Cisco Nexus 9000 Series Switches running NX-OS 10.4

Common Criteria Operational User Guidance and Preparative Procedures

Version: 1.6

Date: 11/6/2025

Americas Headquarters:

Error! Unknown document property name., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Figures

Acronyms

The following acronyms and abbreviations are used in this document:

Table 1: Acronyms

Acronyms / Abbreviations	Definition
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IT	Information Technology
NDcPP	Network Device collaborative Protection Profile
OS	Operating System
PP	Protection Profile
SHS	Secure Hash Standard
SSHv2	Secure Shell (version 2)
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User datagram protocol
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

Terminology

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

Table 2: Terminology

Term	Definition
Authorized Administrator	A person that has authorized access to the TOE to perform configuration and management tasks.
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.

DOCUMENT INTRODUCTION

Prepared By:

Cisco Systems, Inc.

170 West Tasman Dr.

San Jose, CA 95134

This document provides the basis for administration of the Cisco Nexus 9000 Series Switches (Cisco Nexus 9K Series). This Operational User Guidance and Preparative Procedures (AGD) defines the specific TOE configuration and administrator functions, and interfaces, that are necessary to configure and maintain the TOE in the evaluated configuration. All security relevant commands to manage the TSF data are provided within this documentation.

Revision History

Date	Version	Author	Comment
25-01-21	0.9	Cisco Systems Inc.	Published in support of CCEVS-VR-VID11514-2025
25-04-16	1.2	Cisco Systems Inc.	Updated formatting; Convert to NDcPPv3.0e requirements Internal Review

25-04-24	1.3	Cisco Systems Inc.	Format updates;
			Updated FAU_GEN table for NDcPP3.0e;

06-11-25	1.6	Cisco Systems Inc.	Addressing EM1+EM2 and lab comments

1 Introduction

This Operational User Guidance and Preparative Procedures documents the administration of the Cisco Nexus 9000 Series Switches running on Cisco NX-OS 10.4 (herein after referred to as Cisco Nexus 9K Series), TOE, certified under Common Criteria. The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 9200, 9300, 9400, 9500 and 9800. The software is comprised of the NX-OS software image Release 10.4.

The Cisco Nexus 9K Series may be referenced below by the model number series related acronym ex. Nexus 9000 Series, TOE, or Nexus 9K.

1.1 Audience

This document is written for administrators configuring the TOE., specifically the NX-OS 10.4 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 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 on 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 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 Nexus 9K Series 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. Throughout this document, the guides will be referred to by the "#", such as **[4]**.

The [ST] can be obtained at https://www.niap-ccevs.org/products by searching for the TOE, which is the Cisco Nexus 9000 Series Switches. Products currently in evaluation can be viewed on the NIAP Products in Evaluation page, and certified Cisco products can be viewed on the Product Compliance List.

[AGD]s for Cisco products can also be obtained in the Global Government Certifications section at https://www.cisco.com. Full link is below:

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

Table 3: Cisco Documentation

#	Title	Link
[1]	Cisco Nexus 9000 Series Switches Security Target, (Current Version)	Cisco Nexus 9000 Series Switches Running NX-OS 10.4 Security Target
[2]	Cisco Nexus 9000 Series System Management Configuration Guide	Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.4(x)
[3]	Cisco Nexus 9000 Series Security Configuration Guide	Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.4(x)
[4]	Cisco Nexus 9000 Series Fundamentals Configuration Guide	Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 10.4(x)
[5]	Cisco Nexus 9000 Series Command Reference, Release 10.4(x)	Cisco Nexus 9000 Series NX-OS Command Reference (Config Commands), Release 10.4(x) Cisco Nexus 9000 Series NX-OS Command Reference (Show Commands), Release 10.4(x)
[6]	Cisco Nexus 9000 Switch Hardware Installation Guides	**Cisco Nexus 9200 Models:** Cisco Nexus 92348GC-X NX-OS Mode Switch Hardware Installation Guide **Cisco Nexus 9300 Models:** Cisco Nexus 93108TC-FX NX-OS Mode Hardware Installation Guide

#	Title	Link
		Cisco Nexus 9348GC-FX3PH NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 93216TC-FX2 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 93180YC-FX NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 93240YC-FX2 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 93360YC-FX2 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9364C NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9332C NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9336C-FX2 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9364C-GX NX-OS Mode Switch Hardware Installation Guide Cisco Nexus C9316D-GX NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 93600CD-GX NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 93400LD-H1 NX-OS Mode Switch Hardware Installation Guide **Cisco Nexus 9400 Models:** Cisco Nexus 9408 NX-OS Mode Switch Hardware Installation Guide **Cisco Nexus 9500 Models:** Cisco Nexus 9504 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9508 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9516 NX-OS Mode Switch Hardware Installation Guide **Cisco Nexus 9800 Models:** Cisco Nexus 9804 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9808 NX-OS Mode Switch Hardware Installation Guide

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.

Table 4: Supported Hardware

Hardware	Models (PID)
Cisco Nexus 9200 Series	Nexus 92348GC-X (N9K-C92348GC-X)
Cisco Nexus 9300 Series	Nexus 9348GC-FXP (N9K-C9348GC-FXP) Nexus 93216TC-FX2 (N9K-C93216TC-FX2) Nexus 93180YC-FX (N9K-C93180YC-FX) Nexus 93240YC-FX2 (N9K-C93240YC-FX2) Nexus 93360YC-FX2 (N9K-C93360YC-FX2) Nexus 9364C (N9K-C9364C) Nexus 9332C (N9K-C9332C) Nexus 9336C-FX2 (N9K-C9336C-FX2) Nexus 9364C-GX (N9K-C9364C-GX) Nexus 9316D-GX (N9K-C9316D-GX) Nexus 93600CD-GX (N9K-C93600CD-GX) Nexus 93400LD-H1 (N9K-C93400LD-H1)
Cisco Nexus 9400 Series	Nexus 9408 (N9K-C9408) Supervisor 9400-Sup-A (N9K-SUP-A)
Cisco Nexus 9500 Series	Nexus 9504 (N9K-C9504) Nexus 9508 (N9K-C9508) Nexus 9516 (N9K-C9516) Supervisor 9500-Sup-A+ (N9K-SUP-A+) Supervisor 9500-Sup-B+ (N9K-SUP-B+) System Controller N9k-SC-A (N9K-SC-A)
Cisco Nexus 9800 Series	Nexus 9808 (N9K-C9808) Nexus 9804 + fabric module + fan tray (N9K-C9804) + (N9K-C9804-FM-A) + (N9K-C9804-FAN-A) Nexus 9800 36-port + 34-port (N9K-X9836DM-A) + (N9K-X98900CD-A)

Table 5: Supported Software

Software	Version
Cisco NX-OS	10.4

1.4.1 Supported Configurations

The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 9200, 9300, 9400, 9500 and 9800. The software is comprised of the NX-OS software image Release 10.4.

The TOE is a storage networking-class switch for use in small fabrics and large data centers with state-of-the-art multiprotocol and distributed multiservice convergence. It provides multilayer support, greater performance and enhanced operations through features including intelligent services, programmability, automation, analytics, and manageability.

Cisco NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although NX-OS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in this document.

1.5 IT 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:

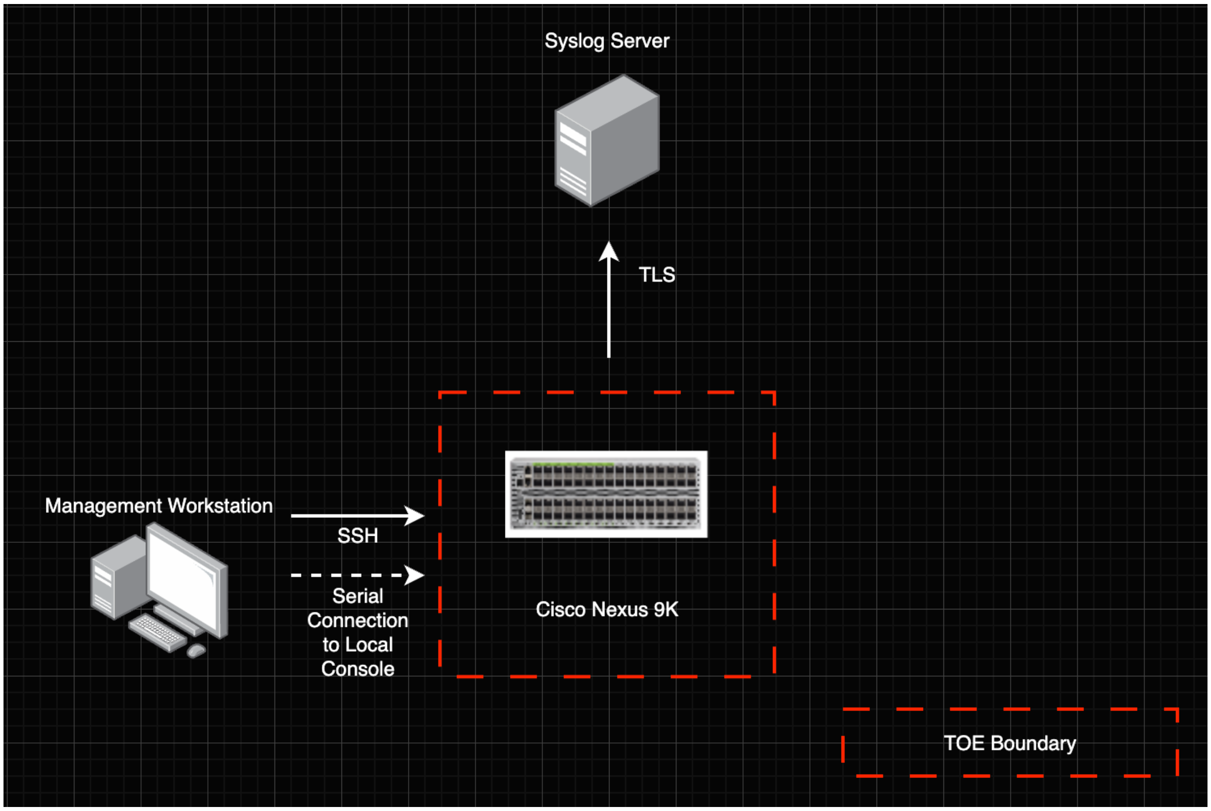
Table 6: Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
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. This interface is accessible and available locally even if the network were to go down.
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.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.

