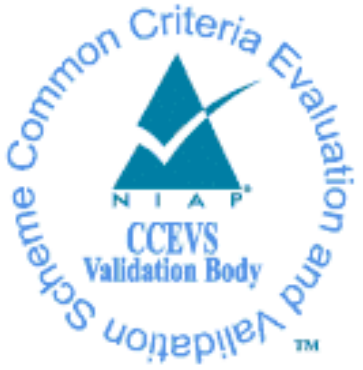
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



Validation Report

for

Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12

Report Number: CCEVS-VR-VID11464-2024
Dated: September 17, 2024
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
Lisa Mitchell
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Allison Keenan
Cody Cummins
Yoel Fortaleza
Linh Le
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 Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 solution provided by Cisco Systems, 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 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 2024. 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 and MACsec Ethernet Encryption*, Version 1.0, 29 March 2023 (CFG_NDcPP-MACsec_v2.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10).

The TOE is the Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12. 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 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 Security Target*, version 0.5, September 13, 2024, 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	Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Network Devices and MACsec Ethernet Encryption*, Version 1.0, 29 March 2023 (CFG_NDcPP-MACsec_v2.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10)
ST	*Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 Security Target*, version 0.5, September 13, 2024
Evaluation Technical Report	*Evaluation Technical Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12*, version 0.3, September 16, 2024
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	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Lori Sarem

3 Architectural Information

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

The Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 TOE is an enterprise access-layer switch for branch office deployments. Switches are used to connect multiple devices, such as computers, wireless access points, printers, and servers on the same network within a building or campus. A switch enables connected devices to share information and talk to each other and is a key building block for any network.

3.1 TOE Description

The Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 TOE is a purpose-built, switching and routing platform enabling connected devices to communicate over a network at layer 2 or 3. The TOE provides Administrative control and management of the network. For communicating with other network devices, the TOE provides AES-128 and AES-256 MACsec encryption. The TOE also provides Layer 3 capabilities, including OSPF, EIGRP, ISIS, RIP, and routed access.

Hardware models only vary in component characteristics. These characteristics affect non-security relevant functions, such as throughput and amount of storage. Since there is no security relevant impact due to differing components, equivalence between all switch models is claimed.

Primary features of the Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches include the following:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Central Processing Unit (CPU) complex with 8-GigaBytes (GB) memory, 16-GB of flash, and an external Universal Serial Bus (USB) 3.0 Solid State Drive (SSD) pluggable storage slot (delivering 120-GB of storage with an optional SSD drive)
- Serial Advanced Technology Attachment (SATA) SSD local storage
- Flash memory Electrically Erasable Programmable Read-Only Memory (EEPROM), used to store the Cisco IOS-XE image (binary program)
- Non-volatile Read Only Memory (ROM) is used to store the bootstrap program and power-on diagnostic programs
- Non-volatile Random Access Memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (e.g., Registered Jack (RJ-45) serial and standard 10/100/1000 Ethernet ports). The number of network interface ports varies by model
- Dedicated management port on the switch, RJ-45 console port, and a USB mini-Type B console connection

- Resiliency with Field Replaceable Units (FRU) and redundant power supply, fans, and modular uplinks

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8.

3.3 TOE Architecture

Deployment of the TOE in its evaluated configuration consists of at least one TOE switch model following the CC installation and configuration guidance document (AGD). The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internet working device and forwarded to their configured destination.

The TOE can be administered interactively using a CLI over a local console connection or remotely over SSH.

The operational environment of the TOE will include at least one MACsec peer. The environment will also include an audit (syslog) server and a Management Workstation. The syslog server is used to store audit records, where the TOE uses TLS 1.2 to secure the transmission of the records. The environment will include a Certificate Authority to provide the TOE with valid certificates and a method to check the peer certificate revocation status.

3.4 Physical Boundaries

The Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 TOE is composed of hardware and software (software image **cat9k_lite_iosxe.17.12.02.SPA.bin** or the **cat9k_iosxe.17.12.02.SPA.bin**). The hardware models are defined in Section 8.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure) or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The TOE stores audit messages in a circular audit trail configurable by the Security Administrator. All audit logs are transmitted to an external audit server over a trusted channel protected with TLS.

4.2 Cryptographic support

The TOE provides cryptographic functions to implement SSH, TLS, and MACsec protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation.

The 9200CX and 9300X/9300LM series devices support MACsec using the proprietary Unified Access Data Plane (UADP) 2.0 Application-Specific Integrated Circuit (ASIC). The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms. The 9500X series support MACsec using the Marvell CDR5M PHY using the 400G MACsec Engine on Marvell Alaska C PHYs version X7121M C0.

SSH and TLS protocols are implemented using the IOS Common Cryptographic Module (IC2M) and CiscoSSL FOM cryptographic modules. IC2M applies to SSH and MACsec and CiscoSSL FOM applies to TLS 1.2. The entropy source for both IC2M and CiscoSSL cryptographic modules is model dependent as listed below:

- 9200CX: ACT2Lite (ACT2) processor

- 9300X/9300LM/9500X: Cisco TRNG Core (CTC)

4.3 Identification and authentication

The TOE implements three types of authentication to provide a trusted means for Security Administrators and remote servers/endpoints to securely communicate: X.509v3 certificate-based authentication for remote syslog servers, password-based authentication for Security Administrators, and pre-shared keys for MACsec endpoints.

