National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3

Report Number: CCEVS-VR-VID11382-2023
Dated: September 19, 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

Jenn Dotson
Sheldon Durrant
Randy Heimann
Lisa Mitchell
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Cody Cummins
Kevin Cummins
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 Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 solution provided by Commscope Technologies LLC. 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 September 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, Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), and Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 05 April 2023 (CFG_NDcPP-WIDS-WLANAS_v1.0) which includes the Base PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0, 30 September 2020 (WIDS10) 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 Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3.

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 *Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target*, version 0.6, September 18, 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	Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 (Specific models identified in Section 7)
Protection Profile	PP-Configuration for Network Devices, Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), and Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 05 April 2023 (CFG_NDcPP-WIDS-WLANAS_v1.0) which includes the Base PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0, 30 September 2020 (WIDS10) and the PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 April 2022 (WLANAS10)
ST	*Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target*, version 0.6, September 18, 2023
Evaluation Technical Report	*Evaluation Technical Report for Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3*, version 0.3, September 11, 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	Commscope Technologies LLC
Developer	Commscope Technologies LLC
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 Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0, 30 September 2020 (WIDS10)
- 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/WIDS10/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/WIDS10/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 WIDS and WLAN PP-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 Wireless Intrusion Prevention System models was not included in the scope of the evaluation and therefore should not 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/WIDS10/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 Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3. The TOE is a distributed TOE. Ruckus Wireless Controller has been designed to eliminate the difficulties administrators experience with building and managing large-scale WLAN networks, to support several Wi-Fi access points and many concurrent Wi-Fi clients. Ruckus Wireless Controllers can support tens of thousands of Ruckus Smart Wi-Fi APs and hundreds of thousands of concurrent Wi-Fi subscribers. The Ruckus carrier-class management system provides feature-rich management of access points, such as RF management, load balancing, adaptive meshing and backhaul optimization and secure connectivity to all wireless clients.

4.1 TOE Evaluated Platforms

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

4.2 TOE Architecture

The Ruckus SmartZone controllers and Access Points Solution (TOE) is a Wireless LAN access system (WLAN) and Wireless Intrusion Detection System (WIDS). The Wireless LAN access system and WIDS system defined in this ST is composed of multiple products operating together to provide secure wireless access to a wired and wireless network. The TOE provides end-to-end wireless encryption, centralized WLAN management, authentication, authorization, and accounting (AAA) policy enforcement. The TOE has the following Access Point TOE components: R650, R750, and R850. The TOE also has the following Wireless Controllers: SmartZone 144, SmartZone 300 (SZ 300), virtual SmartZone (vSZ-E and vSZ-H hosted on a physical device), and virtual SmartZone – Data plane (vSZ-D hosted on a physical device). The TOE is a distributed TOE.

4.3 Physical Boundaries

The physical boundaries of the TOE consist of Wireless Controller and Access Points with WIDS running software version 5.2.1.3. Controller and AP hardware is described in Section 7.

4.3.1 Wireless Controllers

The wireless controller serves client devices using secure authentication protocols, such as 802.1X/EAP. This is combined with policy-based data traffic steering which enterprises can optimize to forward all client traffic appropriately.

SZ 144

SmartZone™ 144 is a Scalable, Resilient, and High Performing Wireless LAN controller for Enterprises. It manages up to up to 2048 AP and 50,000 Clients per unit. SmartZoneOS' unique

architecture enables SZ 144 to be deployed in multiple architectures like centralized and distributed traffic forwarding.

SZ 300
The SmartZone™ 300 (SZ 300) Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The SZ300 supports up to 10,000 AP and 100,000 Clients per unit.

vSZ
The Ruckus Virtual SmartZone™ (vSZ hosted on a physical device) is an NFV-based WLAN controller scale. The vSZ can be deployed in 2 modes, High Scale (vSZ-H) and Essentials (vSZ-E). High Scale supports up to 10,000 AP and 100,000 Clients per unit. Essentials supports up to 2048 AP and 50,000 Clients per unit.

vSZ-D
With the Virtual SmartZone Data Plane (vSZ-D hosted on a physical device), the Ruckus Virtual SmartZone platform launches data plane capabilities that enable tunneled WLAN architectures.

4.3.2 Access Points

The AP components can be centrally managed by the Ruckus Wireless Controller as part of a unified indoor/outdoor wireless LAN. Each AP supports a wide range of value-added applications.

Wireless communications between clients and APs is carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation, the APs use a variation within 802.11a, 802.11ac, 802.11ax, 802.11b, 802.11g and 802.11n for wireless communication. The wireless security protocols that are to be used with the APs are 802.1X/802.1i.

The AP part of the TOE consists of the following component products:

AP	Location Type	Concurrent Users	User Data Rate
R650 (Including R650-WW)	Medium density	512	up to 2974 Mbps
R750 (Including T750SE/T750 Omni and R750-WW)	High density	1024	Up to 2400 Mbps
R850	High Density	1024	Up to 5984 Mbps

The T750SE is the 120-degree sector antenna variants of the R750 respectively and includes all of the same physical features.

The R650-WW and R750-WW are made up of the same hardware and software as the R650 and R750 respectively. The WW SKUs allow the user to choose the country code that determines the selection of radio channels for that country. The US SKUs are locked to radio channels allowed in the US.

The T750 Omni is the outdoor version of the R750.

5 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. User data protection
5. Identification and authentication
6. Security management
7. Protection of the TSF
8. TOE access
9. 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 configuration changes, administrative activities and other auditable events are audited both internally and 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. The TOE also provides a WIDS alerting capability. The WIDS alerts are generated based on signature-based attacks and are related to APs and end user devices (EUDs). All WIDS alerts contain data to identify the malicious or rogue device.

