Cisco Email Security Appliance running AsyncOS 13.0

Common Criteria Operational User Guidance And Preparative Procedures

Version 1.1

29 July 2021

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Content

List of Tables

Acronyms

The following acronyms and abbreviations are common and may be used in this document:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
CSR	Certificate Signing Request
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
NDcPP	collaborative Network Device Protection Profile
NTP	Network Time Protocol
OS	Operating System
POST	Power On Self Test
PP	Protection Profile
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SCP	Secure Copy Protocol
SSHv2	Secure Shell (version 2)
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UCS	Unified Computing System

Terminology

The following terms are common and may be used in this document:

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Email Security Appliance (ESA) running AsyncOS 13.0. This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. Administrators of the TOE may be referred to as administrators, authorized administrators, TOE administrators, semi-privileged administrators, and privileged administrators in this document.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Email Security Appliance (ESA), running AsyncOS 13.0 TOE certified under Common Criteria. The TOE may be referenced below as the ESA or TOE.

1.1 Audience

This document is written for administrators configuring the TOE, specifically the AsyncOS 13.0 software. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use AsyncOS 13.0 software and the various operating systems on which you are running your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Cisco Email Security Appliance (ESA) Security Target (ST). This document covers all the security functional requirements specified in the ST and as summarized in Section 3 Secure Installation and Configuration of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, such as information flow polices and access control, which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the Authorized Administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining ESA operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. Section 7 Modes of Operation of this document provides information for obtaining assistance in using AsyncOS 13.0.

1.3 Document References

This document refers to several Cisco Systems documents. The documents used are shown below in Table 3 Reference Documents. Throughout this document, the guides will be referred to by the "#", such as **[1]**.

Table 3 Reference Documents

Reference number	Document Name	Link
[1]	AsyncOS 13.0 for Cisco Email Security Appliances User Guide	(General Deployment) – https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.html

Reference number	Document Name	Link
		(CLI) – https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/cli_reference_guide/b_CLI_Reference_Guide_13_0.html
[2]	Cisco Content Security Virtual Appliance Installation Guide	https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide.pdf
[3]	Cisco 170 Series Hardware Installation Guide	https://www.cisco.com/c/dam/en/us/td/docs/security/esa/hw/170Series_HW_Install.pdf
[4]	Cisco x95 Series Hardware Installation Guide	https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/hardware/x95_series/Cx95_GSG.pdf
[5]	Release Notes for AsyncOS 13.0 for Cisco Email Security Appliances	https://www.cisco.com/c/dam/en/us/td/docs/security/esa/esa13-0/ESA_13-0_Release_Notes.pdf

1.4 Supported Hardware and Software

Only the hardware and software listed in Section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The hardware is comprised of the following: C190, C195, C390, C395, C690, C690X, C695, C695F and the virtual appliances running on UCS platforms, C100v, C300v and C600v on UCS-C220-M4 and UCS-C220-M5. The software is comprised of the Cisco ESA AsyncOS software version 13.0.

1.5 Operational Environment

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 document. All the following environment components are supported by all TOE evaluated configurations.

Table 4 Required non-TOE Hardware/ Software/ Firmware

Component	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation using an Internet browser for HTTPS	This includes any IT Environment Management workstation with a Email browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any Email browser that supports TLSv1.1 and TLSv1.2 with the supported ciphersuites may be used.

Component	Usage/Purpose Description for TOE performance
Local Console	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 on the physical TOE devices. The Virtual TOE devices' local console is accessible via the underlying hypervisor console mechanism.
Hypervisor (ESXi 6.0)	VMWare ESXi 6.0 Hypervisor, with a single Guest Virtual Machine - C100v, C300v or C600v. The administrator ensures that the hypervisor has been patched with the latest fixes.
Syslog Server	The SCP server on a remote syslog audit server is used for storage of audit records that have been generated by and transmitted from the TOE using SCP over a secure SSHv2 trusted channel.

1.6 Excluded Functionality

The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices, Version 2.1 (NDcPPv2.1).

Table 5 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the TOE.	This mode of operation includes non-FIPS allowed operations.
AsyncOS API	Does not include any claimed or in-scope functionality

2. Secure Acceptance of the TOE

To ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Record the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment number for the shipment, matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also verify that the unit has the following external identification:

Table 6 Evaluated Products and their External Identification

Product Name	Model Number	External Identification
Cisco ESA	C190	Cisco C190 Email Security Appliance
	C195	Cisco C195 Email Security Appliance
	C390	Cisco C390 Email Security Appliance
	C395	Cisco C395 Email Security Appliance
	C690	Cisco C690 Email Security Appliance
	C690X	Cisco C690X Email Security Appliance
	C695	Cisco C695 Email Security Appliance
	C695F	Cisco C695F Email Security Appliance
	C100v, C300v and C600v running on the UCS-C220-M4,	Cisco UCS-C220-M4

Product Name	Model Number	External Identification
	C100v, C300v and C600v running on the UCS-C220-M5	Cisco UCS-C220-M5

The TOE ships with the correct software images installed, however this may not be the evaluated version. Software images for the listed models are available from Cisco.com at the following URL:

https://software.cisco.com/download/home/284900944/type/282975113/release/13.0.0

2.1 Obtaining Common Criteria Evaluated Software Images and Upgrades and Updates

The TOE hardware appliances come pre-installed with a manufacturing image. If the customer needs to upgrade the image, the notifications for available updates for ESA show up on the CLI/GUI of the appliances, and the administrator can choose to initiate the upgrade from right there. For the virtual appliances, administrator will download the image from Cisco.com (CCO) and the updates to image are done similarly to the hardware appliance TOE. Refer to [2] Download the Cisco Content Security Virtual Appliance Image for Online Download process.

Refer to **[1]** System Administration -> Setting Up to Obtain Upgrades and Updates for the configuration steps for your network download upgrades and updates from the Cisco servers. All upgrade images get provisioned to the Updater cloud service which the ESA/WSA reach out to. Image upgrades are saved in /data/install_bits. This directory is not directly accessible to administrators.

The end-user must confirm, once the TOE has booted, that they are indeed running the evaluated version. Using the CLI type the "version" **[1]** command to display the currently running system image filename and the system software release version.

