Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11

Common Criteria Operational User Guidance and Preparative Procedures

Version: 2.3

Date: March 10, 2026

Americas Headquarters:

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

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

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

Table 1: Acronyms and Abbreviations

Acronym / Abbreviations	Definition
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
ESPr	Embedded Services Processors
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
NDcPP	collaborative Protection Profile for Network Devices
OS	Operating System
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association

Acronym / Abbreviations	Definition
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
ST	Security Target
TCP	Transport Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
WAN	Wide Area Network
WIC	WAN Interface Card

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.
Peer router	Another router on the network that the TOE interfaces with.
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.
Vty	vty is a term used by Cisco to describe a virtual terminal and applies to non-local connections (e.g. ssh client sessions).
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 supporting evidence of an evaluation of a specific Target of Evaluation (TOE), Cisco Aggregation Services Router 9000 (ASR9K). 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.

1 Introduction

This Common Criteria Operational User Guidance and Preparative Procedures Preparative Procedures documents the administration of the Cisco ASR 9000 Series Aggregation Services Routers running on Cisco IOS-XR 7.11 TOE (herein after referred to as ASR9K), certified under Common Criteria. The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912 and ASR-9922. The software is comprised of the IOS-XR software image Release 7.11.

1.1 Audience

This document is written for administrators configuring the TOE, specifically the IOS-XR 7.11 software. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking and understand your network topology and the protocols that the devices your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running on your network.

1.2 Purpose

This document 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 Security Target (ST). This document covers all of the security functional requirements specified in the ST and as summarized in Section 3 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 administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining ASR9K operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 Document References

This section lists the Cisco Systems documentation that is also the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 3. Where reference is made to the “Cisco ASR 9000 Series Aggregation Services Routers ” documentation, then the documentation is applicable to the ASR9K model series.

Throughout this document, the guides will be referred to by the “#”, such as **[1]**.

Table 3: Cisco Documentation

#	Title	Link
[1]	Hardware Installation Guide for Cisco Aggregation Services Router 9000	Cisco ASR 9000 Aggregation Services Router Hardware Installation Guide Cisco ASR 9000 Fixed-Port Routers Hardware Installation Guide
[2]	System Setup and Software Installation Guide for Cisco Aggregation Services Router 9000	System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers, IOS XR 7.1.X
[3]	System Security Configuration Guide for Cisco Aggregation Services Router 9000	System Security Configuration Guide for Cisco ASR 9000 Series Routers, Configure MACSec

1.4 Supported Hardware and Software

Only the following hardware and software listed in Table 4 and Table 5 are compliant with the Common Criteria evaluation. Using hardware and software not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

Table 4: Supported Hardware

Hardware	Models
Cisco Aggregation Services Router 9000 (Chassis)	ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912 and ASR-9922

Table 5: Supported Software

Software	Version
IOS XR	7.11

1.5 Operational Environment

1.5.1 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware in its environment:

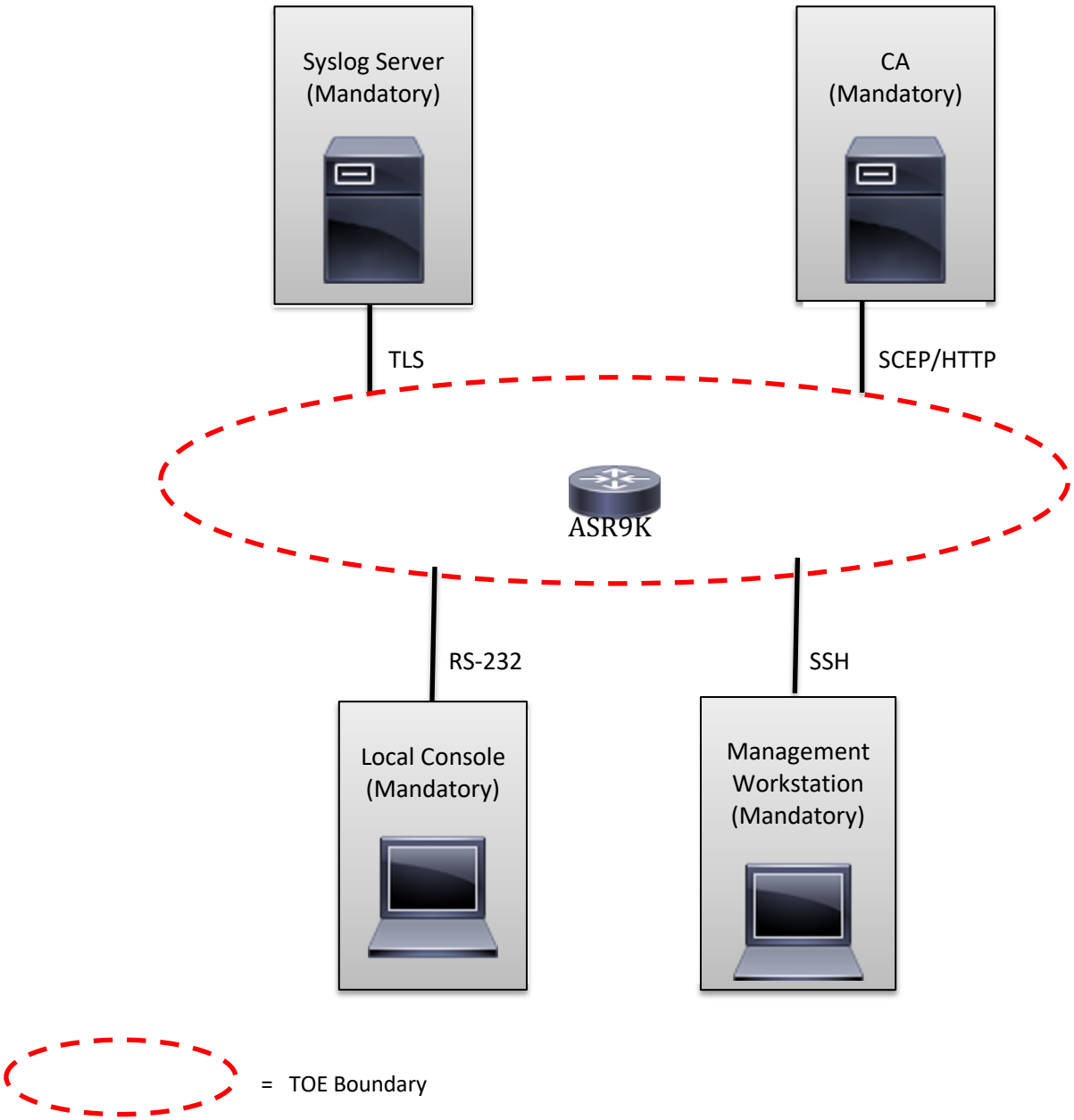
Table 6: Operational Environment Components

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 through SSH protected channels. Any SSH client that supports SSHv2 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.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST
Certificate Authority	Yes	This includes any Operational Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.

1.5.2 Example Target of Evaluation Deployment

The following figure provides a visual depiction of an example TOE deployment:

Figure 1: TOE and Environment



The previous figure includes the following:

- Examples of TOE Models
- The following are considered to be in the IT Environment:
    - Management Workstation (over SSH)
    - Audit (Syslog) Server (over TLS)
    - Local Console
    - Certificate Authority (over HTTP/SCEP)

NOTE: *While the previous figure includes several non-TOE IT environment devices, the TOE is only the ASR9K device. Only one TOE device is required for deployment in an evaluated configuration. For management purposes the TOE provides command line access to administer the TOE.*

1.6 Excluded Functionality

The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 3.0e.

Table 7: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-3 mode of operation	This mode of operation includes non-FIPS allowed operations.
MACsec	MACsec is not included in the evaluation. It must be used as specified in the AGD.
RADIUS	RADIUS is not included in the evaluation. It must be used as specified in the AGD.
TACACS+	TACACS+ is not included in the evaluation. It must remain disabled in the evaluated configuration will be disabled in the evaluated configuration.
LDAP	LDAP is not included in the evaluated configuration. LDAP (Not secure) must remain disabled in the evaluated configuration. Note that LDAP (secure) is allowed over TLS.
IPsec	IPsec was not included in the evaluated configuration. It must remain disabled in the evaluated configuration.
NTP	NTP was not included in the evaluation. It must be disabled in the evaluated configuration as specified in the AGD.

These services are disabled by configuration.

2 Secure Acceptance of the TOE

To ensure the correct TOE is received, the TOE should be examined to ensure that that 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. 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 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 Note 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 note 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). To further ensure proper and secure delivery of the TOE, the recipient must check the models received against the list of TOE component hardware models listed in Table 8, below.