5.2 Communication

The distributed TOE offers secure internal TSF communication via SSH and TLS. Access Points and vSZ-Ds register to the WLAN controller over a dedicated channel and must be approved by the administrator to communicate with each other as parts of the distributed TOE.

5.3 Cryptographic support

The distributed TOE provides cryptographic functions for secure administration access via HTTPS and SSH; for communication between the distributed parts of the TOE via SSH and IPSec; for wireless communication via WPA3/WPA2 and for communication to external systems such as audit log servers via IPSec and RADIUS via TLS. Functions include Key generation, key establishment, key distribution, key destruction, cryptographic operations.

5.4 User data protection

The TOE provides a security policy to monitor authorized and unauthorized APs and EUDs.

5.5 Identification and authentication

The distributed TOE provides secure connectivity to the network for wireless clients via 802.1X authentication. Certificate based authentication is supported via external RADIUS server and password-based authentication is supported via the local authentication mechanism. The distributed TOE provides secure password-based authentication for remote administrators and X.509 certificate-based authentication for TOE components. The distributed TOE also provides strong password requirements that can be configured by the administrator 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.

5.6 Security management

TOE administrators manage the security functions of the TOE's distributed components from the SmartZone Controller, including software updates, via secure HTTPS connection over a web interface. Optionally SSH and the local console can also be used as a method to configure the system via the SmartZone controller. 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 access banner on the controller.

5.7 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 on self-tests fail, a quarantine state is entered. All the components of the distributed TOE use X.509 certificates to authenticate and establish a secure connectivity amongst them. The TOE also allows configuration of timestamps via an NTP server. The TOE protects cryptographic keys and passwords from unauthorized access.

5.8 TOE access

A login banner is offered which provides the ability to have a custom warning/access policy message as per the organization needs. The TOE can restrict wireless access based on TOE interface, 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.

5.9 Trusted path/channels

The TOE communicates to external components in a secure manner. The following secure channels are used to communicate externally – TLS for RADIUS, HTTPS for WebUI administration, SSH for CLI administration, IPsec for audit servers, and WPA3/WPA2 for wireless clients. The registration and joining of TOE components are performed over a dedicated channel. After registration, SSH is used for all management of the distributed TOE components (AP and vSZ-D) by the SmartZone Controller and IPSec is used for the data tunnel.

6 Documentation

The following documents were available with the TOE for evaluation:

- *RUCKUS Common Criteria Configuration Guide for SmartZone and AP, 5.2.1.3,* Part Number: 800-72735-001 Rev D, October 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 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 TOE has the following Access Point TOE components: R650, R750, and R850. The TOE also has the following Wireless Controllers: SmartZone 144, SmartZone 300 (SZ 300), virtual SmartZone (vSZ-E and vSZ-H hosted on a physical device), and virtual SmartZone – Data plane (vSZ-D hosted on a physical device).

The specific hardware information is as follows:

Controller	CPU
Smart Zone 144 (SZ 144)	Intel(R) Xeon(R) CPU D-2143IT (Skylake)
Smart Zone 300 (SZ 300)	Intel(R) Xeon(R) CPU E5-2695 v3 (Haswell)
Ruckus virtual SmartZone (vSZ) on VMware ESXi 7.0	Intel(R) Xeon(R) Silver 4309Y CPU (Ice Lake)
Ruckus virtual SmartZone – Data plane (vSZ-D) on VMware ESXi 7.0	Intel(R) Xeon(R) Silver 4309Y CPU (Ice Lake)

Controller CPU Identification

AP	CPU
R650 (Including R650-WW)	Qualcomm IPQ8071 (ARMv8)
R750 (Including T750SE/T750 Omni and T750-WW)	Qualcomm IPQ8076 (ARMv8)
R850	Qualcomm IPQ8078(ARMv8)

AP CPU Identification

The following configuration options are outside the evaluated configuration:

1) Internal captive portal
2) Soft-GRE to external gateway
3) FIPS/CC mode disabled
4) 802.11r
5) Clustering
6) Non-Proxy Authentication, Authorization & Accounting (AP directly talk to AAA)
7) GTP tunnel

8) SSH based AP administration (in the evaluated configuration, all administration is performed via the Controller)
9) Encrypted/Ruckus GRE

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 Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3*, Version 0.4, September 18, 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/WIDS10/WLANAS10 including the tests associated with optional requirements. The AAR, in section 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

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 Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/WIDS10/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 Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 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/WIDS10/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/WIDS10/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 evaluation team searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 9/7/2023 with the following search terms: “Ruckus”, “SmartZone”, “802.1X”, “openssl”, “openssh”, “ESXi”, “Xeon Processor”, “Qualcom IPQ”.

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 *RUCKUS Common Criteria Configuration Guide for SmartZone and AP, 5.2.1.3*. 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.

Note also that the ability to define authorized SSIDs is implemented by explicitly configuring them for the WLANs managed by the TOE. Unauthorized SSIDs are defined by a separate WIDS rule.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target*, Version 0.6, September 18, 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 Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS)*, Version 1.0, 30 September 2020 (WIDS10).

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

[7] *Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target*, Version 0.6, September 18, 2023 (ST).

[8] *Assurance Activity Report for Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3*, Version 0.4, September 18, 2023 (AAR).

[9] *Detailed Test Report for Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3*, Version 0.4, September 18, 2023 (DTR).

[10] *Evaluation Technical Report for Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3*, Version 0.3, September 11, 2023 (ETR)

[11] *RUCKUS Common Criteria Configuration Guide for SmartZone and AP, 5.2.1.3*, Part Number: 800-72735-001 Rev D, October 2023