When updates, including PSIRTs (bug fixes) to the evaluated imagine are posted, customers are notified that updates are available on both the WebUI and the CLI. There are two option available to upgrade – "download only" and "download and install". In the evaluated configuration, only the "download only" option is used. Before the download process starts, TRACE level logs need to be enabled which would enable the administrator to view the upgrade_logs and updater_logs. The update server sends the server manifest, an xml file with the published hash (secured over a HTTPS connection) for the upgrade package that is being downloaded. The ESA prints out the server manifest file for the benefit of the administrator. E.g.:

<sha384>c62a4407602207d67c7b6c7f76010d2bcd5f58c421e0c5ede9a434fab26cf257a0aa634bd08fe395c4155db819b801a4</sha384>

<path>asyncos/coeus-11-8-0-429/app/default/1</path>

<scheme>http</scheme>

<server>bglr-updates.sgg.cisco.com</server>

<server2>bglr-updates.sgg.cisco.com</server2>

Once the download is complete, the administrator can view the upgrade_logs, that is generated by the ESA. The upgrade_log contains the files that have been downloaded and allows the administrator to compare the published hash with the value that sent over the server manifest

(printed in the updated_logs). If the published hash matches, the administrator can proceed with the installation.

If there is a checksum mismatch, the update will not be installed. Attempts to perform an illegitimate update on the system will be logged into the updater_logs at **DEBUG** level. Following is a sample log entry:

Tue Jun 15 11:34:36 2021 Info: repeng SHA384 Mismatch

3. Secure Installation and Configuration

To ensure the TOE is in its evaluated configuration, the configuration settings outlined in the following sections need to be followed and applied. The evaluated configuration includes the following security features that are relevant to the secure configuration and operation of the TOE.

- Security audit – ensures that audit records are generated for the relevant events and are securely transmitted to a SCP server on a remote syslog server (secure connection is SCP over SSHv2).
- Cryptographic support – ensures cryptography support for secure communications.
- Identification and authentication – ensures a warning banner is displayed at login, that all users are successfully identified and authenticated prior to gaining access to the TOE, the users can only perform functions in which they have privileges, and terminates users after a configured period of inactivity
- Secure Management – provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session for the CLI, HTTPS/TLS session for the GUI or via a local console connection.
- Protection of the TSF - protects against interference and tampering by untrusted subjects by implementing identification, authentication, the access controls to limit configuration to Authorized Administrators and 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. TOE performs testing to verify correct operation of the TOE itself and that of the cryptographic module. Finally, the TOE maintains the date and time.
- TOE access - terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the Authorized Administrator to re-authenticate to establish a new session. The TOE can also be configured to lock the Authorized Administrator account after a specified number of failed logon attempts until an authorized administrator can enable the user account. The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.
- Trusted Path/Channel - allows trusted paths and channels to be established to itself from remote administrators over SSHv2, HTTPS/TLS and initiates outbound SSHv2 tunnels to transmit audit messages to a SCP Server on a remote syslog server.

3.1 Physical Installation

Follow the appropriate Cisco Hardware Installation Guide for your model **[3] or [4]** for hardware installation instructions. For ESA "v" models, see the Cisco Content Security Virtual Appliance

Installation Guide **[2]**, section “Set Up the Virtual Appliance” for detailed instructions for setting up the Virtual Appliance.

During installation please ensure that the TOE is installed as follows:

- The ESA must be protected from unauthorized physical modification.
- The ESA must be located within controlled access facilities, which will prevent unauthorized physical access.

3.2 Options to be chosen during the initial setup of the ESA

The Cisco ESA must be given basic configuration via direct console connection prior to being connected to any network.

The Authorized Administrator must use the System Setup Wizard for the initial setup to ensure a complete configuration. Follow the instructions in the **[1]** Cisco AsyncOS Email User Guide, chapter “Connect, Install, and Configure", section “System Setup Wizard” via the Graphical User Interface (GUI) for initial setup instructions. An authorized administrator can run the System Setup Wizard using a browser **[1]**.

The default password for the Authorized Administrator admin account must be changed during the initial setup configuration meeting the password complexity rules as described in 4.3 Password Complexity .

Note: The following changes must be made according to **[1]** in Chapter “Connect, Install, and Configure” during installation to put the ESA into its evaluated configuration. The general-purpose AsyncOS API is disabled by default and should not be enabled to continue in the Common Criteria evaluated configuration.

3.2.1 FIPS Mode

The TOE must be run in the FIPS mode of operation in the evaluated configuration. The **fipsconfig** command automatically configures the FIPS approved algorithms and key sizes putting ESA into FIPS mode. In addition, all stored passwords and keys will be encrypted in stored configuration files and any email configuration files will be encrypted.

See chapter "Perform System Administration Tasks", section FIPS Compliance [1] for using the **fipsconfig** command. When enabling FIPS mode, the Authorized Administrator must select '**y**' for the 'Do you want to enable encryption to sensitive data in configuration file when FIPS mode is enabled?' This will encrypt all stored passwords and keys. In the evaluated configuration, all passwords and keys must not be stored in plaintext or be readable.

3.2.2 Securing Passwords and Keys

In setting FIPS mode, the Authorized Administrator selected '**y**' for the 'Do you want to enable encryption to sensitive data in configuration file when FIPS mode is enabled?' then all passwords and keys will be encrypted.

When the appliance is in FIPS mode, new sub-options will be displayed to the user asking whether to always save the configuration with encrypted passwords. In the CLI, the **saveconfig** command can be used to encrypt the passwords and keys. In the evaluated configuration, it is required to select **Encrypt passwords** in the **saveconfig** command dialog.

3.3 Network Protocols and Cryptographic Settings

Administrators access the TOE management functionality through the TOE Web GUI interface and can run a subset of commands via the CLI interface. The GUI is Web based and is accessed over HTTPS for remote sessions. The TOE CLI is accessed either via a directly connected console or remotely via a SSHv2 connection. In the evaluated configuration, ESA must be configured to run in FIPS mode to ensure that the Common Criteria evaluated ciphersuites and algorithms are used. Information regarding accessing the TOE CLI may be found in **[1]** Command Line Interface.

3.3.1 Disable Telnet

By default, telnet is disabled. To check that it is disabled the Authorized Administrator can go to **[1]** Chapter Command Line Interface -> Connect, Install, and Configure and Chapter Command Line Interface -> Command Line Interface to use the **interfaceconfig** command. To verify that telnet is disabled on all interfaces (Data 1, Data 2, and Management) by selecting the interface.

3.3.2 SSHv2 Configuration

SSHv2 is enabled by default. This section describes the configuration of SSHv2 for remotely accessing the TOE CLI.

The administrator must choose an SSH client which supports SSHv2 using AES and HMAC-SHA-1 algorithms as well as to ensure that diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521 are the only allowed key exchange methods used for the SSH protocol. The administrator must configure the SSH client to use these algorithms when remotely connecting to the TOE. *Noting* the SSH client only negotiates ssh-rsa during hostkey negotiation.