Table 8: TOE External Identification

Models	Description
ASR-9006-SYS	4 slot 10RU 9006 Distributed chassis
ASR-9010-SYS	8 slot 21RU 9010 Distributed chassis
ASR-9902	2RU 9902 Distributed chassis
ASR-9903	3RU 9903 Distributed chassis
ASR-9904	2 Slot 6RU 9904 Distributed chassis
ASR-9906	4 Slot 14RU 9906 Distributed chassis
ASR-9910	8 Slot 21RU 9910 Distributed chassis
ASR-9912	10 Slot 30RU 9912 Distributed chassis
ASR-9922	22 Slot 44RU 9922 Distributed chassis
A9K-RSP5	9000 Route Processor
A99-RP3	9900 Route Processor
A9K-RSP5-X	9000 Route Processor
A99-RP3-X	9900 Route Processor
A99-RP-F	9902, 9903 Route Processor
A9K-4HG-FLEX, A99-4HG-FLEX	Cisco ASR 9000 400GE Combo Service Edge Line Card
A9K-8HG-FLEX	Cisco ASR 9000 Series 800G Service Edge Combo Line Card
A9K-20HG-FLEX	Cisco ASR 9000 Series 2T Packet Transport Combo Line Card
A99-10X400GE-X , A99-4T	Cisco ASR 9900 4T Service Edge Line Card
A99-32X100GE-X, A99-32HG	Cisco ASR 9900 3.2T Service Edge Line Card (Non-MACsec)
A9903-8HG-PEC	Cisco ASR 9903 Series 2T Port Expansion Card
A9903-20HG-PEC	Cisco ASR 9903 Series 800G Port Expansion Card

Step 7 Approved methods for obtaining the Common Criteria evaluated software image:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. The reason to download to a trusted system within your

organization, such as the management workstation, is to ensure the file has not been tampered with prior to securely copying to the TOE for installation.

- Software images are available from Cisco.com at the following:

  https://software.cisco.com/download/home

- The TOE ships with the correct software images installed, however this may not be the evaluated version.

Step 8 Once the file is downloaded, the authorized administrator verifies that it was not tampered with by either using a hash utility to verify the SHA512 published hash by comparing the SHA512 published hash that is listed on the Cisco website and in Table 9: Evaluated Software Images.

The cryptographic hashes (i.e., public hashes/SHA-512) are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to update the applicable TOE components. The hash value can be displayed by hovering over the software image name under details on the Cisco.com website. If the hashes do not match, contact Cisco Technical Assistance Center (TAC) via https://www.cisco.com/support/.

Step 9 During bootup, the administrator should confirm that the router loads the image correctly by monitoring the console output. Successful digital signature validation will produce the following:

```
Loading Kernel..
Verifying /bzImage...
/bzImage verified using attached signature.
Loading initrd..
Verifying /initrd.img...
/initrd.img verified using Pkcs7 signature.
```

Step 10 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the "**show version**" command to show the system software release version.

Table 9: Evaluated Software Images

Model	Software Version	Image Name	SHA512
ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903,	IOS XR 7.11	asr9k-mini-x64-7.11.1.iso	dce584f0aa7c71b0cbcc4baffc8ace0c5a48c4d24cbc83ce8ec31a472932cd43f8bd3e691988cf006106dbf93b78fd96153c9f552ba4062b02d1b7406ee69a88

Model	Software Version	Image Name	SHA512
ASR-9904, ASR-9906, ASR-9910, ASR-9912, ASR-9922		asr9k-sysadmin-7.11.1.CSCwm03455.tar	c792305d464b12c8d06a16681ba9556c9ed3cd1942ec36c930ad6a558b3a0f7a7e7a759cfd53e1f93dea73bcff3005b20f9d41ff467ee2ba0862f3f2303ecef8
		asr9k-x64-7.11.1.CSCwm03455.tar	5e8b47817baf715037e775ca43b03a5dba8baeae926850a475daf80e9f436b80deae97924f128d30fc60af688dcb444a68b883b432ea4871b3a1eaf7033d55a3
		asr9k-iosxr-infra-64-1.0.0.3-r7111.CSCwm88377.tar	bb2f2c34220f0cc4dcd3906b5087861b0b156ff751f893777b9bb7c724ee8aa97b5a4eaf0880008eeb0bfe3e4ec2f2affeb831043689b5c389efacc0ffe8c56b
		asr9k-iosxr-os-64-1.0.0.3-r7111.CSCwm88377.tar	57e94ddbd603a573e7945c0744ca375f4efe934f69df45c564710b29eb904474b12009248106283dff5763abcd6bc3a66e62047aa4fe1085be21609f7aaa3d93

When updates, including PSIRT (bug fixes) to the evaluated image are posted, customers are notified that updates are available (if they have purchased continuing support), information provided how to download updates and how to verify the updates is the same as described above.

2.1 Verify Package Details

Before you activate a package on the router, you can verify the type of upgrade that is required for the package and whether the package requires a router reload or not. Use the "**show install package**" command in admin mode.

```
RP/0/RSP0/CPU0: router(admin)# show install package
```

2.2 Installing and Activating Packages

NOTE that the evaluated configuration requires **both** the ISO image file and the security patch image shown in Table 9 above.

System upgrade on the ASR9K uses an ISO image file, while the patch installation uses packages and SMUs. This task is also used to install .rpm files. The .rpm file contains multiple packages and SMUs that are merged into a single file.

```
RP/0/RP0/CPU0: router# install add source <src>
RP/0/RP0/CPU0: router# show install request
RP/0/RP0/CPU0: router# show install repository
RP/0/RP0/CPU0: router# show install inactive
RP/0/RP0/CPU0: router# install activate package_name
RP/0/RP0/CPU0: router# show install active
RP/0/RP0/CPU0: router# install commit system
```

Once the packages have been activated verify that they are installed correctly, using the show install active command.

```
RP/0/RSP0/CPU0:router(admin)# show install active
```

Use the show version command to display information about the router, including image names, uptime, and other system information.

```
RP/0/RSP0/CPU0:router(admin)# show version
```

NOTE: *End-users might find that their SSH host key has been regenerated after SMU installation*.

2.3 Commit the Active Software

The active software has to be committed for it to be persistent across reloads. When a package is activated on the router, it becomes part of the current running configuration. To activate the package, enter the **install commit** command in administration EXEC mode.

The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the **show install active** command to display the currently running system image filename and the system software release version.

The bootable USB drive is used to re-image the router for the purpose of system upgrade or boot the router in case of boot failure. The bootable USB drive can be created using a compressed boot file. This is detailed in the “System Setup and Software Installation Guide” **[2].**

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 remote syslog server
- 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 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 router itself and that of the cryptographic module.
- TOE access - terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The administrator can also terminate their own session by exiting out of the CLI. The TOE can also be configured to 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 channels to be established to itself from remote administrators over SSHv2 for CLI access and with the syslog server using TLS.

3.1 Physical Installation

Follow the “Hardware Installation Guide” **[1]** for hardware installation instructions. Follow these directions for connecting all ASR9K models.

3.2 Initial Setup via Direct Console Connection

The ASR9K must be given basic configuration via console connection prior to being connected to any network. Once the hardware is installed follow the "System Setup and Software Installation Guide" for the software installation instructions. Follow these directions for connecting all ASR9K models.

3.2.1 Root username and Password

After booting, the root username and password must be created. These can then be used it to log on to the XR console. When creating the password, follow the guidance for a secure password in section 4.2.

The root system user is the entity authorized to "own" the entire router chassis. The root system user functions with the highest privileges over all router components and can monitor all secure domain routers in the system. At least one root system user account must be created during router setup. Multiple root system users can exist.

