptographic Module

All modules always run in a FIPS-validated mode and the VPN client only uses FIPS-approved algorithms.

3.2 Common Criteria (CC) Mode

To utilize the VPN client as it has been evaluated, the device must be placed into the Common Criteria (CC) Mode. For more information about placing the device into CC Mode review the document *Samsung Android 9 on Galaxy Devices Administrator Guide*, which can be downloaded at the Samsung Knox Portal link found in section 1.5 References.

3.3 VPN Client Settings

The settings here all relate to the configuration of the VPN client profile. The specific settings here can be used for profiles that are compliant with the Common Criteria configuration.

3.3.1 VPN Profile Settings (Standard APIs)

Setting	Value	Description	Class or Method
Profile Management	Profile name	Create, rename and delete VPN profiles	createProfile() setProfileName() deleteProfile()

Setting	Value	Description	Class or Method
VPN Type Setting		The types of VPN connections that can be set. Those listed here are the only validated types.	VPN_TYPE_IPSEC_XAUTH_PSK VPN_TYPE_IPSEC_XAUTH_RSA VPN_TYPE_IPSEC_IKEV2_PSK VPN_TYPE_IPSEC_IKEV2_RSA (see below)
VPN Settings (PSK)		The settings needed to configure the VPN tunnel when using a Pre-Shared Key.	setServerName() setIpSecIdentifier() setIPSecPreSharedKey()
VPN Settings (certificate)		The settings needed to configure the VPN tunnel when using a certificate.	setServerName() setIPSecCaCertificate() setIPSecUserCertificate() setOcspServerUrl()
VPN Optional Network Settings		These settings provide additional network configuration and routing options for the tunnel.	setDnsDomains() setDnsServers() setForwardRoutes()
Always-on VPN	Enable/ Disable	Specifies whether all traffic must go through the specified VPN tunnel. If no connection can be made no traffic will flow.	setAlwaysOnProfile()
User Control	Enable/ Disable	Whether the user is allowed to create new VPN profiles, change profiles or modify the Always-on VPN setting.	allowUserAddProfiles() allowUserChangeProfiles() allowUserSetAlwaysOn()

Table 7 – VPN Profile Settings

3.3.1.1 Valid Certificate Types for IKEv1

The IPsec Xauth RSA setting only accepts RSA 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 to the gateway.

3.3.1.2 Valid Certificate Types for IKEv2

While the menu selection for the type of tunnel states IPsec IKEv2 RSA it is possible to utilize 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.

3.3.1.3 Specifying a Strong Pre-Shared Key

A PSK (Pre-shared key) is like a password, a fixed string used to authenticate the VPN client to the VPN gateway. Since the PSK does not change (or at least does not change often), a strong string should be selected to protect against unauthorized access to the VPN by unknown clients.

The PSK can be entered in two forms: ASCII or HEX. All ASCII characters are supported. HEX keys must start with “0x” as the first two characters entered. If those are the first two characters, the remaining entry will be read as a HEX key. The maximum key size is 64 characters entered.

The PSK will be provided by the organization for entry (since this is something that must match the value on the VPN Gateway). The PSK is recommended to be at least 22 characters long and if not HEX, a mix of letters numbers and symbols.

3.3.1.4 Server Certificate for the Gateway

It is possible to specify a Server Certificate for the Gateway in the configuration of a VPN tunnel. This certificate will override any certificate provided by the Gateway during the negotiation of the tunnel.

This certificate may be loaded through the UI or EDM. See the device User Guidance for more information about loading certificates manually.

3.3.2 VPN Profile Settings (Knox Generic API)

Configuring the VPN via Knox Generic VPN APIs has the benefit of allowing per-app routing to the VPN client. For example, all container packages can be forced to go through one tunnel, while personal applications are routed through another, or not at all.

Using Knox Generic APIs requires installation of the StrongSwan “Proxy APK” on the device, which translates configuration received through these APIs onto the underlying client itself. Note that regardless of the method chosen for configuring it, the built-in StrongSwan client is the same.

