Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Operational User Guidance and Preparative Procedures

Version: 1.1

Date: March 23 2023

EDCS: 23191545

Cisco Systems, Inc.

Table of Contents

List of Tables

Acronyms and Abbreviations

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

Table 1 Acronyms and Abbreviations

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
HDD	Hard-disk drives
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
OS	Operating System
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SM	Service Module
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VIB	VMware ESXi vSphere Installation Bundles

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1. 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 Operational User Guidance with Preparative Procedures documents the administration of the Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series TOE certified under Common Criteria. The Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series is running IOS-XR, version 7.4.1. TOE may be referenced below as the NCS or TOE or simply router.

1.1 Audience

This document is written for administrators configuring and maintaining the TOE. 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 in 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 your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the 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.

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 the TOE operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands.

1.3 Document References

This document refers to several Cisco Systems product documents. The documents used are shown below.

Table 2 Document Reference

Reference number	Document Name	Link
[1]	**Release Notes**	https://www.cisco.com/c/en/us/td/docs/iosxr/n

Reference number	Document Name	Link
	a) Release Notes for Cisco NCS 540 Series Routers, Cisco IOS XR Release 7.4.1 b) Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.1 (This is used for NCS 5700 as well)	cs5xx/release-notes/74x/b-release-notes-ncs540-r741.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/general/74x/release/notes/b-release-notes-ncs5500-r741.html
[2]	Hardware Installation Guide a) Cisco Network Convergence System 540 Small Density Routers Hardware Installation Guide b) Cisco NCS 540 Router Hardware Installation Guide c) Hardware Installation Guide for Cisco NCS 5500 Series Routers d) Hardware Installation Guide for Cisco NCS 5700 Series Fixed-Port Routers	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/hardware/installation/guide/b-ncs540-small-density-routers-hig.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/hardware/installation/guide/b-ncs540-hig.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/hardware-install/b-ncs5500-hardware-installation-guide.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/hardware-install/b-ncs5700-hardware-installation-guide-fixed-port.html
[3]	System Security Command Reference a) System Security Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/security/b-system-security-cr-ncs5500.html
[4]	System Management Configuration Guide a) System Management Configuration Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.4.x b) System Management Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.x	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/system-management/74x/b-system-management-cg-74x-ncs540.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/sysman/74x/b-system-management-cg-ncs5500-74x.html
[5]	System Security Configuration Guide a) System Security Configuration Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.4.x b) System Security Configuration Guide for Cisco NCS 5500 Series Routers, IOS	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/system-security/74x/b-system-security-cg-74x-ncs540.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/security/74x/b-system-security-cg-

Reference number	Document Name	Link
	XR Release 7.4.x	ncs5500-74x.html
[6]	System Setup and Software Installation Guide a) System Setup and Software Installation Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.4.x b) System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.x	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/system-setup/74x/b-system-setup-cg-74x-ncs540.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/system-setup/74x/b-system-setup-cg-ncs5500-74x.html
[7]	System Monitoring Configuration Guide a) System Monitoring Configuration Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.4.x b) System Monitoring Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.x	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/system-monitoring/74x/b-system-monitoring-cg-74x-ncs540.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/system-monitoring/74x/b-system-monitoring-cg-ncs5500-74x.html
[8]	System Monitoring Command Reference a) System Monitoring Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/system-monitoring/b-ncs5500-system-monitoring-cli-reference.html
[9]	Cisco IOS XR System Error Message Reference Guide	https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/error/message/ios-xr-sem-guide.html
[10]	IP Addresses and Services Configuration Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.4.x IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.x	https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/ipaddress/74x/b-ip-addresses-cg-74x-ncs540.html https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/ip-addresses/74x/b-ip-addresses-cg-ncs5500-74x.html

1.4 Supported Hardware and Software

Only the following hardware and software listed below are compliant with the Common Criteria Cisco Network Convergence System 540, 5500 and 5700 Series EAL2 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

The software consists of the Cisco Internet Operating System (IOS) XR software image Release IOS-XR 7.4. The Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500 and NCS5700) Series consists of:

- N540X-8Z16G-SYS-D is a 1RU small density fixed chassis router.
- N540X-8Z16G-SYS-A is a 1RU small density fixed chassis router.
- N540X-16Z4G8Q2C-D is a 1RU medium density fixed chassis router.
- N540X-16Z4G8Q2C-A is a 1RU medium density fixed chassis router.
- NCS-5504-SYS is a 7RU modular chassis in which TOE Line card NC55-32T16Q4H-A is housed.
- NCS-57C3-MOD-SYS is a 3RU fixed chassis router.