3.2.2 Boot verification

The ASR9K completes the boot process using the pre-installed operating system (OS) image. Once the boot sequence has completed to verify the version of IOS-XR use the "**show version".**

3.2.3 Management Interface

To use the management interface for system management and remote communication, you must configure an IP address and subnet mask for the management ethernet interface. To communicate with devices on other networks, you need to configure a default (static) route for ASR9K**.**

1. Enter Configuration mode, type "**configure**".

   Example:

```
RP/0/RP0/CPU0: router# configure
```

2. Enters interface configuration mode for the management interface Type "**interface mgmtEth** *rack/slot/instance/port".*

   Example:

```
RP/0/RP0/CPU0: router(config)# interface mgmtEth 0/RP0/CPU0/0
```

3. Assigns an IP address and a subnet mask to the interface. Type" **ipv4 address** *ipv4-address subnet-mask".*

   Example:

```
RP/0/RP0/CPU0: router(config-if)# ipv4 address 10.1.1.1 255.0.0.0
```

4. Places the interface in an "up" state. Type "**no shutdown".**

   Example:

```
RP/0/RP0/CPU0: router(config-if)# no shutdown
```

5. Exits the management interface configuration mode. Type "**exit".**
6. Specifies the IP address of the default gateway to configure a static route. This must be used for communication with devices on other networks. Type "**router static address-family ipv4 unicast** *0.0.0.0/0default-gateway".*

   Example:

```
RP/0/RP0/CPU0: router(config)# router static address-family ipv4 unicast
0.0.0.0/0 12.25.0.1
```

7. Use the "**commit"** command to save the configuration changes and remain in the configuration session.

3.2.4 Telnet Service

Telnet is disabled by default and in the evaluated configuration **MUST NOT** be enabled.

Telnet should not be used for management purposes as there is no protection for the data that is transmitted.

3.2.5 Disable Console Logging

Console logging **MUST** be manually disabled in the evaluated configuration in order to prevent unauthorized viewing of local audit logs.

Example:

```
RP/0/RP0/CPU0: router# config t
RP/0/RP0/CPU0: router(config)# logging console disable
RP/0/RP0/CPU0: router(config)# commit
```

3.2.6 Enabling FIPS Mode

The following package needs to be installed**.**

Table 10 Packages

Model	Package	SHA512
ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912 and ASR-9922	ASR9K-x64-iosxr-px-k9-7.11.1.tar	d72fb4583021d60aa2a7de043ed411796472eaa0213312bed4abadba4326e56d4953ff0b439e6e890e5754e4423824dae7d2f056945a38504fabeca5aee12f38

```
RP/0/RP0/CPU0: router# install add source <sftp transfer
protocol>//user@server:/package_path/ filename1 filename2>
RP/0/RP0/CPU0: router# show install request
RP/0/RP0/CPU0: router# show install repository
RP/0/RP0/CPU0: router# show install inactive
RP/0/RP0/CPU0: router# install activate package_name
RP/0/RP0/CPU0: router# show install active
RP/0/RP0/CPU0: router# install commit system
```

In the evaluated configuration, FIPS mode of operation must be enabled. By default, FIPS mode is disabled. The "**crypto fips mode**" command needs to be run in order to turn on FIPS mode. A reload is required for the system to operate in FIPS mode.

Enabling FIPS mode restricts the algorithms to ensure that only the permitted algorithms are in the evaluated configuration. The use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

To enable FIPS mode, follow the below steps:

```
RP/0/RP0/CPU0: router#  configure
RP/0/RP0/CPU0: router(config)# crypto fips-mode
RP/0/RP0/CPU0: router(config)# commit
RP/0/RP0/CPU0: router# show logging
RP/0/RP0/CPU0: router#  admin
RP/0/RP0/CPU0: router#  reload location <node-id> all
```

To disable FIPS mode, follow the below steps:

```
RP/0/RP0/CPU0: router#  configure
RP/0/RP0/CPU0: router(config)# no crypto fips-mode
```

```
RP/0/RP0/CPU0: router(config)# commit
RP/0/RP0/CPU0: router# show logging | fips
RP/0/RP0/CPU0: router#  admin
RP/0/RP0/CPU0: router#  reload location all
```

3.2.6.1 Steps to configure SSH server on the router

To establish a SSH connection to the management interface port using the ASR9K IP address, the following steps must be followed.

- Generate the crypto key for SSH using the "**crypto key generate rsa general-keys the_default**" command.
- Once the package has been installed and crypto key for SSH has been generated the SSH server needs to be enabled to only accept SSHv2 client connections. The following commands should be used:

```
RP/0/RP0/CPU0: router# configure
RP/0/RP0/CPU0: router(config)# ssh server v2
RP/0/RP0/CPU0: router(config)# commit
RP/0/RP0/CPU0: router# show ssh session details
```

Generate RSA key material – choose a longer modulus length (2048 or greater) for more secure keys (i.e. 3072 for RSA):

```
P/0/RP0/CPU0: router# configure
RP/0/RSP0/CPU0:router config)# crypto key generate rsa general-keys
the_default
RP/0/RSP0/CPU0:router# How many bits in the modulus [512]: 3072
RP/0/RP0/CPU0: router(config)# commit
RP/0/RSP0/CPU0:router#show crypto key mypubkey rsa
```

NOTE: *Only one set of keys can be configured using the* ***crypto key generate rsa general-keys the_default*** *command at a time. Repeating the command overwrites the old keys.*

RSA keys are generated in pairs—one public RSA key and one private RSA key. This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

NOTE: *If the error "% Please define a domain-name first" is received, enter the command '****ip domain-name [domain name]****'.*

3.2.6.2 Administration of Cryptographic Self-Tests

The TOE provides self-tests consistent with the FIPS 140-2 requirements. When the system is booted up in FIPS mode, the FIPS power-up self-tests run as part of the Power on Startup Test (POST) on the line card modules. These self-test include the following:

- Power-on Self-Tests:
    - Software Integrity Test
    - Noise Source Health Tests
    - Known Answer Tests:
        - AES KAT
        - RSA KAT
        - RNG/DRBG KAT
        - HMAC KAT
        - SHA-1/256/512 KAT
- Conditional Self-Tests (run periodically during normal operation):
    - Continuous Random Number Generator test for DRBG
    - Continuous Random Number Generator test for Entropy Source
    - RSA Pairwise Consistency Test
    - Bypass 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 IOS XR 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. These 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.

- 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.

- 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.

- 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.

- 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.

- Software Integrity Test - The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity.

- Noise Source Health Tests - The Noise Source Health Tests check the functioning of the Noise Source that supplies randomness to the Entropy Source. The tests are designed to detect failure of the Noise Source. These tests are run at startup and continuously during normal operation.

If any of these FIPS self-tests fail, the whole system is moved to the FIPS error state. In this state as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes.

Once the router is in the FIPS error state, any reload of a line card moves it to the failure state. To move the router back to FIPS mode, it has to be rebooted. However, once the router is in FIPS mode, any power-up self-test failure on a subsequent line card reload or

insertion affects only that line card, and only the corresponding line card is moved to the failure state.

If any of the 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.

NOTE: *If an error occurs during the self-test, a SELF_TEST_FAILED system log is generated.*

Example Error Message:

```
Error Message SECURITYD-2-FIPS_SELF_TEST_FAILED: FIPS self-test failure :
[chars]
```

Explanation FIPS self-test failed [chars] for service [chars]

3.2.6.3 Self-Tests

When the system is booted up self-tests are automatically run. The power-up self-tests run on the line cards. If any of these bootup tests fail, the whole system is moved to the error state. In this state, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes.

Once the router is in the error state, any reload of a line card moves it to the failure state. To move the router back to operational mode, it has to be rebooted. However, once the router is in operational mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state.

All ports are blocked from moving to forwarding state during the POST. Only when all components of all modules pass the POST is the system placed in an operational state and ports are allowed to forward data traffic.

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

- Use the **system cores** command to set up core dumps on the system. This will provide additional information on the cause of the crash:

```
RP/0/RP0/CPU0: router#  configure
RP/0/RP0/CPU0: router(config)# system cores slot0:core_file
```

Example:

```
RP/0/RP0/CPU0: router # system cores tftp://x.x.x.x/filename
RP/0/RP0/CPU0: router # show system cores
```

NOTE*: The filename (indicated by filename) must exist in the TFTP server directory.*

- Restart the TOE to perform POST and determine if normal operation can be resumed.

If the problem persists, contact Cisco Technical Assistance via

https://www.cisco.com/support/.

3.2.7 Session Termination

Inactivity settings must trigger termination of the administrator session. By default, console, vty, and tty sessions disconnect after 10 minutes of inactivity. Administrators are advised to maintain this value at 10 minutes or less but greater than zero. NOTE: A 0-minute value will prevent sessions from terminating.

