National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Fortinet FortiSwitch v7.6

Report Number: CCEVS-VR-VID11572-2025
Dated: 19 August 2025
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

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) validation team's assessment of the evaluation of the Fortinet FortiSwitch v7.6 provided by Fortinet, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was performed by the Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Leidos, Inc. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the:

- *collaborative Protection Profile for Network Device*, Version 3.0e, 6 December 2023 [NDcPP]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG]

The TOE is the Fortinet FortiSwitch v7.6. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 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 (CCEVS) and the conclusions of the testing laboratory in the ETR 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 the functional requirements and assurance requirements stated in the Security Target (ST). 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.

The technical information included in this report was obtained from the *Fortinet FortiSwitch v7.6 Security Target*, Version 1.0, August 7, 2025, 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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

Evaluated Product:	Fortinet FortiSwitch v7.6
Sponsor & Developer:	Fortinet, Inc. 899 Kifer Road Sunnyvale, CA 94086
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	15 August 2025
ST:	*Fortinet FortiSwitch v7.6 Security Target*, Version 1.0, August 7, 2025
ETR:	*Evaluation Technical Report for Fortinet FortiSwitch v7.6*, Version 1.0, 8 August 2025
CC:	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Release 5, April 2017
CEM:	*Common Methodology for Information Technology Security Evaluation*, Version 3.1, Release 5, April 2017

Protection Profiles:	*collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021
Conformance Result:	CC Part 2 extended; CC Part 3 conformant
Evaluation Personnel:	Anthony Apted Kofi Owusu Pascal Patin
Validation Personnel:	Jenn Dotson Sheldon Durrant Randy Heimann Lori Sarem

3 TOE Architecture

The TOE comprises a series of scalable Ethernet Switch network devices used to connect devices on Ethernet local area networks (LANs). An instance of the TOE is deployed as a single physical appliance in a network. The models included in the TOE are identified in section 8 and include FortiSwitchOS v7.6 software.

The TOE models differ in terms of number and types of network interfaces. All devices have an RJ-45 serial console port and some also have a dedicated management port. Both provide access to the management interfaces. See section 8 for specification details. All security-relevant functionality is identical across all firmware images. There are no security relevant differences between the appliance models.

Each TOE appliance includes one Intel Atom or Broadcom processor implementing the microarchitecture identified in section 8. The TOE appliances include Fortinet-developed firmware and the FortiSwitchOS v7.6 operating system, developed by Fortinet that is based on the Linux kernel. The operating system has been hardened and does not permit operators (even an authorized administrator) access to the OS. Fortinet also provided a list of included third party components separately, for the purposes of the evaluation activities.

The TOE offers both CLI and GUI management interfaces. The administrator gains access to the CLI locally by using the supplied console cable to connect the device's console port to the serial port on the management computer and using a terminal program. All devices also provide a dedicated management port that can be connected locally using an Ethernet cable connected directly to the management computer, or remotely by connecting to a management network. Whether connected locally or remotely, the administrator can access both the GUI (using HTTPS) and the CLI (using SSH) via the dedicated management port. All administrator authentication is performed by the TOE, using either username/password (for GUI and CLI access) or username/public key (for CLI access).

Figure 1 shows the TOE management interfaces as well as the interface with the remote audit server.

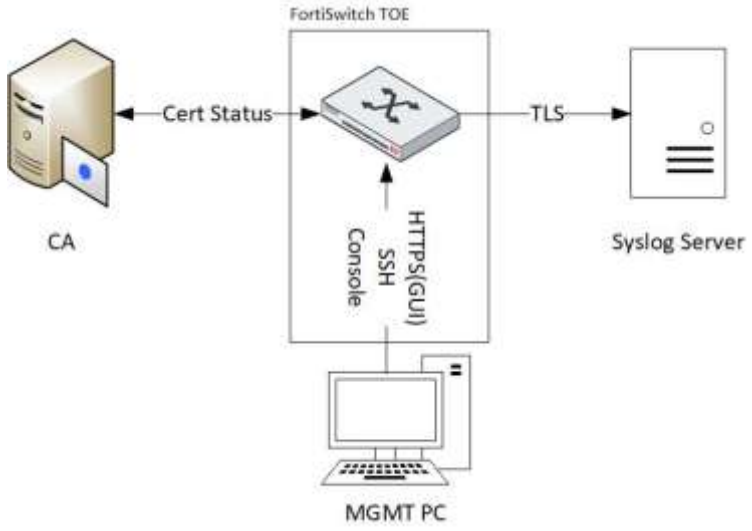

Figure 1 - TOE Interfaces

The TOE in its evaluated configuration requires the following components in its operational environment:

- A TLS-protected syslog server that receives audit events from the TOE
- A client workstation for administrator access to the web GUI and CLI with:
    - A supported browser:
        - Microsoft Edge, version 112
        - Mozilla Firefox®, version 113
        - Google Chrome™ web, version 113.
    - An SSH Client for remote access to the CLI.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

4.1 Security Audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log and export them to a syslog server using a TLS protected channel.

4.2 Cryptographic Support

The TOE provides CAVP certified cryptography in support of its SSH, TLS, self-testing, and for verifying TOE update package signatures. Cryptographic services include key management, random bit generation, symmetric encryption and decryption, digital signature, and secure hashing.

4.3 Identification and Authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of viewing and agreeing to the login banner. The TOE authenticates a user's credentials (password, public key) using local mechanisms provided by the TOE. The TOE also provides X.509 certificate checking for its TLS connections.

4.4 Security Management

The TOE provides CLI and web-based management interfaces that an administrator can access locally or remotely via a network port. Remote connections to the management interfaces are protected with SSH for the CLI and HTTPS for the GUI. The local administrative interface is subject to physical protection. To access the TOE locally, an administrator must directly connect their workstation to the TOE using a serial cable and successfully log in. The management interface is limited to the authorized administrators.

4.5 Protection of the TSF

The TOE implements various self-protection mechanisms. The TOE performs self-tests that cover the correct operation of the TSF. It provides functions necessary to securely update the TOE. It relies upon administrator manually provided time to ensure reliable timestamps. It protects sensitive data such as passwords and cryptographic keys stored on the TOE so that they are not accessible, even by an authorized administrator.

4.6 TOE Access

The TOE will terminate local and remote interactive sessions after a configurable period of inactivity. The TOE additionally provides the capability for administrators to terminate their own interactive sessions. The TOE can be configured to display an advisory and consent warning message before establishing a user session.

4.7 Trusted Path/Channels

When accessed remotely, the CLI and GUI management interfaces are protected by SSH or TLS, thus ensuring protection against modification and disclosure.

The TOE protects communications with the external syslog server from modification and disclosure by using TLS.

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- *collaborative Protection Profile for Network Device*, Version 3.0e, 6 December 2023 [NDcPP]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG]

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

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP/SSHPKG as described for this TOE in the ST. 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.

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 NDcPP with the SSHPKG 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 Guides identified in Section 6, additional customer documentation for the specific TOE models was not included in the scope of the evaluation and 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 NDcPP/SSHPKG and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

Fortinet offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with each TOE model is as follows:

- *NDcPP v3.0e FortiSwitch Technote – FortiSwitch 7.6*, Version 1.0, August 7, 2025
- *Fortinet Administration Guide—Standalone Mode FortiSwitchOS 7.6.0*, October 14, 2024
- *Fortinet CLI Reference—FortiSwitchOS 7.6.0*, August 27, 2024
- *Fortinet Log Reference FortiSwitchOS 7.6.0*, August 12, 2024
- *FortiSwitch 1024E Series (FS-1024E, FS-T1024E) QuickStart Guide*, May 2, 2022
- *FortiSwitch 624F/648F Series (FS-624F, FS-624F-FPOE, FS-648F, FS-648F-FPOE) QuickStart Guide*, August 21, 2024
- *FortiSwitch 424E Series (FS-424E, FS-424E-Fiber, FS-424E-POE, FS-424E-FPOE) QuickStart Guide*, October 7, 2022
- *FortiSwitch M426E-FPOE QuickStart Guide*, September 8, 2023
- *FortiSwitch Rugged 424F POE (FSR-424F-POE) QuickStart Guide*, May 12, 2023
- *FortiSwitch 448E Series (FS-448E, FS-448E-PoE, FS-448E FPoE) QuickStart Guide*, December 22, 2022
- *FortiSwitch 1048E QuickStart Guide*, November 18, 2021
- *FortiSwitch 3032E QuickStart Guide*, March 27, 2024
- *QuickStart Guide FortiSwitch 2048F (FS-2048F)*, November 21, 2023

