National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cisco Email Security Appliance with AsyncOS 15.5

Report Number: CCEVS-VR-VID11420-2024
Dated: September 13, 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

Daniel Faigin

The Aerospace Corporation

Farid Ahmed

Michael Smeltzer

Russ Fink

Robert Wojcik

Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Nil Folquer

Joon Sim

Kevin Steiner

Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Email Security Appliance with AsyncOS 15.5 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 Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, 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 Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.2e.

The TOE is the Cisco Email Security Appliance with AsyncOS 15.5. 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 Email Security Appliance Security Target*, Version 1.0, September 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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
Evaluated Product	Cisco Email Security Appliance with AsyncOS 15.5
Sponsor and Developer	Cisco Systems, Inc.
CCTL	Lightship Security USA 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e
ST	Cisco Email Security Appliance Security Target, Version 1.0, September 2024
Evaluation Technical Report	Cisco Email Security Appliance Evaluation Technical Report, Version 0.4, September 2024
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Nil Folquer, Joon Sim, Kevin Steiner
CCEVS Validators	Aerospace: Daniel Faigin Johns Hopkins APL: Farid Ahmed, Michael Smeltzer, Russ Fink, Robert Wojcik

3. Architectural Information

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

The TOE, which consists of the Cisco Email Security Appliance, is a network device.

3.1. TOE Evaluated Configuration

The TOE consists of one or more appliances as specified in section 3.2 Physical Boundary below, and includes the ESA AsyncOS software version 15.5.

In addition, if the TOE is to be remotely administered, then the management workstation must be connected to an internal network, SSHv2 must be used to remotely connect to the appliance for the CLI interface and HTTPS/TLS for the GUI interface.

A syslog server is used to store audit records, and the connection is secured using SCP over SSHv2. It is recommended that these servers be installed on the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic, in a controlled environment where implementation of security policies can be enforced.

3.2. Physical Boundary

The TOE is a hardware and software solution that makes up the Cisco ESA. The TOE hardware includes the following: C195, C395, C695, C695F and the C100v, C300v, C600v running on Cisco UCS servers. The TOE software is the ESA AsyncOS software version 15.5.

The network, on which they reside, is considered part of the environment.

The TOE comprises the following physical specifications as described in the following table.

Table 2: Hardware Models and Specifications

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
C195 Intel Xeon Silver 4110 (Skylake) processor		1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)	One 770W Redundant power supply	Two 1-GB Base-T Ethernet LAN ports, can be used as management ports RAID mirroring 10/100/1000 Mbps

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
ESA AsyncOS software version 15.5				Two 600-GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives One- 16GB DDR4-2133 DIMM1
C395 Intel Xeon Silver 4116 (Skylake) processor ESA AsyncOS software version 15.5		1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)	Two 770W Redundant power supply	Six 1-Gb Base-T Ethernet LAN ports One management interface (RJ-45), restricted to management use only RAID mirroring 10/100/1000 Two 600 GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives One- 16GB DDR4-2133 DIMM1
C695 Intel Xeon Gold 6126 (Skylake) processor ESA AsyncOS software version 15.5		1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)	Two 770W Redundant power supply	Six 1-GB Base-T Ethernet LAN ports, can be used as management ports RAID mirroring 10/100/1000 Mbps Eight 600-GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
				Two- 16GB DDR4-2666 DIMM1
C695F Intel Xeon Gold 6126 processor (Skylake) ESA AsyncOS software version 15.5		1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)	Two 770W Redundant power supply	Six 1-GB Base-T Ethernet LAN ports, can be used as management ports RAID mirroring 10/100/1000 Mbps Eight 600-GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives Two- 16GB DDR4-2666 DIMM1
C100v, C300v and C600v– installed on UCS-C220-M5 Intel® Xeon® Gold 6248R Series processors (Skylake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine		**Height** 1.7 in. (4.32 cm) **1RU:** **Width** 16.89 in. (43.0 cm) including handles: 18.98 in. (48.2 cm) **Depth** 29.8 in. (75.6 cm) including handles: 30.98 in. (78.7 cm	Up to two of the following hot-swappable power supplies: 770 W (AC) 1050 W (AC) 1050 W (DC) 1600 W (AC) 1050ELV (AC)	**Rear panel** • One 1-GbaseT RJ-45 management port (Marvell 88E6176) • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard) • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
ESA AsyncOS software version 15.5				**Front panel** • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector) **Modular LAN on Motherboard (mLOM) slot** The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards: Cisco Virtual Interface Cards Quad Port Intel i350 1GbE RJ45 Network Interface Card (NIC)
C100v, C300v and C600v– installed on UCS-C240-M5 Intel® Xeon® Gold 6248R Series processors (Skylake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine ESA AsyncOS software version 15.5		**Height** 3.43 in. (8.70 cm) **Width** (including slam latches) 17.65 in. (44.8 cm) Including handles: 18.96 in (48.2 cm) **Depth** 29.0 in. (73.8 cm) Including handles: 30.18 in (76.6 cm)	Up to two of the following hot-swappable power supplies: 1050 W (AC) power supply 1050 W V2 (DC) power supply 1600 W (AC) power supply	Rear panel • One 1-Gbps RJ-45 management port (Marvell 88E6176) • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard) • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards Front panel • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232)

