DataSoft

Secure Tactical VPN Client

CC Configuration Guide

Version – 1.1

Date – July 26, 2023

© 2023 DataSoft Corp, Inc. All rights reserved. This document may be reproduced in full without any modification.

RECORD OF CHANGES

Prepared by:
DataSoft Corp.
10235 S 51st Street, #115
Phoenix, AZ 85044

VERSION	DATE	TITLE OR BRIEF DESCRIPTION
1.0	06/14/2023	Initial Version
1.1	07/26/2023	Added references to allow VPN Gateway to set more restrictive lifetimes

Table of Contents

Table of Figures

No table of figures entries found.

List of Tables

1.0 Introduction

This Configuration Guide documents the administration of the DataSoft Secure Tactical VPN Client for Android, version 2.3.7, as it was certified under Common Criteria. The Secure Tactical VPN Client for Android may be referenced below by the related acronym e.g. VPN Client or simply the TOE.

1.1 Audience

This document is written for administrators installing and configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within DataSoft Corp documentation to get the specific details for configuring and maintaining DataSoft Secure Tactical VPN Client for Android operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 TOE Overview

The TOE product consists of a user space application installed as a standard standalone Android APK for End User Devices (EUD) running on Android 11, 12 or 13 platforms using a kernel earlier than version 5.6. The associated Security Target documents a list of mobile Android devices using during certification testing.

The TOE establishes a secure IPsec trusted channel (which protects the transmitted data from unauthorized disclosure and modification) with a corresponding VPN gateway. The TOE supports IKEv2 connections with IKEv2 VPN gateways, such as the separately evaluated DataSoft RAP-117 VPN Gateway.

When configured with the DataSoft RAP-117, the TOE allowing installed applications to communicate as though connected directly a tactical radio network. The TOE can interoperate with IKEv2 VPN Gateways but also includes extensions to route multicast traffic through the VPN, allowing the TOE to interoperate with DataSoft's small form factor Radio Access Point (RAP), which allows mobile and dismounted operators to perform C2-releated computing functions security across existing tactical communications networks. Since the DataSoft RAP-117 VPN Gateway is a separately evaluated product and the Protection Profiles contain no functional testing of multicast traffic, these products and functionalities may be mentioned in accompanying documents, however only the TOE VPN client and IKEv2 communications are claimed and tested as a part of this evaluation.

1.4 Operational Environment

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration:

Table 1 – Operational Environment Components

Component	Usage/Purpose Description
Certificate Authority	A Certificate Authority is used to provide valid digital certificates for both the TOE's client credentials and for the VPN Gateway's server credentials.
Mobile Platform	The TOE relies on any Android mobile device platforms running Android 11, 12, or 13 using a kernel earlier than version 5.6
VPN Gateway	The TOE supports connections to an IKEv2 VPN Gateway (including the separately evaluated DataSoft RAP-117 VPN Gateway)

The underlying Mobile platform provides some of the security functionality required in [MOD_VPNC_V2.4], and is denoted using the phrase "TOE Platform" in this document.

1.5 Excluded Functionality

The functionality listed below is not included in the evaluated configuration

Table 2 – Excluded Functionality and Rationale

Function Excluded	Rationale
Non-CC or Non-CSfC mode of operation	The TOE includes CC and CSfC modes of operation. These modes allow the TOE to use only approved cryptography and must be enabled in order for the TOE to be operating in its evaluated configuration. See Section 3.2.2 and 3.2.3 for configuring these modes of operation. Outside of these configurations, the TOE requires no additional configuration of cryptographic services to be in a CC-compliant mode.
SSL Tunnel with DLTS tunneling options	[MOD_VPNC_V2.4] only permits IPsec VPN tunnel.

1.6 Security Management

The TOE includes its own cryptographic library that implements approved cryptographic algorithms that the TOE uses to protect communication between itself and a VPN gateway over an unprotected network using IPsec. The TOE provides the entirety of both IKEv2 and IPsec/ESP functionality and does not rely upon Android's Linux kernel for any cryptographic processing other than during IKE peer authentication, where the TOE relies upon Android's Keystore to securely store, manage, and utilize user credentials (certificates and private keys). The TOE also relies upon Android's documented, evaluated APIs to enforce packet routing decisions by Android's network drivers). In addition, the TOE seeds its DRBG from the Platform.