In configuring SSHv2, at least one of the following data integrity algorithms for transport connection is required: *hmac-sha1* and the "None" MAC algorithm is not allowed. These data integrity algorithms can be selected using the **sshconfig** command in the CLI. In addition, the diffie-hellman-group14-sha1 must be selected for the key exchange method used for SSH. SSH transport implementation must use SSH_RSA as its public key algorithm as well as AES-CBC-128, AES-CBC-256, AES-CTR-128 and AES-CTR-256 for encryption.

Authorized Administrator accessing the CLI via SSH can be authenticated using public key cryptography. This requires the user's public key to be entered onto the TOE (using the **sshconfig** > **userkey** command) and associated with the user's account. If there is no public key configured for the user, the user will instead be prompted to enter their username and password to authenticate.

For configuring SSH, the following algorithms and key sizes should be used:

- Cipher Algorithms: aes256-cbc, aes128-cbc, aes256-ctr, aes128-ctr
- MAC: hmac-sha1
- Public key authentication algorithms:
    - SSH client: ssh-rsa, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp512
    - SSH Server: rsa-sha2-256 and, rsa-sha2-512
- KEX Algorithms: diffie-hellman-group14-sha1 is supported by both the SSH server functions of the TOE, while the SSH client also supports ecdh-sha2-nistp256 and ecdh-sha2-nistp521
- Minimum server key size: 2048

During the SSH configuration, you will be prompted, "Do you want to enable host key checking? [N]>, noting the default is '**N**', not to check the host key. In the evaluated configuration, the answer is '**Y**', to enable host key checking.

To ensure a secure posture when connecting to remote hosts, the Authorized Administrator maintains a local database that associates each host name with their corresponding public key or certify the hosts using a trusted certification authority as defined in RFC 425 section 4.1.

In addition, the TOE enforces SSH rekey after one hour and/or after 1GB of data.

3.3.3 TLS Configuration

When ESA is configured for FIPS mode, the below TLS ciphersuites are enforced by default.

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246

Using the CLI interface issue the command **sslconfig** configure the SSL settings. Following is an example of the command and various settings:

```
sslconfig settings:
  GUI HTTPS method:  tlsv1_1 tlsv1_2[1]
  GUI HTTPS ciphers:
      AES128
      AES256
      !SRP
      !AESGCM+DH+aRSA
      !AESGCM+RSA
      !aNULL
```

In addition, when using the **SSLCONFIG** to configure the TLS, you will be promoted, '*Would you like to Enable/Disable TLS Renegotiation for GUI HTTPS?<Y>'*, noting the default is '**Y**' to enable renegotiation. To ensure a secure posture and enhance CPU usage, in the evaluated configuration the answer is '**N**' which will disable TLS Renegotiation for GUI HTTPS.

The default cipher is set as follows:

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

To limit the ciphers to those listed above, edit the default list by adding **!** preceding the ciphers not allowed and then adding the ciphers that are allowed to the list using the **SSLCONFIG**

[1] Noting, TLSv1.0 is not allowed in the evaluated configuration and should not be entered/selected

command **[1] The Commands: Reference Examples -> Networking Configuration / Network Tools**. Following is the cipher set that is allowed in the evaluated configuration:

AES128-SHA:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256

RSA 2048 -is being used for key exchange and authentication there are no specific parameters associated with the server key exchange. Using the above TLS_RSA and TLS_ DHE_RSA ciphers the RSA public key is used for authentication and key exchange.

In the event that the validity of a peer certificate cannot be determined, then ESA does not accept the certificate. There is no action required by the administrator.

3.3.4 Obtaining X.509 Certificates

To use TLS, the TOE must have an X.509v3 certificate and matching private key for securing traffic flowing to and from the TOE. An Authorized Administrator may acquire certificates and private keys from a recognized certificate authority service. A certificate authority is a third-party organization or company that issues digital certificates used to verify identity and distributes public keys. This provides an additional level of assurance that the certificate is issued by a valid and trusted identity. Cisco does not recommend one service over another.

The TOE can generate a Certificate Signing Request (CSR) to submit to a certificate authority to obtain the public certificate. The certificate authority will return a trusted public certificate signed by a private key. Use the **certconfig** command in the CLI to generate the CSR and install the trusted public certificate.

If acquiring or creating a certificate for the first time, search the Internet for “certificate authority services SSL Server Certificates,” and choose the service that best meets the needs of your organization. Follow the service’s instructions for obtaining a certificate.

An Authorized Administrator can view the entire list of certificates in the CLI by using the **print** command after the Authorized Administrator configures the certificates using **certconfig** command **[1]**. Note, that the print command does not display intermediate certificates. See **[1]** section "Working With Certificates" for more detailed information.

When the Authorized Administrator is creating CSR, the subject should include the Name, country (optional), organization name, common name, and email address. When generating a new key, make sure 2048 bit is set for key size. For the Extensions, in the Basic constraints section, choose Certificate Authority for the Type. Note, Subsequent Certificate Signing Requests (CSRs) can be signed via this CA with the Type set to **Not Defined**. Add a Subject Alternative Name (SAN) for the Domain Name System (DNS).

There is no additional config/input to designate a CA as a trusted anchor. ESA implicitly validates it using the chain of certificates that it receive from the user.

3.3.5 Installing the Certificate from a Certification Authority

Step 1 The X.509v3 certificate must be received in PEM format before uploading to ESA.

Step 2 Navigate to the Network > Certificates page

Step 3 Click the name of the certificate that you sent to the Certification Authority for signing.

Step 4 Enter the path to the file on your local machine.

3.3.6 Enabling a Certificate for HTTPS

An Authorized Administrator can enable a certificate for HTTPS services on an IP interface using the **interfaceconfig** command in the CLI.

In the event that the validity of a peer certificate cannot be determined, then the TOE accepts the certificate based on the last known state. There is no action required by the administrator.

3.3.7 Administration of Cryptographic Self-Tests

The TOE provides self-tests consistent with the FIPS 140-2 requirements. These self-tests for the cryptographic functions in the TOE are run automatically during power-on as part of the POST. These self-tests include the following:

- AES Known Answer Test
- RSA Signature Known Answer Test (both signature/verification)
- RNG/DRBG Known Answer Test
- HMAC Known Answer Test
- SHA-1/256/512 Known Answer Test
- Software Integrity Test

During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). Also, during the initialization and self-tests, the module inhibits all access to the cryptographic algorithms.

Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing self-tests and entering FIPS mode. In the event of a power-on self-test failure, the cryptographic module will force the WAS platform to reload and reinitialize the operating system and cryptographic module. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful.

The tests include:

- AES Known Answer Test –

For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.

- RSA Signature Known Answer Test (both signature/verification) –

This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.

- RNG/DRBG Known Answer Test –

For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.

- HMAC Known Answer Test –

For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.

- SHA-1/256/512 Known Answer Test –

For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly.

- Software Integrity Test –

The Software Self-Integrity Test is run automatically whenever the ESA system images are loaded and confirms through use of digital signature verification that the image file that is about to be loaded was properly signed and has maintained its integrity since being signed. The system image is digitally signed by Cisco prior to being made available for download from CCO on Cisco.com website.

Prior to installing the image, the Authorized Administrator can verify the public hash to ensure the files has not been tampered with prior to installing. In addition, the Software Integrity Test is run automatically whenever the WAS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity.

If any self-tests fail, the TOE transitions into an error state. In the error state, all secure data transmission is halted and the TOE outputs status information indicating the failure.

If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated. Following is an example:

> Example Error Message _FIPS-2-SELF_TEST_WAS_FAILURE: "WAS crypto FIPS self test failed at %s."
>
> Explanation FIPS self test on WAS crypto routine failed.

These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behavior will be identified by the failure of a self-test.

If any of the POST fail, the following actions should be taken:

- If possible, review the crashinfo file. This will provide additional information on the cause of the crash
- Restart the TOE to perform POST and determine if normal operation can be resumed

- If the problem persists, contact Cisco Technical Assistance via http://www.cisco.com/techsupport or 1 800 553-2447
- If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance.

3.3.7.1 Key Zeroization

Although key zeroization is handled by the cryptographic module, a wipe command is available to ensure that the keys are zeroized within the old core dump files. As part of the reload command, an option to wipe the data is provided. The wipe option along with the **wipedata** command will overwrite the hard drive with zeros so that the keys are zeroized within the old core dump files.

WipeData (cli->**wipedata**) is a new command that will currently provide two options ("coredump" & "status"). **Coredump** will wipe the core dump files, status will display running, successful or unsuccessful for the last run of the command.

3.4 Logging Configuration

The TOE maintains audit records related to security-relevant operations of the TOE. The Authorized Administrators can access all audit information. The Authorized Administrators can manually download the log files by clicking a link to the log directory on the Log Subscriptions page, then clicking the log file to access.

Depending on the browser as described in the ESA User Guide, an Authorized Administrator can view the file in a browser window, open or save it as a text file. This method uses the HTTP(S) protocol and is the default retrieval method.

It is recommended the Authorized Administrator uses the CLI and associated commands for configuration, changing parameters, loading certificates and setting limits since the UI interface does not provide the necessary level of auditing in the evaluated configuration. Refer to **[1]**, The Commands: Reference Examples.

Information regarding the use of this management functionality, including secure usage guidelines, can be found in chapter "Logging" of **[1]**.

In the evaluated configuration, the log files must be backed up to a SCP server on a remote syslog server. SCP Push must be configured to transfer the audit log files to the SCP server on a remote syslog server using SCP over SSHv2 to ensure the session is secured. See "Logging", section Log Retrieval Methods -> SCP Push **[1]**. Once the SSHv2 connection is configured between the TOE (SSH client) with the SCP server on the remote syslog server (SSH server), the Authorized Administrator can complete the configuration of the SCP server on a remote syslog server using the **logconfig** command in the CLI. This method periodically pushes log files to the SCP server on a remote syslog server using SCP over SSHv2, once the Authorized Administrator configures the SCP Push.

Next the Authorized Administrator defines a log subscription's rollover settings when creating or editing the subscription using the the **logconfig** command in the CLI. The two settings available for triggering a log file rollover are:

- A maximum file size
- A time interval

To set the interval, it can be configured by file size or time. See the "Log Subscriptions" chapter and the section Adding and Editing Log Subscriptions. For example, enter 10m if you want

AsyncOS to roll over the log file when it reaches 10 megabytes. Regarding the rollover by time, it can be customized using day, hour, minutes, and seconds. It could be backed up once a day or every hour depending on how the Authorized Administrator wants to configure the audit backup policy. In the evaluated configuration, the rollover time must be used and must be set for the shortest allotted time, so the records are as close to simultaneously being pushed to the remote syslog server.

This method requires an SSH SCP server on a remote computer using SSHv2 protocol. The subscription requires a username, SSH key, and destination directory on the SCP server on a remote syslog server. Log files are transferred based on a rollover schedule set by the Authorized Administrator.

See Logging, section Log Subscriptions **[1]**

The TOE enables many of the log types by default, most of which include all of the required auditable events. When creating the Log Subscriptions, the Authorized Administrator will be able to add or remove the log subscriptions. The log level for all log types needs to be set to **Information**. The Authorized Administrator should ensure at the least the following logs are included when configuring the Log Subscriptions:

- Using Status Logs
- Using System Logs
- Using CLI Audit Logs
- Using HTTP Logs
- Using Authentication Logs
- Using Configuration History Logs

In addition, the configuration history log consists of a configuration file with an additional section listing the name of the user, a description of where in the configuration the user made changes, and the comment the user entered when committing the change. Each time a user commits a change, a new log is created containing the configuration file after the change.

See chapter "Logging", section Log Subscriptions **[1]**.

Note that the TOE can also export various other log file's audit records to an external SCP server, but these other log files do not contain logs that satisfy the TOE's auditing requirements.

The TOE is capable of detecting when the SSH connection fails. The TOE also stores a local set of audit records on the TOE and continues to do so if the communication with the syslog server goes down. The TOE stores the audit logs locally as configured with the **logconfig** command in the CLI. The size of the local log files is set by an Authorized Administrator using the 'Rollover by File Size' configuration setting. Once the file reaches the specified size it is sent to the syslog server using SCP. These transfers can also be configured based on configured time intervals.

If the SSH connection to the SCP server on a remote syslog serve fails, the log files will remain on the TOE until the connection is restored. On the next SCP Push based on either the maximum log file size being exceeded or on the time interval, the current log file and the log files previously unsuccessfully transferred will be transferred.

In the event audit log storage is exhausted, then ESA will overwrite the oldest records in the audit trail and generate an email alert to this effect and send it to an Administrator.