Security Administrators can compose strong passwords which are stored using a SHA-2 hash. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and will prevent the offending account from making further attempts until a Security Administrator defined period has elapsed or until the Administrator manually unblocks the account.

4.4 Security management

The TOE provides a secure remote administrative interface and a local interface to perform security management functions. This includes ability to configure cryptographic functionality; an access banner containing an advisory notice and consent warning message; a session inactivity timer before session termination; as well as an ability to update TOE software.

The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions.

4.5 Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE provides reliable timestamps to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), and to support accurate audit records.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides an ability to perform software updates and to verify those software updates are from Cisco Systems, Inc.

4.6 TOE access

The TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold period is reached. Once a session has been terminated the TOE requires the user to re-authenticate.

The TOE also displays a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

4.7 Trusted path/channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication paths between itself and remote endpoints.

In addition, the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

5 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 MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10)

That information has not been reproduced here and the NDcPP22e/MACSEC10 should be consulted if there is interest in that material.

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/MACSEC10 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 NDcPP22e and the MACSEC10 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 MACsec Device 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/MACSEC10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 CC Configuration Guide*, Version 0.4, September 13, 2024

Supplemented with:

- *Security Configuration Guide, Cisco IOS XE Dublin 17.12.x (Catalyst 9200 Switches)*, 2023-07-28
- *Security Configuration Guide, Cisco IOS XE Dublin 17.12.x (Catalyst 9300 Switches)*, 2023-07-28
- *Security Configuration Guide, Cisco IOS XE Dublin 17.12.x (Catalyst 9500 Switches)*, 2023-07-28

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

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

7 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 Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12*, Version 0.3, September 16, 2024 (DTR), as summarized in the evaluation *Assurance Activity Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12*, Version 0.3, September 16, 2024 (AAR).

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 Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/MACSEC10 including the tests associated with optional requirements. The proprietary DTR lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluation includes the following hardware models:

- C9200CX-12T-2X2G
- C9200CX-12P-2X2G
- C9200CX-8P-2X2G
- C9200CX-8UXG-2X
- C9300X-48HX, With the following network modules:
  - C9300X-NM-4C
  - C9300X-NM-8M
  - C9300X-NM-2C
  - C9300X-NM-8Y
- C9300X-48TX, With the following network modules:
  - C9300X-NM-4C
  - C9300X-NM-8M
  - C9300X-NM-2C
  - C9300X-NM-8Y
- C9300X-12Y, With the following network modules:
  - C9300X-NM-8M
  - C9300X-NM-2C
  - C9300X-NM-8Y
- C9300X-24Y, With the following network modules:
  - C9300X-NM-4C
  - C9300X-NM-8M
  - C9300X-NM-2C
  - C9300X-NM-8Y
- C9300X-48HXN, With the following network modules:
  - C9300X-NM-8M
  - C9300X-NM-2C
  - C9300X-NM-8Y
- C9300X-24HX, With the following network modules:
  - C9300X-NM-8M
  - C9300X-NM-2C
  - C9300X-NM-8Y
- C9300LM-24U
- C9300LM-48UX
- C9300LM-48T
- C9300LM-48U
- C9500X-28C8D
- C9500X-60L4D

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 Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/MACSEC10.

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 Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 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 document. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP22e/MACSEC10 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. The guide was assessed during the design and testing phases of the evaluation to ensure it was 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/MACSEC10 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 contained in the DTR prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the following sites:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- cve.org CVE Database (https://www.cve.org/),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The search was conducted on September 9, 2024, with the following search terms: “IC2M”, “IOS Common Cryptographic Module”, “CiscoSSL FOM”, “Unified Access Data Plane”, “UADP”, “Cisco Catalyst”, “IOS-XE 17.12”, “Cisco IOS XE 17.12”, “act2lite”, “cisco trng core”, “MACsec”, “MACsec Controller”, “MSC”, “CDR5M PHY”, “catalyst 9200cx”, “catalyst 9300x”, “catalyst 9300lm”, “catalyst 9500x”, “Xilinx ZU3EG”, “ARM Cortex-A53”, “Intel Xeon D-1624N”, “Intel Hewitt-Lake”, “Cisco Silicon One Q200”,

"Intel Xeon D-1564N", "Intel Broadwell", "Marvell Alaska C 88X7121M", "SSH", and "TLS".

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 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 *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 CC Configuration Guide* (AGD) document. As noted in the ST, AAR, and AGD, setting the session inactivity period to "0" disables it; consumers should ensure it is set to a value greater than "0" to be in the evaluated configuration.

As noted in Section 6, consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE and software, either earlier or later, were evaluated. Any additional customer documentation, not listed in Section 6, 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.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 Security Target*, Version 0.5, September 13, 2024.

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 MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 (MACSEC10).

[6] *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 Security Target*, Version 0.5, September 13, 2024 (ST).

[7] *Assurance Activity Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12*, Version 0.3, September 16, 2024 (AAR).

[8] *Detailed Test Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12*, Version 0.3, September 16, 2024 (DTR).

[9] *Evaluation Technical Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12*, Version 0.3, September 16, 2024 (ETR).

[10] *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 17.12 CC Configuration Guide*, Version 0.4, September 13, 2024 (AGD).