EUCC Certification Report

Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M)

Sponsor and developer:	***Cisco Systems, Inc.*** **170 West Tasman Drive** **95134 San Jose, CA** **USA**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**EUCC-3110-2025-12-0098-01 Certification Report**
Report version:	**2**
Project number:	**EUCC-2500098-01**
Author(s):	**Wim Ton, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**3 December 2025**
Number of pages:	**17**
Number of appendices:	**0**

Reproduction of this report is authorised only if reproduced in its entirety.

CONTENTS

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the ‘Uitvoeringswet cyberbeveiligingsverordening’ (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs and Climate Policy.

TrustCB B.V. has been licensed by RDI as a Certification Assessment Body (CAB) for the task of ISO/IEC 17065 Certification Activities up to and including Evaluation Assurance Level High for ICT security products, as well as for protection profiles and is authorised to issue EUCC cybersecurity certificates as an Authorised and notified Dutch Certification Body.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

Reproduction of this report is authorised only if it is reproduced in its entirety.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M). The developer of the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M) is Cisco Systems, Inc. located in San Jose, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Cisco Nexus 9K Series are data center-class switches for use as an aggregation switch in the data center. The Cisco Nexus 9K Series provides multilayer support, greater performance and enhanced operations through features including intelligent services, programmability, automation, analytics, and manageability.

Cisco NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although NX-OS performs many networking functions, this evaluation only addresses the functions that provide for the security of the TOE itself.

The TOE versions differ in the number and type of the network connections and the processing capacity. They are all based on the same processor family, Intel Xeon and all run the same software.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 3 December 2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M), the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

Consumers of the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M) are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

There are no special configuration requirements for the TOE besides the requirements defined in the user guidance. All users shall read these requirements and install the TOE in the operational environment accordingly.

The summary of the threats and security policies which [ST] defines:

- The Threats that are presented in Section 3.2 of [ST] as the threats addressed by the TOE and the IT environment. The assumed level of expertise of the attacker for all identified threats is Basic.
- The only Organizational Security Polices (OSPs) defined for this TOE is to have an access banner.

The results documented in the evaluation technical report [ETR] for this product provide sufficient evidence that the TOE meets the requirements for exact conformance to the collaborative Protection Profile for Network Devices [PP], referencing specific assurance packages ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE.REQ.1, ASE.TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1 and ALC_FLR.2.

The assurance level is recognised by article 52 of [CSA] as ‘substantial’

The evaluation was conducted using the ISO/IEC 18045 :2008, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM) v3.1 revision 5.

TrustCB B.V., as the Dutch NCCA (RDI) licensed Certification Assessment Body for EUCC certification activities, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the EUCC Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

This document was initially issued on 03 December 2025 as version 1 and re-issued 03 December 2025 as version 2 to clarify the presentation of the specific assurance packages referenced in the exact conformance to the [PP]

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ICT product Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M) from Cisco Systems, Inc. located in San Jose, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Cisco Nexus 9200 Series	N9K-92348GC-X
	Cisco Nexus 9300 Series	N9K-C93108TC-FX
		N9K-C9348GC-FXP
		N9K-C93216TC-FX2
		N9K-C93180YC-FX
		N9K-C93240YC-FX2
		N9K-C93360YC-FX2
		N9K-C9364C
		N9K-C9332C
		N9K-C9336C-FX2
		N9K-C9364C-GX
		N9K-C9316D-GX
		N9K-C93600CD-GX
		N9K-C93400LD-H1
	Cisco Nexus 9400 Series Supervisor	9400-Sup-A
	Cisco Nexus 9500 Series	N9K-C9504
		N9K-C9508
		N9K-C9516
		N9K-SUP-A+
		N9K-SUP-B+
		N9K-SC-A
	Cisco Nexus 9800 Series	N9K-C9808
		N9K-C9804
Software	NX-OS 10.4	10.4(5)(M)

To ensure secure usage a set of guidance documents is provided, together with the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M). For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

The name and contact information provided for the holder of the issued Certificate associated with this Certification Report are as follows:

Organisation name:	Cisco Systems, Inc.
Address:	170 West Tasman Drive, 95134 San Jose, CA USA
Certified product contact	certteam@cisco.com

Website link for supplementary cybersecurity information associated with the TOE, in accordance with Article 55 of [EU-EUCC]	https://www.cisco.com/c/en/us/solutions/industries/government/global-government

2.2 Security Policy and Services

Security Audit

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 Authorized Administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides an internal circular audit trail. Audit logs are transmitted to an external audit server over a trusted channel protected with TLS.