1.6 Example Target of Evaluation Deployment

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

Figure 1: Nexus 9000 Series Switches TOE and Environment



The figure above includes the following:

- The TOE model:
    - Cisco Nexus 9000 Series Switch

The following are considered to be in the Operational Environment:

- Management Workstation
- Syslog Server

For management purposes the TOE provides command line access to administer the TOE.

1.7 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.
Bash Shell	Bash shell interface was not included in the evaluation.
DCNM GUI	The DCNM GUI was not included in the evaluated configuration.
HTTP / HTTPS	HTTP / HTTPS was not included in the evaluation. It must be configured to tunnel using SSH as specified in the AGD.
HTTP Server	The HTTP web server is disabled in the evaluated configuration.
IKE	IKE was not included in the evaluation. It must be configured to tunnel using TLS as specified in the AGD.
IPsec	IPsec is not included in the evaluated configuration.
LDAP	LDAP is not included in the evaluated configuration.
NTP	NTP is disabled in the evaluated configuration.
PTP	PTP is not included in the evaluation.
RADIUS	RADIUS is not included in the evaluation.
SNMP	SNMP is disabled in the evaluated configuration.
TACACS+	TACACS+ is disabled in the evaluated configuration.
Telnet	Telnet is disabled in the evaluated configuration.

These services are disabled by configuration.

2 Secure Acceptance of the TOE

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

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

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

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

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

Step 4 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 **Cisco Nexus 9K Series**, 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

Model
Cisco Nexus 9200 models
Cisco Nexus 92348GC-X Switch
Cisco Nexus 9300 models
Cisco Nexus 9348GC-FXP Switch
Cisco Nexus 93216TC-FX2 Switch
Cisco Nexus 93180YC-FX Switch
Cisco Nexus 93240YC-FX2 Switch
Cisco Nexus 93360YC-FX2 Switch
Cisco Nexus 9364C Switch
Cisco Nexus 9332C Switch
Cisco Nexus 9336C-FX2 Switch
Cisco Nexus 9364C-GX Switch
Cisco Nexus 9316D-GX Switch
Cisco Nexus 93600CD-GX Switch
Cisco Nexus 93400LD-H1 Switch
Cisco Nexus 9400 models
Cisco Nexus 9408 Switch
Cisco Nexus 9500 models
Cisco Nexus 9504 Switch
Cisco Nexus 9508 Switch
Cisco Nexus 9516 Switch
Cisco Nexus 9500 modules
Supervisor 9500-Sup-A+
Supervisor 9500-Sup-B+

Model
System Controller N9k-SC-A
Cisco Nexus 9800 models
Cisco Nexus 9804 Switch
Cisco Nexus 9804 modules
Nexus 9800 4-slot chassis fabric module (1st Generation)
Nexus 9800 4-slot chassis fan tray (1st Generation)
Cisco Nexus 9808 Switch
Cisco Nexus 9800 modules
Nexus 9800 36-port 400G Line Card
Nexus 9800 34-port 100G + 14-port 400G Line Card

Step 7 Approved methods for obtaining a Common Criteria evaluated software images:

- 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

- 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 comparing the SHA-512 digital signature that is listed on the Cisco web site and in Table 9: Evaluated Software Images below, by using the show software authenticity file command, or using the show file command on the Cisco Nexus 9K Series. The "show software authenticity file *filename*" command on the Cisco Nexus 9K Series can be used to verify the digital signature of the image.

```
switch# show software authenticity file bootflash: nxos64-cs.10.4.5.M.bin
```

Refer to section "Displaying File Checksums" in **[4]**. If the signatures do not match, contact Cisco Technical Assistance Center (TAC).

Step 9 Install the downloaded and verified software image onto your Cisco Nexus 9K Series.

```
switch# install all nxos bootflash:nxos64-cs.10.4.5.M.bin
```

Start your TOE, as described in **[4]**. Confirm that TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console. The TOE implements digital signature verification on the image being installed and will cancel the update process if the signature fails validation. If the update process fails, contact Cisco Technical Assistance Center (TAC).

Power Up the TOE:

- Power up the TOE by connecting each installed power supply to an AC circuit. If you are using the input-source (*n*+*n*) power mode, connect half of the power supplies to one AC circuit. Connect the other half of the power supplies to another AC circuit. The Input and Output LEDs on each power supply light up (green) when the power supply units are sending power to the switch.

- During Initialization of the TOE, the following will be displayed:

```
Loading from ROMMON with a System Image in Bootflash
```

- When initialization is complete, the following will be displayed:

```
Press RETURN to get started!
```

See **Section 3.2 below** for the initial device setup over the direct console connection once the device is initialized.

NOTE: *If an update fails, the TOE outputs the reason for failure on the CLI and records audit data:*

```
[#                   ]   0% -- FAIL.
Return code 0x40450030 (Digital signature verification failed).
Pre-upgrade check failed. Return code 0x40930011 (Image verification failed).

2024 Dec  5 14:46:09 UTC N9k-C9332D-Lower %AAA-6-AAA_ACCOUNTING_MESSAGE:
update:172.18.152.235@pts/6:admin:install all nxos bootflash:/nxos64-
cs.10.4.5.M.bin.corrupt (FAILURE)

2024 Dec  5 14:51:00 UTC N9k-C9332D-Lower %SYSMGR-3-SERVICE_TERMINATED:
Service "installer" (PID 2591) has finished with error code
SYSMGR_EXITCODE_SYSERR (1).
```

For further analysis of an upgrade failure, use the "show tech-support install" and command:

```
2 Install operation 2 by user 'admin' at Mon Dec  2 12:45:02 2024
```

```
Install add bootflash :nxos64-cs.x.x.x.bin
Start downloading the image.
File downloaded successfully
Verify Patch digital signature
Patch digital signature OK
Patch md5 OK
Verifying Software Compatibility
Verifying Hardware Compatibility
Hardware Compatibility OK
Checking for duplicate package
failure reason:Please remove existing SMU before adding the new one
Install operation 2  "failed because this patch already exists.". at Mon Dec
2 12:45:05 2024
```

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 **[6]** to display the currently running system image filename and the system software release version. See below for the detailed signature value that must be checked to ensure the software has not been modified in anyway.

Table 9: Evaluated Software Images

Model	Software Version	Image Name	SHA 512
N9K-C92348GC-X	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9348GC-FXP	NX-OS 10.4	nxos64-cs.10.4.5.M.bin &	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C93216TC-FX2	NX-OS 10.4	nxos64-cs.10.4.5.M.bin &	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C93180YC-FX	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C93240YC-FX2	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f

Model	Software Version	Image Name	SHA 512
N9K-C93360YC-FX2	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9364C	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9332C	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9336C-FX2	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9364C-GX	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9316D-GX	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C93600CD-GX	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-93400LD-H1	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9408	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f
N9K-C9504	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5d59b728e09a408478305057cc4303f53324f12968c37b9476b22e0c152c9897177c265ff8cda01390618c3605f9d978f

Model	Software Version	Image Name	SHA 512
N9K-C9508	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5 d59b728e09a408478305057cc4303f5 3324f12968c37b9476b22e0c152c9897 177c265ff8cda01390618c3605f9d978f
N9K-C9516	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5 d59b728e09a408478305057cc4303f5 3324f12968c37b9476b22e0c152c9897 177c265ff8cda01390618c3605f9d978f
N9K-C9804	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5 d59b728e09a408478305057cc4303f5 3324f12968c37b9476b22e0c152c9897 177c265ff8cda01390618c3605f9d978f
N9K-C9808	NX-OS 10.4	nxos64-cs.10.4.5.M.bin	2b51f7ca822ad64a142e4f29a11973e5 d59b728e09a408478305057cc4303f5 3324f12968c37b9476b22e0c152c9897 177c265ff8cda01390618c3605f9d978f

When updates, including psirts (bug fixes) to the evaluated imagine 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.

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 that 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 can 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 switch 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 TOE can also be configured to lock the Authorized Administrator account after a specified number of failed login attempts until an authorized administrator can enable the user account. The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

- **Trusted Path/Channel** - allows trusted channels to be established to itself from remote administrators over SSHv2 for CLI access.

3.1 Physical Installation

Follow the *Cisco Nexus 9000 Switch Hardware Installation Guides* **[6]** for hardware installation instructions. Follow these directions for connecting all Nexus 9K Series models.

3.2 Initial Setup via Direct Console Connection

The TOE must be given basic configuration via console connection prior to being connected to any network. The TOE includes an NX-OS Setup Utility that automatically starts upon first booting up the Nexus 9K switch.

The console port is an asynchronous serial port that allows you to connect to the device for initial configuration through a standard RS-232 port with an RJ-45 connector. Any device connected to this port must be capable of asynchronous transmission. Default parameters for your terminal emulator must be configured with the following:

- 9600 baud, 8 data bits, 1 stop bit, and no parity.

3.2.1 Options to be chosen during the initial setup of the Nexus 9K Series

For an un-configured TOE, the setup utility will automatically run a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module. The IP address can only be configured from the CLI. When you power up the switch for the first time assign the IP address. After you perform this step, the Cisco Nexus 9000 Family Fabric Manager can reach the switch through the console port.

To run the setup utility once a switch has already been configured simply execute the "setup" command at the CLI. When setup is initiated, it presents the System Configuration Dialog. This dialog guides the administrator through the initial configuration with prompts for basic information about the TOE and network and then creates an initial configuration file. After the file is created, an authorized administrator can use the CLI to perform additional configuration. For initial setup, follow the directions in Chapter 3 of the *Cisco Nexus 9000 Series Fundamentals Configuration Guide* **[4]** section "*Setting Up Your Cisco NX-OS Device".* The following items must be noted during setup:

1. (Step 2 of Setup Utility) NOTE that secure password standard is optional and wasn't CC-evaluated.

```
Do you want to enforce secure password standard (yes/no): yes
```

To enable password-strength checking after initial TOE setup, use the '`password strength-check`' command.

```
switch# configure terminal
switch(config)# password strength-check
switch(config)# exit
```

2. **(Step 3 of Setup Utility)** Enter the new password for the administrator.

```
Enter the password for admin: admin-password
```

```
Confirm the password for admin: admin-password
```

3. (Step 6 of Setup Utility) Do **NOT** configure the SNMP community string. SNMP management is **not allowed** in the TOE.