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
				Modular LAN on Motherboard (mLOM) slot The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards: Cisco Virtual Interface Cards Quad Port Intel i350 1GbE RJ45 mLOM Network Interface Card (NIC)
C100v, C300v and C600v– installed on UCS-C480-M5 Intel® Xeon® Gold 6248R Series processors (Skylake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine ESA AsyncOS software version 15.5		**Height** 6.9 in. (176 mm) **Width** 19.0 in. (483 mm) **Length** (including front handles and power supplies) 32.7 in. (830 mm)	Power supplies are hot-swappable and rear-accessible. They default to redundant as 2+2 (or 1+1 for servers with only two power supplies	**Front Panel** Drive bay module 1 (drive bays 1 – 8) • Bays 3, 4, 5, 6 support SAS/SATA drives only • Bays 1, 2, 7, 8 support SAS/SATA or NVMe drives Drive bay module 2 (drive bays 9 – 16) • Bays 11, 12, 13, 14 support SAS/SATA drives only • Bays 9, 10, 15, 16 support SAS/SATA or NVMe drives Drive bay module 3 supports either • Optional DVD drive module, or • Bays 19, 20, 21, 22 support SAS/SATA drives only • Bays 18, 18, 23, 24 support SAS/SATA or NVMe drives KVM console connector (used with a KVM cable that provides two USBs, one VGA, and one serial connector)1 CPU module bay 1, the system must have at least one CPU module in bay 1 to boot. It must also have either a CPU module or a blank filler module in bay 2. CPU module bay 2, If no CPU module is present in bay 2, there must be a

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
				blank filler module in bay 2 for the system to boot **Rear Panel** Serial Port (DB-9 connector) VGA Video Port (DB-15 connector) 10 Gb Ethernet ports 10/100/1000 Ethernet dedicated management port USB 3.0 ports (three) Power supplies 1-4 PCIe slots 1-12
C100v, C300v and C600v– installed on UCS-220-M6 Intel® Xeon Gold 6342 Series processors (Ice Lake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine ESA AsyncOS software version 15.5		**2RU:** **Height** 3.42 in. (8.7 cm) **Width** 16.9 in. (42.9 cm) including slam latches: 18.9 in. (48.0 cm) **Depth** 30 in. (76.2 cm)	Up to two of the following hot-swappable power supplies: 1050 W (AC) 1050 W (DC) 1600 W (AC) 2300 W (AC)	**Rear panel** • One 1-GbaseT RJ-45 management port • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard) • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards **Front panel** • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB-15 video connector, and one serial port (RS232) RJ45 connector)

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
				Modular LAN on Motherboard (mLOM) slot The dedicated mLOM slot on the motherboard can flexibly accommodate the following card: Cisco Virtual Interface Cards
C100v, C300v and C600v– installed on UCS-C240-M6 Intel® Xeon Platinum 8360Y Series processors (Ice Lake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine ESA AsyncOS software version 15.5		**2RU:** **Height** 3.42 in. (8.7 cm) **Width** 16.9 in. (42.9 cm) including slam latches: 18.9 in. (48.0 cm) **Depth** 30 in. (76.2 cm)	Up to two of the following hot-swappable power supplies: 1050 W (AC) 1050 W (DC) 1600 W (AC) 2300 W (AC)	**Rear panel** • One 1-GB management port • One 1-GB and one 10-GB auto-negotiating Ethernet ports • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards **Front panel** • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB-15 video connector, and one serial port (DB-9) RJ45 connector) **Modular LAN on Motherboard (mLOM) slot** The dedicated mLOM slot on the motherboard can flexibly accommodate the following card: Cisco Virtual Interface Cards

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All the following environment components are supported by all TOE evaluated configurations.