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

Any additional customer documentation provided with the product or that 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 device as evaluated.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Fortinet FortiSwitch v7.6 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 3.0,* Version 1.0, August 8, 2025

A non-proprietary description of the tests performed is provided in the following document:

- *Assurance Activities Report for Fortinet FortiSwitch v7.6*, Version 1.0, 8 August 2025.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *collaborative Protection Profile for Network Devices* [5] and *Functional Package for Secure Shell (SSH)*.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Evaluation Activities for Network Device cPP* and *Functional Package for Secure Shell (SSH)*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland from October 2024 to June 2025.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

8 TOE Evaluated Configuration

The evaluated version of the TOE consists of Fortinet FortiSwitch v7.6, build 8083, running on the following physical appliances:

- FS-1024E
- FS-T1024E
- FS-624F
- FS-624F FPOE
- FS-648F
- FS-648F FPOE
- FS-424E
- FS-424E FIBER
- FS-424E POE
- FS-424E FPOE
- FSR-424F POE
- FS-M426E FPOE
- FS-448E
- FS-448E POE
- FS-448E FPOE
- FS-1048E
- FS-3032E
- FS-2048F

Evaluation testing covered the following hardware and processors:

- FS-1048E: Intel Atom C2538 (Rangeley microarchitecture)
- FS-448E FPOE: Broadcom BCM56172 with ARM A9 processor (ARM v7 microarchitecture).

The TOE must be deployed as described in section 5.1 of this Validation Report and be configured in accordance with the TOE documentation listed in section 6 above.

Per NIAP Scheme Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

8.1 Excluded Functionality

The Table below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. The features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in this Security Target. Only the following protocols implemented by the TOE have been tested, and only to the extent specified by the security functional requirements: TLS, HTTPS, SSH. The features below are out of scope.

Table 2: Excluded Functionality

Feature	Description
HTTP Management Protocols	Only SSH and HTTPS are used for the remote management protocols to manage the TOE.
802.1X	802.1X is used for network access. The NDcPP does not define requirements for this type of traffic/protocol and therefore it has not been evaluated.
External Authentication (LDAP, RADIUS, TACACS+)	Only local authentication is used for administrative authentication.
Administrator Authentication using X.509 certificates	In the evaluated configuration, identification and authentication of administrators is restricted to password and public-key for the CLI
“Remote Management” Operation Mode	Management modes other than standalone mode (also referred to as “Local Management”) are excluded from the evaluated configuration.
FortiSwitch Cloud management	The TOE is managed in standalone mode without FortiSwitch Cloud (must not be enabled).
ICMP	By default, the TOE disables ICMP Echo Response when placed into FIPS-CC mode.
Any features not associated with SFRs in claimed [NDcPP]	NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities or products are mentioned in the ST, it is for completeness only.

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 team determined the Fortinet FortiSwitch v7.6 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP/SSHPKG.

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 Fortinet FortiSwitch v7.6 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 ST and Guidance documents. Additionally, the evaluation team performed the assurance activities specified in the NDcPP/SSHPKG 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 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 NDcPP/SSHPKG 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 Analysis

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the proprietary Vulnerability Analysis Report prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities.

The evaluation team conducted searches of the following public vulnerability databases:

- National Vulnerability Database (https://nvd.nist.gov/)
- US-Cert (https://www.kb.cert.org/vuls/html/search)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- Fortinet Product Security Incident Response Team (PSIRT) (https://www.fortiguard.com/psirt).

