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:	**NSCIB-CC-2400020-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400020-01**
Author(s):	**Andy Brown**
Date:	**16 March 2025**
Number of pages:	**12**
Number of appendices:	**0**

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

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) 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 (site) security target is a requirements specification document that defines the scope of the evaluation activities.

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

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

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

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.

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 16 March 2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

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.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the 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 Servers1: 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 “Documentation” of this report.

2.2 Security Policy

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 Assumptions and Clarification of Scope

2.3.1 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]*.

2.3.2 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.

2.4 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:

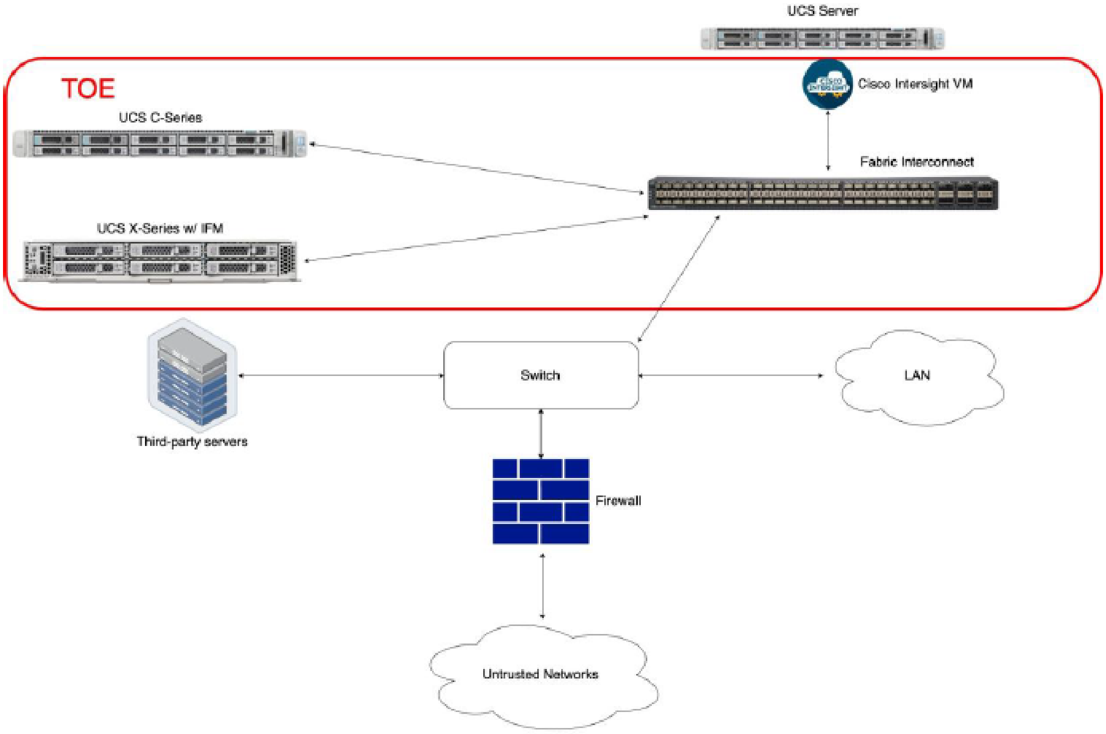

Figure 1 TOE Architecture

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers Common Criteria Operational User Guidance and Preparative Procedures,	V0.7

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed 13 tests, each of which tests an important security feature, and mapped to the relevant SFRs. Test is considered a "pass" if the actual results match the expected results.

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.

2.6.2 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 total test effort expended by the evaluators was 13.125 person-week. During that test campaign, all of the total time was spent on logical tests.

2.6.3 Test configuration

The following TOE components were used in the test setup:

- 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)

2.6.4 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.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 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 Evaluation Results

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**”.

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 Part 2, CC Part 3 conformant**, and to meet the requirements of **EAL 2 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” 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 Intersight Virtual Appliance with IMM Fabric and UCS Servers Security Target, Version 0.12, 10 February 2025 *[ST]* is included here by reference.

4 Definitions

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

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

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 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[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+, 24-RPT-509, version 3.0, 10 March 2025.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST] Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers Security Target, Version 0.12, 10 February 2025

(This is the end of this report.)