NOTE: *The use of SNMP (any version) is outside the scope of NDcPP and was not CC-evaluated.*

4. (Step 7 of Setup Utility) Enter a name for the switch.

Note: *The switch name is limited to 32 alphanumeric characters. The default name is* `switch`*.*

```
Enter the switch name: switch_name
```

5. (Step 8 of Setup Utility) Enter yes (yes is the default) at the configuration prompt to configure out-of-band management.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
```

Enter the mgmt0 IPv4 address:

```
Mgmt0 IPv4 address: ip_address
```

Enter the mgmt0 IPv4 subnet mask:

```
Mgmt0 IPv4 netmask: subnet_mask
```

6. (Step 9 of Setup Utility) Enter yes (yes is the default) to configure the default gateway.

```
Configure the default-gateway: (yes/no) [y]: yes
```

Enter the default gateway IP address.

```
IP address of the default gateway: default_gateway
```

7. (Step 10 of Setup Utility) Enter yes (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

```
Configure Advanced IP options (yes/no)? [n]: yes
```

Note: *No is the default here. However, if you choose not to configure the advanced IP options you will proceed to Step 11.*

8. (Step 11 of Setup Utility) Enter yes (yes is the default) to enable the SSH service.

```
Enabled SSH service? (yes/no) [n]: yes
```

Enter the SSH key type.

```
Type the SSH key you would like to generate (dsa/rsa)? rsa
```

Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768-2048) [1024]: 2048
```

9. **(Step 12 of Setup Utility)** Disable the Telnet service. Ensure that the telnet service is **NOT** enabled by changing the selection to **no**.

```
Enable the telnet service? (yes/no) [y]: no
```

10. (Step 17 of Setup Utility) Do **NOT** enable ntp, so hit enter and accept the default.

```
Configure NTP server? (yes/no) [n]: no
```

11. (Step 26 of Setup Utility) Save configuration. If you do not save the configuration at this point, none of the changes are part of the configuration when the device reboots.

```
Use this configuration and save it? (yes/no) [y]: yes
```

3.2.2 Saving Configuration

NX-OS uses both a running configuration and a startup configuration. Configuration changes affect the running configuration. To save that configuration, the running configuration (held in memory) must be copied to the startup configuration. This may be achieved by using the following command **[4]**, see section "Copying Configuration Files" and "Backing Up Configuration Files":

```
switch# copy nvram:snapshot-config nvram:startup-config
Warning: this command is going to overwrite your current startup-config:
Do you wish to continue? {y/n} [y] y
```

Note: *A shorthand version of the command is **copy run start**.*

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

3.2.3 Installing Security Patches

The Nexus 9K will also need to install the following security patches in order to be in the evaluated configuration:

```
nxos64-cs.CSCwm97343-1.0.0-10.4.5.lib32_64_n9000.rpm
```

To install these security patches, the administrator may use the following commands on the TOE:

```
switch# install add bootflash:nxos64-cs.CSCwm97343-1.0.0-
10.4.5.lib32_64_n9000.rpm activate
```

After the TOE reboots to complete the install process, run the following to commit the package to the startup configuration:

```
switch# install commit nxos64-cs.CSCwm97343-1.0.0-10.4.5.lib32_64_n9000.rpm
switch# copy run start
```

NOTE: *This process must be run for each package being installed.*

3.2.4 Modes of Operation

A Cisco Nexus 9K Series Family Switch has several modes of operation. These modes are as follows:

Booting – while booting, the switches drop all network traffic until the NX-OS image and configuration has loaded. This mode can transition to all the modes below.

BIOS Loader Prompt – When the supervisor modules power up, a specialized BIOS image automatically loads and tries to locate a valid kickstart image for booting the system. If a valid kickstart image is not found, the following BIOS loader prompt displays:

```
loader>
```

System BIOS Setup – This is an interactive text-based program for configuring low-level switch hardware and boot options. When this program is exited, the switch transitions to Booting mode. In this mode the switch has no IP address and therefore does not handle network traffic, thus preventing an insecure state.

Loader Prompt – This mode allows an administrator logged into the local console port to specify a NX-OS image that located on a remote TFTP server. This allows the administrators to use remote repositories to retrieve and store NX images. In this mode, the switch does not handle any network traffic, apart from what is required to perform the TFTP boot, thus preventing an insecure state.

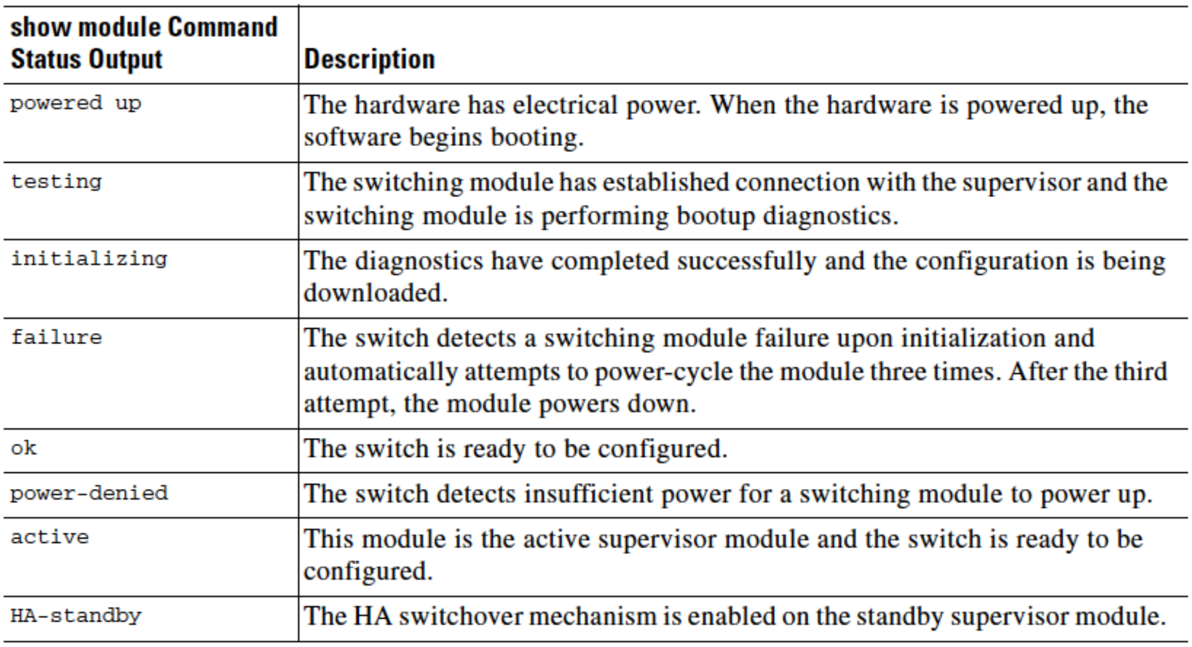
Setup – The switch enters this mode after booting if no configuration exists (eg. First boot). In this mode the switch has no IP address and therefore does not handle network traffic, thus preventing an insecure state. The switch starts an interactive setup program to allow the administrator to enter basic configuration data, such as the switch's IP address, administrator password, and management channels. When the setup program is exited, the switch transitions to the Normal mode.

Normal - The NX-OS image and configuration is loaded, and the switch is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all TOE security functions are operating as configured.

3.2.4.1 Module States

The Nexus 9K Series switches can be deployed with a single or redundant pair of supervisors. The supervisor modules have some additional module states. The '**show module**' command shows the status of the supervisor or I/O cards.

Table 10: Module States



show module Command Status Output	Description
`powered up`	The hardware has electrical power. When the hardware is powered up, the software begins booting.
`testing`	The switching module has established connection with the supervisor and the switching module is performing bootup diagnostics.
`initializing`	The diagnostics have completed successfully and the configuration is being downloaded.
`failure`	The switch detects a switching module failure upon initialization and automatically attempts to power-cycle the module three times. After the third attempt, the module powers down.
`ok`	The switch is ready to be configured.
`power-denied`	The switch detects insufficient power for a switching module to power up.
`active`	This module is the active supervisor module and the switch is ready to be configured.
`HA-standby`	The HA switchover mechanism is enabled on the standby supervisor module.

Table 11: Redundancy Modes: for Supervisor

Mode	Description
Not present	The supervisor module is not present or is not plugged into the chassis.
Initializing	The diagnostics have passed and the configuration is being downloaded.
Active	The active supervisor module and the switch is ready to be configured.
Standby	A switchover is possible.

Failed	The switch detects a supervisor module failure on initialization and automatically attempts to power-cycle the module three (3) times. After the third attempt it continues to display a failed state.
Offline	The supervisor module is intentionally shut down for debugging purposes.
At BIOS	The switch has established connection with the supervisor and the supervisor module is performing diagnostics.
Unknown	The switch is in an invalid state. If it persists call TAC.

3.2.5 Enabling FIPS/CC Mode

In the evaluated configuration the TOE is run in the FIPS and CC mode of operation. The FIPS mode disables the use of weak algorithms and cryptographic keys on the TOE and allows for KAT self-tests to be run. By default, FIPS mode is disabled. The CC mode disables the use of TLS 1.3 version for the TLS syslog communication. Both '`fips mode enable`' and '`system security compliance common-criteria`' commands need to be ran in order to turn on FIPS/CC mode. A reload is required for the system to operate in FIPS/CC mode.

Follow these guidelines before enabling FIPS/CC mode:

- Make your passwords a minimum of eight characters in length.
- Disable Telnet. Administrators should log in using SSH only.
- Disable remote authentication through RADIUS/TACACS+. Only users local to the switch can be authenticated.
- Disable SNMP v1 and v2. Any existing user accounts on the switch that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy. **NOTE** that the use of SNMP (any version) is outside the scope of NDcPP and was not CC-evaluated.
- Disable VRRP.
- Delete all SSH Server RSA1 keypairs.

To enable FIPS mode, follow the steps below:

```
switch# configure terminal
switch (config)# fips mode enable
switch (config)# exit
switch# show fips status
FIPS mode is enabled
switch#
```

Then, follow the steps below to enable CC mode:

```
switch# configure terminal
switch# system security compliance common-criteria
switch# show system security common-criteria
Common-Criteria status: enabled
switch# copy running-config startup-config
switch# reload
```

Refer to the command reference [**5**] and *Cisco Nexus 9000 Series Security Configuration Guide* **[3]** in Chapter "*Configuring FIPS*" Section "*Enabling FIPS Mode*".

