Cisco Nexus 3000 and 9000 Switches Series

CC Configuration Guide

Version: 1.0
Date: September 7 2021

© 2021 Cisco Systems, Inc. All rights reserved. This document may be reproduced in full without any modification.

Table of Contents

List of Tables

List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	*Internet Control Message Protocol*
IP	Internet Protocol
ISDN	*Integrated Services Digital Network*
IT	Information Technology
NDcPP	collaborative Network Device Protection Profile
OS	Operating System
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WIC	WAN Interface Card

Terminology

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

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer switch	Another switch on the network that the TOE interfaces with.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vty	vty is a term used by Cisco to describe a virtual terminal (whereas Terminal is more of a verb or general action term).
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

Document Introduction

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

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Nexus 3000 and 9000 Series Switches (Cisco Nexus 3K & 9K Series). This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged administrators, and privileged administrators in this document.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Nexus 3000 (3100. 3100v, 3100Z, 3200, 3400, 3500, 3600) and 9000 (9200, 9300 and 9500) Series Switches running on Cisco NX-OS 9.3(8) (herein after referred to as Cisco Nexus 3K & 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: 3100. 3100v, 3100Z, 3200, 3400, 3500, 3600, 9200, 9300, 9500. The software is comprised of the NX-OS software image Release 9.3.

The Nexus 3000 Switch Series (Nexus 3K) and the Nexus 9000 Switch Series (Nexus 9K) may be referenced below by the model number series related acronym ex. 3K, 9K, TOE, Nexus 3K series, Nexus 9K Series, or simply switch.

1.1 Audience

This document is written for administrators configuring the TOE, specifically the NX-OS 9.3(8) 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 your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document covers all of the security functional requirements specified in the ST and as summarized in Section 3 of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, 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 3K and Nexus 9K operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 Document References

This document reference several Cisco Systems documents. The documents used are shown below in Table 2. Where reference is made to the

- “Cisco Nexus 3000 Series” documentation, then the documentation is applicable to both the 3100, 3100V, 3100Z, 3200, 3400, 3500, and 3600 model series.
- “Cisco Nexus 9000 Series” documentation, then the documentation is applicable to both the 9200, 9300 and 9500 model series.

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

Table 3 Cisco Documentation

#	Title	Link

[1]	Cisco Nexus 9000 Series Switches Security Target, (Current Version)	https://www.niap-ccevs.org/Product/index.cfm
[2]	Cisco Nexus 3000 Series NX-OS System Management Configuration Guide	• Cisco Nexus 3000 Series NX-OS System Management Configuration Guide, Release 9.3(x) • Cisco Nexus 3400-S NX-OS System Management Configuration Guide, Release 9.3(x) • Cisco Nexus 3548 Series NX-OS System Management Configuration Guide, Release 9.3(x) • Cisco Nexus 3600 Series NX-OS System Management Configuration Guide, Release 9.3(x)
	Cisco Nexus 9000 Series NX-OS System Management Configuration Guide	Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x)
[3]	Cisco Nexus 3000 Series NX-OS Security Configuration Guide	• Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Release 9.3(x) • Cisco Nexus 3400-S NX-OS Security Configuration Guide, Release 9.3(x) • Cisco Nexus 3548 series NX-OS Security Configuration Guide, Release 9.3(x) • Cisco Nexus 3600 Series NX-OS Security Configuration Guide, Release 9.3(x)
	Cisco Nexus 9000 Series NX-OS Security Configuration Guide	Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x)
[4]	Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide	• Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x) • Cisco Nexus 3400-S NX-OS Fundamentals Configuration Guide, Release 9.3(x) • Cisco Nexus 3548 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x) • Cisco Nexus 3600 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x)
	Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide	Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x)

[5]	Cisco Nexus 3000 Series NX-OS Command References (Configuration Commands)	• Cisco Nexus 3000 Series NX-OS Command Reference (Configuration Commands). • Cisco Nexus 3548 Series NX-OS Command Reference (Configuration Commands). • Cisco Nexus 3600 Series NX-OS Command Reference (Configuration Commands). • Cisco Nexus 3400-S NX-OS Command Reference (Configuration Commands)
	Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands), Release 9.3(5)	Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands) Release 9.3(x)
[6]	Cisco Nexus 3600 Series NX-OS Command Reference (Show Commands)	• Cisco Nexus 3000 Series NX-OS Command Reference (Show Commands) • Cisco Nexus 3548 Series NX-OS Command Reference (Show Commands) • Cisco Nexus 3600 Series NX-OS Command Reference (Show Commands) • Cisco Nexus 3400-S NX-OS Command Reference (Show Commands)
	Cisco Nexus 9000 Series NX-OS Command Reference (Show Commands), Release 9.3(5)	Cisco Nexus 9000 Series NX-OS Command Reference (Show Commands), Release 9.3(x)
[7]	Cisco Nexus 3000 Series Hardware Installation Guides	• Cisco Nexus 3000 Series Hardware Installation Guides • Cisco Nexus 3400 Hardware Installation Guides • Cisco Nexus 3400-S Hardware Installation Guides • Cisco Nexus 3500 Series Hardware Installation Guides • Cisco Nexus 3600 Series Hardware Installation Guides

