TRUSTCB
TRUST AND VERIFY

EUCC Certification Report

Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers

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-3110-2025-09-2500093-01-CR**

Report version: **1.0**

Project number: **EUCC-2500093-01**

Author(s): **Alireza Rohani, TrustCB B.V.**
contact: EUCC@trustcb.com

Date: **4 September 2025**

Number of pages: **17**

Number of appendices: **0**

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.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers.

The developer of the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers 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.

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 TOE is a network device that The TOE consists of hardware and software components that support Cisco's unified fabric, which carries multiple types of datacenter traffic over a dedicated fabric hardware (in the form of stand-alone appliances, chassis-integrated modules, and converged network adapters). Cisco Intersight provides a role-based access control (RBAC) policy to control the separation of administrative duties and provide a security log of all changes made.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 04 September 2025 with the approval of the [ETR][1]. The certification procedure has been conducted in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024.

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 Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers, 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 Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers 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 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.
- No Organizational Security Polices (OSPs) have been defined for this TOE.

The results documented in the evaluation technical report *[ETR]* for this product provide sufficient evidence that the TOE meets the EAL2 augmented assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2. This assurance level is recognised by article 52 of [CSA] as ‘substantial’

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, Revision 1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1 *[CC]* (Parts 1, 2, 3, 4, 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

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ICT product Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers 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 UCS X-Series: Chassis: UCSX-9508 M6 Compute Nodes (servers): UCSX-210C-M6 VIC in M6 compute nodes: UCSX-V4-Q25GME, UCSX-V4-PCIME, or UCSX-V4-PCIME M7 Compute Nodes (servers): UCSX-210C-M7, UCSX-410C-M7 VIC in M7 compute nodes: UCSX-ME-V5Q50G-D, UCSX-ML-V5Q50G-D, UCSX-ML-V5D200G-D, or UCSX-V4-PCIME Cisco UCS C-Series Servers and Virtual Interface Cards (VIC): M6 Servers: UCSC-C220-M6, UCSC-C225-M6, UCSC-C240-M6, UCSC-C245-M6 VIC for M6 C-Series servers: UCSC-PCIE-C25Q-04, UCSC-PCIE-C100-04, UCSC-P-V5Q50G, UCSC-P-V5D200G, UCSC-M-V25-04, UCSC-M-V5Q50G, UCSC-M-V100-04, UCSC-M-V5D200G M7 Servers: UCSC-C220-M7, UCSC-C240-M7 VIC for M7 C-Series servers: Same as for M6 C-Series servers. Cisco Fabric Interconnect (FI): UCS-FI-6454, UCS-FI-64108, and/or UCS-FI-6536 Cisco Intelligent Fabric Modules (IFM): For M6 compute nodes: UCSX-I-9108-25G, UCSX-I-9108-100G For M7 compute nodes: UCSX-I-9108-25G-D, UCSX-I-9108-100G-D	N/A
Software	Cisco Intersight Virtual Appliance (PVA)	1.0.9-677
	Cisco Intersight Managed Mode (IMM)	4.3(4.240074)
	Cisco UCS C-Series Server Firmware	4.3(4.240152)
	Cisco UCS X-Series Server Firmware	5.2(0.230127)

To ensure secure usage a set of guidance documents is provided, together with the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers. For details, see section 2.5 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

The following website link has been provided 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-certifications/common-criteria.html

2.2 Security Services

The major security features provided by the TOE are summarized as follows:

Cisco Intersight stores audit information to assist the administrator in monitoring the security state of the TOE as well as troubleshooting various problems that arise throughout the operation of the system. Intersight may be configured to send records to an external syslog server. The remote audit server is outside the TOE boundary. The TOE provides the ability to audit the actions taken by authorized administrators. Audited events include start-up and shutdown, configuration changes, administrative authentication, and administrative log-off. The TOE provides the capability for authorized administrators to review the audit records stored within the TOE.

VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that Ethernet frames are presented to interfaces within the same VLAN.

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and Organizations. A role defines the privileges of a user in the system and the Organization defines the domains that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and Organizations.

The TOE supports two methods of authenticating administrator logins to Intersight: a local user database; or a remote authentication server accessed either via LDAPS. Remote authentication may be used to centralize user account management to an external authentication server. The system has a default user account, “admin”, which cannot be modified or deleted. This account is the system administrator account and has full privileges. Each local user account must have a unique username that does not start with a number.

The TOE can be managed via Intersight via graphical user interface (over TLSv1.2 or TLSv1.3), or command line (over SSHv2) or via virtual console to access Intersight via ESXi). Any of these administrative interfaces can be used in the evaluated configuration of the TOE. For all management channels, users have a default read-only authorization to access non-sensitive management objects (keys and passwords are never exposed to an external management interface). Additional user privileges each grant access to modify specific management objects. An administrator can use the Intersight GUI to perform management tasks for all physical and virtual devices within the TOE.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE and in validating service requests.