1.5 Operational Environment

1.5.1 Supported non-TOE Hardware/Software/Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with an 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.
NTP Server	No	An NTP server is an optional component of the operational environment that would allow for synchronizing the TOE clocks with an external time source.
Audit (syslog) Server	No	A syslog server is an optional component for use with the TOE. It is a supplemental storage system for audit logs, but it does not provide audit log storage for the TOE.

1.6 Excluded Functionality

Following is the functionality that is excluded from the evaluated configuration. Not including this functionality does not affect the requirements being claimed.

Table 4 Excluded Functions

Excluded Functionality	Rationale
Telnet	Telnet sends authentication data in plain text. This feature is disabled by default and must remain disabled in the evaluated configuration.
SNMP	SNMP may allow an unauthorized third party to gain access to a network device. This feature will be disabled in the evaluated configuration.

2. Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that it 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 in which 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 obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

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

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

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

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

Table 5 Evaluated Products and their External Identification

Product Name	External Identification
Cisco Network Convergence System 540 Small Density Router - N540X-8Z16G-SYS-D	N540X-8Z16G-SYS-D
Cisco Network Convergence System 540 Small Density Router - N540X-8Z16G-SYS-A	N540X-8Z16G-SYS-A
Cisco Network Convergence System 540 Medium Density Router - N540X-16Z4G8Q2C-D	N540X-16Z4G8Q2C-D
Cisco Network Convergence System 540 Medium Density Router - N540X-16Z4G8Q2C-A	N540X-16Z4G8Q2C-A
Cisco Network Convergence System 5500 Series - NCS-5504-SYS	NCS-5504-SYS
Cisco Network Convergence System 5700 Series - NCS-57C3-MOD-SYS	NCS-57C3-MOD-SYS

Step 7 After the TOE hardware has been installed and set up, follow the steps below for the approved methods for obtaining a Common Criteria evaluated software image:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following: https://software.cisco.com/download/home [Login to CCO is required to download, but not to search.]

Step 8 Once the file is downloaded, you may choose to verify the software image from the trusted system. To verify the published hash, you can use a checksum utility of your choice to compute the hash for the downloaded image file and then compare the results against the image hash listed below.

If the hashes do not match, contact Cisco Technical Assistance Center (TAC) www.cisco.com/go/offices. Login to CCO is required.

Table 6 Evaluated Software Images

Models	Software Version	Image Name	Image hash values
N540X-8Z16G-SYS-D N540X-8Z16G-SYS-A	IOS XR 7.4.1	ncs540l-aarch64-7.4.1.iso	744d5adb7e7cca2be7aa9a615d84c613d8dd162a9c438f6d36963cd67439a6b361d17a4251fccef6c8be93c46fc43df1f65db06228fe85012e7baf732593945d
N540X-16Z4G8Q2C-D		ncs540l-x64-7.4.1.iso	dfa3b8685964cebd1558ad96cc810fb79512f35996794decb515a2ab0377caf034c50be264ae43a91a3e56b8

Models	Software Version	Image Name	Image hash values
N540X-16Z4G8Q2C-A			ab4f8866774c987e539db732ffe2a19fba7f9026
NCS-5504-SYS NCS-57C3-MOD-SYS		NCS5500-iosxr-7.4.1.tar	c98035eae1f3b85a650c2cff575f623bc2b55d458adb42c0b7806c759015da2d778cf995736c1fa790b05b2003a7515ee5e1b0d602c1ece1a808cb024590623e

Step 9 Install the downloaded and verified software image onto your TOE as described in [6] 'Perform System Upgrade and Install Feature Packages.'

VerifyPackage 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.

Install and Activate Packages

System upgrade on the TOE is done using an ISO image file, while the patch installation is done using 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. Please find detailed instructions on Installing packages in [6] 'Perform System Upgrade and Install Feature Packages.'

Software packages remain inactive until activated with the **install activate** command. To activate a package on your router, use the **install activate** command in administration EXEC mode.

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**

Commit the Active Software

The active software has to be committed in order 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.