	Cisco Nexus Mode Switch Hardware Installation Guides	• Cisco Nexus 92348GC-X NX-OS Mode Switch Hardware Installation, • Cisco Nexus 92160YC-X NX-OS Mode Switch Hardware Installation • Cisco Nexus 92300YC NX-OS Mode Switch Hardware Installation • Cisco Nexus 9272Q NX-OS Mode Switch Hardware Installation • Cisco Nexus 9348GC-FXP NX-OS Mode Switch Hardware Installation • Cisco Nexus 93216TC-FX2 NX-OS Mode Switch Hardware Installation • Cisco Nexus 93180YC-EX NX-OS Mode Switch Hardware Installation • Cisco Nexus 93240YC-FX2 NX-OS Mode Switch Hardware Installation • Cisco Nexus 93360YC-FX2 NX-OS Mode Switch Hardware Installation • Cisco Nexus 9364C NX-OS Mode Switch Hardware Installation • Cisco Nexus 9332C NX-OS Mode Switch Hardware Installation • Cisco Nexus 9364C-GX NX-OS Mode Switch Hardware Installation • Cisco Nexus 9316D-GX NX-OS Mode Switch Hardware Installation • Cisco Nexus 93600CD-GX NX-OS Mode Switch Hardware Installation • Cisco Nexus 93108TC-EX NX-OS Mode Switch Hardware Installation • Cisco Nexus 93108TC-FX NX-OS Mode Switch Hardware Installation • Cisco Nexus 93240YC-FX2 NX-OS Mode Switch Hardware Installation • Cisco Nexus 9336C-FX2-Z NX-OS Mode Switch Hardware Installation • 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 2000 Series Hardware Installation Guide (Optional)

[8]	Cisco Nexus 3000 Series NX-OS System Messages Reference	• Cisco Nexus 3000 Series NX-OS System Messages Reference • Cisco Nexus 3400 NX-OS System Messages Reference • Cisco Nexus 3548 NX-OS System Messages Reference • Cisco Nexus 3600 Series NX-OS System Messages Reference
	Cisco Nexus 9000 Series NX-OS System Messages Reference	Cisco Nexus 9000 Series NX-OS System Messages Reference, Release 9.3(5)
[9]	FIPS Certificate	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

1.4 Supported Hardware and Software

Only the hardware and software listed in section 1.5 of the Security Target (ST) and listed in Table 3 and 4 below is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The TOE is a hardware and software solution that makes up the Nexus 3K and 9K.

Table 4 Supported Hardware and External identifier

Product Name	External Identification
Cisco Nexus 3100 models	
Cisco Nexus 3172PQ Switch	N3K-C3172PQ-10GE
Cisco Nexus 3172PQ -XL Switch	N3K-C3172PQ-XL
Cisco Nexus 3172TQ Switch	N3K-C3172TQ-10GT N3K-C3172TQ-32T
Cisco Nexus 31128PQ Switch	N3K-C31128PQ-10GE
Cisco Nexus 3100v models	
Cisco Nexus 31108PC-V Switch	N3K-C31108PC-V
Cisco Nexus 31108TC-V Switch	N3K-C31108TC-V
Cisco Nexus 3132Q-V Switch	N3K-C3132Q-V
Cisco Nexus 3100Z models	
Cisco Nexus 3132C-Z Switch	N3K-C3132C-Z
Cisco Nexus 3200 models	
Cisco Nexus 3232C Switch	N3K-C3232C
Cisco Nexus 3264C-E Switch	N3K-C3264C-E
Cisco Nexus 3400 models	
Cisco Nexus 34180-YC Switch	N3K-C34180YC
Cisco Nexus 3464C Switch	N3K-C3464C
Cisco Nexus 3432D-S Switch	N3K-C3432D-S
Cisco Nexus 3408-S Switch	N3K-C3408-S