Together, the TOE and TOE platform perform device-level X.509 certificate-based authentication of the VPN Gateway during IKEv2 key exchange. Device-level authentication allows the TOE to establish a secure channel with a trusted VPN Gateway. The secure channel is established only after each endpoint successfully authenticates each other. The TOE utilizes its own cryptographic functions to perform self-tests that ensure the TOE's integrity and algorithm correctness. In the event that a connection cannot be established to determine the validity of a certificate, the TOE will reject the certificate and this behavior is not configurable.

The TOE always enforces a "full-tunnel VPN" and thus subjects all traffic to IPsec/ESP encryption. The TOE does not offer any additional configuration of SPD rules or order other than simply connecting and disconnecting to the configured VPN network. By default, the TOE enforces lifetimes of 24 hours or less for IKEv2 SAs and 7 hours or less for CHILD/ESP SAs. These settings are not configurable. The TOE relies on the VPN Gateway for configuring any stricter values for SA lifetimes.

The TOE contains several other configurable security settings as addressed under Section 3.2 TOE Configuration. See this section for additional information on these configuration options. Beyond configuring CC-specific or CSfC-specific configuration options under individual VPN profile, no additional configuration of the cryptographic engine is needed.

The TOE relies upon the VPN Gateway to prevent IPsec connections where the CHILD/ESP SA has a cipher key length greater than that of the IKEv2 SA.

The TOE makes use of network connectivity as it allows users to initiate IPsec VPN connections and accesses no sensitive information repositories.

The TOE is compiled with all necessary compilation flags to ensure that bugger overflow protection mechanisms are invoked and no additional platform mechanisms need to be specifically enabled.

2.0 Procedures and Operation Guidance for IT Environment

To configure and operate in its evaluated configuration, the TOE requires a minimum one (1) Certificate Authority (CA), one (1) VPN Gateway with correctly configured server credentials, and one (1) compatible Android mobile device with correctly configured client credentials. This document addresses just the TOE functionality, i.e. the Secure Tactical VPN Client. The EUD, WiFi and VPN Gateway (i.e. RAP-117) are outside the scope of this document.

2.1 Public Key Infrastructure (PKI) Notes

This section provides guidance on the use of a PKI toolset used by the customer to generate public/private keys and to sign certificate requests for the TOE. A PKI toolset is not provided by DataSoft but a CSfC-approved one is needed during the provisioning process.

- An external Certificate Authority (CA) will need to sign certificates for use by the TOE.
- The CA that signs the certificate used by TOE must use 384-bit ECDSA keys.
    - Signed certificates can be imported in PEM or PKCS#7 format.
- To meet CSfC requirements, all public/private key pairs used for IPSec should be generated with 384-bit ECDSA keys. This includes the following RAP VPNs:
    - Data traffic IPSec VPN between the RAP and EUD
    - rsyslog IPSec VPN between the RAP and the audit log server
- TOE configurations have strict CRL checking turned on so valid CRLs need to be imported when configuring each TOE.
    - CRL files must be in PEM format.

3.0 Operational Guidance for the TOE

The following sections provide guidance on configuring, starting and stopping the TOE.

3.1 Installing the TOE

The TOE is available on the Google Playstore and is signed with DataSoft's unique developer private key. Administrators should use the Google Play Store application on the EUD to obtain and install the latest version of the TOE.

3.2 TOE Configuration

By default, the TOE does not ship with any pre-built VPN configuration profiles. The TOE offers two main methods of generating VPN profiles: manually through the UI or through an imported sswan file (see later section 3.2.1 Importing a Configuration). Both methods of VPN profiles exhibit the same functional behavior as long as they were configured with the same profile settings.

A new VPN configuration can be manually added from the application's home screen using the "Add VPN Profile" option on the top right of the main screen. Selecting this option brings up a new menu where users can input the server information, client authentication information, trusted CA certificate information, an optional profile name, and advanced settings. Under advanced settings, the user has additional options for server/client identities, DNS servers, MTU of the VPN tunnel device, server port, NAT-T keepalive internal, certificate requests, OSCP/CRL support, strict revocation checking, RSA/PSS signatures, IPv6 transport address, IKEv2 Algorithms, and IPsec/ESP algorithms. Some of these settings do not affect the security functionality for the secure IPsec (IKEv2) connection; however the user should refer to the later sections for CC-specific and CSfC-specific configurations which must be set in order to be compliant with their given deployment.