Verify the installation using the **install verify packages** command.

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 **[5]** 'Verify Boot Operation' to show the system software release version.
- Use the **show install active** command **[5]** to display the currently running system image filename and the system software release version.

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 on how to download updates and how to verify the updates is the same as described above.

3. Secure Installation and Configuration

3.1 Physical Installation

Follow the TOE Hardware Installation Guide **[2]** for hardware installation instructions for the specific TOE model.

3.2 Initial Setup via Direct Console

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

Once the software has been committed, an authorized administrator needs to connect to the console port. On first login the username and password for the root system user will need to be created. The following example shows the root system username and password configuration for a new router, and it shows the initial log in:

RP/0/RSP0/CPU0: Enter root system
username: <username1>
RP/0/RSP0/CPU0: Enter secret:
RP/0/RSP0/CPU0: Enter secret again:

When creating the password, follow the guidance for a secure password in section 4.2.

Note: The secret line in the configuration command script shows that the password is hashed for obfuscation. When you enter the password during configuration and login, the password is hidden.

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. See the System Setup and Software Installation Guide **[6]** for more information.

3.2.1 Administrator Configuration and Credentials

The TOE must be configured to use a username and password for each administrator and one password for the admin command. Ensure all passwords are stored encrypted by using the 7 option with the password command. See **[3]** System Security Command Reference and **[6]** System Security Configuration Guide, chapter "Configuring AAA Services", section "Configuring Users"

RP/0/RSP0/CPU0:router#**configure**
RP/0/RSP0/CPU0:router(config)#**username user1**
RP/0/RSP0/CPU0:router(config-un)#**password 7 K$e%y^&*()t@#!s**

RP/0/RSP0/CPU0:router(config-un)# **commit**
RP/0/RSP0/CPU0:router(config-un)# **show running-config**

Configure local AAA authentication:

RP/0/RSP0/CPU0:router(config)# **aaa authentication login default local**

RP/0/RSP0/CPU0:router(config)# **aaa authorization exec default local**

3.2.2 Saving Configuration

IOS-XR uses both a running configuration and a starting configuration. Configuration changes affect the running configuration; in order to save that configuration, the running configuration (held in memory) must be copied to the startup configuration. This may be achieved by using the **copy run start** command.

RP/0/RSP0/CPU0:router# **copy run start**
disk0:/config/running/alternate_cfg:/router.cfg Destination file name (control-c to abort): [/router.cfg]?

The destination file already exists. Do you want to overwrite? [no]: **yes**

This command should be used frequently when making changes to the configuration of the router. If the router reboots and resumes operation when uncommitted changes have been made, these changes will be lost and the router will revert to the last configuration saved.

3.2.3 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

3.2.4 Steps to configure SSH Server on the router

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

RP/0/RSP0/CPU0:router# **crypto key generate rsa general-keys rsakeypair**

RP/0/RSP0/CPU0:router# How many bits in the modulus [512]: **2048**

RP/0/RSP0/CPU0:router#**show crypto key mypubkey rsa**

RSA keys are generated in pairs—one public RSA key and one private RSA key. This command is not saved in the router configuration; the RSA keys generated by this command, however, 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: *Only one set of keys can be configured using the* ***crypto key generate*** *command at a time. Repeating the command overwrites the old keys.*

Note: *If the configuration is not saved to NVRAM with a "****copy run start****", the generated keys are lost on the next reload of the router.*

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

3.2.4.1 Configure SSH ciphers

SSH ciphers should be configured as follows:

RP/0/RSP0/CPU0:router#**configure terminal**

RP/0/RSP0/CPU0:router(config)#**ssh server algorithms cipher aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-ctr aes192-ctr aes256-ctr**

RP/0/RSP0/CPU0:router(config)#**commit**

RP/0/RSP0/CPU0:router(config)#**exit**

3.2.4.2 SSH Public key authentication

An administrator can configure SSH public key authentication by importing their public key to the TOE.

3.2.5 Self-tests

The self-tests for the cryptographic functions in the TOE are run automatically during power on as part of the Power on Startup Test (POST).

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.

3.2.6 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 #**configure**

RP/0/RP0/CPU0:router(config)#**line default**

RP/0/RP0/ (config-line)#**exec-timeout *minutes seconds***

The line console setting is not immediately activated for the current session. The current console session must first be exited. When the user logs back in, the inactivity timer will be activated for the new session.