Product Name	External Identification
Cisco Nexus 3500 models	
Cisco Nexus 3524-X Switch	N3K-C3524P-10GX
Cisco Nexus 3524-XL Switch	N3K-C3524P-XL
Cisco Nexus 3548-X Switch	N3K-C3548P-10GX
Cisco Nexus 3548-XL Switch	N3K-C3548P-XL
Cisco Nexus 3600 models	
Cisco Nexus 36180YC-R Switch	N3K-C36180YC-R
Cisco Nexus 3636C-R Switch	N3K-C3636C-R
Cisco 9200 models	
Cisco Nexus 92348GC-X Switch	N9K- C92348GC-X
Cisco Nexus 92160YC-X Switch	N9K-C92160YC-X
Cisco Nexus 92300YC Switch	N9K-C92300YC
Cisco Nexus 9272Q Switch	N9K-C9272Q
Cisco 9300 models	
Cisco Nexus 93108TC-EX Switch	N9K-C93108TC-EX
Cisco Nexus 93108TC-FX Switch	N9K-C93108TC-FX
Cisco Nexus 9348GC-FXP Switch	N9K-C9348GC-FXP
Cisco Nexus 93216TC-FX2 Switch	N9K-C93216TC-FX2
Cisco Nexus 93180LC-EX Switch	N9K-C93180LC-EX
Cisco Nexus 93180YC-EX Switch	N9K-C93180YC-EX
Cisco Nexus 93180YC-FX Switch	N9K-C93180YC-FX
Cisco Nexus 93240YC-FX2 Switch	N9K-C93240YC-FX2
Cisco Nexus 93360YC-FX2 Switch	N9K-C93360YC-FX2
Cisco Nexus 9364C Switch	N9K-C9364C
Cisco Nexus 9332C Switch	N9K-C9332C
Cisco Nexus 9336C-FX2 Switch	N9K-C9336C-FX2
Cisco Nexus 9364C-GX Switch	N9K-C9364C-GX
Cisco Nexus 9316D-GX Switch	N9K-C9316D-GX
Cisco Nexus 93600CD-GX Switch	N9K-C93600CD-GX
Cisco 9500 models	
Cisco Nexus 9504 Switch	N9K-C9504
Cisco Nexus 9508 Switch	N9K-C9508
Cisco Nexus 9516 Switch	N9K-C9516
Supervisor 9500-Sup-A	N9K-SUP-A
Supervisor 9500-Sup-A +	N9K-SUP-A+
Supervisor 9500-Sup-B	N9K-SUP-B
Supervisor 9500-Sup-B +	N9K-SUP-B+
System Controller N9k-SC-A	N9K-SC-A

Table 5 Supported Software

Software	Version
Cisco NX-OS	9.3(5)

1.4.1 Supported Configurations

The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 3100, 3100V, 3100Z, 3200, 3400, 3500, 3600, 9200, 9300,. The software is comprised of the NX-OS software image Release 9.3(8).

The Cisco Nexus 3000 and 9000 Series Switches that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware. All security functionality is enforced on the Nexus 3000 and Nexus 9000 Series switches.

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 Operational Environment

1.5.1 Supported non-TOE Hardware/ Software/ Firmware

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

Table 6 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST.

1.6 Example target of Evaluation Development

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

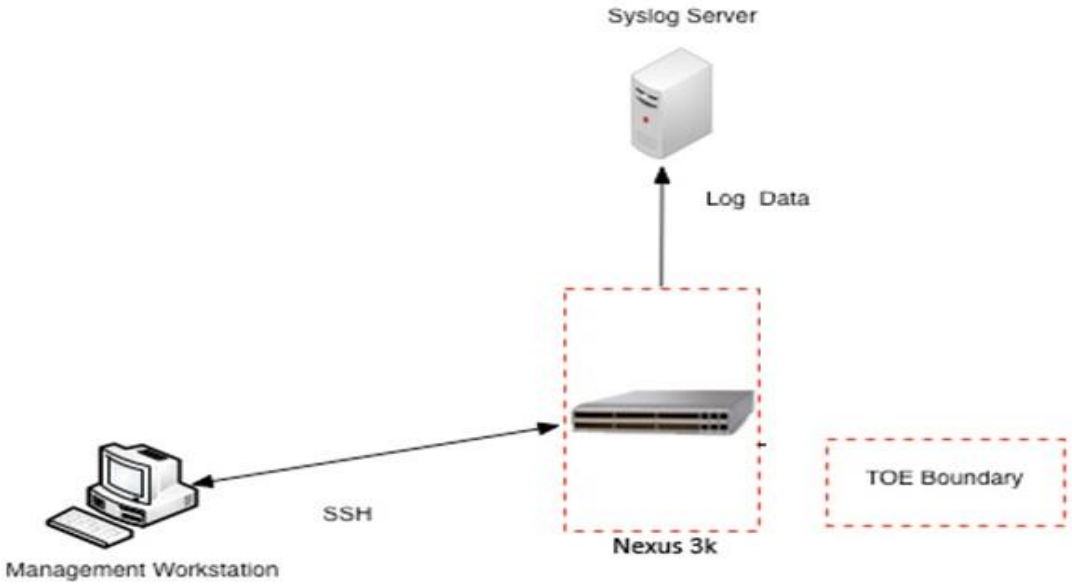

Figure 1 Cisco Nexus 3000 and Environment

The previous figure includes the following:

- The TOE models:
  - Cisco Nexus 3000 Series
- The following are considered to be in the IT Environment:
  - Management Workstation
  - Syslog Server