3.2.5.1 Administration of Cryptographic Self-Tests

The TOE provides self-tests consistent with the FIPS 140-3 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 supervisor and line card modules. These self-tests include the following:

- AES Known Answer Test
- HMAC Known Answer Test
- RNG/DRBG Known Answer Test
- SHA-1/SHA-256/SHA-384/SHA-512 Known Answer Test
- RSA Signature Known Answer Test (both signature/verification)
- Software Integrity Test

During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). Also, during the initialization and self-tests, the module inhibits all access to the cryptographic algorithms. Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing self-tests and entering FIPS mode. In the event of a power-on self-test failure, the cryptographic module will force the IOS 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 - Involves verifying the integrity of the loaded software image by checking its digital signature against a trust local key. This test happens automatically at start-up.

Note: *Once all FIPS self-tests are successful, system logs are generated stating that FIPS mode has been initialized and enabled.*

Example FIPS Messages:

```
%CERT_ENROLL-6-CERT_EN_MESSAGE: FIPS register succeeded
%DAEMON-6-SYSTEM_MSG: <<%FIPS-6-SET_FIPS_MODE>> FIPS mode is Enabled for
service Syslog Sup Node Cfg - syslogd[14561]
%USER-2-SYSTEM_MSG: FIPS mode is Enabled for service securityd - securityd
%AUTH-6-SYSTEM_MSG: Operating in CiscoSSL FIPS mode - dcos_sshd[27914]
```

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 switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it must be rebooted. However, once the switch 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]
```

The system log above shows the FIPS self-test failed [chars] for service [chars].

3.2.5.2 Self-Tests

When the system is booted up self-tests are automatically run. The power-up self-tests run on the supervisor and 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 switch is in the error state, any reload of a line card moves it to the failure state. To move the switch back to operational mode, it must be rebooted. However, once the switch 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:

- Restart the TOE to perform POST and determine if normal operation can be resumed.
    - If the problem persists, contact Cisco Technical Assistance via:
    - https://mycase.cloudapps.cisco.com/case or 1 800 553-2447

3.2.6 Administrator Configuration and Credentials

The Cisco Nexus 9K Series must be configured to use a username and password for each administrator and one password for the enable command. There are three possible passwords: enable password, enable secret, and virtual terminal (vty) password. Enable password provides the local console password for accessing the User mode.

Warning: If an unprivileged administrator user has this password and has access to the local console, they will be able to issues all commands.

3.2.6.1 Assigning User Roles

NOTE: *In the CC-evaluated configuration, all roles and privileges are considered to be authorized administrators.*

All NX-OS administrators will have a role assigned to them. See *Cisco Nexus 9000 Series Command Reference* **[5]** for the following commands.

User accounts have the following main attributes:

- Username
- Password
- Expiry date
- User roles

An authorized administrator can enter the password in clear text format [*0*] or encrypted format [*5*]. Starting from NX-OS Release 8.2(1), user accounts will have passwords encrypted with SHA-2 by default. Encrypted format passwords are saved to the running configuration without further encryption.

You can configure up to a maximum of 256 user accounts. By default, the user account does not expire unless you explicitly configure it to expire. The expire option determines the date when the user account is disabled. The following words are reserved and cannot be used to configure users:

bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Cisco NX-OS supports user names that are created with alphanumeric characters or specific special characters (+ [plus], = [equal], _ [underscore], - [hyphen], \ [backslash], and . [period]) when created locally, provided that the user name starts with an alphanumeric character. Local user names cannot be created with any special characters (apart from those specified). "**5**" specifies that the password is in encrypted format.

```
switch(config)# username name password [0|5|7] user-password [role role-name]
```

Note: *If no role-name is specified the account will be assigned the default role, network-admin.*

Example:

```
switch(config)# username NewUser password 5 4Ty18Rnt@ role network-admin
switch(config)# exit
switch(config)# (Optional) copy running-config startup-config
```

Each user role can have up to 16 rules. The rule number that an administrator specifies determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1. Regardless of the read-write rule configured for a user role, some commands can only be executed through the predefined network-admin role. For more information on user roles, see the Cisco Nexus 9000 Series Command Reference **[5]** and section "Configure Roles" **[3]**.

3.2.7 Password Length

To prevent administrators from choosing insecure passwords, each password must be at least 8 characters long and can be a maximum of 127 characters.

Password strength checking can be enabled, but this is ***optional***. This setting prevents you from creating weak passwords for user accounts. A strong password has the following characteristics:

- Is at least eight characters long
- Does not contain many consecutive characters (such as abcd)
- Does not contain many repeating characters (such as aaabbb)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Optional: To configure password strength checking, follow these steps:

```
switch# configure terminal
switch(config)# password strength-check
switch(config)# end
switch# copy running-config startup-config
```

With this enabled, the TOE enforces a minimum of 8 characters in a user password with characters from at least 3 of the following classes required:

- Lower-case letters
- Upper-case letters
- Digits and special characters

Note: *These settings are applied to all new passwords, not to existing passwords.*

To enable restricted password length on the TOE, follow the steps below:

```
switch# configure terminal
switch(config)# userpassphrase min-length 15 max-length 15
switch(config)# exit
```

The TOE allows for passwords to be composed of any combination of upper- and lower-case letters, numbers, and the following special characters: “@”, “$”, “%”, “^”, “&”, “*”, “(“, “)”,[“+”, “=”, “_”, “-“, “\”, and “.”.

3.2.8 Session Termination

Inactivity settings must trigger termination of the administrator session. These settings are configurable with the “*exec-timeout*” command shown below:

Note: *“line console” configures the local console session timeout and “line vty” configures SSH.*

```
switch# configure terminal
switch(config)# line console
switch(config-console)# exec-timeout minutes
…
switch# configure terminal
switch(config)# line vty
switch(config-console)# exec-timeout minutes
```

The range for `minutes` is from 0 to 525600 minutes. A value of 0 minutes disables the session timeout and therefore should not be used ensure an inactivity timeout is enforced. The default is 30 minutes.

Configuration of these settings is limited to the privileged administrator (see Section 4).

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

To manually log out of a CLI session (console or SSH), use the “exit” command once in EXEC mode. The “end” command will return the user back to EXEC mode from any configuration mode that they may be in.

3.3 Network Protocols and Cryptographic Settings

3.3.1 Remote Administration Protocols

By default, telnet for management purposes is disabled and the Secure Shell (SSHv2) server is enabled. The SSH setting is configured during the initial setup. To edit the ssh configuration see Chapter “*Configuring SSH Services and Telnet*” **[3]**. If SSH is ever disabled, the command to enable ssh is the ‘feature ssh’ command shown below:

```
switch# configure terminal
switch(config)# feature ssh
switch(config)# no feature telnet
```

SSH Server Configuration:

1. Generate an RSA SSH keypair for the TOE to serve as the SSH Server Host Key**.** Be sure to choose a longer modulus length for more secure keys (i.e., 2048 for RSA):

```
switch# configure terminal
switch(config)# ssh key rsa [ 2048 ]
switch(config)# exit
switch# copy run start
```

The TOE also allows for ECDSA key pairs to be generated:

```
switch# configure terminal
switch(config)# ssh key ecdsa [ 256 | 384 | 521 ]
switch(config)# exit
switch# copy run start
```

SSH keys are generated in pairs—one public SSH key and one private SSH key. The “crypto key generate” command is not saved in the switch configuration; however, the SSH 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.

To manually delete an RSA or ECDSA keypair on the TOE, use the following commands:

```
switch# configure terminal
switch(config)# crypto key zeroize rsa [ keypair label ]
switch(config)# no ssh key ecdsa [ 256 | 384 | 521 ]
```

Note 1: *If the configuration is not saved to NVRAM with a "***copy run start***", the generated keys are lost on the next reload of the switch.*

Note 2: *If the error "% Please define a domain-name first" is received, enter the command '***ip domain-name [domain name]***'.*

2. Specify the SSH key to be used for SSH user public key authentication. This is done by pasting your public key data into the CLI with the command below. Both local password-based and public key-based authentication may be enabled on the TOE at the same time:

```
switch(config)# username admin sshkey sshpubkey
```

To delete an SSH keypair for a user, use the "no" form of the above command:

```
switch(config)# no username admin sshkey sshpubkey
```

3. Configure SSH Login Grace Time:

```
switch(config)# ssh login-gracetime [10-600 seconds]
```

4. Configure Maximum Number of SSH Login Attempts:

```
switch(config)# ssh login-attempts [1-10]
```

5. Customize SSH Cryptographic Algorithms:

```
switch(config)# ssh kexalgos [all | WORD]
```

Supported KexAlgos:

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

```
switch(config)# ssh macs [all | WORD]
```

Supported MACs:

- *hmac-sha2-256*
- hmac-sha2-512

```
switch(config)# ssh ciphers [all | WORD]
```

Supported Ciphers:

- *aes128-ctr*
- *aes256-ctr*

```
switch(config)# ssh keytypes [all | WORD]
```

Supported Keytypes:

- *rsa-sha2-256*
- *ecdsa-sha2-nistp256*
- *ecdsa-sha2-nistp384*
- ecdsa-sha2-nistp521

To view all active SSH algorithms:

```
switch# show ssh [kexalgos, macs, keytypes, ciphers]
```

To disable SSH algorithms, use the “no ssh” command shown below:

```
switch(config)# no ssh kexalgos diffie-hellman-group1-sha1 diffie-hellman-
group14-sha1 curve25519-sha256 curve25519-sha256@libssh.org

switch(config)# no ssh macs hmac-sha1 hmac-sha2-384 hmac-sha1-etm@openssh.com
hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com

switch(config)# no ssh keytypes ecdsa-sha2-nistp256-cert-v01@openssh.com
ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-
v01@openssh.com ssh-rsa-cert-v01@openssh.com
```

6. Customize SSH Rekey Limits:

```
switch(config)# ssh rekey max-data [data] max-time [time]
```

The TOE will react to the first threshold reached above.

The supervisor module mgmt0 port should be configured with an inbound access list to increase security by restricting access to specific source host/subnet addresses destined to specific management protocols configured on the Nexus 9000 Series. The access-list entries will vary depending on the management protocols that are enabled. Access-list statistics can be tracked per ACL entry if the ACL command **statistics per-entry** is configured. The supervisor module CPU performs access-list processing when an access-list is applied to the mgmt0 port.