3.2.7 User Lockout

User accounts must be configured to lock out 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 [1-24]**

RP/0/RP0/CPU0:ROUTER(config-pp)#**lockout-time minutes *5 [minutes 5-59, hours 1-23, days 1-225]***

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**

3.3 Network Protocols and Cryptographic Settings

3.3.1 Remote Administration Protocols

Telnet for management purposes is not allowed in the evaluated configuration. The TOE, in FIPS mode, is configured to only allow the permitted data integrity algorithms and cipher suites.

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**

SSH public-key based authentication:

The steps to co-configure the TOE to support public-key based authentication are listed below:

First, the following steps must performed to convert the RSA key into an 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 router and copied into the hard disk by using the following steps:

RP/0/RP0/CPU0:ROUTER#**crypto key import authentication rsa** harddisk:/id_rsa.pub-raw

RP/0/RSP1/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 purposes refer to for more details in chapter "Implementing Secure Shell" of **[5]**.

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 key-exchange algorithms

RP/0/RP0/CPU0:ROUTER(config)#**ssh server algorithms key-exchange diffie-hellman-group14-sha1**

RP/0/RP0/CPU0:ROUTER(config)#**commit**

RP/0/RSP0/CPU0: router #**crypto key gen rsa**

The name for the keys will be the_default. Only 2048 bit modulus allowed while in FIPS mode. Automatically selecting 2048 bit modulus size. Generating RSA keys ...

Done w/ crypto generate keypair [OK]

RP/0/RSP0/CPU0:ROUTER #**config terminal**

RP/0/RSP0/CPU0:ROUTER (config)#**ssh server vrf mgmt**

RP/0/RSP0/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/RSP0/CPU0:ROUTER(config)#**ssh server logging**
RP/0/RSP0/CPU0:ROUTER (config)#**ssh server v2** RP/0/RSP0/CPU0:ROUTER (config)#**commit** RP/0/RSP0/CPU0:ROUTER (config)#**end**

RP/0/RSP0/CPU0:ROUTER (config)#**ssh time-out 60**

RP/0/RSP0/CPU0:ROUTER (config)#**ssh server rekey-time 60**

RP/0/RSP0/CPU0:ROUTER (config)#**ssh server rekey-volume 1024**

The management plane is the logical path of all traffic that is related to the management of a routing platform. In addition, the management plane is used to manage a device through its connection to the network. See the Router System Security Configuration Guide [4] "Management Plane Protection Commands," section “Configuring a Device for Management.”

1. RP/0/RSP0/CPU0:router# **configure**
2. RP/0/RSP0/CPU0:router(config)# **control-plane**
3. RP/0/RSP0/CPU0:router(config-ctrl)# **management-plane**
4. RP/0/RSP0/CPU0:router(config-mpp)# **inband**
5. RP/0/RSP0/CPU0:router(config-mpp-inband)# **interface {type instance | all}**

Ex. RP/0/RSP0/CPU0:router(config-mpp-inband)# interface GigabitEthernet 0/6/0/1

6. RP/0/RSP0/CPU0:router(config-mpp-inband-Gi0_6_0_1)# **allow {protocol | all} [peer]**
   Ex. RP/0/RSP0/CPU0:router(config-mpp-inband-Gi0_6_0_1)# allow sshv2 [peer]
7. RP/0/RSP0/CPU0:router(config-sshv2-peer)# **address ipv4 {peer-ip-address | peer ip- address/length}**
   Ex. RP/0/RSP0/CPU0:router(config-telnet-peer)# address ipv4 10.1.0.0/16
8. RP/0/RSP0/CPU0:ROUTER(config)#**commit**

3.3.2 Logging Configuration

Logging of command execution must be enabled. See chapter "Configuring Logging and Logging Correlation" in **[8]** *System Monitoring Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 Series Routers.*

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: NCS5508 (config)#**logging hostnameprefix TOE: NCS5508**
5. RP/0/RSP0/CPU0: NCS5508 (config)#**service timestamps log datetime year localtime msec**
6. RP/0/RSP0/CPU0: NCS5508 (config)#**service timestamps debug datetime year localtime msec**
7. RP/0/RSP0/CPU0: NCS5508 (config)#**commit**
8. RP/0/RSP0/CPU0: NCS5508 (config)#**end**