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

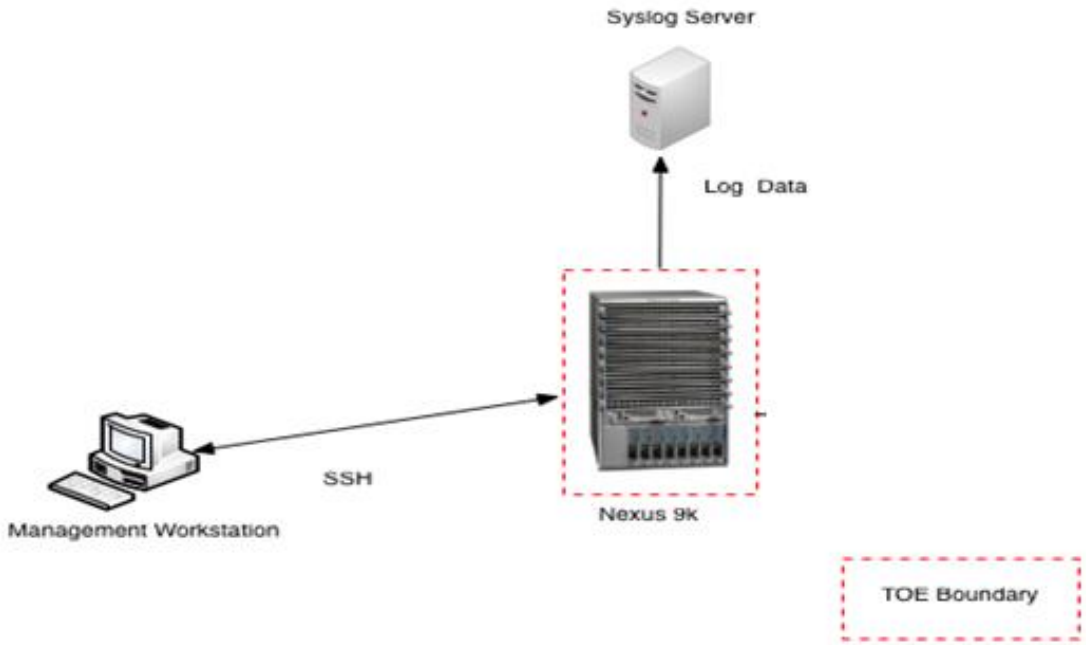

Figure 2 Cisco Nexus 9000 and Environment

The previous figure includes the following:

- The TOE models:
  - Cisco Nexus 9000 Series
- The following are considered to be in the IT Environment:
  - Management Workstation
  - Syslog Server

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

1.7 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 7 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet will be disabled in the evaluated configuration.
SNMP	SNMP will be disabled in the evaluated configuration.
NTP	NTP will be disabled in the evaluated configuration.
DCNM GUI	The DCNM GUI was not included in the evaluated configuration.
Bash shell	Bash shell interface was not included in the evaluation.
PTP	PTP is not included in the evaluation.

These services will be disabled by configuration. The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 2.2e.

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. Ifit 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 Nexus 3K and 9K TOE, the recipient must check the models received against the list of TOE component hardware models listed in **Error! Reference source not found.** Supported Hardware and External identifier.

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: http://www.cisco.com/cisco/software/navigator.html.
- The TOE ships with the correct software images installed, however this may not be the evaluated version.

Step 8 Once the file is downloaded, the authorized administrator verifies that it was not tampered with by either using a hash utility to verify the SHA512 published hash by comparing the SHA512 published hash that is listed on the Cisco web site and in **Error! Reference source not found.** below or by using the

show file command on the Nexus 3K and 9K. The "show file *filename* SHA512sum" command on the Nexus 3K and 9K can be used to verify the SHA512 published hash. Refer to section "Displaying File Checksums" in **[4]**. If the hashes do not match, contact Cisco Technical Assistance Center (TAC), https://tools.cisco.com/ServiceRequestTool/create/launch.do.

Table 8 Evaluated Software Images

Software Version	Filename	Description	SHA 512
NX-OS 9.3(8)	nxos.9.3.8.bin	Cisco Nexus 9000/3000 Standalone Switch	009eaebe96915b0f30eabb16e30c8240b ee16d7194f01d68204c992cc0fae4a3c29 b74ba88f12868a85027be1ed65b22ebc5 ed61306c552f1dd877584a1764fa

For the Cisco Nexus 9500 switches the Operating System resides on the Supervisors and not the chassis or System Controller so these are listed as Not Applicable (N/A) for software image.

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

Step 9 Install the downloaded and verified software image onto your Nexus 3K and 9K as described in section “Setting Up Your Cisco NX-OS Device” of Chapter 3 "Using the Cisco NX-OS Setup Utility" in the *Fundamentals Configuration Guide* **[4]**. Start your Nexus 3K and 9K as described in **[4]**. Confirm that your Nexus 3K and 9K loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

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]** shows the system software release version. See below for the detailed hash value that must be checked to ensure the software has not been modified in anyway.