4. Secure Management

4.1 Authorized Administrators

In the evaluated configuration, the administrator accounts must be created on the TOE itself. See chapter "Administering User Accounts" [1] and section Adding Local User Accounts for instructions on creating user accounts and assigning roles. ESA provides multiple pre-defined user roles with varying levels of permissions. The predefined administrative roles map to the Authorized Administrator role. The roles are privileged and semi-privileged with varying administrative access. See Table 32-1 under Working with User Accounts > User Roles of **[1]** for a detailed listing of roles and associated privileges. Below is a brief listing of administrative roles and associated access:

- "admin" default user account that has full access to all system configuration settings. Note, this account is not subject to the lock out at the local console. This is to ensure the administrators do not get totally locked out of the TOE.
- "Administrators" have full access to all system configuration settings. This Authorized Administrator account does meet the lockout criteria at the local console and when remotely connected to the TOE via the GUI (secured with HTTPS/TLS) and therefore should be used for the daily management of the TOE.
- "Operators" are restricted from creating, editing, or removing user accounts and cannot use the following commands: **resetconfig**, **upgradecheck**, **upgradeinstall**, **systemsetup** or running the System Setup Wizard.
- "Technician" can perform system upgrades, reboot the appliance, and manage key features.

4.2 Identification and Authentication

All users, Authorized Administrators of the TOE must be identified and authenticated prior to gaining access to the TOE and the security functions. Configuration of Identification and Authentication settings is restricted to the privileged administrator.

The TOE uses local authentication and authorization secured using SSHv2 for the CLI and HTTPS/TLS for the GUI.

4.3 Password Complexity

This section describes the required password complexity rules when setting the password during initial setup as well as for all subsequent administrator accounts that are created.

By default, the password can be set from 0 to 128 characters, however in the evaluated configuration the password length must be configured to enforce a minimum of 15 characters. The number that is set, is the minimum number of charters that will be required, and the upper limit value can be a range of 15 characters or greater. See chapter "Distributing Administrative Tasks", section Passphrases -> Configuring Restrictive User Account and Passphrase Settings **[1]** for instructions on setting password rules. As noted in [1], to enforce the passphrases with these characteristics, the Authorized Administrator will need to use the applicable settings on the web page.

All ESA Administrator accounts must meet the following password complexity rules:

combination of upper and lower-case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)” and must be at least 15 characters.

To further configure the password complexity rules, the Authorized Administrator can select the password cannot include any dictionary words in the System Administration -> Users page in the Local User Account & Passphrase Settings section and clicking Edit Settings **[1]**. In addition, the Authorized Administrator can also create a document (text) with a list of words and phrases that cannot be used as or within a defined password.

4.4 Adding a Login Banner

In the evaluated configuration a login banner must be created for all Authorized Administrator accounts accessing the TOE via the CLI or GUI locally and remotely. Instructions for configuring the login banner see **[1]** section Additional Security Settings for Accessing the Appliance. In the CLI, use the **adminaccessconfig** > **banner** command to create the login banner. After creating the banner, commit your changes.

4.5 Use of Administrative Session Lockout and Termination

The TOE provides the Authorized Administrator the ability to configure the number of failed login attempts before locking the account. The TOE also provides the Authorized Administrator the ability to configure the length of time that an inactive administrative session remains open. After the configured period of time, the administrative session is locked, and no further activity is allowed to until the Authorized Administrator has been successfully re-authenticated to the TOE. Lastly, the TOE also provides the capability for the Authorized Administrator to terminate their own active sessions. See **[1]** User Network Access.

4.5.1 User Lockout

User accounts must be configured to lockout after a specified number of authentication failures. This applies to consecutive failures on the TOE during a given session and is not affected by the SSH session disconnections after their default number of failures. See [1] Distributing Administrative Tasks -> Locking and Unlocking a User Account.

To set the number of failed attempts, perform the following steps:

Step 1 Choose Management Appliance > System Administration > Users.

Step 2 Scroll down to the Local User Account and Password Settings section.

Step 3 Click Edit Settings.

Step 4 Configure settings:

User account lock – this is where the Administrator can set the number from 1-60, the default is 5, though in the evaluated configuration this is required to be set 3.

The default admin account can also be used to unlock users as this account is not subject to the lockout criteria and should only be used as an emergency account and not for daily management of the TOE.

To unlock a user account, open the user account by clicking on the user name in the Users listing and click Unlock Account.

The *userconfig* command can be used to unlock a user account through the CLI as shown in the example of a locked user account ***karthi1*** below –

vm21esa0122.cs21> userconfig

Users:

1. admin - "Administrator" (admin)

2. karthi1 - "karthi1" (admin) (locked)

External authentication: Disabled

Two-Factor Authentication: Disabled

Choose the operation you want to perform:

- NEW - Create a new account.

- EDIT - Modify an account.

- DELETE - Remove an account.

- POLICY - Change passphrase and account policy settings.

- PASSPHRASE - Change the passphrase for a user.

- ROLE - Create/modify user roles.

- STATUS - Change the account status.

- EXTERNAL - Configure external authentication.

- TWOFACTORAUTH - Configure Two-Factor Authentication.

- DLPTRACKING - Configure DLP tracking privileges.

- URLTRACKING - Configure URL tracking privileges.

[]> status

Enter your Passphrase to make changes:

Enter the username or number to edit.

[]> 2

This account is locked by the administrator.

Do you want to make this account available? [N]> Y

Account karthi1 is now available.

Users:

1. admin - "Administrator" (admin)

2. karthi1 - "karthi1" (admin)

Note, it is assumed Administrators are trusted and the TOE is located in a protected area and once the TOE is configured and operational, administration is performed using the CLI and/or the GUI interfaces.

4.5.2 Inactive Session Termination

In the evaluated configuration inactivity in an active session, must trigger termination of the administrator session in the GUI and CLI after a specified time lapse. This setting is are

configurable as described in chapter Distributing Administrative Tasks ->Configuring Session Timeouts **[1]**. The inactivity timeout must be set for both the GUI and CLI.

Using the CLI interface, perform the following steps:

> The **adminaccessconfig** > **timeout** command can be used to set the inactivity for both the GUI and CLI interface. It is recommended the inactivity time period should not be more than 10 minutes.

Note, the default time lapse is 30 minutes.

4.5.3 Session Termination

In the evaluated configuration the Authorized Administrator can terminate their active sessions by clicking **logout** on the Administrators GUI webpage or typing **Exit** on the CLI.

4.6 Setting the Time

Setting the local hardware clock is restricted to the Authorized Administrator. See chapter "Perform System Administration Tasks" section System Date and Time Management **[1]** for configuring the time. The time can be set manually via the Time Zone or Time Settings page from the System Administration menu in the GUI or by using the following commands in the CLI: **settime**.