Cryptographic Support

The TOE provides cryptography in support of remote administrative management via SSHv2 and secures the session between the TOE and remote syslog server using TLS.

Identification and authentication

The TOE provides authentication services for administrative users wishing to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE is configured to require a minimum password length of 8 characters as well as password-strength checking that prevents the use of weak passwords. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection.

Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco NX-OS is not a general-purpose operating system and access to Cisco NX-OS memory space is restricted to only Cisco NX-OS functions.

TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The administrator can also terminate their own session by exiting out of the CLI.

The TOE can display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

Trusted path/channel

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access. Nexus 9K also allows a trusted channel to be established with a syslog server using TLS.

Secure update

An Authorized Administrator can update the TOE software. Updates are only accepted by the TOE if they bear a valid signature from Cisco.

2.3 Vulnerability handling and Assurance Continuity Policies

The following vulnerability policy has been identified as applicable to the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M):

Document Reference: Cisco Nexus 9000 Series Switches running NX-OS 10.4 Life-Cycle Support Vulnerability Management and Disclosure (EUCC) version 1.0

The developer identified measures in place, including:

- When a vulnerability affecting the TOE is confirmed and deemed remediable through the Vulnerability Impact Analysis (VIA), Cisco initiates a structured process to implement corrective action while maintaining EUCC certification compliance.
- Cisco uses CDETS as a bug tracking system. CDETS ensures traceability from intake through resolution. It captures history, ownership, and all changes made to each record.
- Changes are managed through formal change control and follow the process for changes to a certified ICT product as described by [EUCC] Annex IV.3, with any necessary updates to the certification implemented before the fix can be deployed.
- Customers are notified of vulnerabilities through Cisco’s standard communication channels, including the Notification Service and PSIRT alerts.

2.3.1 Assurance Continuity Policy

This is a new product certification. An assurance continuity policy was not provided.

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST]. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

2.4.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The ST states that:

- The TOE must be installed and operated in a secure location.
- The TOE does not protect against non-management network traffic, e.g. DoS is out of scope.

The following network protocols are not part of the evaluated configuration:

- FTP
- HTTP(S)
- IPsec, IKE
- LDAP(S)
- NTP
- Radius
- SNMP
- TACACS+
- Telnet
- Bash shell
- TFTP