Table 3: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration using the CLI interface through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration using the web GUI interface through HTTPS/TLS protected channels. Any web browser that supports TLSv1.1 and TLSv1.2 with the supported ciphersuites may be used.
Local Console	Yes	This includes any IT Environment console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
SMTP Server	Yes	This includes any SMTP servers that the TOE receives and sends email traffic. This functionality was not evaluated.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit audit log messages using SCP over a secure SSHv2 trusted channel.
CA Server	Yes	This includes any IT Environment CA Server to validate X509 certificates
Update Server	Yes	This includes updates for the potentially malicious files of various types to filter traffic for restricted content. This functionality was not evaluated.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1.1. Security Audit

The Cisco Email Security Appliance provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

Auditable events include:

- failure on invoking cryptographic functionality such as establishment, termination and failure of cryptographic session establishments and connections;
- modifications to the group of users that are part of the Authorized Administrator roles;
- all use of the user identification mechanism;
- any use of the authentication mechanism;
- Administrator lockout due to excessive authentication failures;
- any change in the configuration of the TOE;
- changes to time;
- initiation of TOE update;
- indication of completion of TSF self-test;
- maximum sessions being exceeded;
- termination of a remote session;
- attempts to unlock a termination session and
- initiation and termination of a trusted channel

The TOE is configured to transmit its audit messages to an SCP server on a remote syslog server. Communication with the syslog server is protected using SCP over SSHv2, and the TOE can determine when communication with the syslog server fails. If the connection fails, the session will need to be reestablished following the configuration settings described in the Cisco Email Security Appliance (ESA) Common Criteria Configuration Guide document.

The audit logs can be viewed on the TOE using the appropriate CLI commands and GUI webpages. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the Authorized Administrator to clear audit data stored locally on the TOE.

4.1.2. Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates, based on ESA on the platforms and processors as noted in section 3.1.

The TOE provides cryptography in support of other Cisco ESA security functionality. The ESA software calls the Cisco FIPS Object Module (FOM) v7.3a that has been validated in accordance with the specified standards to meet the requirements listed below and all the algorithms claimed have CAVP certificates.

Refer to the table below for algorithm certificate references.

Table 4: Claimed Certificates

CPU Family	CPU Model (Microarchitecture)	FOM Version	Physical Appliances/Platform	CAVP Certificate
Intel Xeon Scalable	Intel Xeon Silver 4110 (Skylake)	CiscoSSL FOM 7.3a	C195	A4446
Intel Xeon Scalable	Intel Xeon Silver 4116 (Skylake)	CiscoSSL FOM 7.3a	C395	A4446
Intel Xeon Scalable	Intel Xeon Gold 6126 (Skylake)	CiscoSSL FOM 7.3a	C695, C695F	A4446
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Skylake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C220-M5	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Skylake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C240-M5	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Skylake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C480-M5	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Icelake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C220-M6	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Icelake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C240-M6	A4595

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
AES	Used for symmetric encryption/decryption	CBC (128, 256) CTR (128, 256) GCM (128, 256)	A4446 A4595	CiscoSSL FOM 7.3a	FCS_COP.1/DataEncryption

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
SHS (SHA-1, SHA-256, SHA-384 and SHA-512)	Cryptographic hashing services	Byte Oriented	A4446 A4595	CiscoSSL FOM 7.3a	FCS_COP.1//Hash
HMAC SHA-1 HMAC SHA-256	Keyed hashing services and software integrity test	Byte Oriented	A4446 A4595	CiscoSSL FOM 7.3a	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with NIST SP 800-90A	CTR_DRBG (AES 256)	A4446 A4595	CiscoSSL FOM 7.3a	FCS_RBG_EXT.1
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation, PKCS#1 v.1.5, 2048 bit key,	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen
CVL – KAS-ECC	Key Agreement	NIST Special Publication 800-56A	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.2
CVL SSH/TLS	Key Agreement	NIST Special Publication 800-56A	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.2

The TOE provides cryptography in support of remote administrative management via SSHv2 for the CLI and HTTPS/TLS for the GUI. SCP over SSHv2 is used to secure the transmission of audit records to the SCP server on the remote syslog server. In addition, the TOE uses the X.509v3 certificate for securing the TLS connections.

The TOE also authenticates software updates to the TOE using a published hash.

4.1.3. Identification and authentication

The TOE provides authentication services for administrative users connecting to the TOE's secure CLI and GUI administrative interfaces, using SSHv2 and HTTPS/TLS, respectively, to secure the connections. Prior to an administrator logging in, a login banner is presented at both the CLI and GUI interfaces. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to the TOE and any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as character complexity rules.

