National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
DataSoft RAP-117

Report Number:	**CCEVS-VR-VID11377-2023**
Dated:	**July 26, 2023**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lauren Brandt
Randy Heimann
Lisa Mitchell
Linda Morrison
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Tyler Catterton
Tammy Compton
Khai Van
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of DataSoft RAP-117 solution provided by DataSoft Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in July 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the PP-Configuration for Network Devices, VPN Gateways, and Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 December 2022 which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (VPNGW12) and the PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 April 2022 (WLANAS10).

The Target of Evaluation (TOE) is the DataSoft RAP-117.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the DataSoft RAP-117 Security Target, Version 1.4, July 25, 2023 and analysis performed by the validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	DataSoft RAP-117 (Specific models identified in Section 7)
Protection Profile	PP-Configuration for Network Devices, VPN Gateways, and Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 December 2022 which included the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (VPNGW12) and the PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 April 2022 (WLANAS10)
ST	DataSoft RAP-117 Security Target, Version 1.4, July 25, 2023
Evaluation Technical Report	Evaluation Technical Report for DataSoft RAP-117, Version 0.3, July 25, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	DataSoft Corporation
Developer	DataSoft Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	The MITRE Corporation

3 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (VPNGW12)
- PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 April 2022 (WLANAS10)

That information has not been reproduced here and the NDcPP22e/VPNGW12/WLANAS10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/VPNGW12/WLANAS10 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices with the VPN Gateway and WLAN Access System Modules and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e/VPNGW12/WLANAS10 and applicable

Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is the Datasoft RAP-117 (HW version 2.0 and FW version 2.2.0).

The TOE provides a small form factor Radio Access Point (RAP), which allows mobile and dismounted operators to perform Command and Control (or “C2”) related computing functions securely across existing tactical communications networks. With the ability to process the data communications for a variety of C2-related applications, the TOE is a subsystem that provides lightweight wireless connectivity (with support for multicast traffic) between commercial mobile computing platforms (i.e., smartphone, tablet, etc.) and the secure military radios at the tactical edge.

4.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 7 below.

4.2 TOE Architecture

An administrator uses a dedicated provisioning application (running on the administrator's workstation) to administer the TOE. The NDcPP terms the dedicated provisioning application as a "Management Component" and because the TOE independently satisfies all SFRs in the cPP (as well as the SFRs of the PP Modules) without the Management Component, the NDcPP22e prescribes that the TOE be certified (by itself) according to the cPP and without the Management Component. "Figure 4: Non-distributed TOE use case" in the NDcPP22e depicts the TOE and its dedicated provisioning applications.

As a result, the TOE boundary includes only the TOE itself, and the dedicated provisioning application (along with the administrator's workstation upon which the application runs) lies in the TOE's Operational Environment.

4.3 Physical Boundaries

The RAP-117 is composed of the necessary hardware and software for the wireless personal area network (PAN) interface and routing between the tactical radio and other customer equipment and the hardware and software necessary to configure the equipment.

5 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support

3. Identification and authentication
4. Security management
5. Packet filtering
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

5.1 Security audit

The TOE provides auditing capabilities to provide a secure and reliable way to trace all changes to the system. Any administrative configuration changes during provisioning and other auditable events are audited internally and then transmitted externally over a secure communication channel to an audit server. All audited events have the necessary details like timestamp, event log, event code, and identity of the party involved to provide a comprehensive audit trail.

5.2 Cryptographic support

The TOE provides cryptographic functions for secure administration access via SSH; for communications with VPN clients via IPsec; for wireless communication via WPA2/WPA3 and for communication to external systems such as audit log servers and RADIUS via IPsec. Functions include Key generation, key establishment, key distribution, key destruction, and cryptographic operations.

5.3 Identification and authentication

The TOE provides secure connectivity between wireless clients via 802.1X authentication. The TOE supports certificate based authentication via external RADIUS server and supports SAE authentication via a local authentication mechanism. The TOE provides secure password-based and public key based authentication for remote administrators. The TOE also provides strong password requirements that the administrator can configure, including length, session timeout and password complexity. Consecutive unsuccessful attempts beyond a certain limit will result in locking of the user for a specified duration of time or until user unlock by another administrator.

5.4 Security management

TOE administrators manage the security functions of the TOE through a SSH CLI. Administration cannot be performed from a wireless client. The TOE also provides the ability to configure the session activity timeout of an administrator and to configure the TOE’s access banner.

5.5 Packet filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established with trusted VPN peers and VPN Clients. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

5.6 Protection of the TSF

The TOE provides image integrity verification to validate the authenticity of the images before loading them. Upon every boot up, power on self-tests are conducted to validate the integrity of the software components. If power-up self-tests fail, the TOE halts boot. The TOE also allows manual configuration of the TOE's real time clock (RTC) by administrators. The TOE protects cryptographic keys and passwords from unauthorized access.

5.7 TOE access

The TOE offers a login banner which provides the administrator to ability to display a custom warning/access policy message as per the organization needs. The TOE is capable of restricting wireless access based on time and day. The TOE provides the ability to configure an inactivity timeout which terminates the session beyond the inactivity period configured. An administrator can also terminate their own session.

5.8 Trusted path/channels

The TOE communicates to external components in a secure manner using WPA2/WPA3 for wireless clients and using IPsec for VPN Clients, a RADIUS server, and a syslog server. The TOE also employs SSH to secure remote administrative sessions.

6 Documentation

The following documents were available with the TOE for evaluation:

- DataSoft RAP-117 WLAN Access System and IPsec VPN Gateway CC Configuration Guide, Version 1.2, July 25, 2023

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 Evaluated Configuration

The evaluated configuration consists of the DataSoft RAP-117 (HW version 2.0 and FW version 2.2.0).

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for DataSoft RAP-117, Version 0.3, July 25, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/VPNGW12/WLANAS10 including the tests associated with optional requirements. The AAR in sections 1.1 lists the tested devices.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the RAP-117 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/VPNGW12/ WLANAS10.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the DataSoft RAP-117 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP22e/VPNGW12/WLANAS10 related to the examination of the information contained in the TSS.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e/VPNGW12/WLANAS10 and recorded the results in a Test Report, summarized in the AAR.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “RAP 117”, “Datasoft”, “openssl 3.1.0”, “Radio Access Point”, “strongswan”, “rsyslog”, “Freescale”, “Freescale i.MX6UL rev1.2 696 MHz”, “Linux kernel 5.4”, “wpa2”, “wpa3”, “TCP”, “IPSEC”, “sidebridge”

The validation team reviewed the work of the evaluation team,and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the DataSoft RAP-117 WLAN Access System and IPsec VPN Gateway CC Configuration Guide and any supporting documentation listed in the Configuration Guide. No versions of the TOE and software, either earlier or later, were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *DataSoft RAP-117 Security Target, Version 1.4, July 25, 2023*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)

[5] PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (VPNGW12)

[6] PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 April 2022 (WLANAS10).

[7] DataSoft RAP-117 Security Target, Version 1.4, July 25, 2023 (ST).

[8] Assurance Activity Report for DataSoft RAP-117, Version 0.3, July 25, 2023 (AAR).

[9] Detailed Test Report for DataSoft RAP-117, Version 0.3, July 25, 2023 (DTR).

[10] Evaluation Technical Report for DataSoft RAP-117, Version 0.3, July 25, 2023 (ETR)

[11] DataSoft RAP-117 WLAN Access System and IPsec VPN Gateway CC Configuration Guide, Version 1.2, July 25, 2023 (AGD)