3.3.2.1 Logging console on/off

This will turn on logging events to be displayed on 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**

RP/0/RSP0/CPU0:router#(config)# **commit**

Disable the audit events being displayed on the console:

RP/0/RSP0/CPU0:router#(config)#**no logging console**

RP/0/RSP0/CPU0:router#

(config)# **commit**

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 archive**
RP/0/RSP0/CPU0:router(config-logging- arch)# **file-size 10**

3.3.2.3 Change logging severity of audit logs sent to a remote syslog server

The following example shows how to change the configuration logging severity with debugging level severity (level 7):

RP/0/RSP0/CPU0:router# **configure**

RP/0/RSP0/CPU0: NCS5508 (config)# **logging trap debugging**

The following example shows how to reset the configuration log severity to its default value (Informational or level 6):

RP/0/RSP0/CPU0:router# **configure**

RP/0/RSP0/CPU0: NCS5508 (config)#**no logging trap debugging**

3.3.3 Logging Protection

If an authorized administrator wants to back up the logs to a syslog server, protection must be provided for the syslog server communications. If the syslog server is not directly co-located with the TOE, the syslog server must be located in a physically protected facility and connected to a device capable of establishing an secure connection with the TOE. This will protect the syslog records as they traverse the public or non-trusted networks.

4. Secure Management

4.1 User Roles

The TOE differs from IOS in that IOS-XR controls permissions via a usergroup / taskgroup model. Cisco IOS-XR software user attributes form the basis of the Cisco IOS-XR software administrative model. See the **[5]** System Security Configuration Guide chapter "Configuring AAA Services"

Each administrator user is associated with the following attributes:

- User ID - ASCII string that identifies the user uniquely across an administrative domain
- Password - Length limitation of 2 to 253 characters for passwords and one-way encrypted secrets
- Group - List of user groups (at least one) of which the user is a member (thereby enabling attributes such as task IDs). The groups consist of user groups, task groups, and associated task IDs.

The user group concept in IOS-XR relates to a group of users with common characteristics. An administrator user that logs in to an IOS-XR router may have one or more user groups assigned to it. Some user groups exist by default and other custom groups may be configured. **Table** 7 lists the predefined user and task groups in IOS-XR.

Administrator Categories

Router users are classified into the following categories:

- Root system user (complete administrative authority) - 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.
- Root Secure Domain Router (SDR) user (specific SDR administrative authority) - A root SDR user controls the configuration and monitoring of a particular SDR. The root SDR user can create users and configure their privileges within the SDR. Multiple root SDR users can work independently. A single SDR may have more than one root SDR user.
- SDR user (specific SDR user access) - An SDR user has restricted access to an SDR as determined by the root-system user or root SDR user. The SDR user performs the day- to-day system and network management activities. The tasks that the secure domain router user

is allowed to perform are determined by the task IDs associated with the user groups to which the SDR user belongs.

All categories above are considered authorized administrator. Depending on the assigned group the administrator has full or limited control as specified in the User Groups section below.

User Groups

A user group defines a collection of users that share a set of attributes, such as access privileges. Cisco IOS-XR software allows the system administrator to configure groups of users and the job characteristics that are common in groups of users. Users are not assigned to groups by default hence the assignment needs to be done explicitly. A user can be assigned to more than one group. Each user may be associated with one or more user groups. User groups have the following attributes:

- A user group consists of the list of task groups that define the authorization for the users. All tasks, except cisco-support, are permitted by default for root system users.
- Each user task can be assigned read, write, execute, or debug permission.
- Predefined User Groups
- User-Defined User Groups
- User Group Inheritance

Table 7: Predefined User and Task Groups

The Cisco software provides a collection of user groups whose attributes are already defined. The predefined groups are as follows:

User Groups / Task Groups	Purpose	Category
cisco-support	Used by Cisco Support Team. Provides access to troubleshooting commands. / Cisco support personnel tasks	SDR User
provisioning	Provides the ability to display and configure network, files, and user-related entities	SDR User
retrieve	Provides the ability to display network, files, and user-related information	SDR User
netadmin	Provides the ability to control and monitor all system- and network-related parameters.	SDR User
operator	Provides very basic user privileges. / Operator day-to-day tasks	SDR User
read-only-tg	Provides the ability to perform any show command, but no configuration ability	SDR User

root-lr	Provides the ability to control and monitor the specific SDR. / Secure domain router administrator tasks	Root SDR
maintenance	Provides the ability to display, configure and execute commands for network, files, and user-related entities	SDR User
sysadmin	Provides the ability to control and monitor all system parameters but cannot configure network protocols. / System administrator tasks	SDR User
serviceadmin	Provides the ability to service administration tasks, for example, session border controllers (SBC)	SDR User

Administrators can configure their own user groups to meet particular needs.