Setting	Value	Description	Class or Method
Create and Configure Profile		Create a VPN profile. **The profile configuration is provided as a JSON string**	createVpnProfile()
Per-app VPN	All packages added	Specify packages that will use the VPN profile	addPackagesToVpn() addAllPackagesToVpn() addContainerPackagesToVpn() addAllContainerPackagesToVpn ()
VPN Profile Activation		Activate/Deactivate the given profile	activateVpnProfile()
Profile Management		Create, rename and delete VPN profiles	removeVpnProfile()

Table 8 – VPN Activation APIs

Setting	Value	Description	JSON Key
VPN Basic Settings		The basic settings for the VPN tunnel.	host username password authentication_type

Setting	Value	Description	JSON Key
Authentication Type Setting		The types of VPN connections that can be set. Those listed here are the only validated types.	ipsec_xauth_psk ipsec_xauth_rsa ipsec_ike2_psk ipsec_ike2_rsa
VPN Settings (PSK)		The settings needed to configure the VPN tunnel when using a Pre-Shared Key.	pre_shared_key
VPN Settings (certificate)		The settings needed to configure the VPN tunnel when using a certificate.	ca_cert_alias user_cert_alias server_cert_alias
VPN Optional Network Settings		These settings provide additional network configuration and routing options for the tunnel.	dns_search_domains dns_servers frwd_routes
Always-on VPN	Enabled	Specifies whether all traffic must go through the specified VPN tunnel. If no connection can be made no traffic will flow.	connectionType

Table 9 – VPN Settings

Provided the profile configuration string has been created as per the next section, the API flow for creating and starting a VPN connection will be createVpnProfile() -> addPackagesToVpn() -> activateVpnProfile() API.

The API flow for removing a VPN profile will be activateVpnProfile() (De-activate it) -> removeVpnProfile() API.

3.3.2.1 JSON Configuration String

```
{
  "KNOX_VPN_PARAMETERS": {
    "profile_attribute": {
      "profileName": "ss1",
      "host": "",
      "isUserAuthEnabled": true,
      "vpn_type": "ipsec",
      "vpn_route_type": 1
    },
    "knox": {
      "connectionType": "keepon",
      "chaining_enabled": "-1",
      "uidpid_search_enabled": "0"
    },
    "vendor": {
      "basic": {
       "autoretry": "1",
        "username": "sampleu",
        "password": “samplepw",
        "authentication_type": "type",
        "host": "111.111.111.111"
      },
      "ipsec_xauth_psk": {
        "identifier": "test@sta.com",
        "pre_shared_key": "example",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ]
      },
      "ipsec_xauth_rsa": {
        "user_cert_alias": "",
        "ca_cert_alias": "",
        "server_cert_alias": "",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ]
      },
      "ipsec_ike2_psk": {
        "identifier": "test@sta.com",
        "pre_shared_key": "example",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ]
      },
      "ipsec_ike2_rsa": {
        "user_cert_alias": "",
        "ca_cert_alias": "",
        "server_cert_alias": "",
        "dns_search_domains": [],
        "dns_servers": [
          "8.8.8.8"
        ],
        "frwd_routes": [
          "10.0.0.0\/8"
        ],
        "ocsp_url": ""
      }
    }
  }
}
```

Example Xauth-PSK JSON (Other configurations in gray)

3.3.2.2 Valid Certificate Types for IKEv1

The IPsec Xauth RSA setting only accepts RSA 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 to the gateway.

3.3.2.3 Valid Certificate Types for IKEv2

While the menu selection for the type of tunnel states IPsec IKEv2 RSA it is possible to utilize 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.

3.3.2.4 Specifying a Strong Pre-Shared Key

A PSK (Pre-shared key) is like a password, a fixed string used to authenticate the VPN client to the VPN gateway. Since the PSK does not change (or at least does not change often), a strong string should be selected to protect against unauthorized access to the VPN by unknown clients.

The PSK can be entered in two forms: ASCII or HEX. All ASCII characters are supported. HEX keys must start with “0x” as the first two characters entered. If those are the first two characters, the remaining entry will be read as a HEX key. The maximum key size is 64 characters entered.

The PSK will be provided by the organization for entry (since this is something that must match the value on the VPN Gateway). The PSK is recommended to be at least 22 characters long and if not HEX, a mix of letters numbers and symbols.

3.3.2.5 Server Certificate for the Gateway

It is possible to specify a Server Certificate for the Gateway in the configuration of a VPN tunnel, by providing the server_cert_alias string corresponding to a certificate previously installed into the keystore. This certificate will override any certificate provided by the Gateway during the negotiation of the tunnel.

This certificate may be loaded through the UI or EDM. See the device User Guidance for more information about loading certificates manually.