These settings are configurable as follows:

```
RP/0/RP0/CPU0: router(config)#vty default 0 4 line-template default
RP/0/RP0/CPU0: router(config)#line default
RP/0/RP0/CPU0: router (config-line)#exec-timeout minutes seconds
RP/0/RP0/CPU0: router(config)#line console
RP/0/RP0/CPU0: router (config-line)#exec-timeout minutes seconds
RP/0/RP0/CPU0: router(config)#commit
```

3.2.8 Logout

An administrator can manually logout from the evaluated configuration either from the local console or remotely with the following command: **exit.**

3.2.9 User Lockout

User accounts must be configured to lockout after a specified number of authentication failures.

```
RP/0/RP0/CPU0: router(config)#aaa password-policy policy
RP/0/RP0/CPU0: router(config-pp)#authen-max-attempts 5
RP/0/RP0/CPU0: router(config-pp)#lockout-time minutes 1
RP/0/RP0/CPU0: router(config)#username test1
RP/0/RP0/CPU0: router(config-un)#password-policy policy password
passwordtest123
RP/0/RP0/CPU0: router(config-un)#commit
```

NOTE: *Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.*

3.3 Network Protocols and Cryptographic Settings

3.3.1 Remote Administration Protocols

Telnet for management purposes is disabled by default. IOS XR only supports SSHv2 with the following by default.

- encryption algorithms, aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, and aes256-gcm@openssh.com to ensure confidentiality of the session.
- hashing algorithms hmac-sha2-256 and hmac-sha2-512 to ensure the integrity of the session.
- SSH transport implementation public key algorithms: rsa-sha2-256 and rsa-sha2-512.
- Key Exchange Algorithms: ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521

To only allow ssh for remote administrator sessions, use the **transport input ssh** command.

```
RP/0/RP0/CPU0: router(config)#line default
RP/0/RP0/CPU0: router(config-line)#transport input ssh
RP/0/RP0/CPU0: router(config-line)#commit
```

3.3.1.1 Enter configuration mode

Enter Configuration mode, type "**configure**".

Example:

```
RP/0/RP0/CPU0: router# configure
```

3.3.1.2 SSH public-key based authentication

For IOS-XR, public keys must be provided as a binary-coded modulus. Therefore, commonly used keys suitable for OpenSSH must be transformed before they can be used with IOS-XR. Below is a method to perform this transformation on a management workstation.

First, the following steps need to be performed to convert the RSA key into a XR-friendly format–

```
1. cut -f2 -d\ < deb1.pub > test_rsa.pub
2. more test_rsa.pub
3. base64-1.5/base64 -d test_rsa.pub >! test_rsa_dec.pub [base64 is a Linux
utility]
```

```
4. cat test_rsa_dec.pub | tr -d "\n" >! test_rsa_dec_check.pub
```

The key is then imported into the TOE and copied into the harddisk: by using the following steps-

```
RP/0/RP0/CPU0: router# crypto key import authentication rsa username admin
harddisk:/id_rsa.pub-raw
RP/0/RP0/CPU0: router # show crypto key authentication rsa
```

SSHv2 is used for monitoring and for command-line interface (CLI) access. The following steps configure the TOE to use SSH for remote administration. When SSHv2 is configured using SSH server v2, only SSHv2 client connections will be accepted. If the SSH connection is unintentionally broken, SSH client will need to re-authenticate to establish the connection with the SSH server again.

To configure encryption algorithms:

```
RP/0/RSP0/CPU0: router# configure
RP/0/RP0/CPU0: router(config)#ssh server algorithms cipher aes256-cbc aes128-
cbc aes128-gcm@openssh.com aes256-gcm@openssh.com
RP/0/RP0/CPU0: router(config)#commit
```

To disable hashing algorithms:

```
RP/0/RSP0/CPU0: router# configure
RP/0/RP0/CPU0: router(config)#ssh server disable hmac hmac-sha1
RP/0/RP0/CPU0: router(config)#commit
```

NOTE: *The "none" MAC algorithm is not allowed.*

To configure host key algorithms:

```
RP/0/RSP0/CPU0: router# configure
RP/0/RP0/CPU0: router(config)#ssh server algorithms host-key rsa
RP/0/RP0/CPU0: router(config)#commit
```

To configure key-exchange algorithms:

```
RP/0/RSP0/CPU0: router# configure
RP/0/RP0/CPU0: router(config)#ssh server algorithms key-exchange ecdh-sha2-
nistp256
RP/0/RP0/CPU0: router(config)#commit
RP/0/RSP0/CPU0: router #crypto key gen rsa
RP/0/RP0/CPU0: router #config terminal
RP/0/RP0/CPU0: router (config)#ssh server vrf mgmt
RP/0/RP0/CPU0: ios(config)#commit
RP/0/RP0/CPU0: router (config)#ssh server access-list 170 permit ip 30.0.0.0
0.255.255.255 40.0.0.0 0.255.255.255
RP/0/RP0/CPU0: router (config)#ssh server logging
RP/0/RP0/CPU0: router (config)#ssh server v2
```

```
RP/0/RP0/CPU0: router (config)#commit
RP/0/RP0/CPU0: router# (config)#end
RP/0/RP0/CPU0: router# (config)#ssh timeout 60
RP/0/RP0/CPU0: router# (config)#ssh server rekey-time 60
RP/0/RP0/CPU0: router# (config)#ssh server rekey-volume 1024
```

NOTE: *The "ssh server rekey-time <minutes>" and "ssh server rekey-volume <data in megabytes>" commands configure the SSH rekey to a limit of 60 minutes and 1024MB (1 gigabyte binary) of data. Based on time the administrator will need to wait for 60 minutes before the rekey occurs. The TOE will begin re-key based upon the first threshold reached.*

3.3.2 Logging Configuration

Logging of all required audit events related to TOE security functions must be enabled. To get some of the required audit records with the required information, debugging may need to be turned on/configured. In doing so, a large amount of audit records may be generated.

```
1. RP/0/RSP0/CPU0: router# configure
2. RP/0/RSP0/CPU0: router (config)#logging trap debugging
3. RP/0/RSP0/CPU0: router (config)#logging 10.34.0.1 vrf default severity
debugging
4. RP/0/RSP0/CPU0: router (config)#logging hostnameprefix "TOE:ASR 9000"
5. RP/0/RSP0/CPU0: router (config)#service timestamps log datetime year
localtime msec
6. RP/0/RSP0/CPU0: router (config)#service timestamps debug datetime year
localtime msec
7. RP/0/RSP0/CPU0: router (config)# aaa accounting commands default start-
stop local
8. RP/0/RSP0/CPU0: router (config)#commit
9. RP/0/RSP0/CPU0: router (config)#end
```

3.3.2.1 Logging console on/off

This will turn on logging events to be sent to the console. An authorized administrator will see the audit events display on the console while commands are being entered.

```
RP/0/RSP0/CPU0: router# configure
RP/0/RSP0/CPU0:router# (config)# logging console informational
RP/0/RSP0/CPU0: router# (config)# commit
RP/0/RSP0/CPU0: router# (config)# logging console disable
```

3.3.2.2 Set logging size

This example shows how to set the maximum log file size to 10 MB:

```
RP/0/RSP0/CPU0: router(config)# logging buffered <2097152-125000000>
```

3.3.2.3 Turn logging on/off

The following example shows how to enable configuration logging:

```
RP/0/RSP0/CPU0: router# configure
RP/0/RSP0/CPU0: router (config)# logging trap debugging
```

The following example shows how to clear the configuration log by disabling and then re-enabling the configuration log:

```
RP/0/RSP0/CPU0: router# configure
RP/0/RSP0/CPU0: router (config)#no logging trap debugging
```

3.3.2.4 Logging Protection

To protect against audit data loss the TOE must be configured to send the audit records securely (through TLS) to an external Secure Syslog Server. By default system messages are logged to the console and the logfile, for the evaluated configuration the severity level must be set to “debugging” to ensure all required audit events related to the TOE Security Functions are audited and sent to the syslog server.

It is recommended that the implemented syslog server complies with the standards documented in RFC 5424. It is also expected that the software is the current version and is regularly updated with the latest patches.

Section 3.3.3 provides instructions once X.509 certificates have been configured.

Using a secure TLS connection for Syslog Server is required in the evaluated configuration: The minimum TLS version for use to TLS 1.2 with support for the following ciphers that are available by default in FIPS mode.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

To verify the TLS version being run use the command:

```
RP/0/RSP0/CPU0:router# show ssl
```

If any of the established trusted channels/paths are unintentionally broken, the connection will need to be re-established following the configuration settings as described in this document.

3.3.3 X.509 Certificates

For secure syslog, the remote server must be authenticated via a trustpoint configuration. The validity of certificates is verified with each connection to the syslog server. First, an authorized administrator must configure a hostname and IP domain on the router.

The router supports Subject Alternative Name (SAN) and Common Name (CN) with precedence for SAN reference identifiers for a successful connection. The Domain Name system (DNS) name in the SAN is used to match to the configured reference identifier in the instructions below.