4.7 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See 2 Secure Acceptance of the TOE above in this document; specially steps 7 and 9 for the method to download and verify an image prior to running it on the TOE.

5. Security Relevant Events

ESA is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server. The details for protection of that communication are covered in 3.4 Logging Configuration.

ESA can generate many types of logs, recording varying types of information. Log files contain the records of regular activity and errors from various components of the system. A log subscription associates a log type with a name, logging level, and other constraints such as size and destination information; multiple subscriptions for the same log type are permitted.

The log type indicates what information will be recorded within the generated log such as message data, system statistics, binary, or textual data. An Authorized Administrator selects the log type when creating a log subscription. See chapter "Logging", section Log Subscriptions **[1]**.

To prevent log files on the appliance from becoming too large, AsyncOS performs a “rollover” and archives a log file when it reaches a user-specified maximum file size or time interval and creates a new file for incoming log data. Based on the retrieval method defined for the log subscription, the older log file is stored on the appliance for retrieval or delivered to an external computer. In the evaluated configuration, SCP Push must be configured see 3.4 Logging Configuration for more information.

The auditable events table below include the security relevant events that are applicable to the TOE. The table also includes general applicable events.

Deleting Audit Records, audit logs cannot directly be deleted through the administrator interfaces. To remove a log subscription, the **logconfig** command in the CLI. See chapter "Logging", section Log Subscriptions for more information **[1]**.

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited.

The local audit trail consists of the individual audit records; one audit record for each event that occurred. The audit fields in each audit event will contain at a minimum the following:

Example Audit Event:

> Sun Dec 1 21:37:18 2013 Info: PID 54414: User admin logged out from session because of inactivity timeout.
>
> Date: Dec 1
>
> Time: 21:37:18
>
> Type of event: Info

Subject identity: Available when the command is run by an authorized TOE administrator user such as “User admin”. In cases where the audit event is not associated with an authorized user, an IP address may be provided for the Non-TOE endpoint and/ or TOE.

Outcome (Success or Failure): Success may be explicitly stated with “success” or “passed” contained within the audit event or is implicit in that there is not a failure or error message. More specifically for failed logins, a “Login failed” will appear in the audit event. For successful logins, a “Login success” will appear in the associated audit event. For failed events “failure” will be denoted in the audit event. For other audit events a detailed description of the outcome may be given in lieu of an explicit success or failure.

Additional Audit Information: As described in Column 3 of Table 7 below.

As noted above, the information includes at least all of the required information. Example audit events are included in the table below.

Table 7 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents	Sample Log Record
FAU_GEN.1	Start-up of the audit functions	None.	Mon Apr 19 14:41:45 2021 Info: System is coming up.
	Shut-down of the audit functions	None.	Mon Apr 19 14:55:04 2021 Info: System is shutting down.
	Administrative login	Name of user account shall be logged if individual user accounts are required for administrators	See FIA_UIA_EXT.1 below.
	Administrative logout	Name of user account shall be logged if individual user accounts are required for administrators	See FTA_SSL.4 below.
	Changes to TSF data related to configuration changes	In addition to the information that a change occurred it shall be logged what has been changed.	See FMT_SMF.1 below.
	Generating/import of cryptographic keys	In addition to the action itself a unique key name or key reference shall be logged.	Tue Apr 20 09:03:43 2021 Info: Certificate profile is updated by user admin with name good-client-cert.com with key type rsaEncryption with serial number 01 with fingerprint DB:93:EF:CD:A8:70:ED:A7:41:B2:B1:CC:6F:0D:39:31:31:98:AA:8C

SFR	Auditable Event	Additional Audit Record Contents	Sample Log Record
	Changing of cryptographic keys	In addition to the action itself a unique key name or key reference shall be logged.	Keys cannot be changed.
	Deleting of cryptographic keys	In addition to the action itself a unique key name or key reference shall be logged.	(From system_logs after deleting a certificate.) Tue Apr 20 09:05:45 2021 Info: Certificate profile is deleted by user admin with name good-client-cert.com
	Resetting passwords	Name of related user account shall be logged.	Tue Apr 20 11:44:58 2021 Info: PID 79785: User admin performed user management action for account read : Account Passphrase Assignment Done Tue Apr 20 11:44:58 2021 Info: PID 79785: User admin performed user management action for account read : Account Updated
FAU_GEN.2	None.	None.	
FAU_STG_EXT.1	None.	None.	
FCS_CKM.1	None.	None.	
FCS_CKM.2	None.	None.	
FCS_CKM.4	None.	None.	
FCS_COP.1/DataEncryption	None.	None.	
FCS_COP.1/SigGen	None.	None.	
FCS_COP.1/Hash	None.	None.	
FCS_COP.1/KeyedHash	None.	None.	
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	Reason for failure.	HTTPS session failure: Tue Nov 26 02:56:39 2013 Info: Error in https connection from host 10.142.40.74 port 51840 - (336036069, 'error:140780E5:SSL routines:SSL23_READ:ssl handshake failure'
FCS_RBG_EXT.1	None.	None.	
FCS_SSHC_EXT.1	Failure to establish an SSH session	Reason for failure.	Thu Dec 19 04:52:19 2013 Info: An authentication attempt by the user ***** from 10.76.69.125 failed using an SSH
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.	Thu Dec 19 04:52:19 2013 Info: An authentication attempt by the user ***** from 10.76.69.125 failed using an SSH connection
FCS_TLSS_EXT.1	Failure to establish an TLS session	Reason for failure.	Tue Nov 26 02:56:39 2013 Info: Error in https connection from host 10.142.40.74 port 51840 - (336036069, 'error:140780E5:SSL routines:SSL23_READ:ssl handshake failure')

SFR	Auditable Event	Additional Audit Record Contents	Sample Log Record
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address). 2	Tue Apr 20 08:43:01 2021 Info: User "read" is locked after 5 consecutive login failures. The failed login attempt will terminate any active sessions. Last login attempt was from 10.10.7.22
FIA_PMG_EXT.1	None.	None.	
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**Successful Login from Serial Port/Console**: Wed Jan 29 10:49:28 2014 Info: The user admin successfully logged on from cuau0 **Failed Login from Serial Port/Console:** Wed Jan 29 10:51:02 2014 Info: An authentication attempt by the user ***** from cuau0 failed *(For all authentication attempts via serial/console port, there will be no IP information that will be logged.)* **Successful login from GUI:** Tue Nov 26 11:26:48 2013 Info: The user admin successfully logged on from 10.142.40.203 using an HTTPS connection. **Failed login attempt from GUI:** Tue Nov 26 11:27:12 2013 Info: An authentication attempt by the user admin from 10.142.40.203 failed.
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	See FIA_UIA_EXT.1 above.
FIA_UAU.7	None.	None.	
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure	Tue Apr 20 09:17:05 2021 Info: User admin has performed certificate related operation which has failed due to Validation Error : Certificate has already expired.
	Any addition of trust anchors in the TOE's trust store	Identification of certificates added as trust anchor in the TOE's trust store	Tue Apr 20 09:09:54 2021 Info: CA Custom list has been enabled by user admin with key type rsaEncryption with serial number 00 with fingerprint 76:F7:93:C2:B1:0E:D4:54:B8:1A:7D:8D:CE:DB:7B:6E:4C:52:84:06

[2] Origin could be an interface as well (eg. Serial console, management console, etc.) as long as it is unambiguous.

