National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Fortinet FortiWLM Wireless Manager 8.5
Version 1.0

Report Number: CCEVS-VR-11179-2021

Dated: 11/22/2021

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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome F Myers
Swapna Katikaneni
Alex Korobchuk
Dale Schroeder
Aerospace Corporation
Joyce Baidoo
Anne Gugel
John Hopkins University APL

Common Criteria Testing Laboratory

Dayanandini Pathmanathan
Rahul Joshi
Riya Thomas
Swapnil Lad
Siddhant Kasley

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the **Fortinet FortiWLM Wireless Manager 8.5** TOE. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in November 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

The TOE identified in this VR 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), as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]. This VR 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 ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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 ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are an interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance 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(s) 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	Fortinet FortiWLM Wireless Manager 8.5
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
Security Target	Fortinet FortiWLM Wireless Manager 8.5 Security Target, v2.9
Evaluation Technical Report	Evaluation Technical Report for Fortinet FortiWLM Wireless Manager 8.5, version 0.4
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Fortinet, Inc.
Developer	Fortinet, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Jerome F Myers Swapna Katikaneni Alex Korobchuk Dale Schroeder *Aerospace Corporation* Joyce Baidoo

	Anne Gugel *John Hopkins University APL*

3 Architectural Information

The TOE is a network device that provides management of wireless controllers and access points.

3.1 Deployment

Figure 1 shows an example deployment of the TOE (enclosed in blue) in the context of a Fortinet controller-managed wireless network.

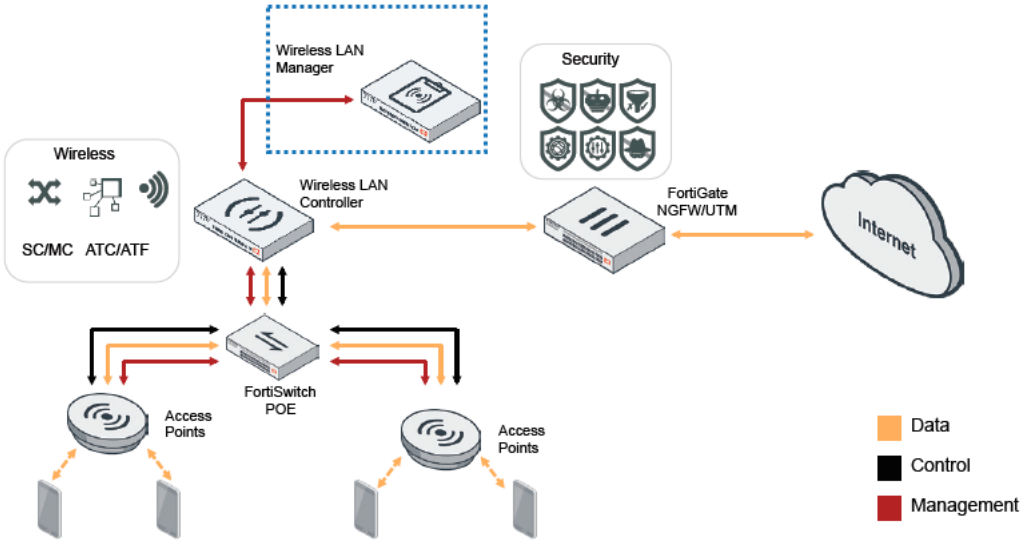

Figure 1: Example TOE deployment

3.2 Interfaces

The TOE interfaces are shown in Figure 2.

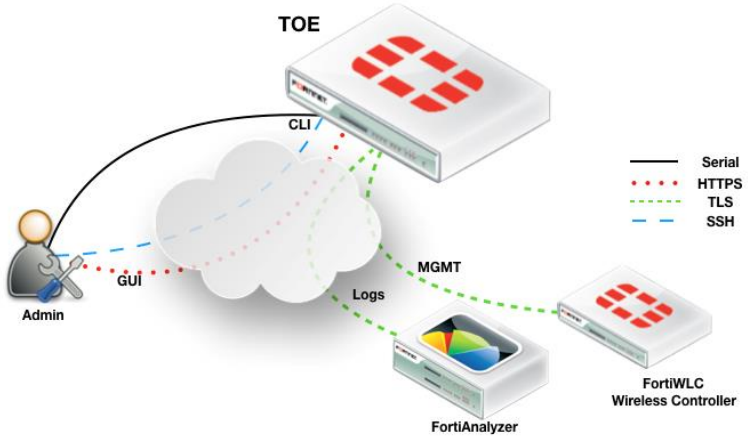

Figure 2: TOE interfaces

The TOE interfaces are as follows:

a) **CLI.** Administrative CLI via direct serial connection or SSH.

b) **GUI.** Administrative web GUI via HTTPS.

c) **Logs.** Forwarding of logs to a remote audit server, which must be a Fortinet FortiAnalyzer, via TLS.

d) **MGMT.** Management of FortiWLC Wireless Controllers via TLS.