2.5 Architectural Information

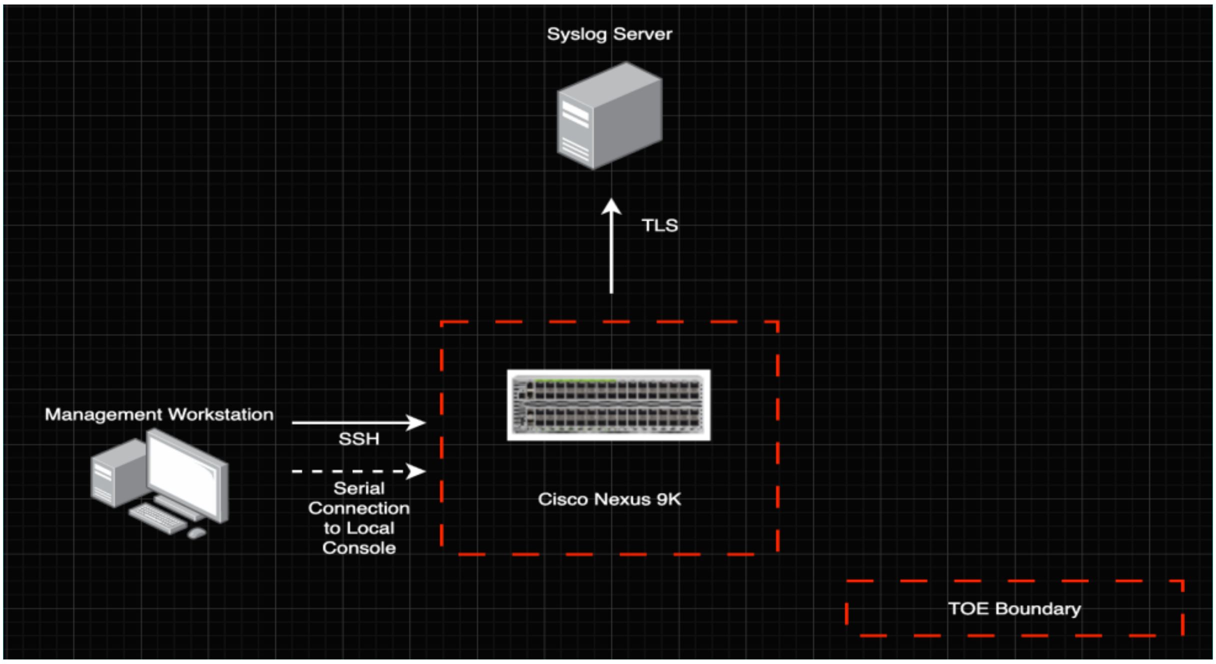


Figure 1 The TOE in its environment

2.6 Supplementary Cybersecurity Information

The contact information for the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M) was provided as: certteam@cisco.com

The following website link was provided for supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

This link provides further details and links for:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M);
- The period during which Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M) security support will be offered to end users; stated as 5 years aligning with the validity of the issued EUCC certificate.

- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M):
- the online repository listing publicly disclosed vulnerabilities related to the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M) and to any relevant cybersecurity advisories:

The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M):

Identifier	Revision	Date
Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target,	2.1	03 December 2025
Cisco Nexus 9000 Series Switches running NXOS 10.4 Common Criteria Operational User Guidance and Preparative Procedures	6	06 November 2025

2.7 Lifecycle Management processes and production facilities

Not applicable to this evaluation,

2.8 ICT Product Testing

2.8.1 Identification of CAB and ITSEF

TrustCB is the Certification Assessment Body, licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC substantial and high certification activities.

TrustCB point of contact: EUCC@trustcb.com

Testing was performed by following ITSEF: SGS Brightsight B.V

2.8.2 Identification of used assurance components

The assurance components used in the product testing were **EAL1** augmented with **ALC_FLR.2 and ASE_SPD.1** as defined by, and detailed in, [CC] and [CEM].

These assurance components align with an exact conformance to the Collaborative Protection Profile for Network Devices [PP],

Security Target evaluation	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.1
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.1
TOE summary specification	ASE.TSS.1
Development	
Functional specification	ADV_FSP.1
Guidance documents	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1
Life cycle support	

Labelling of the TOE	ALC_CMC.1
TOE CM coverage	ALC_CMS.1
Flaw Remediation	ALC_FLR.2
Tests	
Independent testing	ATE_IND.1
Vulnerability assessment	
Vulnerability analysis	AVA_VAN.1

2.8.3 EUCC State of the Art documents and Protect Profiles

No EUCC state-of-the-art documents were used for this evaluation. The NIAP Collaborative Protection Profile for Network Devices [PP] was referenced for this evaluation, stating “exact conformance”.

2.8.4 Testing approach and depth

The evaluator has assessed results from a previous evaluation on the TOE and determined the following test strategy as valid for this evaluation:

- The execution of the crypto tests was witnessed by the evaluator in a remote session with the developer, since access to the developer’s CAVS account is required for these tests.
- Additional test cases test to confirm the version of the TOE, to supplement coverage of SFRs and/or TSFI, and to further exercise the behaviour of critical functionality.
- During functional testing, an issue was found that resulted in an update to 10.4(5)(M). After analysis by the evaluator, only the tests concerning the affected TSFI were re-run.

2.8.5 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination several potential vulnerabilities were identified.
- CWE vulnerability focus: Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also, during this examination several potential vulnerabilities were identified.
- Use of Scanning tools: The evaluator runs vulnerability scanning tools to identify potential vulnerabilities
- Public vulnerability search: Several additional potential vulnerabilities were identified during a search in the public domain

The evaluator conducted a public domain vulnerability search up until 29 August 2025 to check whether any new vulnerabilities are published since the previous TOE certification was performed. Additionally, the evaluator re-executed a number of tests using scanning tools to verify if any new potential vulnerabilities could impact any of the services running on the TOE in the evaluated configuration.

The total test effort expended by the evaluators was1.5 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.8.6 Test configuration

The tests were executed on the N9K-C9336C-FX2– Intel Xeon D-1526 (Broadwell) version of the TOE. All TOE versions use the same security relevant firmware and equivalent security relevant hardware.