3. Secure Installation and Configuration

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

- Security audit – ensures that audit records are generated for the relevant events and are securely transmitted to a remote syslog server
- Cryptographic support – ensures cryptography support for secure communications
- Identification and authentication – ensures a warning banner is displayed at login, that all users are successfully identified and authenticated prior to gaining access to the TOE, the users can only perform functions in which they have privileges, and terminates users after a configured period of inactivity
- Secure Management – provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection.
- Protection of the TSF - protects against interference and tampering by untrusted subjects by implementing identification, authentication, the access controls to limit configuration to Authorized Administrators and the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software. TOE performs testing to verify correct operation of the 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 administrator can also terminate their own session by exiting out of the CLI. The TOE can also be configured to display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.
- Trusted Path/Channel - allows trusted channels to be established to itself from remote administrators over SSHv2 for CLI access and with the syslog server using TLS.

3.1 Physical Installation

Follow the Cisco Nexus Mode Switch Hardware Installation and Reference Guides **[7]** for hardware installation instructions. Follow these directions for connecting Nexus 3K models, Nexus 9K models.

3.2 Initial Setup via Direct Console Connection

The Nexus 3K and 9K must be given basic configuration via console connection prior to being connected to any network.

3.2.1 Options to be chosen during the initial setup

For an un-configured Nexus 3K and 9K the setup utility will automatically run at initial startup of the switch from the CLI console. 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 NX-OS 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) Enable password-strength checking by using the command "**password strength-check**", see *Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands)* **[5]** and **[3]** *Cisco*

Nexus 9000 Series NX-OS Security Configuration Guide "Characteristics of strong passwords". This will ensure the password complexity rules are automatically enforced when an administrator user creates their password.

Example:
Do you want to enforce secure password standard (yes/no) [y]: ***y***

2. (Step 3 of Setup Utility) Enter a strong password for the administrator
For the evaluated configuration passwords must be a minimum length of **15** characters and composed of any combination of upper and lower case letters, numbers, and the following special characters: *["<", ",", ">", ".", ":", ";", "/", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")",[no other characters]*];

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

Note: SNMP is not part of the evaluated configuration and **must be disabled**.

4. Configure advanced IP options such as the static routes, default network, DNS, and domain name is optional

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

Note: No is the default here. However, if you choose not to configure the advanced IP options you will skip steps 12-15.

5. (Step 15 of Setup Utility) Telnet service. Telnet is disabled by default. To ensure that the telnet service is **NOT** enabled, select **no** during setup.
Telnet should not be used for management purposes as there is no protection for the data that is transmitted.

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

6. (Step 16 of Setup Utility) SSH is enabled by default, however some of the settings will need to be setup**.** Enable the SSH service by entering yes. You can then enter the key type and number of key bits. For more information, see "Generating SSH Server Keys" from **[3]**. RSA keys of 2048 bits or greater must be used.

Example:
Enable the ssh service? (yes/no) [y]: ***yes***
Type of ssh key you would like to generate (dsa/rsa) : ***rsa***
Number of key bits <768-2048>: ***2048 (or higher)***

7. (Step 17 of Setup Utility) NTP was not part of the evaluated configuration and must be **disabled**.
Do **NOT** enable ntp, To accept the default of '**no**', hit enter..

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

8. (Step 22 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.

Example:
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, in order to save that configuration the running configuration (held in memory) must be copied to the startup configuration. This may be achieved by using the 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 short hand 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 Modes of Operation

A Nexus 3K and 9K Family Switches have 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 of 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 console port to specify a NX-OS image on a TFTP server to load. 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.

3.2.3.1 Module States

The Nexus 3K and 9K 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 9 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 10 Redundancy Modes: for Supervisor

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.

3.2.4 Enabling FIPS Mode

In the evaluated configuration the TOE is run in the FIPS mode of operation, refer to [9] for the certificates associated with the evaluated configuration. By default, FIPS mode is disabled. The "fips mode enable" command needs to be run in order to turn on FIPS mode. A reload is required for the system to operate in FIPS mode.

Enabling FIPS mode restricts the algorithms to ensure that only the permitted algorithms are in the evaluated configuration.
To enable FIPS mode, follow the below steps:
Switch# **configure terminal**

Switch (config)# **fips mode enable**

Switch (config)# **exit**

Switch# **show fips status**

FIPS mode is enabled

Switch# **copy running-config startup-config**

Switch# **reload**

Refer to the command references [**5**] and [**6**.

3.2.4.1 Administration of Cryptographic Self Tests

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

- Power-on Self-Tests:
  - Firmware Integrity Test
  - Known Answer Tests:
    - AES KAT
    - DRBG KAT
    - HMAC KAT
    - KAS ECC KAT
    - KAS FFC KAT
    - RSA KAT
    - SP 800-56B RSA key wrap/unwrap KAT
- Conditional Self-Tests (run periodically during normal operation):
  - Continuous Random Number Generator test for DRBG
  - Continuous Random Number Generator test for Entropy Source
  - RSA Pairwise Consistency Test

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 NX-OS 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.