The TOE also provides an automatic lockout when a user attempts to authenticate but enters invalid information. When the threshold for a defined number of authentication attempt failures has exceeded the configured allowable attempts, the user is locked out until an Authorized Administrator can re-enable the user account.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

4.1.4. 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 HTTPS/TLS (GUI interface), SSHv2 (CLI interface) session or via a direct local console connection. The TOE provides the ability to securely manage:

- ability to administer the TOE locally and remotely
- ability to configure the access banner
- ability to configure the session inactivity time before session termination or locking
- ability to update the TOE, and to verify the updates using published hash prior to installing those updates
- ability to configure the authentication failure parameters
- ability to configure the cryptographic functionality
- ability to re-enable an administrator account
- ability to configure the audit behavior
- ability to set the time

The CLI is the main interface used to administer the TOE, since all functionality to configure, securely manage and to monitor the TOE is available via the CLI. The GUI can also be used, but not all functionality to configure the TOE is available in the GUI. Therefore, in the evaluated configuration it is recommended to use the CLI to perform all configuration and setting of the security functions and to securely mange the TOE.

The TOE supports the security administrator role and is referred to as the Authorized Administrator. Only the Authorized Administrator can perform the above security relevant management functions.

Authorized Administrators can create configurable login banners to be displayed at time of login and can define an inactivity timeout threshold for each admin interface to terminate sessions after a set period of inactivity has been reached.

4.1.5. 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 AsyncOS is not a general-purpose operating system, and access to Cisco AsyncOS memory space is restricted to only Cisco AsyncOS functions.

The TOE performs testing to verify correct operation of the TOE itself and of the cryptographic module.

The TOE internally maintains the date and time. This date and time are used as the timestamp applied to audit records generated by the TOE. The TOE provides the Authorized Administrators the capability to update the TOE's clock manually to maintain a reliable timestamp.

Finally, the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

4.1.6. 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 be successfully re-identified and re-authenticated to establish a new session. Sessions can also be terminated if an Authorized Administrator enters the "exit" command.

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

4.1.7. Trusted path/Channels

The TOE allows trusted path to be established to itself from remote administrators over SSHv2 for the CLI and HTTPS/TLS for the GUI. The TOE also uses SCP over SSHv2 to push the audit logs to a SCP server on a remote syslog server.

5. Assumptions

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

- *collaborative Protection Profile for Network Devices, Version 2.2e*

That information has not been reproduced here and CPP_ND_V2.2E should be consulted if there is interest in that material.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2E as described for this TOE in the Security Target. 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 clarifying. 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 in accordance with the assurance activities specified in the CPP_ND_V2.2E and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- 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 CPP_ND_V2.2E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Cisco Email Security Appliance running AsyncOS 15.5 Common Criteria Operational User Guidance And Preparative Procedures,* Version 1.0, September 12, 2024

Additional guidance documentation includes the following:

- User Guide for AsyncOS 15.5.2 for Cisco Secure Email Gateway - MD (Maintenance Deployment), first published August 19, 2024
- CLI Reference Guide for AsyncOS 15.5.2 for Cisco Secure Email Gateway - MD (Maintenance Deployment), first published August 19, 2024
- Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide, published April 30, 2024
- Cisco Email Security Appliance C195, C395, C695, and C695F Hardware Installation Guide, last modified January 23, 2023
- Best Practice Guide for Anti-Spam, Anti-Virus, Graymail and Outbreak Filters, updated January 9, 2020

All documentation delivered with the product is relevant to and within the scope of the TOE.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Cisco Email Security Appliance NDcPPv2.2E Detailed Test Report*, which is not publicly available. The *Cisco Email Security Appliance Assurance Activity Report*, Version 1.0, September 2024 provides an overview of testing and the prescribed assurance activities.

8.1. Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA lab in Baltimore, MD from November 2023 through July 2024. Remote observation testing was performed and attended by the vendor, evaluation team, validation team and NIAP CCEVS in June 2024. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.3. Test Configuration

The TOE testing environment components are identified in the following tables.