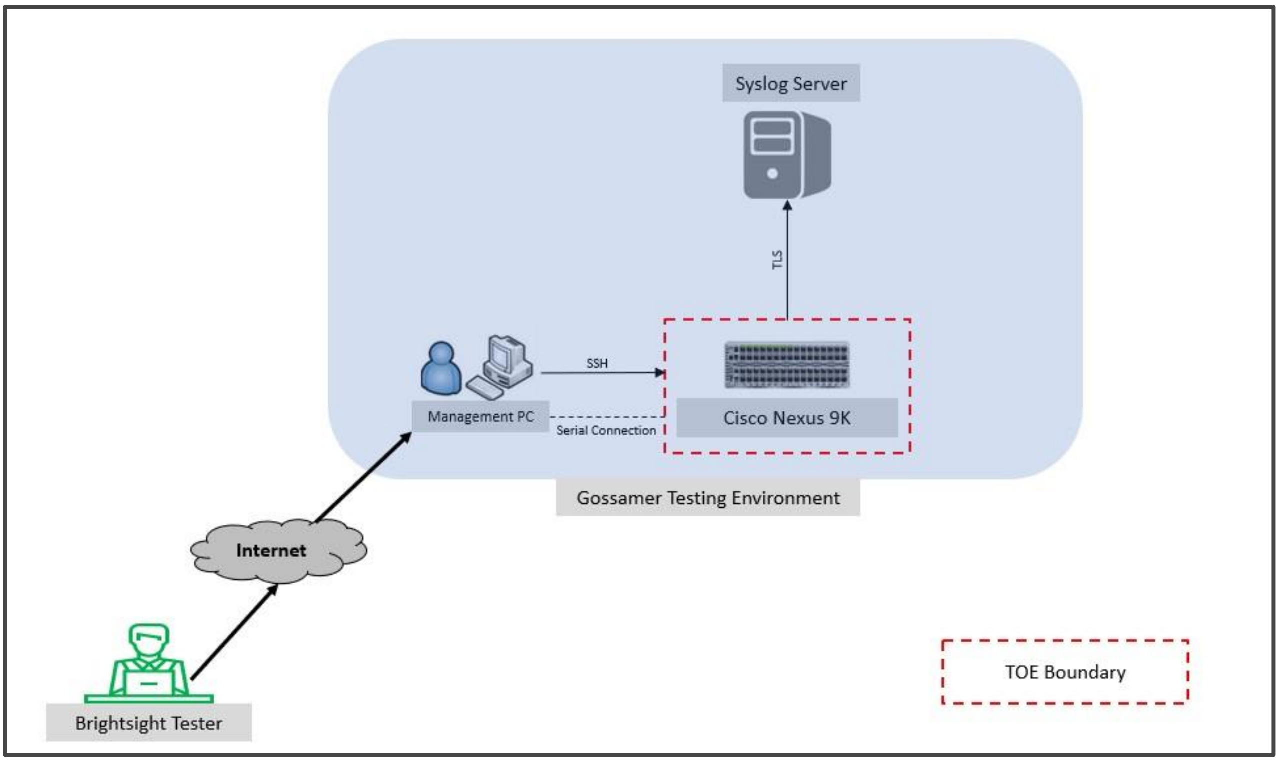


Figure 2. Baseline test setup

2.8.7 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.8.8 Reused Evaluation Results

This was a new evaluation and certification under EUCC.

No sites have been visited as part of this evaluation.

2.8.9 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M). The evaluated configuration is “FIPS mode”, with an external syslog server.

The user can check the FIPS state with the “*show fips status*” command. The user can check the version of the TOE software with the “*show version*” command. The hardware version is printed on a label on the outside of the TOE.

2.9 Results of the evaluation and information regarding the certificate

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is “**Pass**”.

2.9.1 Assessment against each assurance requirement

<u>ASE</u>

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.1
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.1
TOE summary specification	ASE.TSS.1

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target *[ST]* and its components. The TOE introduction, conformance claim, security problems, security objectives, security requirements, TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements in the [PP] augmented with ALC_FLR.2. No issues or deviations were identified.

ADV

ADV	
Functional specification	ADV_FSP.1

The evaluation has demonstrated that the developer's evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. Accordingly, the ADV activities meet the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified.