3.3 Physical Scope

The physical boundary of the TOE includes the Fortinet hardware equipped with Araneus Alea II USB Entropy Token and software which is delivered to the customer via commercial courier. *The software function that reads the entropy data periodically checks whether the inserted USB device has a vendor ID matching Araneus and a product ID matching the Alea token. If any other USB device is inserted, the TOE will refuse to recognize it and display an error via console.*

The TOE models in scope are shown in Table 2.

Table 2: TOE models

Model	CPU	Target Deployment
FWM-100D	Intel Celeron J1900 (Bay Trail)	Small enterprise
FWM-1000D	Intel Core i7-4790S (Haswell)	Large enterprise

3.3.1 Guidance Documents

The TOE includes the following guidance documents (PDF):

a) Fortinet FortiWLM Wireless Manager 8.5 FIPS140-2 and Common Criteria Technote

b) Fortinet FortiWLM Wireless Manager 8.5 User Guide

c) Fortinet FortiWLM Wireless Manager Release Notes Version 8.5

d) Fortinet Hardware Guides:

i) Fortinet FortiWLM 100D QuickStart Guide

ii) Fortinet FortiWLM 1000D QuickStart Guide

3.3.2 Non-TOE Components

The TOE operates with the following components in the environment:

a) **Audit Server.** The TOE makes use of a FortiAnalyzer for remote logging.

b) **FortiWLC Wireless Controller.** The TOE manages Fortinet FortiWLC Wireless Controllers.

4 Security Policy

The TOE provides the following security functions:

a) **Security Audit.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server (FortiAnalyzer) over TLS.

b) **Cryptographic Support.** The TOE implements cryptographic libraries and protocols in support of its functions. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 3.

c) **Identification and Authentication.** The TOE implements authentication mechanisms, authentication failure handling, password management and X.509 certificate validation services.

d) **Security Management.** The TOE restricts the ability to manage its functions to Security Administrators.

e) **Protection of the TSF.** The TOE protects cryptographic keys and administrator passwords, performs a suite of self-tests and ensures the authenticity and integrity of software updates through digital signatures.

f) **TOE Access.** The TOE implements session locking, session termination and displays access banners.

g) **Trusted path/channels.** The TOE protects the integrity and confidentiality of communications.

Table 3: CAVP Certificates

SFR	Capability	Key Size / Curve / Mod	Cryptographic Library	Certificate
FCS_CKM.1	RSA KeyGen (186-4)	2048	Fortinet FortiWLM SSL Cryptographic Library	C1653
	ECDSA KeyGen (186-4)	P-256		
	FFC KeyGen	(DH Group 14)		n/a
FCS_CKM.2	RSA (RFC 3447)	n/a		n/a
	KAS-ECC Component	P-256		C1653
	FFC Schemes	(DH Group 14)		n/a
FCS_COP.1 /DataEncryption	AES-CBC	128, 256		

SFR	Capability	Key Size / Curve / Mod	Cryptographic Library	Certificate
FCS_COP.1 /SigGen and SigVer	RSA SigGen (186-4) RSA SigVer (186-4)	2048	Fortinet FortiWLM SSL Cryptographic Library	C1653
FCS_COP.1 /Hash	SHA-1 SHA-256 SHA-384 SHA-512	160, 256, 384, 512		
FCS_COP.1 /KeyedHash	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512		
FCS_RBG_EXT.1	CTR_DRBG (AES)	-	Fortinet FortiWLM RBG Cryptographic Library	C1652

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Identifier	Description
A.PHYSICAL_ PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_ FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

Identifier	Description
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_ INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Identifier	Description
T.UNAUTHORIZED_ ADMINISTRATOR_ ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_ CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow

Identifier	Description
	attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_ COMMUNICATION_ CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_ AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_ COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_ FUNCTIONALITY_ COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_ CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_ FUNCTIONALITY_ FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 Organizational Security Policies

The following table lists the Organization Security Policies followed by the TOE.