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 has to 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]*

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

Also an exhaustive list of NX-OS error messages are located in the *Cisco Nexus 3000 Series NX-OS System Messages Reference , Cisco Nexus 9000 Series NX-OS System Messages Reference* **[8].**

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 has to 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, the following actions should be taken:

- Use the **system cores** command to set up core dumps on the system. This will provide additional information on the cause of the crash:
  switch# **configure terminal**
  switch(config)# **system cores slot0:core_file**
  Example:
  switch# **system cores tftp://x.x.x.x/filename**

switch# **show system cores**

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

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

If the problem persists, contact Cisco Technical Assistance via http://www.cisco.com/techsupport or 1 800 553-2447

3.2.5 Administrator Configuration and Credentials

The Nexus 3K and 9K must be configured to use a username and password for each administrator. Ensure all passwords are stored encrypted by using the following listed commands. See **[5]** *Cisco Nexus 3000 Series NX-OS Command Reference (Configuration Commands)*, *Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands)* and **[3]** *Cisco Nexus 9000 Series NX-OS Security Configuration Guide* – Chapter 18 Configuring Password Encryption for the following commands:

Switch# **key config-key ascii**
Switch# **conf terminal**
Switch (config)# **feature password encryption** aes
Switch (config)# (Optional) **show encryption service stat**
Switch (config)# **copy run start**

Configures local AAA authentication:

Switch# configure terminal
TOE-common-criteria(config)# **aaa authentication login default local**

3.2.5.1 Assigning User Roles

All NX-OS administrators will have a role assigned to them. See **[5]** *Cisco Nexus 3000 Series NX-OS Command Reference (Configuration Commands)*, *Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands)* for the following commands:

User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

The commands below, enables the authorized administrator to enter the global configuration mode and display the user roles available. An authorized administrator can configure other user roles, if necessary.

For the username command, valid characters are uppercase letters A through Z, lowercase letters a through z, numbers 0 through 9, hypen (-), period (.), underscore (_), plus sign (+), and equal sign (=). The at symbol (@) is not supported in local usernames. "5" specifies that the password is in encrypted format.

Switch (config)# **configure terminal**
Switch (config)# (Optional) **show rol**

Switch (config)# **username [user-id] [password [0 | 5] password] [role role-name]**

Example:
switch(config)# username NewUser password 5 4Ty18Rnt!Cn%9aP network-admin

Switch (config)# **exit**
Switch (config)# (Optional) **show user-account**
Switch (config)# (Optional) **copy running-config startup-config**

An authorized administrator can configure up to 64 user custom user roles. Each user role can have up to 256 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 be executed only through the predefined network-admin role. For more information on user roles, see the Cisco Nexus 3000 Series NX-OS Security Command Reference, Cisco Nexus 9000 Series NX-OS Security Command Reference **[6]**.

3.2.6 Password Length

To prevent administrators from choosing insecure passwords, each password must be at least 15 characters long. The password strength checking must be enabled. See *Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Cisco Nexus 9000 Series NX-OS Security Configuration Guide – Chapter 3 Configuring Secure Login Features – Restricting the Password length* **[3]**.

The command is **userpassphrase {min-length *min-length* | max-length *max-length* }**
To enable restricted password length, follow the steps below:

Switch# **configure terminal**
Switch (config)# **userpassphrase min-length 15 max-length 15**
Switch (config)# **exit**
Switch# **userpassphrase length**
Displays the minimum and maximum length of the user password
Switch# **copy running-config startup-config**
Switch# **reload**

Note: passwords can be set from 6 -127 characters. For the evaluated configuration the minimum length must be set to 15.

3.2.7 Session Termination

Inactivity settings must trigger termination of the administrator session. Refer to *Cisco Nexus 3000 Series NX-OS Command Reference (Configuration Commands), Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands)* ***[5]***. Configuration of these settings is limited to the privileged administrator (see Section 4.1).

3.2.7.1 Configuring Port Console

To configure a timeout after inactivity is follows:

Switch#**configure terminal**
Switch (config)# **line console**
Switch (config)# **exec-timeout** *minutes*
Switch (config)# **exit**

Switch# **show line console**
Switch# **copy running-config startup-config**

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.

3.2.7.2 Configuring Virtual Terminals

A timeout for inactive virtual terminal sessions can be configured. An Authorized Administrator from the global configuration mode, is required to enter the line mode in order to set up a timeout on inactivity from a virtual terminal

.