ALC

ALC	
CM capabilities	ALC_CMC.1
CM Scope	ALC_CMS.1
Flaw remediation	ALC_FLR.2

The evaluation has demonstrated that the developer's evidence meets ALC specified. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in accordance with the CM plan to maintain all configuration items by automated means. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. Accordingly, the ALC activities satisfy the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified.

ATE

ATE	
Independent testing	ATE_IND.1

For the evaluator's independent testing, the overall approach for test selection, goals for the witnessing session, and independent test plan were clearly outlined. The evaluator's testing results showed that all sampled tests were passed. Accordingly, the ATE activities satisfy the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.1

The evaluator conducted a public domain vulnerability search. Additionally, the evaluator executed a number of tests using scanning tools to verify if new potential vulnerabilities could impact any of the services running on the TOE in the evaluated configuration, fuzzing tests on the network interfaces and privilege escalation on the CLI.

Consequently, the AVA activities were performed in full compliance with the assurance requirements in the [PP] augmented with ALC_FLR.2, providing a substantial level of confidence in the TOE's resistance to exploitation.

2.9.2 Overall result of evaluation

The Security Target claims ‘exact’ conformance to the Protection Profile “collaborative Protection Profile for Network Devices, v3.0e” (NDcPP_V3.0) with the Functional Package for Secure Shell (SSH) V1.0 *[PKG_SSH]* dated 13 May, 2021, referencing specific assurance packages ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE.REQ.1, ASE.TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1 and ALC_FLR.2.

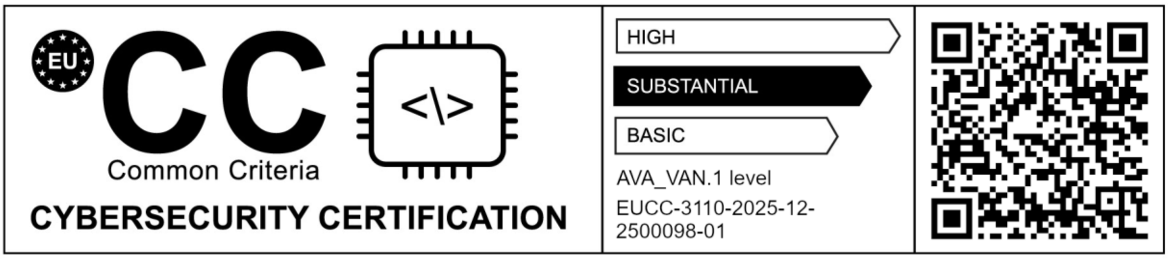
Based on the above evaluation results the evaluation lab concluded the Cisco Nexus 9000 Series Switches, software version Cisco NX-OS version 10.4(5)(M) to be **CC Part 2 extended, CC Part 3 conformant.** The results implied that the product satisfies the security requirements specified in Security Target *[ST]*. The assurance level defined by the [PP] is recognised by article 52 of [CSA] as ‘substantial’.

2.10 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2025-12-0098-01

Date of issuance: 3 December 2025 and with a validity period of **5 years**.



2.11 Comments/Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

3 Security Target

The Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target, v2.1, 03 December 2025 *[ST]* is included here by reference.

The TOE is a purpose-built data center-class switch for use as an aggregation switch in the data center.

Section 1.3 of the *[ST]* describes the evaluated ICT product. The security functionality of the evaluated ICT product is represented by the implementation of the selected components of *[CC]*(Part2) and are listed in section 5.2 of the *[ST]*, Summary of TOE Security Functional Requirements.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report
ACL	Access Control List
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CLI	Command Line Interface
DoS	Denial of Service.
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
LAN	Local Area Network
MAC	Message Authentication Code
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
TCP	Transmission Control Protocol
TRNG	True Random Number Generator
VLAN	Virtual LAN

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision **Error! Reference source not found.**, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision **Error! Reference source not found.**, April 2017

[PP] collaborative Protection Profile for Network Devices, v3.0e, 06 December 2023

[CPP_ND_SD_V3.0E] Evaluation Activities for Network Device cPP, v3.0e, 06 December, 2023

[PKG_SSH] Functional Package for Secure Shell (SSH), v1.0, 13 May, 2021

[ETR] Evaluation Technical Report “Cisco Nexus 9000 Series Switches running on NXOS 10.4” – NDcPP, 25-RPT-805, v2.0, 03 December 2025

[EU-CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[EU-EUCC] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

[EU-EUCC-amdt.1] Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

[ST] Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target, v2.1, 03 December 2025

(This is the end of this report.)