Identifier	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].
- Consistent with the expectations of the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- 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.
- The evaluated version of the TOE is Fortinet FortiWLM Wireless Manager 8 Build 8.5-2fips-7 as identified in the security target.
- Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 3 to ensure the evaluated configuration is established and maintained.
- Consumers need to pay specific attention to all the functionality and features that are explicitly excluded from the scope of the evaluation and are identified in Section 2.5.1 of the ST.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Fortinet FortiWLM Wireless Manager 8.5 FIPS 140-2 and Common Criteria Technote, dated 19 November 2021.
- Fortinet FortiWLM Wireless Manager 8.5 User Guide, Apr. 22, 2021.
- Fortinet FortiWLM Wireless Manager Release Notes Version 8.5.1 December 22,2020.
- Fortinet FortiWLM 100D QuickStart Guide, Apr. 22, 2021.
- Fortinet FortiWLM 1000D QuickStart Guide, Apr. 22, 2021.

These are the only documents that should be trusted for the configuration, administration, and use of the TOE in the evaluated configuration. If other documents are referenced in CC Supplemental User Guide, only the sections of other documents referenced should be trusted and used to configure and operate the TOE.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website

7 TOE Evaluated Configuration

The evaluated version of the TOE is FortiWLM 8.5-2fips-7. Common Criteria compliant operation requires the customer to follow the secure procedures for installation and operation of the FortiWLM unit using the documentation provided in section 6 of this report and place the FortiWLM unit in its FIPS-CC mode of operation.

The physical boundary of the TOE includes the Fortinet hardware equipped with Araneus Alea II USB Entropy Token and software which is delivered to the customer via commercial courier. The software function that reads the entropy data periodically checks whether the inserted USB device has a vendor ID matching Araneus and a product ID matching the Alea token. If any other USB device is inserted, the TOE will refuse to recognize it and display an error via cons

The TOE models in scope are as below

Model	CPU	Target Deployment
FWM-100D	Intel Celeron J1900 (Bay Trail)	Small enterprise
FWM-1000D	Intel Core i7-4790S (Haswell)	Large enterprise

Use of non-CC evaluated features

FIPS-CC mode does not prevent you from using features that were not part of the evaluated configuration. However, the following features must not be used in the evaluated configuration.

7.1 Excluded Functionality

For the TOE to be in the evaluated configuration, the following functions must not be enabled/used:

a) The Virtual Edition of the application suite

b) SNMP

c) Remote authentication (e.g. RADIUS, LDAP, TACACS+)

d) IPv6

e) Service Assurance Manager (SAM), Spectrum Manager, Wireless Intrusions Prevention System (WIPS)

f) Logging to syslog server

g) Logging to FortiCloud

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Fortinet FortiWLM Wireless Manager 8.5, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

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 the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]. A description of the Test Tools and Test Configurations used in the evaluation may be found in Section 3 and 4 of the Assurance Activity Report.

.

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 documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all 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 Fortinet FortiWLM Wireless Manager 8.5 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP.

9.1 Evaluation of Security Target

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 Fortinet FortiWLM Wireless Manager 8.5 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

The validator 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 Development Documentation

The evaluation team applied each EAL 1 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 STs TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] related to the examination of the information contained in the TOE Summary Specification.

The validator 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] related to the examination of the information contained in the operational guidance documents.

The validator 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. A list of the databases searched, the search terms, and the dates when the searches were performed may be found in Section 6.6.1 of the AAR.

The validator 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 addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], 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 test activities 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 performed the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

Forti Analyzer, a Fortinet product outside the scope of this evaluation, is required for external storage of audit logs in the evaluated configuration. Specifically, logging to external audit servers other than the FortiAnalyzer must not be enabled/used in the evaluated configuration.

11 Annexes

Not applicable.

12 Security Target

Fortinet FortiWLM Wireless Manager 8.5 Security Target v2.9, November 2021.

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 VR:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Fortinet FortiWLM Wireless Manager 8.5 Security Target v2.9 dated November 2021.
6. Fortinet FortiWLM Wireless Manager 8.5 FIPS 140-2 and Common Criteria Technote dated November 2021.
7. Assurance Activity Report for Fortinet FortiWLM Wireless Manager v8.5, dated November 2021.
8. Evaluation Technical Report for Fortinet FortiWLM Wireless Manager 8.5 dated November 2021.
9. Vulnerability Assessment for Fortinet FortiWLM Wireless Manager v8.5, dated November 2021.
10. Test Report for Fortinet FortiWLM 100D Wireless Manager 8.5, dated November 2021
11. Test Report for Fortinet FortiWLM 1000D Wireless Manager 8.5, dated November 2021