```
switch(config)# ip access-list mgmt0-access
switch(config-acl)# statistics per-entry
switch(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22
switch(config)# line vty
switch(config-line)# access-class mgmt0-access in
```

3.3.2 Local Logging Configuration

The Cisco Nexus 9000 Series Switches supports local logging of events which are referred to as system messages in the Nexus 9K Series documentation. Logs are stored in local system files in NVRAM.

Log messages are not saved across system reboots. However, a maximum of 100 log messages with a severity level of critical and below (levels 0, 1, and 2) are saved in NVRAM. The severity level for logging to the console can be changed by command '`logging console`', but NVRAM can't be changed. By default, system message logging to the console is enabled messages at the critical severity level. The default onboard logging file name is *messages*. The '`logging logfile`' global configuration command enables copying of system messages to an internal log file and optionally sets the size of the file.

```
switch# configure terminal
switch(config)# logging console
```

(Optional) Sets severity level of logs sent to the console:

```
switch(config)# logging console [0-7]
```

Displays current system message logging events:

```
switch# show logging
```

Displays the contents of the default log file:

```
switch# show logging logfile
```

Displays contents of the log file stored in NVRAM:

```
switch# show logging NVRAM
```

Displays logging information:

```
switch# show logging info
```

Displays last few lines of a log file:

```
switch# show logging last 2
```

Displays switching module logging status:

```
switch# show logging module
```

Displays monitor logging status:

```
switch# show logging monitor
```

Displays server information:

```
switch# show logging server
```

By default, the switch logs normal but significant system messages to an onboard logfile and the system console as they occur. The onboard logfile is circular and can store up to the last 1200 messages. The file name can have up to 80 characters and the file size ranges from 4096 bytes to 4194304 bytes. Messages stored in the onboard logfile can be viewed using the CLI.

The accounting feature tracks and maintains a log of every management configuration used to access the switch. This information can be used to generate reports for troubleshooting and auditing purposes. Accounting logs can be stored locally. For more information on configuring system logging see **[2]**, section "Configuring System Message Logging".

3.3.2.1 Remote Logging Configuration

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. The TOE will then simultaneously record logs locally and send logs remotely as configured by the administrator. For instance, all emergency, alerts, critical, errors, and warning message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the switch is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information and the switch functionality is not affected.

The TOE uses the following TLS parameters for connections to an external Secure Syslog Server:

Supported TLS Versions:

- *TLSv1.2*

Supported Ciphers:

- *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268.*
- *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,*

- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,*
- *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,*
- *TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,*
- *TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,*
- *TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*

Supported EC Curves:

- *secp256r1*
- *secp384r1*
- *secp521r1*

NOTE: *The TLS parameters above are hard-set by the TOE once put into CC/FIPS mode.*

Since this functionality is not enabled by default, refer to "*Configuring System Messages Logging to Remote Logging Destinations*" in **[2]** to configure this option. You will also need to configure local logging. It is recommended to read the entire chapter in **[2]** to become familiar with the concept and configuration before configuring local and remote logging.

Setting up Remote Syslog Server:

```
switch# configure terminal
switch(config)# no ip http client tls-version TLSv1.3
switch(config)# logging server name [severity-level] [port number ] [ secure
[trustpoint client-identity name]]
```

Use the **secure** option to use TLS and optionally set the secure destination port (default is 6514) to encrypt the connection to the remote logging server using TLS. For TLS authentication to succeed, identity certificates must be signed by trusted CAs and must be installed using **crypto** commands. By default, certificates from all trust points are sequentially tried until authentication succeeds. The TOE verifies the server certificate Optionally, the certificates used for authentication may be restricted to a single trust point by specifying the **trustpoint client-identity** option. Use the facility option to specify a different logging category.

When establishing a TLS connection, the TOE supports reference identifiers of type DNS-ID and IP address and will seek a match to the DNS domain name or IP address respectively in the subjectAltName extension. If the TOE determines there is a mismatch in the presented identifier, it will not establish the TLS trusted channel connection. The TOE supports the use of wildcards within certificates. The TOE does not support certificate pinning.

The TOE supports peer certificate verification against a locally trusted CA and uses OCSP for certificate revocation checking to validate certificates. CA certificates must have the CA flag set to “True” in the basicConstraints extension to be accepted by the TOE. Server certificates must have the “Server Authentication” purpose in the extendedKeyUsage field, and OCSP Responders must have the “OCSP Signing” purpose. If the TOE determines that a certificate is invalid or is unable to reach the OCSP Responder, it will not establish the TLS trusted channel connection. Administrators may then choose to:

- Confirm that the OCSP Responder is up and reachable,
- Confirm all CA certificates have a CA flag set to “True”,
- Confirm peer certificates are valid and signed by a trusted CA.

The TOE is constantly renegotiating the connection to push syslog data as needed. If connection to the remote logging server is interrupted, the TOE will continue to save logs locally while attempting to renegotiate with the server. The renegotiation attempts by the TOE will continue until the connection is restored, no matter the length of time.

3.3.3 X.509 Certificates

NOTE: *X.509v3 certificates are being used for authentication of the TLS channel between the Nexus 9K Switch and the syslog server.*

For host authentication, Cisco NX-OS devices provide X.509 digital certificate support. The *Cisco Nexus 9000 Series Security Configuration Guide* **[3]** provides an example on how to configure X.509 certificates on the Cisco Nexus 9K Series.

Configure the switch FQDN:

```
switch# configure terminal
switch(config)# switchname SwitchA
switchA(config)#
```

Configure the DNS domain name for the switch:

```
switch(config)# ip domain-name example.com
switch(config)#
```

Configure an RSA trustpoint:

```
switch(config)# crypto ca trustpoint myCA
switch(config-trustpoint)#
```

The example declares a trust point CA called "myCA" that the switch should trust and enters trust point configuration submode for this trust point.

Note: *The maximum number of trust points that you can declare on a switch is 16.*

Create an RSA key-pair for the switch:

```
switchA(config)# crypto key generate rsa label myKey exportable modulus 2048
switchA(config)# show crypto key mypubkey rsa
```

To remove an RSA key-pair from the switch:

```
switch(config)# crypto key zeroize rsa [ keypair label ]
```

Associate the RSA key-pair to the trust point:

```
switchA(config)# crypto ca trustpoint myCA
switchA(config-trustpoint)# rsakeypair myKey
switchA(config-trustpoint)# end
switchA(config)# show crypto ca trustpoints
```

Authenticate the CA that you want to enroll to the trust point. The authenticating CA can be using an RSA or ECDSA CA certificate:

```
switch(config)# crypto ca authenticate myCA

xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
```

```
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5
Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12

Do you accept this certificate? [yes/no]: y
```

Configure Certificate Revocation Checking:

```
switch(config)# crypto ca trustpoint myCA
switch(config-trustpoint)# ocsp url http://<ocsp responder>
switch(config-trustpoint)# revocation-check ocsp
```

Generate a CSR to enroll with a trust point:

```
switch(config)# crypto ca enroll myCA

Create the certificate request..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: abc123
The subject name in the certificate will be: SwitchA.example.com
Include the switch serial number in the subject name? [yes/no]: no
Include an IP address in the subject name [yes/no]: yes
ip address: 192.168.31.162
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

Import signed certificate:

```
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

Verify the certificate configuration:

```
switchA(config)# show crypto ca certificates
```

Copies the running configuration to the start-up configuration:

```
switchA(config)# copy running-config startup-config
```

4 Secure Management

Based on the user ID and password combination provided, switches perform local authentication or authorization using the local database or remote authentication.

4.1 User Roles

All users on the NX-OS are considered to be administrator users. An authorized administrator which is also referred to as a security administrator can create and manage administrator user accounts and assign roles that limit access to operations on the Cisco NX-OS device.

Administrator user roles contain rules that define the operations allowed for the user who is assigned the role. Each administrator user role can contain multiple rules and each administrator user can have multiple roles. For example, if role1 users are only allowed access to configuration commands, and role2 users are only allowed access to debug commands, then users who belong to both role1 and role2, can access configuration and debug commands. An authorized administrator can also limit access to specific VLANs, virtual routing and forwarding instances (VRFs), and interfaces.

The Cisco NX-OS software provides the following default user roles:

- network-admin - Complete read-and-write access to the entire Cisco NX-OS device, except commands that modify profiles of other users.
- network-operator - Complete read access to the entire Cisco NX-OS device.
- server-admin - Complete read access to the entire Cisco NX-OS device and upgrade capability.

An authorized user cannot change these default roles and their associated privileges. NX-OS does allow for custom roles to be created. Chapter "*Configuring User Accounts and RBAC*", Section "*Role-Based Authorization*" in **[3]** describes how to configure the administrator user accounts with the associated roles that give the administrator specific access.

Information related to the System Security functions for the Nexus 9K Network-Admin and Network-Operator roles can be found in Chapter "*Configuring User Accounts and RBAC*" in **[3]**.

4.2 Clock Management

Clock management is restricted to the privileged administrator.

NOTE: *NTP is not included in the evaluated configuration. Use the command shown below to disable the NTP service.*

```
switch(config)# no feature ntp
```

For instructions to set the time zone for the clock, refer to section "Configuring the Time Zone" in chapter “Basic Device Management” in [**4**].

```
switch(config)# clock timezone zone-name offset-hours offset-minutes
```

Example:

```
switch(config)# clock timezone EST -5 0
```

To manually set the clock see section "Manually Setting the Device Clock" in chapter “Basic Device Management” in **[4]**.