3.3.3 Certificate/Key Management Settings

Setting	Value	Description	Class or Method
Import Certificates	Certs	Import CA Certificates into the Trust Anchor Database or the credential storage. The choice of storage is dependent on the type of certificate being imported.	installCertificate() installCertificatesFromSdCard() installCertificateWithType() installClientCertificate() (for VPN)
Remove Individual Certificates	Cert names	Remove Individual certificates from the database or credential store	removeCertificate()
Remove All Certificates		This will clear all imported Certificates (except the built-in TAD)	clearInstalledCertificates()
Certificate Revocation Checking	Enable for All apps	Specifies that CRL checking is enabled for all apps on the device	isRevocationCheckEnabled()

Table 10 – Certificate/Key Management Settings

3.4 VPN Gateway Configuration Control

There are many configuration options for a VPN tunnel that only be configured from the gateway. The VPN client will utilize these settings from the gateway configuration to construct the secure tunnel. The following is a list of the settings that must be configured through the gateway:

- Encryption settings – while the VPN client will use FIPS validated encryption, the gateway will specify which algorithms should be used.
- IKE Protocols & Authentication – the gateway specifies which IKE protocols authentication techniques are required for establishing the connection.

- IPsec Session Key cryptoperiod – the gateway specifies the session key cryptoperiod and can be used to configure periods under 1 hour in duration.

3.5 Using the VPN Client

3.5.1 Always-on Tunnel

When the device has a tunnel configured for Always-on VPN, all traffic will automatically go through this tunnel, and if for some reason a connection for the tunnel cannot be made, no traffic will be allowed to communicate off the device.

3.5.2 "Normal" VPN Tunnels

When VPN tunnels are configured and no tunnel is specified as Always-on, then the user must select the tunnel to be used. The user will select the tunnel from those available at ***Settings/Connections/More connection settings/VPN***.

4 Device Delivery and Updates

4.1 Secure Device Delivery

While a Samsung device requires initial configuration before it can be added to the enterprise environment, it is also critical to ensure that the device is received prior to configuration in a secure manner, free from tampering or modification.

It is very important that the devices to be deployed into the enterprise be obtained from reputable carriers to reduce the likelihood that tampering of devices may occur.

Upon receipt, the boxes containing the device should have both a tracking label and two labels placed at either end of the box to indicate whether the box has been opened prior to delivery. If these seals are broken, do not accept the device and return it to your supplier.

The tracking label should look similar to Figure 1 - Tracking Label, while the two tamper labels should appear similar to Figure 2 - Security Seal (Black) or Figure 3 - Security Seal (White).