SFR	Auditable Event	Additional Audit Record Contents	Sample Log Record
	Any replacement of trust anchors in the TOE's trust store (if applicable)	Identification of certificates replaced as trust anchor in the TOE's trust store (if applicable)	Certificates cannot be replaced.
	Any removal of trust anchors in the TOE's trust store	Identification of certificates removed as trust anchor in the TOE's trust store	Mon Apr 19 15:03:17 2021 Info: CA System list has been disabled by user admin
FIA_X509_EXT.2	None.	None.	
FIA_X509_EXT.3	None.	None.	
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None	See FPT_TUD_EXT.1 below.
FMT_MTD.1/CoreData	None	None.	
FMT_MTD.1/CryptoKeys	None	None	
FMT_SMF.1	All management activities of TSF data.	None	**Examples -** **Changing lock out limits:** Tue Apr 20 08:31:34 2021 Info: PID 18893: User admin performed user management action for account admin : passphrase and account policy settings updated **Changing password:** Tue Apr 20 11:53:46 2021 Info: PID 83366: User admin entered ''; prompt was '\nOld passphrase:New Passphrase:\nPlease enter the new passphrase again:Your passphrase has been changed.\nvm21esa0023.cs21> ' **Changing TOE banner:** Tue Apr 20 08:22:58 2021 Info: PID 18893: User admin entered ''; prompt was '\nEnter or paste the banner text here.
FMT_SMR.2	None.	None.	
FPT_SKP_EXT.1	None.	None.	
FPT_APW_EXT.1	None.	None.	
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated	For discontinuous changes to time: The old and new values for the	**Manual Clock update via CLI:** Thu Dec 19 10:16:00 2013 Info: PID 16996: User admin entered 'User admin

SFR	Auditable Event	Additional Audit Record Contents	Sample Log Record
	or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	time. Origin of the attempt to change time for success and failure (e.g., IP address).	connected from remote ip 10.76.69.46 updated time from Thu Dec 19 09:46:54 2013 GMT to Thu Dec 19 15:16:00 2013 GMT **Manual update from WebUI:** Thu Dec 19 11:16:35 2013 Info: The system time was changed from Thu, 19 Dec 2013 12:46:53 to Thu, 19 Dec
FPT_TST_EXT.1	None.	None.	
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success and failure)	None.	**Accepted Update**: * Fri May 9 15:01:14 2014 Debug: Acquiring dynamic manifest from stage-updates.ironport.com:443 Fri May 9 15:01:14 2014 Debug: Sending client manifest: <?xml version="1.0" encoding="iso-8859-1"?> Fri May 9 15:01:14 2014 Debug: Network Participation: Attempting to connect to host: stage-updates.ironport.com port: 443 Fri May 9 15:01:15 2014 Debug: Network Participation: Successfully connected to host: stage-updates.ironport.com port: 443 <sha384>d696f0391f33a71685ba360cf292e922ef31f8f355 dc7dd600cfcc230baa614297a94e5fea046195b3e3762c079 a9ff5</sha384> <path>case/1.0/case/default/1391719393485731</path> <scheme>http</scheme> <server>stage-updates.ironport.com</server> <server2>stage-updates.ironport.com</server2> <display_version>3.3.1-009</display_version> <application allow_from="7d274877716b78127c33c8930de054453721 0951b93a9ad8360816c85688e5090937750718db8d4d52e5 a3ff927c8b6ec4fd696132c13fabfaef9492e655d757a1b78c 519307aa4910b20bfd20ef7797bde66755d9e14c372885ef4 a26fd1b77b4bda1f8bdcf055c55db00f94433ca955ab89c56 6dcd3f51a612e1f23ab906954b088f9cf37ffecc799f71cc9e1 af90d7a4b1dc0c26df66fe2a746dbfbd055bcad691f3422b59 a213ef24dfa5c92f8bf0a4a6044f1c7756e313d4d8a427fc6a d" name="mcafee" version="5"> **Sample Log** Fri May 9 15:01:17 2014 Info: Acquired server manifest, starting update 2 Fri May 9 15:01:17 2014 Info: Server manifest specified an update for case **Rejected update:** Fri May 9 15:08:30 2014 Debug: Network Participation: Attempting to connect to host: updater01.ibqa.sgg.cisco.com port: 443 Fri May 9 15:08:30 2014 Debug: Network

SFR	Auditable Event	Additional Audit Record Contents	Sample Log Record
			Participation: Successfully connected to host: updater01.ibqa.sgg.cisco.com port: 443 Fri May 9 15:08:30 2014 Info: The manifest was malformed. Fri May 9 15:09:30 2014 Debug: Skipping update request for "cloudmark" Fri May 9 15:09:30 2014 Debug: dlp updates disabled Fri May 9 15:09:30 2014 Debug: Skipping update request for "dlp"
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None	**When user is logged out of CLI session because of inactivity timeout:** Sun Dec 1 21:37:18 2013 Info: PID 54414: User admin logged out from session because of inactivity timeout. **Unlocking of an [local] interactive session:** See FIA_UIA_EXT.1 for sample logs for serial port/console
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	**SSH:** Tue Apr 20 08:08:05 2021 Info: CLI: User admin logged out from 10.10.7.22 because of inactivity timeout **Web UI:** Tue Apr 20 08:09:52 2021 Info: GUI: User admin logged out from session MMzPZbvy0Pos5E3wUVFY because of inactivity timeout
FTA_SSL.4	The termination of an interactive session.	None.	**When user is logged out of CLI session because of inactivity timeout:** Sun Dec 1 21:37:18 2013 Info: PID 54414: User admin logged out from session because of inactivity timeout. **When user is logged out of GUI session because of inactivity timeout:** Tue Dec 3 05:42:44 2013 Info: User admin logged out from session rVXB6Wi7TpnS4BO3tbGV because of inactivity timeout.
FTA_TAB.1	None.	None.	
FTP_ITC.1	Initiation of the trusted channel.	None.	Tue Apr 20 07:54:22 2021 Trace: authentication:debug1: Connecting to 10.10.4.22 [10.10.4.22] port 22. Tue Apr 20 07:54:22 2021 Trace: command session starting Tue Apr 20 07:54:22 2021 Trace: authentication:debug1: Connection established.