A user group can derive attributes from another user group. (Similarly, a task group can derive attributes from another task group). For example, when user group A inherits attributes from user group B, the new set of task attributes of the user group A is a union of A and B. The inheritance relationship among user groups is dynamic in the sense that if group A inherits attributes from group B, a change in group B affects group A, even if the group is not re-inherited explicitly.

Task groups are defined by lists of permitted task IDs for each type of action (such as read, write, and so on). The task IDs are basically defined in the router system. The operational tasks that enable users to control, configure, and monitor Cisco software are represented by task IDs. A task ID defines the permission to run an operation for a command. Users are associated with sets of task IDs that define the breadth of their authorized access to the router.

Task IDs

Each user is associated with one or more user groups. Every user group is associated with one or more task groups; in turn, every task group is defined by a set of task IDs. Consequently, a user's association with a particular user group links that user to a particular set of task IDs. A user that is associated with a task ID can execute any operation associated with that task ID.

Table 8: Task ID Classes

Operation	Description
Read	Specifies a designation that permits only a read operation.
Write	Specifies a designation that permits a change operation and implicitly allows a read operation.
Execute	Specifies a designation that permits an access operation; for example, ping.

Debug	Specifies a designation that permits a debug operation.

An administrator can show the tasks associated with a specific user, using the command “show user tasks”. Refer to the Chapter: Authentication, Authorization, and Accounting Commands in the *System Security Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers* for available commands and associated roles and privilege levels.

All task IDs can be found in *System Security Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers*.

When creating a new account with an existing account name, the existing account will be overwritten with the new credentials and privileges given to the new account.

Note: Deleting an administrator account with an active session from another administrator account will not result in the session termination automatically. The administrator deleting the account must first clear the session then delete the account.

4.2 Passwords

The password complexity is not enforced by the router by default but must be administratively set in the configuration. To prevent administrators from choosing insecure passwords, each password must be at least 8 characters long. See the **[5]** *System Security Configuration Guide*, chapter "Configuring AAA Services", section "Configuring Users".

Use the following command to set the minimum length to 8 or greater.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#aaa password-policy policy
RP/0/RSP0/CPU0:router(config)#min-length 8
```

Note: Details for the **security passwords min-length** command can be found in [5] Section configuring AAA Services: Passwords can be composed of any combination of characters that includes characters for at least three of these four character sets: upper case letters, lower case letters, numerals, and the following special characters: “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”. Configure the router to enforce that complexity requirement by using enabling “**special-num**”.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#aaa password-policy policy
  RP/0/RSP0/CPU0:router(config)# special-num
```

To store the passwords securely please use one of the following in order to make the password unreadable:

RP/0/RSP0/CPU0:router(config-un)# {**secret** *5* | **password** *7*}

4.3 Clock Management

Clock management is restricted to the privileged administrator. Use the **clock set** command for initial configuration. The **clock timezone** command should be entered before the clock is set because it defines the difference between the system time and Coordinated Universal Time (UTC). When an authorized administrator sets the time, the router uses the **clock timezone** command setting to translate that time to UTC after the system time is configured. The system internally keeps time in UTC. When you type the **show clock** command, the router displays the system time.

RP/0/RSP0/CPU0:router# **configure**
RP/0/RSP0/CPU0:router(config)# **clock timezone pst -8**
RP/0/RSP0/CPU0:router(config-if)# **commit**
RP/0/RSP0/CPU0:router# **clock update-calendar**

Note: the **clock update-calendar** command updates the hardware clock (calendar clock) with the new clock settings.

To manually set the time of the TOE, the following commands should be used.