Table 5: Devices in the Testing Environment

Name / HW / SW	Description / Functions	Test Tools
C395 HW: Intel Xeon Silver 4116 (Skylake) processor SW: ESA AsyncOS software version 15.5	Fully tested TOE model TLS SSH	N/A
C100V HW: Intel® Xeon® Gold 6248R Series processors (Skylake), with VMware ESXi 7.0 Hypervisor, with a	Fully tested TOE model TLS SSH	N/A

Name / HW / SW	Description / Functions	Test Tools
single Guest Virtual Machine SW: ESA AsyncOS software version 15.5		
Services VM HW: Test Hypervisor SW: Debian 4.19.289-2	Logging Server (SSH) DNS Server	syslog-ng 3.19.1 dnsmasq 2.80
GL VM HW: Test Hypervisor SW: Kali 6.6.9-1kali1	TLS Server TLS Client SSH Server SSH Client	Greenlight 3.0.53 OpenSSL 3.0.8 OpenSSH 9.6p1 Wireshark 3.4.4
Management Workstation HW: Lenovo ThinkPad SW: Windows 10	Remote system to access the TOE/TOE environment. SSH Client (SSH) HTTPS/Browser Client (TLS)	OpenSSH for Windows 8.1p1 Google Chrome 108.0.5359.125 Wireshark 3.6.5
Test Hypervisor HW: Dell PowerEdge R440 SW: ESXi, 7.0.3	Hypervisor for the Services VM and Management Workstation	None
Netgear Switch HW: ProSafe Plus GS105E	Physical disconnect packet captures	N/A

Table 6: Tools Used for Testing

Tool name	Version	Description
Lightship Greenlight	3.0.53	Tool used for SSH, TLS and X509 testing
OpenSSL	3.0.8	OpenSSL was used for simple TLS server or TLS client connections and as an OCSP responder

Tool name	Version	Description
OpenSSH	9.6.p1	SSH client and server for FCS_SSHS_EXT and FCS_SSHC_EXT testing
Wireshark	3.4.4 (Linux) & 3.6.5 (Windows)	Used for packet capture and analysis
Apache	2.4.46	Web server for hosting CRLs
Google Chrome	108.0.5359.125	Access TOE GUI

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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined the Cisco Email Security Appliance with AsyncOS 15.5 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in CPP_ND_V2.2E.

9.1. Evaluation of 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 Email Security Appliance with AsyncOS 15.5 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 Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CPP_ND_V2.2E related to the examination of the information contained in the TSS.

The Validation 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 Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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 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 CPP_ND_V2.2E 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 in the *Cisco Email Security Appliance Vulnerability Assessment*, Version 0.2, September 2024, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on August 19, 2024, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures:
    - http://cve.mitre.org/cve/
    - https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: http://www.zerodayinitiative.com/advisories

- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
- Cisco Security Advisory: https://sec.cloudapps.cisco.com/security/center/publicationListing.x#~FilterByProduct

The Evaluation team performed a search using the following keywords:

- Cisco C195
- Cisco C395
- Cisco C695
- Cisco C695F
- Cisco C100v
- Cisco C300v
- Cisco C600v
- UCS-C220-M5
- UCS-C220-M6
- UCS-C240-M5
- UCS-C480-M5
- UCS-C240-M6
- Cisco ESA
- Cisco Email Security Appliance
- Cisco AsyncOS
- Intel Xeon Gold 6126
- Intel Xeon Gold 6342
- Intel Xeon Silver 4116
- Intel Xeon Silver 4110
- Intel Xeon Gold 6248r
- Intel Xeon Platinum 8360Y
- OpenSSH
- CiscoSSL FOM
- OpenSSL
- FreeBSD
- CiscoSSH

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 test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM and performed the Assurance Activities in the CPP_ND_V2.2E and correctly verified that the product meets the claims in the ST.

10. Validator Comments

As indicated in Section 6, the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. 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 be relied upon when configuring or operating the device as evaluated.

11. Annexes

Not applicable.

12. Security Target

Cisco Email Security Appliance Common Criteria Security Target, Version 1.0, September 2024.

13. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020*
6. *Evaluation Activities for Network Device cPP, December-2019, Version 2.2*
7. *Cisco Email Security Appliance Common Criteria Security Target*, Version 1.0, September 2024
8. *Cisco Email Security Appliance running AsyncOS 15.5 Common Criteria Operational User Guidance And Preparative Procedures*, Version 1.0, September 2024
9. *Cisco Email Security Appliance Assurance Activity Report*, Version 1.0, September 2024
10. *Cisco Email Security Appliance Vulnerability Assessment*, Version 0.2, September 2024
11. *Cisco Email Security Appliance Evaluation Technical Report*, Version 0.4, September 2024
12. *Cisco Email Security Appliance NDcPPv2.2E Detailed Test Report*, Version 0.4, September 2024
13. *Cisco Email Security Appliance NDcPPv2.2E Test Results*, Version 0.4, September 2024