Switch#**configure terminal**
Switch (config)# **line vty**
Switch (config-line)# **exec-timeout** *minutes*
Switch (config-line)# **exit**
Switch (config)# **exit**
Switch# **show running-config all | begin vty**
Switch# **copy running-config startup-config**

Statistics can be enabled with the access list **statistics per-entry**. The following example illustrates a basic policy that permits SSH traffic from a specific subnet to all IP addresses configured. All traffic is permitted if an access-class is applied to the VTY port and the associated access-list is deleted from the configuration.

```
n9000(config)# ip access-list vty-acl-in
n9000(config-acl)# permit tcp x.x.x.x/24 any eq 22
n9000(config)# line vty
n9000(config-line)# ip access-class vty-acl-in in
```

3.2.8 Logout

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

3.3 Network Protocols and Cryptographic Settings

3.3.1 Remote Administration Protocols

Telnet for management purposes is disabled by default. By default, the Secure Shell (SSHv2) server is enabled. NX-OS only supports SSHv2 with the following by default.

- encryption algorithms, aes128-ctr, aes256-ctr, *AEAD_AES_128_GCM, AEAD_AES_256_GCM* to ensure confidentiality of the session.
- hashing algorithms hmac-sha1, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM and *AEAD_AES_256_GCM* to ensure the integrity of the session.
- SSH transport implementation public key algorithms: rsa-sha2-256, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521
- Key Exchange Algorithms: diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384 and Ecdh-sha2-nistp521
- MACs: hmac-sha1,hmac-sha2-256,hmac-sha2-512

The command to enable ssh is the feature ssh command **[5].** The SSH setting is configured during the initial setup. To edit the ssh configuration see "Configuring SSH" from **[3],** chapter 7. The below steps are included as a reference since SSHv2 is enabled by default

3.3.1.1 SSH Server Configuration

1. Generate RSA key material **[5]** choose a longer modulus length for more secure keys (i.e., 2048 for RSA and 256):

   Switch (config)# **ssh key rsa** *i0*

   For the evaluated configuration 2048 must be selected.

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

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

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

2. To enable ssh, use the enable ssh server command:

   TOE-common-criteria(config)# **feature ssh**[1]

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. 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.

n9000(config)# **ip access-list mgmt0-access**
n9000(config-acl)# **statistics per-entry**
n9000(config-acl)# **permit tcp x.x.x.x/x b.b.b.b/32 eq 22**
n9000(config-acl)# **permit tcp x.x.x.x/x b.b.b.b/32 eq tacacs**
n9000(config)# **line vty**
n9000(config-line)# **access-class mgmt0-access in**
.

3.3.1.2 Specifying the SSH Public Keys for user Accounts

To specify SSH public keys, The *Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Configuring SSH and Telnet* **[3]** provides summary steps:

Switch # **configure terminal**
Switch (config)# **username** *username* **sshkey** *ssh-key*

[1] **feature ssh** was introduced to replace the **ssh server enable** command

Switch (config)# exit
Switch # **copy running-config startup-config**

3.3.1.3 Generating SSH ReKeys thresholds

To generate SSH Rekey thresholds, The The *Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Configuring SSH and Telnet* **[3**] provides summary steps. For the evaluated configuration max-data must be set to 1g and max-time must be set to 60 minutes.

Switch # **configure terminal**
Switch (config)# **ssh rekey max-data** *1g* **max-time** *60m*
Switch # **copy running-config startup-config**

3.3.1.4 Generating SSH ECDSA Keys

To generate SSH edcsa, The *Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Configuring SSH and Telnet* **[3**] provides summary steps, while SSH Key **[5]** provides the syntax for the SSH Key command:

Switch # **configure terminal**
Switch (config)# **no feature ssh** **(**to disable ssh)
Switch (config)# **ssh key ecdsa** *i0*
i0 is for the key size in bits (256, 384 or 521)
Switch (config)# **ssh rekey max-data** *1g* **max-time** *60m*
Switch (config)# **feature ssh** **(**to enable ssh)
Switch (config)**#exit**
Switch # **show ssh key ecdsa**
Switch # **copy running-config startup-config**

3.3.1.5 Zeroize RSA Keys

To zeroize all RSA keys use the following command:
Switch**# crypto key zeroize rsa**

3.3.2 Logging Configuration

The Nexus 3k and 9K can be configured to generate an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include events related to the enforcement of information flow policies, identification and authentication related events, and administrative events. Additionally, the startup and shutdown of the TOE generates an audit record to indicate the TOE is up and operational or is shutting down and all processes are stopping. Configuring System Message Logging" in reference document **[2]** provides information on system logging and the severity levels.

A complete list of available audit messages for the Nexus 3k and 9K product, beyond what is required for the evaluated configuration can be found in reference document **[8]**.

By default, the device outputs messages to terminal sessions and logs system messages to a log file.
To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled so that the audit records are being generated for the required auditable events.

- Timestamps must be enabled for the audit records. The default is seconds.