RP/0/RSP0/CPU0:router#**clock set hh:mm:ss date month year**

4.3.1 NTP Server

Use of an NTP server is optional. Configuring an NTP Server is described in [4] Configuring Network Time Protocol.

RP/0/RSP0/CPU0:router# **configure**
RP/0/RSP0/CPU0:router(config)# **ntp**
RP/0/RSP0/CPU0:router(config-ntp)# **server** *ip-address* [**vrf** *vrf*] [**version** *number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] **[source** *type interface-path-id*] [**prefer**] [**burst**] [**iburst**]
RP/0/RSP0/CPU0:router(config-ntp)# **peer** *ip-address* [**vrf** *vrf*] [**version** *number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] **[source** *type interface-path-id*] [**prefer**]
RP/0/RSP0/CPU0: router(config-ntp)# **commit**

4.4 Access Control Lists

The TOE may be configured as described in [10] IP Addresses and Services Configuration Guide.

An administrator must create and assign an ACL to an interface before enabling the interface.

Access lists on the TOE use a ternary content-addressable memory (TCAM) (internal and external) to perform the lookup and action resolution on each packet.

A User-Defined TCAM Key (UDK) can be configured using the following command:

hw-module profile tcam format access-list [ipv4 | ipv6] qualifiers [location rack/slot/cpu0]

If you want to use common ACL when a UDK is configured, you can add the common-acl option to the UDK.

The User-Defined Field (UDF) allows you to define a custom qualifier by specifying the location and size of the field, using the following UDF command:

udf udf-name header [inner | outer] [l2 | l3 | l4] offset byte-offset length no
of bytes

The UDF can then be added to a UDK as follows:

hw-module profile tcam format access-list [ipv4 | ipv6] qualifiers [udf1 udf-name udf2 udf-name] [location rack/slot/cpu0]

Note: The maximum of ACEs per ACL should not exceed 2000 per interface.

4.4.1 IPv4 and IPv6 Key

User-defined TCAM key (UDK) definition is supported for ingress, traditional (uncompressed) IPv4 and IPv6 ACLs.

The following table shows the qualifier fields that are supported in the IPv4 and IPv6 key formats.

Table 9: Qualifier Fields Supported in IPv4 and IPv6 Key Formats

Parameter	IPv4	IPv6
Source Address	Enabled	Enabled
Destination Address	Enabled	Enabled
Source Port	Enabled	Enabled

Destination Port	Enabled	Enabled
Port Range	Enabled	Not supported
Protocol/Next Header	Enabled	Enabled
Fragment bit	Enabled	Not supported
Packet length	Disabled	Disabled
Precedence/DSCP	Disabled	Enabled
TCP Flags	Enabled	Enabled
TTL Match	Disabled	Disabled
Interface based	Disabled	Not supported
UDF 1-7	Disabled	Disabled
ACL ID	Enabled	Enabled
common ACL bit	Enabled by default for IPv4/IPv6 on shared mode. Disabled by default for IPv4/IPv6 on unique mode.	Enabled by default for IPv4/IPv6 on shared mode. Disabled by default for IPv4/IPv6 on unique mode.
Interface-based (RIF)	Disabled	Disabled

Table 10: Actions Fields Supported in IPv4 and IPv6 Key Formats

Parameter	IPv4	IPv6
Permit	Enabled	Enabled
Deny	Enabled	Enabled
Log	Enabled	Enabled
Capture	Enabled	Enabled
Stats Counter	Deny stats is always Enabled (permit stats has its own hw-module command)	Deny stats is always Enabled
TTL Set	Enabled	Enabled

To enable the monitoring of the packet count that is permitted based on the ACL rules, use the following configuration, and then reload the line card or router as required:

```
/* Enable an egress ACL on on a hardware module profile. */
Router(config)# hw-module profile acl egress layer3 interface-based

Router(config)# commit
Router(config)# end
Router# reload location all
```

To edit the ACL configuration, remove the hw-module configuration, edit the ACL configuration, and then enable the hw-module configuration again.

To Configure IPv4 ACLs and IPv6 see [10] sections, Configuring IPv4 ACLs and Configuring IPv4 ACLs.

The Network Stack IPv4 and IPv6 features are used to configure and monitor Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6). These are described in 10] section Implementing Network Stack IPv4 and IPv6.