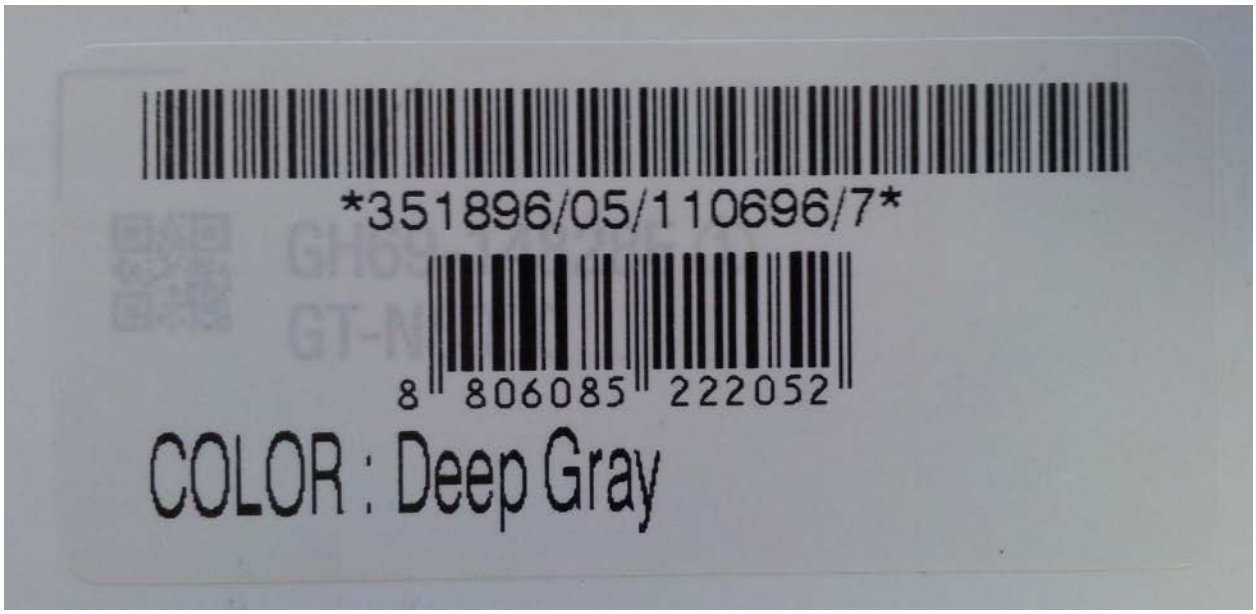


Figure 1 - Tracking Label

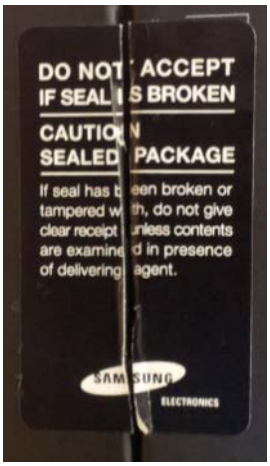


Figure 2 - Security Seal (Black)

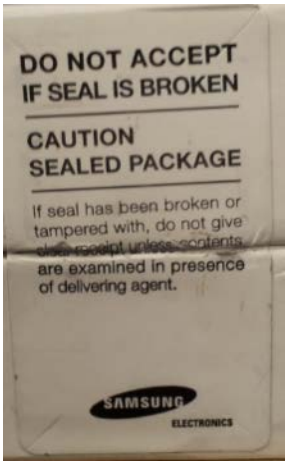


Figure 3 - Security Seal (White)

4.1.1 Evaluation Version

There are a number of components to determining the device that is being used and the components on that device (such as the operating system version, the build version, etc.). These are all contained under *Settings/About device*. The following are version information that can be found:

- ***Model number*** – this is the hardware model
- ***Android version*** – this is the Android OS version
- ***Build number*** – this is the specific binary image version for the device
- ***Security Software Version*** – this shows the Common Criteria evaluations and the version of the software components related to those evaluations on the device

For the Common Criteria evaluation version information see section 1.4.2 Device Details.

4.2 Secure Updates

Once a device has been deployed, it may be desirable to accept updates to the software on the device to take advantage of the latest and greatest features of Samsung Android. Updates are provided for devices as determined by Samsung and the carriers based on many factors. VPN Client updates will be provided as part of the firmware update process.

When updates are made available, they are signed by Samsung with a private key that is unique to the device/carrier combination (i.e. a Galaxy S10 on Verizon will not have an update signed with the same key as a Galaxy S10 on AT&T). The public key is embedded in the bootloader image, and is used to verify the integrity and validity of the update package.

When updates are made available for a specific device (they are generally rolled out in phases across a carrier network), the user will be prompted to download and install the update (see the User Guide for more information about checking for, downloading and installing the update). The update package is checked automatically for integrity and validity by the software on the device. If the check fails, the user is informed that there were errors in the update and the update will not be installed.

For more information about controlling the update process, review the document *Samsung Android 8 on Galaxy Devices Administrator Guide*, which can be downloaded at the Samsung Knox Portal link found in section 1.5 References.

5 Operational Security

5.1 Modes of Operation

The TOE can be operated in four different modes, depending on the role of the user accessing the device:

- Administrator mode;
- User mode;
- Error mode; and
- Recovery mode

A device is considered to be in Administrator mode before it is delivered to the user. The device is prepared and configured for deployment in the enterprise environment via the Samsung Enterprise SDK. The TOE administrators are trusted to follow and apply all administrator guidance in a trusted manner. An unprivileged user will not have access to this mode of operation.

If an error or operational failure occurs during the transition from Administrator mode (causing the device to enter the Error mode of operation) to User mode, the administrator should follow the guidance for the EDM he failure and restore the device to normal operational abilities. If it is not possible to adequately eliminate the error or operational failure, the device is not to be delivered to an end user and should be returned to the supplier.

After the device is configured in accordance with the Common Criteria evaluated settings, the device is ready for deployment to a user. When the user receives the device, only the TouchWiz user interface will be visible and no further changes to the security configuration are possible. Once deployed to a user, the device will be operating in User Mode. Within User Mode, the only security relevant functions accessible for the user are ‘lock screen password protection’, ‘change of password’ and ‘local device wipe’. Typically, an administrator will not access the device in this mode of operation.

The TOE may also be placed into Recovery mode, bypassing the standard boot process and allowing configuration changes to be made to the installation of Android. However, since this requires the boot loader for the device to be unlocked and is therefore considered out of scope for this environment.