SFR	Auditable Event	Additional Audit Record Contents	Sample Log Record
	Termination of the trusted channel.	None.	Tue Apr 20 07:54:22 2021 Info: Push success for subscription authentication: Log authentication.@20210420T074416.s pushed via SCP to remote host 10.10.4.22:22 Tue Apr 20 07:54:22 2021 Trace: command session starting Tue Apr 20 07:54:22 2021 Trace: authentication:Connection closed.
	Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt	Tue Apr 20 09:32:13 2021 Critical: Log Error: Push error for subscription cli_logs: SCP failed to transfer to 10.10.4.22:22: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
FTP_TRP.1/Admin	Initiation of the trusted channel.	None.	See FIA_UIA_EXT.1 for administrative login.
	Termination of the trusted channel.		See FTA_SSL.4 for administrative logout.
	Failures of the trusted path functions.		See FIA_UIA_EXT.1 for examples.

5.1 Deleting Audit Records

The TOE provides the privileged administrator the ability to delete audit records stored within the TOE. This is done with the "**clear logging"** command **[1]** C commands -> clear logging.

5.2 Reviewing Audited Events

ESA maintains logs in multiple locations: local storage of the generated audit records and can be configured to simultaneous offload of those events to the external syslog server. For the most complete view of audited events and to view all auditable events defined in the Security Target administrators should review the various audit log on a regular basis.

Using the appropriate CLI commands and GUI pages the Authorized Administrator can review audited events. The information provided in the audit records include the date and time of the event, the type of event, subject identity that caused the event, the outcome of the event, and additional information related to the event. The types of events that are audited include, initiation and termination of a trusted channel; administrators login and logout, changes to TSF data related to configuration changes, generating and importing of, changing, or deleting of cryptographic keys, resetting passwords and initiation of TOE update.

6. Network Services and Protocols

The table below lists the network services/protocols available on the Email Security Appliance as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

Table 8 Protocols and Services

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	No restrictions.
DNS	Domain Name Service	Yes	Yes	No	n/a	No restrictions.
FTP	File Transfer Protocol	Yes	No	No	n/a	Use SCP or HTTPS instead.
HTTP	Hypertext Transfer Protocol	Yes	For copy	Yes	No	For other HTTP functions, such as “copy”, recommend using HTTPS instead,
HTTPS	Hypertext Transfer Protocol Secure	Yes	Yes	Yes	Yes	No restrictions.
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	No restrictions.
IMAP4S	Internet Message Access Protocol Secure version 4	Yes	Over TLS	No	n/a	No restrictions.
LDAP	Lightweight Directory Access Protocol	Yes	No	No	n/a	If used for authentication of TOE users, configure TLS as described in section 3.3.3 of this document.
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	No	No	n/a	If used for authentication of TOE users, configure TLS as described in section 3.3.3 of this document.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
NTP	Network Time Protocol	Yes	Yes, but is not claimed in the evaluated configuration and was not tested	No	n/a	Any configuration. Use of key-based authentication is recommended.
RADIUS	Remote Authentication Dial In User Service	Yes	No	No	n/a	If used for authentication of TOE users, secure through TLS.
SCP	Secure Copy Protocol over SSH	Yes	Yes	Yes	Yes	Configure SSH as described in section 3.3.2 of this document.
SMTP	Simple Mail Transfer Protocol	Yes	Yes	No	n/a	Recommended to use SMTPS instead.
SMTPS	SMTP over TLS	Yes	Over TLS	No	n/a	Configure TLS as described in section 3.3.3 of this document.
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	Yes	Yes	No	Outbound (traps) only. Recommended to tunnel through TLS.
SSH	Secure Shell	Yes	Yes	Yes	Yes	As described in the relevant section of this document.
SSL (not TLS)	Secure Sockets Layer	Yes	No	Yes	No	Use TLS instead.
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use SSH instead.
TLS	Transport Layer Security	Yes	Yes	Yes	Yes	Configure TLS as described in section 3.3.3 of this document
TFTP	Trivial File Transfer Protocol	Yes	No	No	n/a	Recommend using SCP or HTTPS instead.

The table above does not include the types of protocols and services listed here:

- OSI Layer 2 protocols such as CDP, VLAN protocols like 802.11q, Ethernet encapsulation protocols like PPPoE, etc. The certified configuration places no restrictions on the use of these protocols however, evaluation of these protocols was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.

- Protocol inspection engines that can be enabled with "inspect" commands because inspection engines are used for filtering traffic, not for initiating or terminating sessions, so they're not considered network 'services' or 'processes' in the context of this table. The certified configuration places no restrictions on the use protocol inspection functionality however, evaluation of this functionality was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.

7. Modes of Operation

ESA has several modes of operation, these modes are as follows:

Booting – while booting, ESA does not allow access to the administrator interfaces until the ESA image and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation.

Normal - The ESA image and configuration is loaded and ESA is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all ESA based security functions are operating while operating ESA has little interaction with the administrator.

Following operational error, the TOE reboots (once power supply is available) and enters booting mode. The only exception to this is if there is an error during the Power on Startup Test (POST) during bootup, then the TOE will shut down. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file. Within the POST, self-tests for the cryptographic operations are performed.

8. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. The following identifies the requirements and the associated security measures of the authorized users.

Table 9 Security Objective for the Operational Environment

Security Objective for the Operational Environment	Definition of the Security Objective	Responsibility of the Administrators
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	ESA must be installed to a physically secured location that only allows physical access to authorized personnel.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	None. AsyncOS is a purpose-built operating system that does not allow installation of additional software.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	Administrators will ensure protection of any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.) and ensure appropriate operational environment measures and policies are in place for all other types of traffic.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE and maintain secure communications with components of the operational environment.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must download updates, including psirts (bug fixes) to the evaluated image to ensure that the security functionality of the TOE is maintained
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must securely store and appropriately restrict access to credentials that are used to access the TOE (i.e. private keys and passwords)
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	Administrators must securely wipe the TOE of any and all sensitive information prior to removing from the operational environment.

9. Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

9.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

9.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find

information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com