```
switch# clock set time day month year
```

Example:

```
switch# clock set 15:00:00 30 May 2008 Fri May 30 15:14:00 PDT 2008
```

4.3 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the privileged administrator.

The Cisco Nexus 9K Series can be configured to use any of the following authentication methods:

- Local authentication (password or SSH public key authentication);

Password Login Example:

```
ssh admin@10.83.84.184
(admin@10.83.84.184) Password:

This is a test banner for purposes of NDcPPv2.2e
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2024, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular
```

```
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
N9k-C9332D-Lower#
```

Log Message:

```
2025 Jan 21 13:30:57 UTC N9k-C9332D-Lower %DAEMON-6-SYSTEM_MSG: Accepted
keyboard-interactive/pam for admin from 172.18.152.235 port 47156 ssh2 -
dcos_sshd[16298]
```

Public Key Login Example:

```
ssh admin@10.83.84.184 -i admin-ssh -o PasswordAuthentication=no

This is a test banner for purposes of NDcPPv2.2e
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2024, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
N9k-C9332D-Lower#
```

Log Message:

```
2025 Jan 21 13:30:42 UTC N9k-C9332D-Lower %DAEMON-6-SYSTEM_MSG: Accepted
publickey for admin from 172.18.152.235 port 54552 ssh2: RSA
SHA256:maSw2ESOitDdQP6ABDbZlQ932EOI/nN/dbynuqmUWn8 - dcos_sshd[16165]
```

For more information on SSH key authentication, please refer to Section 3.3.1 above. The *Cisco Nexus 9000 Series Security Configuration Guide* [3] also includes chapters named "Configuring User Accounts and RBAC" and "Configuring SSH Services and Telnet" that discuss this function more thoroughly.

4.4 Login Banners

The TOE may be configured by the privileged administrators with banners using the **banner motd** command. This banner is displayed before the username and password prompts. To create a banner of text, use the command below. See *Cisco Nexus 9000 Series Command Reference* **[5].**

```
switch# configure terminal
switch(config)# banner motd #Welcome to the switch#
switch(config)# show banner motd
Welcome to the switch
switch(config)#
```

Note: *In the **banner motd** command the characters surrounding the banner text in the given configuration line are delimiters, the character itself is not limited to #, it can be any character the administrator chooses to denote the beginning and end of the banner.*

4.5 Authentication failure

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

```
switch(config)# aaa authentication rejected attempts(1-65535) in seconds(1-
65535) ban seconds(1-65535)
```

Example:

```
switch# configure terminal
switch(config)# aaa authentication rejected 5 in 60 ban 600
switch(config)# end
switch# copy run start
```

This example would lock accounts after 5 consecutive login failures within 1 minute, and the account would be automatically unlocked after 10 minutes. Configuration of these settings is limited to the privileged administrator (see Section 4.1).

To view a list of currently locked accounts:

```
switch# show aaa local user blocked
```

To unlock a locked account:

```
switch# clear aaa local user blocked username username
```

NOTE: *Local console logins are not affected by lockouts. This allows the TOE to always maintain administrator access.*

4.6 Product Updates

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

5 Security Relevant Events

The TOE can 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 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. The first message displayed is the oldest message in the buffer.

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:

```
switch# clear logging logfile
Clear logging buffer [confirm] <ENTER>
switch# clear logging nvram
```

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 fields in each audit event will contain at a minimum the following: Date, Time, User, and Action.

Example Audit Event:

```
Sun Mar 31 02:50:39
2024:type=update:id=10.1.2.3@pts/0:user=admin:cmd=configure terminal ;
username user1 password 0 ******** (SUCCESS)
```

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

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

Table 12 Audit Events and Sample Record

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

FAU_GEN.1	Start-up and shutdown of audit functions.	No additional information.	NX-OS cannot stop and start logs, so logging stops and starts with the shutdown and start-up of the switch. Below shows the audit event for starting and stopping sending logs to remote syslog server.
			`2024 Dec 31 01:36:58 nx9336-FX2 %AAA-6-AAA_ACCOUNTING_MESSAGE:update:console0:admin:configure terminal ; logging server 172.16.16.152 use-vrf management (SUCCESS)`
			`2024 Dec 31 01:37:22 nx9336-FX2 %SYSLOG-5-SYSTEM_MSG: Logging server with hostname/IP 172.16.16.152 unconfigured - syslogd[15210]`

FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.	**Ability to configure the transmission of audit data to an external IT entity:** `Dec 31 09:06:46 nx9336 nx9336-FX2: 2024 Dec 31 14:07:41 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging server example.com secure use-vrf management (SUCCESS)`
FCS_SSH_EXT.1	**[selection:** Failure to establish SSH connection, None]	Reason for failure. [selection: Non-TOE endpoint of attempted	**Failure to establish an SSH session, with reason for failure:** *no matching key exchange method*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

		connection (IP Address) , None]	`2024 Dec 31 01:51:02 nx9336-FX2 %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.51 port 58616: no matching key exchange method found. Their offer: diffie-hellman-group14-sha256,ext-info-c [preauth] - dcos_sshd[19549]`
			Failure to establish an SSH session, with reason for failure: *no matching cipher*
			`2024 Dec 31 01:45:23 nx9336-FX2 %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.51 port 58210: no matching cipher found. Their offer: aes128-cbc [preauth]- dcos_sshd[18866]`
			Failure to establish an SSH session, with reason for failure: *no matching MAC*
			`2024 Dec 31 01:47:27 nx9336-FX2 %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.51 port 58374: no matching MAC found. Their offer: hmac-sha1 [preauth]- dcos_sshd[19075]`
			Failure to establish an SSH session, with reason for failure: *no matching host key type*
			`2024 Dec 31 01:46:26 nx9336-FX2 %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.51 port 58292: no matching host key type found. Their offer: ssh-rsa [preauth] - dcos_sshd[18968]`

	[**selection:** Establishment of SSH connection, None]	[selection: Non-TOE endpoint of connection (IP Address) , None]	**Establishment of an SSH session:** `2018 Jun  1 17:17:12 nexus9k %DAEMON-6-SYSTEM_MSG: Accepted keyboard-interactive/pam for admin from 10.31.0.101 port 49868 ssh2 - dcos_ sshd[21990]`

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

	[selection: Termination of SSH connection session, None]	[selection: Non-TOE endpoint of connection (IP Address) , None]	**Termination of SSH session:**
			`Jan  3 07:49:58 nx9336 nx9336-FX2: 2025 Jan  1 12:50:36 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: stop:console0:admin:shell terminated gracefully`
			`Jan  3 07:49:58 nx9336 nx9336-FX2: 2025 Jan  1 12:50:36 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin - login[7508]`

	[selection: Dropping of packet(s) outside defined size limits, None]	[selection: Packet size , 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`

FCS_TLSC_EXT.1	Failure to establish an TLS session	Reason for failure.	**Invalid Cipher:**
			`Dec 17 20:20:06 nx9336 nx9336-FX2: 2024 Dec 18 01:21:02 UTC: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 172.16.16.51:6514 in [vrf: management] [ Protocol: TLSv1.2 ]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] - syslogd[15135]`
			`Dec 17 20:20:13 nx9336 nx9336-FX2: 2024 Dec 18 01:21:09 UTC: %SYSLOG-4-SYSTEM_MSG: SSL_connect:  SSL_get_error() = 1 SSL_connect error: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure  - syslogd[15135]`
			Missing Server EKU:
			`01.06 12:31:54 LOG5[348]: Connection reset: 0 byte(s) sent`

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			to SSL, 0 byte(s) sent to socket 2025.01.06 12:31:54 LOG5[349]: Service [secure_syslog] accepted connection from 172.16.16.133:60251 2025.01.06 12:31:54 LOG3[349]: SSL_accept: 14094413: error:14094413:SSL routines:ssl3_read_bytes:sslv3 alert unsupported certificate] **Wrong Certificate Type:** 2025 Jan 4 17:35:02 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1416F17F:SSL routines:tls_process_server_certificate:wrong certificate type - syslogd[15082] **Null Ciphersuite:** 2025 Jan 4 17:43:15 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1421C0F8:SSL routines:set_client_ciphersuite: unknown cipher returned - syslogd[15082] 2025 Jan 4 17:43:15 nx9336-FX2 %SYSLOG-6-SYSTEM_MSG: SSL_connect failed with SSL_ERROR_SYSCALL - syslogd[15082] **Server selects not proposed cipher:** 2025 Jan 4 17:45:15 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1421C0F8:SSL routines:set_client_ciphersuite: unknown cipher returned - syslogd[15082] **Invalid Curve:** 2025 Jan 4 20:36:25 nx9336-FX2

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			%SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:141A417A:SSL routines:tls_process_ske_ecdhe:wrong curve - syslogd[15082] 2025 Jan 4 20:36:25 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 172.16.16.51:6514 in [vrf: management] [Protocol: TLSv1.2]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] - syslogd[15082] **Invalid TLS Version:** 2025 Jan 4 20:40:14 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol - syslogd[15082] **Modified Finished Message:** 2025 Jan 4 20:47:54 nx9336-FX2 %SYSLOG-6-SYSTEM_MSG: SSL_connect failed with SSL_ERROR_SYSCALL - syslogd[15082] 2025 Jan 4 20:47:54 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1416C095:SSL routines:tls_process_finished:digest check failed - syslogd[15082] **Plaintext Finished Message:** 2025 Jan 4 20:50:33 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1408F081:SSL routines:ssl3_get_record:block

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			cipher pad is wrong - syslogd[15082] 2025 Jan 4 20:50:33 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 172.16.16.51:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher : AES128-SHA]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown :shutdown while in init] - syslogd[15082] **Modified Hello Nonce:** 2025 Jan 4 20:52:35 nx9336-FX2 %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:140943FC:SSL routines:ssl3_read_bytes:sslv3 alert bad record mac - syslogd[15082] **Subject name validation fail:** Dec 24 15:33:43 nx9336 nx9336-FX2: 2024 Dec 24 20:34:39 UTC: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 172.16.16.51:6514 in [vrf: management] [Protocol: TLSv1.3]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] - syslogd[15187] Dec 24 15:35:18 nx9336 nx9336-FX2: 2024 Dec 24 20:36:14 UTC: %SYSLOG-5-SYSTEM_MSG: Subject Name validation Failed for SSL connection to 172.16.16.51:6514 in [vrf: management] - syslogd[15187] Dec 24 15:35:18 nx9336 nx9336-FX2: message repeated 2 times: [2024 Dec 24 20:36:14 UTC: %SYSLOG-5-SYSTEM_MSG: Subject Name validation Failed for SSL connection to 172.16.16.51:6514

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			`in [vrf: management]`

FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).	`Jan  3 06:40:13 nx9336 nx9336-FX2: message repeated 2 times: [ 2025 Jan  3 11:41:07 UTC: %DAEMON-3-SYSTEM_MSG: error: maximum authentication attempts exceeded for invalid user test from 172.16.16.52 port 38036 ssh2 [preauth] - dcos_sshd[475]]`
			`Jan  3 06:40:13 nx9336 nx9336-FX2: 2025 Jan  3 11:41:07 UTC: %DAEMON-6-SYSTEM_MSG: Disconnecting invalid user test 172.16.16.52 port 38036: Too many authentication failures [preauth] - dcos_sshd[475]`

FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**Successful Console Login:**
			`Jan  3 06:25:32 nx9336 nx9336-FX2: 2025 Jan  3 11:26:26 UTC: %AUTHPRIV-6 SYSTEM_MSG: pam_unix(login:session): session opened for user admin by admin(uid=0) - login[31068]`
			Failed Console Login:
			`Jan  3 06:25:09 nx9336 nx9336-FX2: 2025 Jan  3 11:26:03 UTC: %AUTHPRIV-5-SYSTEM_MSG: FAILED LOGIN (1) on '/dev/pts/0' FOR 'admin', Authentication failure - login[31068]`
			Successful SSH/CLI Login (Password):
			`Jan  3 06:37:51 nx9336 nx9336-FX2: 2025 Jan  3 11:38:46 UTC: %AUTHPRIV-6-SYSTEM_MSG:pam_unix(dcos_sshd:session): session opened for user admin by (uid=0) - dcos_sshd[32634]`
			Failed SSH/CLI Login (Password):

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			Dec 30 21:03:31 nx9336 nx9336-FX2: 2024 Dec 31 02:04:26 UTC: %AUTHPRIV-5-SYSTEM_MSG: Login failed for user **** - dcos_sshd[20979] **Successful SSH/CLI Login (Public Key):** Jan 3 06:29:15 nx9336 nx9336-FX2: 2025 Jan 3 11:30:09 UTC: %DAEMON-6-SYSTEM_MSG: Accepted publickey for admin from 172.16.16.52 port 38026 ssh2: ECDSA SHA256:v4L9fU2L3HCLq2fc1lRkOr9CmESEBCMiuWbca4Zr/L8 - dcos_sshd[31707] Jan 3 06:29:15 nx9336 nx9336-FX2: 2025 Jan 3 11:30:09 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session opened for user admin by (uid=0) - dcos_sshd[31707] **Failed SSH/CLI Login (Public Key):** Jan 3 06:36:13 nx9336 nx9336-FX2: 2025 Jan 3 11:37:08 UTC: %AUTHPRIV-5-SYSTEM_MSG: Login failed for user **** - dcos_sshd[32388] Jan 3 06:36:13 nx9336 nx9336-FX2: 2025 Jan 3 11:37:08 UTC: %DAEMON-3-SYSTEM_MSG: error: PAM: Authentication failure for ***** from 172.16.16.52 - dcos_sshd[32386]
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	See FIA_UIA_EXT.1 above for all audits related to the use of the identification and authentication mechanism.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure of certificate validation Identification of certificates added, replaced or	**Add Trust Anchor:** See FMT_SMF.1

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

	Any addition, replacement or removal of trust anchors in the TOE's trust store	removed as trust anchor in the TOE's trust store	**Remove Trust Anchor:**
			See FMT_SMF.1
			Missing Basic Constraints:
			`Jan  3 12:10:23 nx9336 nx9336-FX2: 2025 Jan  1 17:11:01 UTC: %SYSLOG-4-SYSTEM_MSG: err: 24, subject: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-no-basic-constraints-rsa issuer: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subca-rsa strict mode: 1  - syslogd[15203]`
			`Jan  3 12:10:23 nx9336 nx9336-FX2: 2025 Jan  1 17:11:01 UTC: %SYSLOG-4-SYSTEM_MSG: SSL_connect:  SSL_get_error() = 1 SSL_connect error: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed - syslogd[15203]`
			Basic Constraints False for CA:
			`Jan  3 12:23:36 nx9336 nx9336-FX2: message repeated 2 times: [ 2025 Jan  1 17:24   :14 UTC: %SYSLOG-4-SYSTEM_MSG: err: 24, subject: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-ca-flag-false-rsa issuer: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subca   -rsa strict mode: 1  - syslogd[15203]]`
			`Jan  3 12:23:36 nx9336 nx9336-FX2: 2025 Jan  1 17:24:14 UTC: %SYSLOG-4-SYSTEM_M   SG: SSL_connect:  SSL_get_error() = 1 SSL_connect error: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed - syslogd[15203]`

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			Jan 3 12:23:36 nx9336 nx9336- FX2: message repeated 2 times: [2025 Jan 1 17:24 :14 UTC: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect e rror: error:1416F086:SSL routines:tls_process_server_certi ficate:certificate verify failed - syslogd[15203]] **Certificate Revoked:** Jan 3 11:51:56 nx9336 nx9336- FX2: 2025 Jan 1 16:52:34 UTC: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP certificate is revoked! - syslogd[15203] Jan 3 11:51:56 nx9336 nx9336- FX2: message repeated 2 times: [2025 Jan 1 16:52:34 UTC: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP certificate is revoked! - syslogd[15203] **Corrupt Cert ASN1:** Jan 3 11:58:05 nx9336 nx9336- FX2: 2025 Jan 1 16:58:43 UTC: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag - syslogd[15203] **Corrupt Cert Signature:** Jan 3 12:06:49 nx9336 nx9336- FX2: 2025 Jan 1 17:07:28 UTC: %DAEMON-2-SYSTEM_MSG: TLS certificate verification: Error, certificate signature failure - syslogd[15203] Jan 3 12:06:49 nx9336 nx9336- FX2: 2025 Jan 1 17:07:28 UTC: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:0409D068:rsa routines::bad

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

			`signature  - syslogd[15203]`
			Corrupt Public Key:
			`Jan  3 12:04:40 nx9336 nx9336-FX2: 2025 Jan  1 17:05:17 UTC: %SYSLOG-6-SYSTEM_MSG: SSL_connect failed with SSL_ERROR_WANT_READ - syslogd[15203]`
			`Jan  3 12:04:40 nx9336 nx9336-FX2: 2025 Jan  1 17:05:17 UTC: %DAEMON-6-SYSTEM_MSG: nxos_ssl_check_ocsp: cert subject /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl51-16x.example.com issuer /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-rsa  - syslogd[15203]`
			No OCSP Signing:
			`Jan  3 11:55:41 nx9336 nx9336-FX2: 2025 Jan  1 16:56:19 UTC: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP verify error. Disconnecting!  - syslogd[15203]`
			`Jan  3 11:55:41 nx9336 nx9336-FX2: message repeated 2 times: [ 2025 Jan  1 16:56:19 UTC: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP verify error. Disconnecting!  - syslogd[15203]]`
			Invalid Chain:
			`Jan  3 12:26:30 nx9336 nx9336-FX2: 2025 Jan  1 17:27:08 UTC: %DAEMON-2-SYSTEM_MSG: TLS certificate verification: Error, self signed certificate in certificate chain  - syslogd[15203]`
			`Jan  3 12:26:30 nx9336 nx9336-FX2: 2025 Jan  1 17:27:08 UTC: %SYSLOG-4-SYSTEM_MSG: err: 19, subject: /C=US/ST=MD/L=Catonsville/O=GSS/CN=rootca-unacceptable-rsa issuer: /C=US/ST=MD/L=Catonsville/O=GSS/CN=rootca-unacceptable-rsa strict mode: 1  - syslogd[15203]`