If the channel fails due to a certificate error, the administrator should verify that the certificate does not have any of the following issues:

- The certificate is not signed by the CA with cA flag set to TRUE.
- The certificate is not signed by a trusted CA in the certificate chain.
- The certificate Common Name (CN) or Subject Alternative Name (SAN) does not match the expected DNS name(i.e., reference identifier).
- The certificate has been revoked or modified.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# hostname [name]
```

Example:

```
RP/0/RSP0/CPU0:router(config)# hostname myhost
RP/0/RSP0/CPU0:router(config)# domain name [domain name]
```

Example:

```
RP/0/RSP0/CPU0:router# domain name mydomain.com
RP/0/RSP0/CPU0:router# commit
RP/0/RSP0/CPU0:router# domain ipv4 host [host-name] [v4ipaddress]
```

Example:

```
RP/0/RSP0/CPU0:router# domain ipv4 host host1 192.168.7.18
```

NOTE: *The below command displays information about the CA certificate.*

```
RP/0/RSP0/CPU0: router# show crypto ca certificates
```

Declaring a Certification Authority and Configuring a Trusted Point

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint ca-name
```

Example:

```
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url CA-URL
```

Example:

```
RP/0/RSP0/CPU0:router(config-trustp)#enrollment url http://myca.domain.com
```

NOTE: *The below command is optional:*

```
 RP/0/RSP0/CPU0:router(config-trustp)# query url LDAP-URL
```

Example:

```
RP/0/RSP0/CPU0:router# query url ldap://my-ldap.domain.com
RP/0/RSP0/CPU0: router# commit
RP/0/RSP0/CPU0: crypto ca authenticate ca-name
```

Example:

```
RP/0/RSP0/CPU0:router# crypto ca authenticate myca
RP/0/RSP0/CPU0: router# crypto ca enroll ca-name
```

Example:

```
RP/0/RSP0/CPU0: router# crypto ca enroll myca
```

To control the extended key usage, use the command "extended-key-usage match serverAuth" in the trustpoint:

```
RP/0/RSP0/CPU0: router# extended-key-usage match serverAuth
```

Revocation Mechanism for PKI Certificate Status Checking:

When the router receives a certificate from a peer, it searches its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL is used. Otherwise, the router downloads the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. If the certificate appears on the CRL, your router cannot accept the certificate and will not authenticate the peer. This is the routers default behavior with no configuration required.

3.3.4 Logging to Syslog Server via TLS

Once the above steps are complete, then logging to the syslog server via TLS needs to be setup. To protect against audit data loss the TOE must be configured to send the audit records securely (via TLS) to an external Secure Syslog Server. You can use the server hostname for this configuration. Based on the configured severity, the router sends syslogs to the server. Logging severity options include alerts, critical, debugging, emergencies, errors, informational, notifications and warnings.

```
RP/0/RP0/CPU0: router #conf
RP/0/RP0/CPU0: router (config)# logging tls-server syslog server name
RP/0/RP0/CPU0: router (config)# min-version tls1.2 max-version tls1.2
RP/0/RP0/CPU0: router (config-logging-tls-peer)# trustpoint LS-ROOT-CA
RP/0/RP0/CPU0: router (config-logging-tls-peer)# severity debugging
RP/0/RP0/CPU0: router (config-logging-tls-peer)# tls-hostname xyz.cisco.com
RP/0/RP0/CPU0: router (config-logging-tls-peer)# commit
```

4 Secure Management

Cisco IOS XR devices perform authentication using the local database. The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE.

The term "Authorized Administrator" refers to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.

The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.

Manual software updates can only be done by the authorized administrator through CLI. These updates include software upgrades. The Security Administrators (a.k.a Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.

4.1 User Roles

The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE.

The term "Authorized Administrator" refers to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.

The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.

Manual software updates can only be done by the authorized administrator through CLI. These updates include software upgrades. The Security Administrators (a.k.a Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.

4.2 Passwords

For the evaluated configuration passwords must be a minimum length of 8 characters, a maximum of 253 characters, and composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")";

```
RP/0/RSP0/CPU0: router# configure
RP/0/RSP0/CPU0: router(config)# aaa password-policy policy
RP/0/RSP0/CPU0: router(config)# min-length 15
```

Configure the router to enforce that complexity requirement by using special characters by enabling "**special-char**". "**special-char**" specifies the number of special characters allowed in the password policy, in integer.

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)#aaa password-policy policy
RP/0/RSP0/CPU0:router(config)# special-char <integer>
```

4.3 Clock Management

Clock management is restricted to the privileged administrator. Use the clock set command for initial configuration. The 'clock set' command updates both the software as well as hardware clock.

```
RP/0/RP0/CPU0: router# clock set hh:mm:ss { day month | month day } year
RP/0/RP0/CPU0: router# show clock
16:18:28.927 PST Tue Feb 10 2025
```

4.4 Login Banners

The TOE may be configured by the privileged administrators with banners using the **banner motd** command. This banner is displayed after the username and before password prompts. To create a banner of text "This is a banner" use the command.

```
RP/0/RP0/CPU0: router#  configure
RP/0/RP0/CPU0: router(config)# banner motd #Welcome to the ASR 9000 Series#
```

4.5 Product Updates

The chapter –"Perform System Upgrade and Install Feature Packages" in **[2]** lists the detailed steps necessary to install packages and perform software upgrades. Below is a summary of steps necessary to upgrading the software on the router.

1. Execute:

```
install add source <sftp transfer protocol>//user@server:/package_path/
filename1 filename2>
```

2. show install request
3. show install repository
4. show install inactive
5. Execute one of these:

```
install activate package_name
or
install activate id operation_id
```

6. show install active
7. install commit

Verification of the authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image.

5 Security Relevant Events

The TOE 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 administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above. The details for configuration of these settings are covered in Section 3.3.2 above.

The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer.

When configured for a syslog backup the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space overwrites older events.

Table 11 below include the security relevant events that are applicable to the TOE.

5.1 Deleting Audit Records

The TOE provides the privileged Administrator the ability to delete audit records audit records stored within the TOE.

This is done with the clear logging command.

```
RP/0/RSP0/CPU0:router# clear logging
Clear logging buffer [confirm] [y/n] :y
```

5.2 Audit Records Description

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 record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. The audit fields in each audit event will contain at a minimum the following:

Example Audit Event:

```
Nov 19 2022 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self-test info: (AES
encryption/decryption ... passed)