The TOE allows trusted paths to be established to itself from remote administrators over for CLI access (SSH) or HTTPS for web UI access.

2.3 Vulnerability handling and Assurance Continuity Policies

The following vulnerability policy has been identified as applicable to the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers

Document reference:

CISCO Intersight Virtual Appliance with IMM Fabric and UCS Servers Life-Cycle Support Vulnerability Management and Disclosure (EUCC), v0.1, 08 May 2025

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 3.1 of the *[ST]*.

The user guidance as outlined in section 4 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 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 3.1 of the *[ST]*.

2.5 Architectural Information

The TOE, Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers, hereafter referred to as Cisco Intersight, is a unified computing solution, which provides access layer networking and servers.

The logical architecture can be depicted as follows:

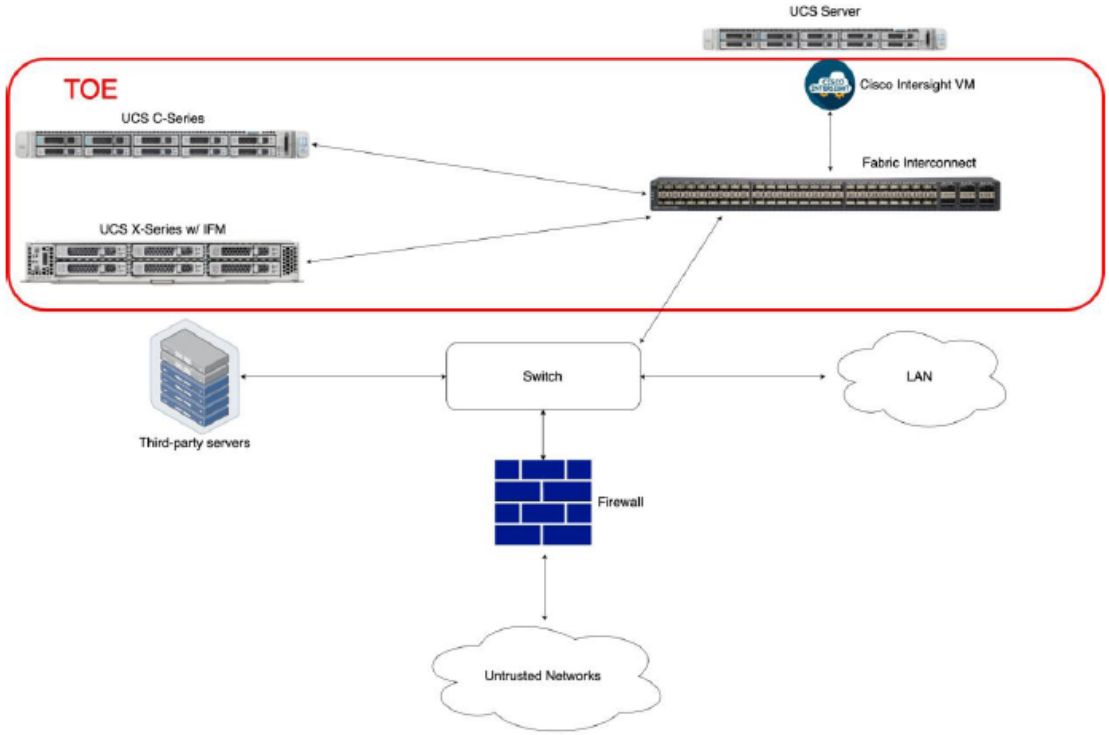


Figure 1 TOE Architecture

2.6 Supplementary Cybersecurity Information

The contact information for the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers 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 Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers;
- The period during which Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers 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 Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers:
- the online repository listing publicly disclosed vulnerabilities related to the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers and to any relevant cybersecurity advisories:

The following documentation is provided with the product by the developer to the customer for the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers:

Identifier	Revision	Date
Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers Security target	Rev. 0.3	2025-05-14
Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers, Common Criteria Operational User Guidance and Preparative Procedures, EDCS-24888933	Rev. 0.7	2025-02-10

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 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 component(s) used in the product testing were **EAL2 augmented with ALC_FLR.2**, as defined by, and detailed in, [CC] and [CEM].

2.8.3 EUCC State of the Art documents and Protect Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

No conformance to any production profile was claimed in this evaluation.

2.8.4 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and SFR-enforcing module level. The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The security mechanisms that aren't covered by the developer tests are covered through independent testing:

- Verify preparative procedures to confirm that the TOE can be prepared securely for operation
- Verify account protection
- Verify whether the log may leak sensitive information such as password
- Verify the LDAPS functionality
- Perform public domain vulnerability scan and verify no additional ports open
- Verify no access during TOE initialization process
- Verify the REST API authentication

In addition to the developer tests, the evaluator derived and executed 6 additional functional tests.