The TOE provides the user the ability to specify the "Server" (i.e., the VPN gateway) identifier. The TOE uses this value to compare against the Distinguished Name (DN) found in the peer's (VPN Gateway's) presented IKE auth certificate.

The TOE's UI presents an interface to Androids System UI to import a certificate (chain) and private key in p12/PFX format, or alternatively, the user can separate load the p12 file through Android's System UI (an MDM Agent or Device Policy Controller can also import p12 certificates as directed by an MDM server). When creating a new VPN profile, the TOE prompts the user to select the certificate/private key they wish the TOE to use during IKE authentication. The TOE does not install with any default credentials, nor does it store any credentials imported by the user as this is maintained by the platform (Android Keystore) and is simply leveraged by the TOE.

Similarly, the TOE's UI presents the option for configuring trusted Certificate Authorities used to verify the server certificate. The user has the option when creating a new VPN profile to "Select automatically", which will load all certificates from the platform's trusted certificate store, or to manually select a CA certificate from the platform truststore. Assuming the server's certificate matches the configured identifier, the TOE then validates that it can construct a certificate path from the server's certificate through any intermediary CAs to the CA certificate specified by the user in the VPN configuration. If the TOE can successfully build the certificate path, then the TOE will next check the validity of the certificates (e.g., checking its validity dates and that the CA flag is present in the basic constraints section for all CA certs). Assuming the certificates are

valid, the TOE finally checks the revocation status of all certificates (starting with the server's certificate and working up the chain). The TOE will reject any certificate for which it cannot determine the validity and reject the connection attempt.

Once a VPN profile is created, it can be edited by long-pressing the VPN profile and selecting "Edit" which will bring up the menu to change any of the configuration options. Similarly, a VPN profile can be copy or removed by long-pressing the application and selecting either "Copy" or "Delete"

3.2.1 Importing a Configuration

This option is available to pre-configure a VPN profile and deploy it to a phone. The imported profiles contain the same settings available to the user under manual configurations, however the end user is responsible for ensuring that the resulting VPN profile is still compatible with the CC-specific or CSfC-specific configurations either by verifying the values in the imported swan file or by editing the imported profile after the initial import and before its first use.

To import a sswan profile on the EUD, start TOE, click on the 3 dots in the upper right corner and select "Import VPN profile" and select the sswan file that was just copied to the EUD.

- Click on "IMPORT CERTIFICATE FROM VPN PROFILE"
- Type in password used as enrollment code (e.g. 12345678) during p12 creation
- For certificate type, select "VPN & app user certificate", OK
- Name this certificate: leave unchanged, OK
- When prompted for cert to use, use the newly created one during p12 creation (old certs will remain on EUD unless they are manually deleted via:
    - Settings->Security->Advanced settings->Encryption & credentials->User credentials, select cert to delete and Uninstall
- Select "IMPORT" in upper right-hand corner to complete the VPN profile import process

3.2.2 CC-Specific Configurations

In order to be compliant with Common Criteria, the above configuration options must be set on the TOE.

1. The TOE UI supports multiple VPN types, however only IKEv2 Certificate authentication is supported as part of this evaluation
2. The TOE uses only ECC key exchange/establishment and the TOE uses it exclusively as part of IKEv2 and ESP negotiation. As a result, only ECC client credentials should be configured and the TOE should only be used to connect to servers using ECC server credentials
3. The TOE requires certificate requests and strict revocation checking to be enabled in order to correctly process X509 certificates
4. The UI presents options for both OCSP and CRLs, however the TOE only supports the use of CRLs. As a result, the OCSP option has been disabled so that the UI option does

not change any behavior, however the user should ensure that CRL is still enabled.

5. The TOE supports several algorithms for IPsec/ESP and IKEv2 that are not able to be claimed under Common Criteria. As a result, the user should restrict the IPsec/ESP and IKEv2 algorithms using the following configuration strings in the UI or by ensuring the "ike-proposal" or "esp-proposal" values in the sswan file are set to the same values. While the TOE supports both AES in CBC mode or GCM mode, the TOE is not able to configure limit algorithms and have both of these enabled at the same time. As a result, the user should use either the CBC or GCM strings below depending on their use case