Date: Nov 19
Time: 13:55:59
Type of event: %CRYPTO-6-SELF_TEST_RESULT
Subject identity: Available when the command is run by an authorized TOE
administrator user such as “user: lab”. 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:
Example audit events are included in Table 11 below. The auditable events
that result from administrative actions are included in Table 11 and are
designated with ‘Administrative Actions’ within the Auditable Events column.
```

Table 11: Audit Events and Sample Records

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record

FAU_GEN.1	Start-up and shutdown of audit functions.	None.	**Turn on logging to host:**
			
			`RP/0/RSP1/CPU0:Mar 31 10:11:48.515 IST: locald_DLRSC[260]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "logging hostnameprefix 10.105.236.78" by root from TTY /dev/pts/3 console`
			
			Turn off logging to host:
			
			`RP/0/RSP1/CPU0:Mar 31 10:16:39.076 IST: locald_DLRSC[260]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "no logging hostnameprefix 10.105.236.78" by root from TTY /dev/pts/3 console`
			
			Administrative Actions
			Change logging settings:
			
			`RP/0/RSP1/CPU0:Mar 31 10:17:33.122 IST: locald_DLRSC[260]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "logging buffered debugging" by root from TTY /dev/pts/3 console`
			
			Clear logging:
			
			`RP/0/RP0/CPU0:Jan 24 05:45:48.880 EST: locald_DLRSC[353]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "clear logging" by admin from TTY /dev/pts/0 console`
			
			`RP/0/RSP1/CPU0:Mar 31 10:18:20.072 IST: locald_DLRSC[260]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "clear logging" by root from TTY /dev/pts/3 console`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
FAU_GEN.2	None.	None.	See "Administrative Actions" in this table.
FAU_STG_EXT.1	None.	None.	**Administrative Action: Turn on logging to host:** `RP/0/RP0/CPU0:Feb 6 20:09:24.652 UTC: locald_DLRSC[353]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "logging hostnameprefix 10.14.0.1" by admin from TTY /dev/pts/0 console`

FCS_CKM.1	None.	None.	**Administrative Action: Generate RSA key:**
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:28.754 UTC: cepki[148]: %SECURITY-CEPKI-6-KEY_INFO : crypto key RSA generated, label:the_default, modBits:2048`
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:28.784 UTC: cepki[148]: %SECURITY-CEPKI-6-INFO : key database updated`

FCS_CKM.4	None.	None.	**Administrative Action: Zeroize RSA key:**
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:00.842 UTC: cepki[148]: %SECURITY-CEPKI-6-KEY_INFO : crypto key RSA zeroized, label:the_default`
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:00.863 UTC: cepki[148]: %SECURITY-CEPKI-6-INFO : key database updated`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
FCS_SSH_EXT.1	[Failure to establish SSH connection]	Reason for failure. [Non-TOE endpoint of attempted connection (IP Address)]	**Failure to establish SSH session:** RP/0/RSP1/CPU0:Mar 26 13:44:55.964 UTC: SSHD_[65830]: %SECURITY-SSHD-4-INFO_FAILURE : Failed authentication attempt by user 'root' from '10.105.236.78' on 'vty0' RP/0/RSP1/CPU0:Mar 26 13:45:29.662 UTC: SSHD_[65830]: %SECURITY-SSHD-6-INFO_GENERAL : Client closes socket connection RP/0/RSP1/CPU0:Mar 26 13:45:29.662 UTC: SSHD_[65830]: %SECURITY-SSHD-3-ERR_GENERAL : Failed to receive User authentication request **Administrative Actions:** RP/0/RSP1/CPU0:Mar 26 13:41:00.209 UTC: SSHD_[65682]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated user 'root' from '10.105.236.78' on 'vty0'(cipher 'aes128-ctr', mac 'hmac-sha2-256') RP/0/RSP1/CPU0:Mar 26 13:41:45.863 UTC: SSHD_[65682]: %SECURITY-SSHD-6-INFO_USER_LOGOUT : User 'root' from '10.105.236.78' logged out on 'vty0'
	[Establishment of SSH connection]	[Non-TOE endpoint of connection (IP Address)]	**Establishment SSH session:** RP/0/RSP1/CPU0:Mar 26 13:41:00.209 UTC: SSHD_[65682]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated user 'root' from '10.105.236.78' on 'vty0'(cipher 'aes128-ctr', mac 'hmac-sha2-256')

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
	[Termination of SSH connection session]	[Non-TOE endpoint of connection (IP Address)]	**Termination of SSH session:** `RP/0/RSP1/CPU0:Mar 26 13:41:45.863 UTC: SSHD_[65682]: %SECURITY-SSHD-6-INFO_USER_LOGOUT : User 'root' from '10.105.236.78' logged out on 'vty0'`
	[Dropping of packet(s) outside defined size limits]	[None]	**Oversized SSH packet:** `2024 Dec 31 01:51:36 nx9336-FX2 %AAA-6-AAA_ACCOUNTING_MESSAGE: stop:192.168.144.51@pts/3:admin: shell terminated because the ssh session closed`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record

FCS_TLSC_EXT.1	Failure to establish an TLS session	Reason for failure	**Establishment of a TLS session:**
			
			`RP/0/RSP0/CPU0:May 18 12:31:08.138 UTC: syslogd[204]: %OS-SYSLOG-5-LOG_NOTICE : Secure Logging: Successfully established TCP connection , server :10.105.227.148`
			
			`RP/0/RSP0/CPU0:May 18 12:31:08.267 UTC: syslogd[204]: %SECURITY-PKI-6-LOG_INFO : Certificate verified successfully`
			
			`RP/0/RSP0/CPU0:May 18 12:31:08.268 UTC: syslogd[204]: %SECURITY-XR_SSL-6-CERT_VERIFY_INFO : SSL Certificate verification: Peer certificate verified successfully`
			
			`RP/0/RSP0/CPU0:May 18 12:31:08.275 UTC: syslogd[204]: %OS-SYSLOG-5-LOG_NOTICE : Secure Logging: Successfully established TLS session , server :10.105.227.148`
			
			Failure to establish a TLS Session:
			
			`RP/0/RSP0/CPU0:May 18 12:27:18.332 UTC: syslogd[204]: %OS-SYSLOG-5-LOG_NOTICE : Secure Logging: Failed to establish TCP connection , server :10.105.227.148`
			
			Termination of a TLS session:
			
			`RP/0/RSP0/CPU0:May 18 12:31:52.808 UTC: syslogd[204]: %OS-SYSLOG-5-LOG_NOTICE : Secure Logging: TLS session disconnected, server :10.105.227.148`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record

FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.
	
	Administrator lockout due to excessive authentication failures.
		Origin of the attempt (e.g., IP address)	**Unsuccessful login / authentication failure :**
			
			`RP/0/RSP1/CPU0:Mar 30 16:28:07.753 IST: SSHD_[69074]: %SECURITY-SSHD-4-INFO_FAILURE : Failed authentication attempt by user 'test' from '10.105.227.126' on 'vty0'`
			
			`RP/0/RSP1/CPU0:Mar 30 16:28:09.576 IST: locald_DLRSC[260]: %SECURITY-LOCALD-5-USER_PASSWD_LOCKED : User 'test' is temporarily locked out for exceeding maximum unsuccessful logins.`
			
			`RP/0/RSP1/CPU0:Mar 30 16:28:15.272 IST: locald_DLRSC[260]: %SECURITY-LOCALD-5-USER_PASSWD_UNLOCKED : User 'test' is unlocked for authentications.`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
FIA_PMG_EXT.1	None.	None.	Administrative Action: RP/0/RSP1/CPU0:R2(config)#aaa password-policy policy min-length 15 RP/0/RSP1/CPU0:R2(config)#username root password-policy policy password cisco123 RP/0/RSP1/CPU0:R2(config)#commit Fri Mar 27 11:01:19.503 IST % Failed to commit one or more configuration items during a pseudo-atomic operation. All changes made have been reverted. Please issue 'show configuration failed [inheritance]' from this session to view the errors RP/0/RSP1/CPU0:R2(config)#show configuration failed Fri Mar 27 11:01:26.586 IST !! SEMANTIC ERRORS: This configuration was rejected by !! the system due to semantic errors. The individual !! errors with each failed configuration command can be !! found below. username root password-policy policy password 7 13061E010803557878 !!% 'LOCALD' detected the 'fatal' condition 'Password is shorter than minimum required length.'

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record

FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	**Use of identification/authentication:**
			
			`RP/0/RSP1/CPU0:Mar 26 13:44:55.964 UTC: SSHD_[65830]: %SECURITY-SSHD-4-INFO_FAILURE : Failed authentication attempt by user 'root' from '10.105.236.78' on 'vty0'`
			
			`RP/0/RSP1/CPU0:Mar 26 13:45:29.662 UTC: SSHD_[65830]: %SECURITY-SSHD-6-INFO_GENERAL : Client closes socket connection`
			
			`RP/0/RSP1/CPU0:Mar 26 13:45:29.662 UTC: SSHD_[65830]: %SECURITY-SSHD-3-ERR_GENERAL : Failed to receive User authentication request`
			
			Administrative Action:
			See Audit events in FIA_UAU_EXT.2

FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**Login as an administrative user at the console:**
			
			`RP/0/RSP1/CPU0:Mar 27 11:16:21.798 IST: exec[67616]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'root' from 'console' on 'con0_RSP1_CPU0'`
			
			Failed login via the console:
			
			`RP/0/RSP1/CPU0:Mar 27 11:16:12.348 IST: exec[67616]: %SECURITY-LOGIN-4-AUTHEN_FAILED : Failed authentication attempt by user '<unknown>' from 'console' on 'con0_RSP1_CPU0'`
			
			See FCS_SSHS_EXT.1 for remote login audit events.

FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate
	
	Any addition, replacement or removal of trust anchors in the TOE's trust store.
		Reason for failure of certificate validation
		
		Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
			Certificate Verified:
			
			`RP/0/RSP0/CPU0:May 18 15:09:10.832 UTC: pki_cmd[66819]: %SECURITY-PKI-6-LOG_INFO : Certificate verified successfully`
			
			Certificate Granted:
			
			`RP/0/RSP0/CPU0:May 18 11:57:05.245 UTC: pki_cmd[68759]: %SECURITY-PKI-6-LOG_INFO : certificate is granted`
			
			Certificate Failure:
			
			`RP/0/RSP0/CPU0:May 18 12:14:28.273 UTC: pki_cmd[69113]: %SECURITY-PKI-6-ERR_1_PARAM : Failed to get/generate CA certificate.`
			
			`% Failed to validate subordinate CA certificate`
			
			Certificate Updated:
			
			`RP/0/RSP0/CPU0:May 18 12:02:31.125 UTC: cepki[309]: %SECURITY-CEPKI-6-INFO : certificate database updated`
			
			CA Certificate Expiry info:
			
			`RP/0/RSP0/CPU0:May 18 12:22:02.008 UTC: cepki[309]: %SECURITY-CEPKI-7-CERT_TIMER : Certificate Expiration Timer activated for 299970946 seconds (TIME left for 60 DAYS). Trustpoint Name = ca-root, Certificate Type = CA certificate, Index=10`
			
			Router Certificate Expiry info:
			
			`RP/0/RSP0/CPU0:May 18 12:22:02.011 UTC: cepki[309]: %SECURITY-CEPKI-1-CERT_EXPIRING_ALERT : Certificate expiring WITHIN A DAY. Trustpoint Name= ca-root,`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
			Certificate Type= Router certificate, Serial Number= 01:10, Issuer Name= CN=ca-root,OU=GCT,O=Cisco,L=RTP,ST=NC,C=US, Subject name= ST=KA,CN=ASR9K.cisco.com,OU=SPBU,O=Cisco Systems,C=IN, Time Left= 0 days, 23 hours, 58 minutes, 49 seconds **Trustpoint Unconfigure:** RP/0/RSP0/CPU0:May 19 18:15:22.350 UTC: cepki[379]: %SECURITY-CEPKI-6-WARNING : It is the operator's responsibility to repeat the authenticate and enroll steps for any changes to the keys, or to the trustpoint configuration details.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.	See FPT_TUD_EXT.1
FMT_MTD.1/CoreData	None.	None.	None

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record

FMT_MTD.1/CryptoKeys	None.	None.	**Generate RSA key:**
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:28.754 UTC: cepki[148]: %SECURITY-CEPKI-6-KEY_INFO : crypto key RSA generated, label:the_default, modBits:2048`
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:28.784 UTC: cepki[148]: %SECURITY-CEPKI-6-INFO : key database updated`
			
			Zeroize RSA key:
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:00.842 UTC: cepki[148]: %SECURITY-CEPKI-6-KEY_INFO : crypto key RSA zeroized, label:the_default`
			
			`RP/0/RSP1/CPU0:Mar 26 11:50:00.863 UTC: cepki[148]: %SECURITY-CEPKI-6-INFO : key database updated`

FMT_SMF.1	All management activities of TSF data.	None.	**Administrative login and logout:** RP/0/RSP1/CPU0:Mar 26 13:41:00.209 UTC: SSHD_[65682]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated user 'root' from '10.105.236.78' on 'vty0'(cipher 'aes128-ctr', mac 'hmac-sha2-256') RP/0/RSP1/CPU0:Mar 26 13:41:45.863 UTC: SSHD_[65682]: %SECURITY-SSHD-6-INFO_USER_LOGOUT : User 'root' from '10.105.236.78' logged out on 'vty0' **Security related configuration changes:** RP/0/RSP1/CPU0:Mar 31 14:52:45.971 IST: locald_DLRSC[260]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "ssh server algorithms key-exchange diffie-hellman-group14-sha1" by root from TTY /dev/pts/3 console **Generating/import of, changing, or deleting of cryptographic keys:** RP/0/RSP1/CPU0:Mar 30 10:10:30.664 IST: cepki[164]: %SECURITY-CEPKI-6-KEY_INFO : crypto key RSA(public key authentication) generated, label:root, modBits:2048 RP/0/RSP1/CPU0:Mar 30 10:23:47.629 IST: cepki[164]: %SECURITY-CEPKI-6-KEY_INFO : crypto key RSA generated, label:the_default, modBits:2048 RP/0/RSP1/CPU0:Mar 30 10:24:06.964 IST: cepki[164]: %SECURITY-CEPKI-6-KEY_INFO : crypto key RSA zeroized, label:the_default **Resetting passwords:** RP/0/RSP1/CPU0:R2(config)#RP/0/RSP1/CPU0:Mar 31 14:49:33.121

			IST: locald_DLRSC[260]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "username root password <removed>" by root from TTY /dev/pts/3 console **Starting and stopping services:** RP/0/RSP1/CPU0:Mar 31 14:46:56.394 IST: sysmgr_control[68696]: %OS-SYSMGR-4-PROC_SHUTDOWN_NAME : User root (con0_RSP1_CPU0) requested a shutdown of process cepki at 0/RSP1/CPU0 RP/0/RSP1/CPU0:Mar 31 14:47:22.709 IST: sysmgr_control[68729]: %OS-SYSMGR-4-PROC_START_NAME : User root (con0_RSP1_CPU0) requested a start of process cepki at 0/RSP1/CPU0 **Modify access banner:** Feb 3 16:38:58 ncs1k 2118: TOE:NCS1000 RP/0/RP0/CPU0:2020 Feb 3 21:37:06.274 : locald_DLRSC[380]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "banner login c test login banner c " by root from TTY /dev/pts/4 192.168.144.254 **Configure SSH:** Feb 3 16:38:59 ncs1k 2254: TOE:NCS1000 RP/0/RP0/CPU0:2020 Feb 3 21:37:07.686 : locald_DLRSC[380]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "ssh server logging" by root from TTY /dev/pts/4 192.168.144.254 Feb 3 16:38:59 ncs1k 2256: TOE:NCS1000 RP/0/RP0/CPU0:2020 Feb 3 21:37:07.703 : locald_DLRSC[380]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "ssh timeout 10" by root

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
			from TTY /dev/pts/4 192.168.144.254 Feb 3 16:38:59 ncs1k 2258: TOE:NCS1000 RP/0/RP0/CPU0:2020 Feb 3 21:37:07.720 : locald_DLRSC[380]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "ssh server rekey-time 1440" by root from TTY /dev/pts/4 192.168.144.254 Feb 3 16:38:59 ncs1k 2260: TOE:NCS1000 RP/0/RP0/CPU0:2020 Feb 3 21:37:07.742 : locald_DLRSC[380]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "ssh server algorithms key-exchange diffie-hellman-group14-sha1" by root from TTY /dev/pts/4 192.168.144.254 Feb 3 16:38:59 ncs1k 2262: TOE:NCS1000 RP/0/RP0/CPU0:2020 Feb 3 21:37:07.759 : locald_DLRSC[380]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "ssh server rekey-volume 1024" by root from TTY /dev/pts/4 192.168.144.254 Feb 3 16:38:59 ncs1k 2264: TOE:NCS1000 RP/0/RP0/CPU0:2020 Feb 3 21:37:07.776 : locald_DLRSC[380]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "ssh server
FPT_RPL.1	Detected replay attempt	None.	**Replay attempt:** LC/0/0/CPU0:Apr 23 20:03:45.447 UTC: macsec_ea[374]: %OS-PLATFORM_MACSEC-6-LATE_PACKET : inPktsLate:0x3a2 Interface:Hu0/0/0/7

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record

FPT_TST_EXT.1	Execution of this set of TSF-self-tests. Detected integrity violations.	For integrity violations, the TSF code file that caused the integrity violation.	**TSF self-test completed:**
			
			`RP/0/RSP1/CPU0:Mar 26 04:38:17.356 UTC: cepki[164]: %SECURITY-PKI-6-LOG_INFO_DETAIL : FIPS POST Successful for cepki`
			
			TSF Self-test fail:
			
			`RP/0/RSP1/CPU0:Apr 3 10:24:52.303 IST: ssh_conf_verifier[1171]: %INFRA-REBOOT_LIB-6-REBOOT_INITIATED : Reboot initiated with code:134217766 cause:'c3m_set_fips_mode, Fatal Fault, FIPS POST Failure requested by: Process ID: 10511 (ssh_conf_verifier) app_name: ssl' reboot timeout:2 shutdown delay: 0`

FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.	**Success:**
			
			`RP/0/RSP1/CPU0:Mar 27 11:46:22.485 IST: sdr_instmgr[1308]: %INSTALL-INSTMGR-2- OPERATION_SUCCESS : Install operation 34 finished successfully`
			
			Failure:
			
			`RP/0/RP0/CPU0:2019 Dec 3 16:50:12.531 : sdr_instmgr[1202]: %INSTALL-INSTMGR-3-OPERATION_ABORT : Install operation 2 aborted`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated 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)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	**Time change:** `RP/0/RSP1/CPU0:Mar 26 11:00:00.001 IST: iosclock[67557]: %INFRA - INFRA_MSG-5-CLOCK_TIME_UPDATE : User root(con0_RSP1_CPU0) updated clock from Thu Mar 26 11:42:39 2020 to Thu Mar 26 11:00:00 2020`

FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.	**Termination of local session:**
			
			`RP/0/RSP1/CPU0:Mar 31 15:14:56.359 IST: locald_DLRSC[260]: %SECURITY-LOCALD-5-USER_PASSWD_UNLOCKED : User 'test' is unlocked for authentications.`
			
			`RP/0/RSP1/CPU0:Mar 31 15:12:26.218 IST: locald_DLRSC[260]: %SECURITY-LOCALD-5-USER_PASSWD_LOCKED : User 'test' is temporarily locked out for exceeding maximum unsuccessful logins.`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record

FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	**Termination of remote session:**
			
			`RP/0/RSP1/CPU0:Mar 27 14:00:35.655 IST: SSHD_[66934]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated user 'root' from '10.105.227.126' on 'vty0'(cipher 'aes128-ctr', mac 'hmac-sha2-256')`
			
			`RP/0/RSP1/CPU0:Mar 27 14:01:37.410 IST: SSHD_[66934]: %SECURITY-SSHD-6-INFO_USER_LOGOUT : User 'root' from '10.105.227.126' logged out on 'vty0'`
			
			Administrative Action:
			
			`RP/0/RP0/CPU0:Feb 6 21:14:31.764 UTC: locald_DLRSC[353]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "line console exec-timeout 0 60" by admin from TTY /dev/pts/0 console`

FTA_SSL.4	The termination of an interactive session.	None.	**Termination of interactive session:**
			