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

			`Jan  3 12:26:30 nx9336 nx9336-FX2: 2025 Jan  1 17:27:08 UTC: %SYSLOG-4-SYSTEM_MSG: SSL_connect:  SSL_get_error() = 1 SSL_connect error: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed - syslogd[15203]`
			Unreachable Revocation Server:
			`Jan  3 11:38:01 nx9336 nx9336-FX2: 2025 Jan  1 16:38:39 UTC: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP responder not reachable. Disconnecting!  - syslogd[15203]`
			Expired Certificate:
			`Jan  3 11:41:57 nx9336 nx9336-FX2: message repeated 2 times: [ 2025 Jan  1 16:42:35 UTC: %DAEMON-2-SYSTEM_MSG: TLS certificate verification: Error, certificate has expired  - syslogd[15203]]`
			`Jan  3 11:49:30 nx9336 nx9336-FX2: 2025 Jan  1 16:50:08 UTC: %DAEMON-6-SYSTEM_MSG: nxos_ssl_check_ocsp: cert subject /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl51-16x.example.com issuer /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-issued-by-expired-rsa - syslogd[15203]`
			`Jan  3 11:49:30 nx9336 nx9336-FX2: 2025 Jan  1 16:50:08 UTC: %DAEMON-2-SYSTEM_MSG: nxos_ssl_check_ocsp:No issuer, skipping ocsp check - syslogd[15203]`

FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.	See FPT_TUD_EXT.1

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

FMT_SMF.1	All management activities of TSF data.	None.	**Ability to administer the TOE locally and remotely:**
			See FIA_UIA_EXT.1
			Ability to configure the access banner:
			`Dec 30 21:36:49 nx9336 nx9336-FX2: 2024 Dec 31 02:37:44 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; banner motd 'This is the Gossamer Test Banner (SUCCESS)`
			Ability to configure the remote session inactivity time before session termination:
			Console:
			`Dec 30 21:44:27 nx9336 nx9336-FX2: 2024 Dec 31 02:45:22 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; line console ; exec-timeout 10 (SUCCESS)`
			SSH:
			`Dec 30 21:45:47 nx9336 nx9336-FX2: 2024 Dec 31 02:46:43 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; line vty ; exec-timeout 10 (SUCCESS)`
			Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates:
			See FPT_TUD_EXT.1
			Ability to configure the authentication failure parameters for FIA_AFL.1:
			Console:
			`Dec 31 09:05:59 nx9336 nx9336-FX2: 2024 Dec 31 14:06:54 UTC:`

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

			`%AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; aaa authentication rejected 3 in 60 ban 180 (SUCCESS)`
			SSH:
			`Dec 31 09:09:03 nx9336 nx9336-FX2: 2024 Dec 31 14:09:59 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh key rsa 2048 (SUCCESS)`
			Ability to modify the behavior of the transmission of audit data to an external IT entity:
			`Dec 31 09:06:46 nx9336 nx9336-FX2: 2024 Dec 31 14:07:41 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging server example.com secure use-vrf management (SUCCESS)`
			Ability to manage the cryptographic keys:
			SSH:
			`Dec 31 09:09:03 nx9336 nx9336-FX2: 2024 Dec 31 14:09:59 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh key rsa 2048 (SUCCESS)`
			Delete Key:
			`Dec 31 09:08:58 nx9336 nx9336-FX2: 2024 Dec 31 14:09:54 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh key rsa (SUCCESS)`
			See also audits below for ability to manage the TOE's trust store and the trusted public keys database.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			Ability to configure the cryptographic functionality: Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh kexalgos all (SUCCESS) Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh ciphers all (SUCCESS) Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh macs all (SUCCESS) Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh ciphers aes128-cbc (SUCCESS) Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh ciphers aes192-cbc (SUCCESS) Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh ciphers aes192-ctr (SUCCESS) Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh macs hmac-sha2-256-etm@openssh.com (SUCCESS)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

			`Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh macs hmac-sha1-etm@openssh.com (SUCCESS)`
			`Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh kexalgos curve25519-sha256@libssh.org (SUCCESS)`
			`Dec 31 09:12:12 nx9336 nx9336-FX2: 2024 Dec 31 14:13:07 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh keytypes ssh-rsa (SUCCESS)`
			Ability to configure the thresholds for SSH rekeying:
			`Jan  2 13:48:22 nx9336 nx9336-FX2: 2025 Jan  2 18:49:16 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh rekey max-data 10M max-time 60M (SUCCESS)`
			Ability to set the time which is used for timestamps:
			See FPT_STM_EXT.1
			Reset Passwords:
			`Jan  2 13:49:50 nx9336 nx9336-FX2: 2025 Jan  2 18:50:45 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; username testuser password ******** (SUCCESS)`
			Ability to configure the reference identifier for the peer:
			`2025 Jan  2 19:40:29 nx9336-FX2 %AAA-6-AAA_ACCOUNTING_MESSAGE:`

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			update:console0:admin:configure terminal ; ip name-server 172.16.16.51 source-interface mgmt0 (SUCCESS) 2025 Jan 2 19:42:37 nx9336-FX2 %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging server example.com 7 secure use-vrf management (SUCCESS) **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors:** Create Trustpoint: Jan 2 22:21:09 nx9336 nx9336-FX2: 2025 Jan 3 03:22:03 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint testpoint (SUCCESS) Import CA Cert: Jan 2 22:22:47 nx9336 nx9336-FX2: 2025 Jan 3 03:23:42 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:CA certifcate/chain configuration done for trustpoint testpoint Jan 2 22:22:47 nx9336 nx9336-FX2: 2025 Jan 3 03:23:42 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca authenticate testpoint (SUCCESS) Generate CSR: Jan 2 23:00:46 nx9336 nx9336-FX2: 2025 Jan 3 04:01:40 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:created Certificate Signing Request for

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record

			`trustpoint append`
			`Jan  2 23:00:46 nx9336 nx9336-FX2: 2025 Jan  3 04:01:40 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca enroll append (SUCCESS)`
			Remove Trustpoint & Certs:
			`Jan  2 22:45:32 nx9336 nx9336-FX2: 2025 Jan  3 03:46:26 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:deleted CA certificate/chain from trustpoint testpoint`
			`Jan  2 22:45:32 nx9336 nx9336-FX2: 2025 Jan  3 03:46:26 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:removed configuration for trustpoint testpoint`
			`Jan  2 22:45:32 nx9336 nx9336-FX2: 2025 Jan  3 03:46:26 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no crypto ca trustpoint testpoint (SUCCESS)`
			Ability to manage the trusted public keys database:
			Configure public key authentication:
			`Jan  2 23:23:43 nx9336 nx9336-FX2: 2025 Jan  3 04:24:38 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:::rsa key created with size:2048`
			`Jan  2 23:23:43 nx9336 nx9336-FX2: 2025 Jan  3 04:24:38 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh key rsa 2048 force`

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			(SUCCESS) Configure User with public key: Jan 2 13:47:10 nx9336 nx9336-FX2: 2025 Jan 2 18:48:05 UTC: %DAEMON-6-SYSTEM_MSG: Postponed publickey for admin from 192.168.144.51 port 58908 ssh2 [preauth] - dcos_sshd[27086] Jan 2 13:47:10 nx9336 nx9336-FX2: 2025 Jan 2 18:48:05 UTC: %DAEMON-6-SYSTEM_MSG: Accepted publickey for admin from 192.168.144.51 port 58908 ssh2: ECDSA SHA256:v4L9fU2L3HCLq2fc1lRkOr9CmESEBCMiuWbca4Zr/L8 - dcos_sshd[27086] Remove public key and association with user: 2025 Jan 3 04:22:11 nx9336-FX2 %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no username test (SUCCESS)
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).	Jan 3 06:43:22 nx9336 nx9336-FX2: 2025 Jan 1 11:44:00 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:clock set 11:44:00 1 January 2025 (SUCCESS)
FPT_TUD_EXT.1	Initiation of update; result of the update	None.	**Failure:** 2024 Dec 27 17:12:06 nx9336-FX2

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	attempt (success and failure)		%AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; boot nxos bootflash:/nxos64-cs.10.4.5.M.zero.bin (FAILURE) **Success:** 2025 Jan 1 19:23:45 nx9336-FX2 %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:install all nxos bootflash:/nxos64-cs.10.4.3.F.bin (SUCCESS)
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.	Jan 3 07:56:24 nx9336 nx9336-FX2: 2025 Jan 1 12:57:02 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: stop:console0:admin:shell terminated because of session timeout Jan 3 07:56:25 nx9336 nx9336-FX2: 2025 Jan 1 12:57:03 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin - login[7677]
FTA_SSL.3	The termination of a *remote* session by the session locking mechanism. Administrative Actions: Specifying the inactivity time period.	None.	Jan 3 07:51:22 nx9336 nx9336-FX2: 2025 Jan 1 12:52:00 UTC: %DAEMON-6-SYSTEM_MSG: Received disconnect from 172.16.16.52 port 38038: reason 11: disconnected by user - dcos_sshd[7848] Jan 3 07:51:22 nx9336 nx9336-FX2: 2025 Jan 1 12:52:00 UTC: %DAEMON-6-SYSTEM_MSG: Disconnected from user admin 172.16.16.52 port 38038 - dcos_sshd[7848]
FTA_SSL.4	The termination of an interactive session.	None.	Jan 3 07:49:58 nx9336 nx9336-FX2: 2025 Jan 1 12:50:36 UTC: %AAA-6-AAA_ACCOUNTING_MESSAGE: stop:console0:admin:shell terminated gracefully

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			`Jan  3 07:49:58 nx9336 nx9336-FX2: 2025 Jan  1 12:50:36 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin - login[7508]`

FTP_ITC.1	Initiation of the trusted channel.
	Termination of the trusted channel.
	Failure of the trusted channel functions.
		None.
		None.
		Reason for failure.
			Establish TLSC Session:
			`Dec 17 20:42:14 nx9336 nx9336-FX2: 2024 Dec 18 01:43:09 UTC: %SYSLOG-5-SYSTEM_MSG: Successfully established SSL connection to 172.16.16.51:6514 in [vrf: management] Protocol: TLSv1.2 Cipher: ECDHE-RSA-AES256-SHA384  - syslogd[15135]`
			Termination of TLSC Session:
			`Dec 17 20:42:07 nx9336 nx9336-FX2: 2024 Dec 18 01:43:02 UTC: %SYSLOG-5-SYSTEM_MSG: Successfully tore down SSL connection to 172.16.16.51:6514 in [vrf: management] [ Protocol: TLSv1.2 Cipher: ECDHE-RSA-AES128-SHA256 ]. - syslogd[15135]`
			Failures of TLSC Session:
			See FCS_TLSC_EXT.1 for audits associated with TLSC session failures.

FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None. None. Reason for failure.	**Establish SSH Session:** See FIA_UIA_EXT.1 for Audits of successful establishment of SSH sessions. **Terminate SSH Session:** See FTA_SSL.3 and FTA_SSL.4. **Failures of SSH Session:** See FCS_SSHS_EXT.1 for Audits associated with failures of SSH Sessions.

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 13: Protocols and Services

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed to use in the certified configuration
DHCPS	Dynamic Host Configuration Protocol Secure	Yes	Yes	Yes	Yes	**YES**
DNS	Domain Name Service	Yes	Yes	No	n/a	**YES**
FTP	File Transfer Protocol	Yes	No	No	n/a	**NO**
HTTP	Hypertext Transfer Protocol	Yes	No	Yes	No	**NO**
HTTPS	Hypertext Transfer Protocol Secure	Yes	No	Yes	No	**NO**
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	**YES**
IKE	Internet Key Exchange	Yes	No	Yes	No	**NO**
Kerberos	A ticket-based authentication protocol	Yes	No	No	n/a	**NO**
LDAP not secure	Lightweight Directory Access Protocol	Yes	No	No	n/a	**NO**
LDAP secure	LDAP over Secure Sockets Layer	Yes	Over TLS	No	n/a	**NO**
NTP	Network Time Protocol	Yes	Yes	No	No	**NO**
RADIUS	Remote Authentication Dial In User Service	Yes	No	No	n/a	**NO**

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed to use in the certified configuration
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	No	Yes	No	**NO**
SSH	Secure Shell	Yes	No	Yes	Yes	**YES** **As described in the relevant section of this document.**
Syslog	Syslog Server	Yes	Yes	No	n/a	**YES** **Use with TLS.**
TACACS+	Terminal Access Controller Access-Control System Plus	Yes	No	No	n/a	**NO**
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	**NO**
TLS	Transport Layer Security	Yes	No	Yes	No	**YES** **As described in the relevant section of this document.**
TFTP	Trivial File Transfer Protocol	Yes	Yes	No	n/a	**NO**

7 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 14: 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 Nexus 9000 is installed and maintained within a secure physical location.
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 must not add any general-purpose computing capabilities (e.g., compilers or user applications) to the Nexus 9000.
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. 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 TOE's trust store in case such certificate can no longer be trusted.	Administrators must be properly trained in the usage and proper operation of the Nexus 9000 and all the enabled functionalities. These administrators must follow the provided guidance.

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 ASA 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.

8 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 wwww.cisco.com.

8.1 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.

8.2 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

8.2.1 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.

8.2.2 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

8.2.3 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.

8.3 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