   CBC:
   IPsec/ESP Algorithms:
   aes128-aes256-sha1-sha2_256-sha2_384-sha2_512
   IKEv2 Algorithms:
   aes128-aes256-sha1-sha2_256-sha2_384-sha2_512-ecp256-ecp384
   GCM:
   IPsec/ESP Algorithms:
   aes128gcm128-aes256gcm128-sha1-sha2_256-sha2_384-sha2_512
   IKEv2 Algorithms:
   aes128gcm128-aes256gcm128-sha1-sha2_256-sha2_384-sha2_512-ecp256-ecp384

3.2.3 CSfC-Specific Configurations

The separately evaluated DataSoft RAP-117 has a CSfC compliant mode to ensure that only compliant algorithms can be used in secure IPsec connections. As a result, the TOE does not need any special CSfC-specific configurations when connecting to the RAP as the VPNGW will be responsible for negotiating the correct algorithms for communication. Optionally, the TOE can be configured with the following algorithm strings to ensure the same limitation on the client side:

CBC:
IPsec/ESP Algorithms:
aes256-sha384-ecp384, aes256-sha512-ecp384
IKEv2 Algorithms:
aes256-sha2_384-sha2_512-ecp256-ecp384
GCM:
IPsec/ESP Algorithms:
aes256gcm128-sha2_384-sha2_512
IKEv2 Algorithms:
aes256gcm128-sha2_384-sha2_512-ecp256-ecp384

By default, the TOE only supports tunnel mode, IKEv2 with NAT traversal, IKEv2 SA lifetimes based on length of time, DH groups that use at least 256/284 bits of security, and ensures IKEv2 nonces have a probability of repeating during the life of an IPsec SA of less than 1 in 2^(128,192) in compliance with CSfC selections for VPN Clients. No further configuration is

needed to ensure the TOE is in a CSfC-compliant mode for these selections.

See section 2.1 Public Key Infrastructure for additional notes regarding ensuring that the TOE is configured with CSfC-conformant client credentials.

3.3 Establish a VPN Connection

Open the TOE on the EUD. The Status should show "No active VPN". Below the status message, there should be a RAP VPN profile listed for the certificate and key that was loaded earlier. Click on the configured VPN profile to activate the IPSec tunnel. The TOE status should change to "Connected".

3.4 Monitor and Troubleshoot

If the EUD data rates are above the network's capacity for an extended period, the periodic VPN rekey packets may timeout and the TOE will become disconnected from the VPN gateway.

1. To recover from this condition, open the TOE on the EUD and reconnect to the VPN gateway per the instructions in Section 3.3.
2. The TOE automatically logs data. If log files are required to be captured from the EUD, there are two options:
    a. If the EUD is connected to the Internet, log files can be emailed from within the app with "View Log->Send Log File" and enter and email address where the log should be sent
    b. If the EUD is not connected to the Internet, connect the EUD to a computer with a USB cable. Then, use the "adb" tool to retrieve the logs.

3.5 Disconnecting VPN Client

The TOE can be disconnected by selecting "Disconnect" in the TOE application. To reconnect, tap the RAP VPN configured profile. The RAP VPN profile can be deleted by long pressing on the profile name and selecting DELETE. This should only be done if new certificates and keys and being generated and loaded on the RAP and EUDs.

3.6 Self-Test

The TOE performs a series of self-tests upon loading/execution. These include cryptographic algorithm self-tests for all of the claimed algorithms within its OpenSSL library. Upon failure of any of the individual self-tests, the TOE will halt execution and display an error message to the user before exiting the application. Only after correctly passing all self-tests will the TOE permit

any security functions. Details about self-test results can be found under the device internal logcat storage.

3.7 Current Version and Trusted Updates

The current version of the TOE is reported alongside application information under the EUD's Settings application. This information can be accessed by long pressing the TOE icon on the EUD and then selecting App Info and scrolling to the bottom. The TOE uses a major, minor, and build number.

DataSoft makes TOE updates through the APK package format and distributes updated APKs through the Google Play Store. To initiate an update, the user can use the Play Store application to download any available update. An update is determined successful if the version number is updated and the Play Store no longer reports an update is available. DataSoft signs the Secure Tactical VPN Client APK with a unique developer private key to ensure authenticity of updates which is then verified by the Google Play Store and EUD.

4.0 Obtaining Documentation and Submitting a Service Request

Customers are provided with a User Guide that provides detailed information on the use of the TOE in various use cases. Documentation may be requested by contacting DataSoft.

5.0 Contacting DataSoft

DataSoft Corp can be contacted via phone 480-763-5777 x402, or email support@datasoft.com