			`RP/0/RSP1/CPU0:Mar 27 14:00:35.655 IST: SSHD_[66934]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated user 'root' from '10.105.227.126' on 'vty0'(cipher 'aes128-ctr', mac 'hmac-sha2-256')`
			
			`RP/0/RSP1/CPU0:Mar 27 14:01:37.410 IST: SSHD_[66934]: %SECURITY-SSHD-6-INFO_USER_LOGOUT : User 'root' from '10.105.227.126' logged out on 'vty0'`

Requirement	Auditable Event	Additional Audit Record Contents	Sample Record
FTA_TAB.1	None.	None.	**Administrative Action:** `RP/0/RP0/CPU0:Feb 6 21:46:18.642 UTC: locald_DLRSC[353]: %SECURITY-LOCALD-6-LOCAL_CMD_ACCT : CLI CMD: "banner login d This is a banner. d " by admin from TTY /dev/pts/0 console`
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	Also see logs provided by FCS_TLS_EXT.1
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None.	See logs provided by FCS_SSHS_EXT.1

6 Network Services and Protocols

The table below lists the network services/protocols available on the TOE 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.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the ***Command Reference*** guides listed above in this document.

Table 12: 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	Yes	No restrictions.
FTP	File Transfer Protocol	Yes	No	No	No	Out of scope of the evaluation
HTTP	Hypertext Transfer Protocol	Yes	No	Yes	No	Out of scope of the evaluation
HTTPS	Hypertext Transfer Protocol Secure	Yes	No	Yes	No	Out of scope of the evaluation
ICMP	Internet Control Message Protocol	Yes	No	Yes	No	Out of scope of the evaluation
IKE	Internet Key Exchange	Yes	No	Yes	No	Out of scope of the evaluation
Kerberos	A ticket-based authentication protocol	Yes	No	No	No	Out of scope of the evaluation
LDAP	Lightweight Directory Access Protocol	Yes	No	No	n/a	Out of scope of the evaluation

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	No	No	No	Out of scope of the evaluation.
MACsec	Media Access Control Security	?	No	?	No	Out of scope of the evaluation
RADIUS	Remote Authentication Dial In User Service	Yes	No	No	No	Out of scope of the evaluation
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	No	Yes	No	Out of scope of the evaluation.
SSH	Secure Shell	Yes	No	Yes	Yes	As described in the relevant section of this document.
SSL (not TLS)	Secure Sockets Layer	Yes	No	Yes	No	Use SSH instead.
TACACS+	Terminal Access Controller Access-Control System Plus	Yes	No	No	No	Out of scope of the evaluation
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use SSH instead.
TLS	Transport Layer Security	Yes	Yes	No	No	As described in the relevant section of this document.
TFTP	Trivial File Transfer Protocol	Yes	No	No	No	Out of scope of the evaluation.

7 Modes of Operation

An IOS-XR router has several modes of operation, these modes are as follows:

Booting – while booting, the routers drop all network traffic until the router image and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation. During booting, an administrator may press the break key on a console connection within the first 60 seconds of startup to enter the ROM Monitor mode of operation. This Booting mode is referred to in the IOS-XR guidance documentation as "ROM Monitor Initialization".

Additionally if the router does not find a valid operating system image it will enter ROM Monitor mode and not normal mode therefore protecting the router from booting into an insecure state.

Normal - The IOS-XR router image and configuration is loaded and the router is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all router based security functions are operating. While operating the router have little interaction with the administrator. However, the configuration of the router can have a detrimental effect on security. Misconfiguration of the router could result in the unprotected network having access to the internal/protected network

ROM Monitor – This mode of operation is a maintenance, debugging, and disaster recovery mode. While the router is in this mode, no network traffic is routed between the network interfaces. In this state the router may be configured to upload a new boot image from a specified TFTP server, perform configuration tasks and run various debugging commands.

NOTE: If nvram is empty and a reload is done, IOS-XR will try to boot automatically from an image top down that is in the flash directory. Make sure the valid IOS-XR image is listed above any other images in flash.

It should be noted that while no administrator password is required to enter ROM monitor mode, physical access to the router is required; therefore, the router should be stored in a physically secure location to avoid unauthorized access which may lead to the router being placed in an insecure state.

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.

All ports are blocked from moving to forwarding state during the POST. Only when all components of all modules pass the POST is the system placed in FIPS PASS state and ports are allowed to forward data traffic.

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 https://www.cisco.com/support/.
- If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance

8 Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions, and adheres to the environment security objectives listed below. The environment security objective identifiers map to the environment security objectives as defined in the Security Target.

Table 13: Operational Environment Security Measures

Environment Security Objective	IT Environment Security Objective Definition	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment	Administrators must ensure the TOE is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
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.	Administrators will make sure there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE.
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.	None
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the	Administrators must be properly trained in the usage and proper operation of the TOE and all the provided functionality per the implementing organization's operational security policies. These administrators must follow the provided guidance.

	TOE's trust store in case such certificate can no longer be trusted.	
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 regularly update the TOE to address any known vulnerabilities.
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 protect their access credentials wherever they may be.
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.	Administer must follow guidance on how to securely protect sensitive residual information on equipment discarded or removed.

9 Obtaining Documentation

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 www.cisco.com.

9.1 Document 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

9.2.1 Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

https://www.cisco.com/c/en/us/support/index.html

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

https://id.cisco.com/signin/register

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website in the More Tools section:

https://www.cisco.com/c/en/us/support/web/tools-catalog.html

Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

9.2.2 Submitting a Service Request

Using the online Cisco Support Assistant is the fastest way to open S3 and S4 support case (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the Cisco Support Assistant provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The Cisco Support Assistant is located at this URL:
https://supportassistant.cisco.com

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227) EMEA: +32 2 704 55 55USA: 1 800 553-2447

Further information can be found in the “Contact TAC by Phone” section at the support page:
https://www.cisco.com/c/en/us/support/index.html

9.2.3 Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) – Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

9.3 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Commerce provides a variety of Cisco products, documentation, estimates, and software. Visit Cisco Commerce at this URL:

  https://apps.cisco.com/Commerce/guest

- Cisco Learning Locator publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Learning Locator titles and other information, go to this URL:

  https://learninglocator.cloudapps.cisco.com/#/home

- Cisco Learning Network

- Cisco Community is a hub that allows fellow Cisco peers and specialists to ask for help, share expertise, and grow professionally. It includes access to Webinars and Events, DevNet and Partner Hubs, and Cisco Café blogs. Cisco Community can be accessed at this URL:

  https://community.cisco.com

- The Newsroom stays up to date with the latest tech trends and information. This can be accessed at this URL:

  https://newsroom.cisco.com/c/r/newsroom/en/us/index.html

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  https://www.cisco.com/c/en/us/products/index.html

- Additional information for anything Cisco-related can be found here:

https://www.cisco.com/c/en/us/about/sitemap.html