The evaluation team performed these searches several times, most recently on August 8, 2025, using the following search terms:

- The list of software and hardware components that comprise the TOE:
  - “FortiSwitch”, “FortiSwitchOS” as the product
  - Appliance identifications: FS(W)-T1024E; FS(W)-1024E; FS(W)-624F (covering also FS(W)-624F FPOE); FS(W)-648F (covering also FS(W)-648F FPOE); FS(W)-424E (covering also FS(W)-424E FIBER, FS(W)-424E POE, and FS(W)-424E FPOE); FS(W)-M426E FPOE; FSR-424F POE; FS(W)-448E (covering also FS(W)-448E POE and FS(W)-448E FPOE); FS(W)-1048E; FS(W)-3032E; and FS(W)-2048F
  - Processor:
    - Intel Atom C3338
    - Intel Atom C2538
    - Intel Atom C3558
    - Broadcom BCM56174

- Broadcom BCM56160
- Broadcom BCM56170
- Broadcom BCM56172

- The processors consist of the following microarchitectures:
  - Denverton microarchitecture
  - Rangeley microarchitecture
  - ARM v7 microarchitecture
- Software:

Note, third-party component version numbers used within the TOE are considered to be proprietary information—the version numbers were provided to the evaluation team and used in the search.

- Linux Kernel
- Apache httpd
- OpenSSH
- OpenSSL
- FortiSwitch Crypto Library v7.6
- Curl
- Python
- OpenLDAP
- Jitterentropy

The evaluation team conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

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 instructions in the Guidance documents defined in Section 6 and any additional guidance that it references. 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 needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Specifically, Section 8 defines functionality that was excluded from or not allowed in the evaluated configuration.

Per NIAP Scheme Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration. As noted in Fortinet PSIRT FG-IR-24-435, the user should ensure they are using FortiSwitchOS version 7.6.1 (which includes the tested functionality in 7.6 build 8083).

11 Security Target

The ST for this product's evaluation *is Fortinet FortiSwitch v7.6 Security Target*, Version 1.0, 7 August 2025.

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

13 Bibliography

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

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

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements*, 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] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 3.1, Revision 5, 00 April 2017

[5] *collaborative Protection Profile for Network Devices*, Version 3.0e, December 6, 2023

[6] *Evaluation Activities for Network Device cPP*, Version 3.0e, December 6, 2023

[7] *Functional Package for Secure Shell (SSH)*, Version 1.0, May 13, 2021

[8] *Fortinet FortiSwitch v7.6 Security Target*, Version 1.0, August 7, 2025

[9] *NDcPP v3.0e FortiSwitch Technote – FortiSwitch 7.6*, Version 1.0, August 7, 2025

[10] *Fortinet Administration Guide—Standalone Mode FortiSwitchOS 7.6.0*, October 14, 2024

[11] *Fortinet CLI Reference—FortiSwitchOS 7.6.0*, August 27, 2024

[12] *Fortinet Log Reference FortiSwitchOS 7.6.0*, August 12, 2024

[13] *FortiSwitch 1024E Series (FS-1024E, FS-T1024E) QuickStart Guide*, May 2, 2022

[14] *FortiSwitch 624F/648F Series (FS-624F, FS-624F-FPOE, FS-648F, FS-648F-FPOE) QuickStart Guide*, August 21, 2024

[15] *FortiSwitch 424E Series (FS-424E, FS-424E-Fiber, FS-424E-POE, FS-424E-FPOE) QuickStart Guide*, October 7, 2022

[16] *FortiSwitch M426E-FPOE QuickStart Guide*, September 8, 2023

[17] *FortiSwitch Rugged 424F POE (FSR-424F-POE) QuickStart Guide*, May 12, 2023

[18] *FortiSwitch 448E Series (FS-448E, FS-448E-PoE, FS-448E FPoE) QuickStart Guide*, December 22, 2022

[19] *FortiSwitch 1048E QuickStart Guide*, November 18, 2021

[20] *FortiSwitch 3032E QuickStart Guide*, March 27, 2024

[21] *QuickStart Guide FortiSwitch 2048F (FS-2048F)*, November 21, 2023.

[22] *Assurance Activities Report for Fortinet FortiSwitch v7.6*, Version 1.0, August 8, 2025

[23] *Fortinet FortiSwitch v7.6 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 3.0*, Version 1.0, August 8, 2025

[24] *Fortinet FortiSwitch v7.6 Vulnerability Assessment*, Version 1.0, August 8, 2025

[25] *Evaluation Technical Report for Fortinet FortiSwitch v7.6*, Version 1.0, August 8, 2025.