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 August 28th 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 was two weeks. All of the test effort was on the logical tests.

2.8.6 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was:

- Cisco Intersight Virtual Appliance (PVA) v1.0.9-677 (running on UCS C220 M7S)

- Fabric Interconnect UCS-FI-6464 with IMM 4.3 (4.240074)
- UCS C220 M6N v4.3(4.240152)

The ITSEF assessed the differences between the above configuration and the possible configurations of the TOE (all the configurations of the TOE are stated in *[ST]* table 4), and concluded that they do not negatively impact security. All the test results obtained on the tested configuration are fully applicable to the TOE configurations stated in the *[ST]*.

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 certification under EUCC however documentary evaluation results of an earlier version of the TOE certified under the Netherlands Scheme for Certification in the area of IT security (NSCIB-CC-2400020-01) have been partially reused. Vulnerability analysis and penetration testing has been renewed.

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 Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers.

2.9 Results of the evaluation

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

The verdict of each claimed assurance requirement is "**Pass**".

2.9.1 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
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 EAL2 augmented with ALC_FLR.2. No issues or deviations were identified.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.2
TOE design	ADV_TDS.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. The subsystem/module level model is sensible, useful, and shows TSFIs and subsystem/module decomposition. The security architecture is thoroughly explained, design compliance rationale is complete and coherent, and necessary evidence is extracted per alternative approach. The evaluator confirmed why the TSF is well-structured. SFRs were inspected, with findings mapped to the implementation representation in both evaluation meetings. Accordingly, the ADV activities meet the assurance requirements for EAL2 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 for EAL2 augmented with ALC_FLR.2, with no issues or deviations identified.

ALC

ALC	
CM capabilities	ALC_CMC.2
CM Scope	ALC_CMS.2
Delivery	ALC_DEL.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. Delivery procedures were well-documented, ensuring security during TOE distribution. 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 for EAL2 augmented with ALC_FLR.2, with no issues or deviations identified.

ATE

ATE	
Coverage	ATE_COV.1
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2

The evaluation has demonstrated that the developer's evidence for ATE requirements meets all specified requirements. The testing approach used by the developer effectively covered the TSFIs. The developer's rationale for testing all TSFIs was presented and verified. The developer test results show that for all tests either the result was pass or a proper rationale was given why the test failed. 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 for EAL2 augmented with ALC_FLR.2, with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.2

The evaluator conducted a public domain vulnerability search up until 28 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.

Consequently, the AVA activities were performed in full compliance with the assurance requirements EAL2 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

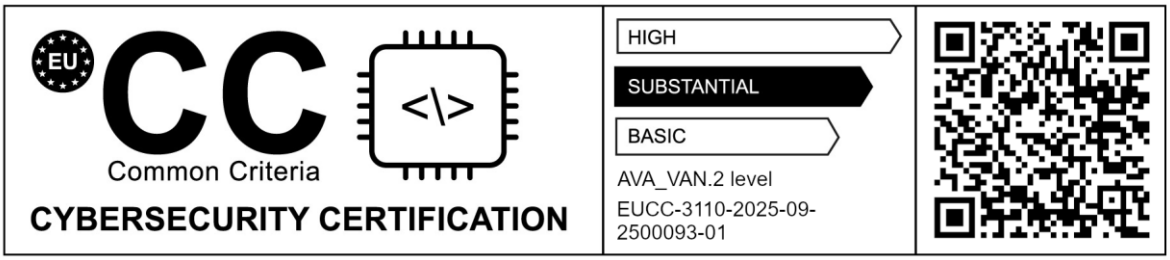
Based on the above evaluation results the evaluation lab concluded the Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 UCS X-Series Servers and UCS C-Series Servers, to be **CC:2022 revision 1 Part 2 conformant, CC:2022 revision 1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as 'substantial', and to meet the requirements of **EAL2 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Certificate information and scheme label

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

Unique identifier: EUCC-3110-2025-09-2500093-01

Date of issuance: 04-09-2025 and with a validity period of **5 years**.



2.11 Comments/Recommendations

The user guidance as outlined in section 2.5 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 Summary of the Security Target

The Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers, v0.3, 14 May 2025 *[ST]* is included here by reference.

The TOE, Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers, is a unified computing solution, which provides access layer networking and servers.

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]*, 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
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report

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, CC:2022 Parts 1, 2, 3, 4 and 4, Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[DEV_DOCS]	For developer documentation used in the evaluation effort, see [ETR]
[ETR]	Evaluation Technical Report “Cisco Intersight Virtual Appliance 1.0.9 with IMM Fabric 4.3 and UCS X-Series and UCS C-Series Server” – EAL2 augmented, 25-RPT-744, version 1.0, 28 August 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)
[ST]	Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers, v0.3, 14 May 2025

(This is the end of this report.)