4.5 Login Banners

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

```
RP/0/RSP0/CPU0:ROUTER(config)#banner motd c THIS IS THE MOTD BANNER
c
RP/0/RSP0/CPU0:ROUTER(config)#banner exec c THIS IS THE EXEC BANNER c
RP/0/RSP0/CPU0:ROUTER(config)#banner login c THIS IS THE LOGIN BANNER
c
RP/0/RSP0/CPU0:ROUTER(config)#commit
RP/0/RSP0/CPU0:ROUTER (config)#end
```

where c is the delimiting character. The delimiting character may be any character except "?", and it must not be part of the banner message.

4.6 Product Updates

The chapter "Perform System Upgrade and Install Feature Packages" in [6] lists the detailed steps necessary to install packages and perform software upgrades.

Here's the summary of steps necessary to upgrading the software on the router:

1. Execute:
   - **install add source** *<ftp or 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*
    - **install activate id** *operation_id*
6. **show install active**
7. **install commit**

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

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 details for protection of that communication are covered in Section 3.3.3.

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.

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, it overwrites older events. Table 11 below includes 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 with 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 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.

To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled and the audit records are being generated for the required auditable events.

Additional Audit Information is described in Column 3 of Table 12 below.

Table 11: Auditable Events

Security Functional Requirement	Auditable Event	Additional Audit Record Contents
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UID.2	All use of the identification mechanism.	Provided user identity, origin of the attempt (e.g., IP address).

Security Functional Requirement	Auditable Event	Additional Audit Record Contents
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	None
FMT_MTD.1	All modifications to the values of TSF data	The identity of the authorized administrator performing the operation.
FMT_SMF.1	Use of the management functions	The identity of the authorized administrator performing the operation.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	None
FTP_TRP.1	Attempts to use the trusted path functions.	Identification of the user associated with all trusted path invocations including failures, if available.

5.3 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.

6. 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 have 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. the 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, thus 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 has little interaction with the administrator. The configuration of the router can, however, 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.

To ensure the correct image is booted on startup use the boot system command:

> RP/0/RSP0/CPU0:router# **system boot-sequence** { *primary-device [secondary-device]* **| disable** } [**location** { *node-id* **| all** }]

It should be noted that while no administrator password is required to enter ROM monitor mode, physical access to the router is required; the router should, therefore, 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 is if there is an error during the POST during bootup; if there is an error during POST, 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. The same cryptographic POSTs can also be run on demand as described in Section 3.2.3; when the tests are run on demand after system startup has completed (and the syslog daemon has started), error messages will be written to the log.

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

7. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. Table 13 identifies the requirements and the associated security measures of the authorized users.

Table 12 Environment Objectives

Security Objective for the Operational Environment (from the Security Target)	**Definition of the Security Objective** (from the Security Target)	**Responsibility of the Administrators**
OE.ADMIN	The Authorized Administrator are well trained and trusted to manage the TOE and to configure the IT environment and required non-TOE devices for the proper network support.	Authorized Administrators must be trained and must read, understand and follow the guidance in this document to securely install and operate the TOE.
OE.CONNECTION	The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.	Authorized Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE.
OE.LOCATE	The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.	The TOE and the operational environment components must be installed in a controlled environment where access is controlled. The Authorized Administrator is responsible for the secure operation of the TOE. While the Authorized Administrator may be assigned responsibility of some or all of the operational environment components, that responsibility is not covered by this document unless specifically document within. The operational environment components include the following: Remote administration of the TOE using the CLI, this remote connection is secured with SSHv2,

		NTP for timestamp synchronization.
OE.PHYSEC	The operational environment of the TOE shall have a physical security policy preventing unauthorized physical access to the TOE. The policy must document physical security controls including access control, physical separation of hardware, and monitoring policies to ensure no unauthorized physical access to the TOE is allowed.	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 [this document, Sect. 7]. The Administrator must ensure that a security policy describing the physical security controls to prevent the unauthorized physical access to the TOE is produced and has been implemented to ensure only authorised physical access to the TOE is allowed.

8. Related Documentation

Use this document in conjunction with the Network Convergence System documentation at the following location:

- IOS XR v7.4 documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

8.1 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 the following sites:

- http://www.cisco.com

8.2 Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

8.3 Documentation Feedback

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

You can email 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.

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

We appreciate your comments.

9. 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 provide 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