  TOE-common-criteria (config)#**logging timestamp**{ microseconds| milliseconds| seconds}
- Set the size logging file. The range is from 4096 to 4194304 bytes

  TOE-common-criteria (config)#**logging logfile** *logfile-name severity-level* [**size** *bytes*]

- To view logfiles after they have been saved. Refer to **[6]** for the show logging syntax.
  TOE-common-criteria (config)#**show logging logfile**

- To generate logging messages for failed and successful login attempts in the evaluated configuration, issue the login on-failure and login on-success commands. Note these requirements are syslog level 6 (informational) so if debugging level (**logging buffer debug**) of audit is not set as a default, then at least informational (**logging buffer informational**) level will need to be set: The *Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Cisco Nexus 9000 Series NX-OS Security Configuration Guide* **[3**] provides an example.

  Switch (config)# **login on-failure log**
  Switch (config)# **login on-success log**

- To enable SSH Logging. This requires debug level (7) auditing.

  TOE-common-criteria # **configure terminal**
  Switch (config)# **terminal log-all**
  Switch (config)# **logging logfile** *logfile-S* **7 size 4096**
  Switch (config)# **logging level daemon 7**
  Switch (config)# **logging level auth 7**
  Switch (config)# **logging level authpriv 7**
  Switch (config)# **copy running-config startup-config**
- To append hostname, an IP address or text string to the syslog messages.
  Switch (config)# **logging origin-id** {**hostname**| **ip** *ip-address*| **String** *text-string*}

- Enable debugging in privileged EXEC mode enter the following:
  Switch (config)# **logging debug**

- To protect against audit data loss if the Nexus 9K fails, the audit records can be saved to a file by using the global configuration command:

  Switch (config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]

Note: Debug level auditing is required for specific protocols and events to ensure the audit records with the level of information are generated to meet the requirements in the Security Target. When that level of auditing is required, it is annotated as such throughout this document.

Before you start a debug command, always consider the output that this command will generate and the amount of time this can take. Before debugging, look at your CPU load with the "**show processes cpu"** command **[6]**. Verify that you have ample CPU available before you begin the debugs and use the debug commands with caution.

3.3.2.1 Remote Logging

To protect against audit data loss the TOE must be configured to send the audit records securely (via TLS) to an external Secure Syslog Server. By default system messages are logged to the console and the logfile,

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

Since this functionality is not enabled by default refer to "Configuring System Messages Logging, - Configuring Secure Syslog Servers" in **[2]** to configure this option. For the evaluated configuration the reference identifier is *host* referenced in "Configuring System Messages Logging, - Configuring Secure Syslog Servers" in **[2]** command

Switch (config)# **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]

You will also need to configure local logging. Refer to **[2]** Configuring System Message Logging to configure local logging. It is recommended to read the entire "Configuring System Messages Logging" section to become familiar with the concept and configuration before configuring local and remote logging.

Using a secure TLS connection for Syslog Server is required in the evaluated configuration: The minimum TLS version for use to TLSv1.2 with support for the following ciphers.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The following NIST curves are supported by default in the evaluated configuration: secp256r1, secp384r1. No administrator configuration is required in order to use these curves.

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

Once the syslog server is setup, the following will send a static syslog in NX-OS whenever a user executes any cli. Cli_log is the applet name.

Switch#**configure terminal**
Switch(config)#**event manager applet** *cli_log*
Switch(config-applet)# event cli match ".*"
Switch(config-applet)# action 1.0 syslog msg CLi executed
Switch(config-applet)#action 2.0 event-default
Switch(config)#**copy running-config startup-config**

For more information refer to [2] *Configuring the Embedded Event Manager*.

3.3.3 X509 Certificates

For secure syslog, the remote server must be authenticated via a trustpoint configuration. Refer to **[2]** *Configuring the CA Certificates***.**

- Configuring the CA Certificates
  Switch# **configure terminal**
  Switch (config)# **crypto ca trustpoint** *trustpoint-name*
  Switch (config-trustpoint)#**crypto ca authenticate** *trustpoint-name*
  Switch (config)# **show crypto ca certificate**
  Switch (config)# **copy running-config startup-config**

3.3.3.1 Peer Certificate Verification

The Cisco NX-OS software verifies certificates received from peers during security exchanges for applications. The applications verify the validity of the peer certificates. The Cisco NX-OS software performs the following steps when verifying peer certificates:

- Verifies that the peer certificate is issued by one of the locally trusted CAs.
- Verifies that the peer certificate is valid (not expired) with respect to current time.
- Verifies that the peer certificate is not yet revoked by the issuing CA.
- Verifies that the peer certificate includes Server Authentication in extendedKeyUsage.
- Verifies that the reference identifier of the peer certificate matches what has been configured.

3.3.3.2 Certificate Revocation

The Cisco NX-OS software can check the revocation status of CA certificates. Online Certificate Status Protocol (OCSP) is a method to check certificate revocation when a peer has to retrieve this revocation information and then validate it to check the certificate revocation status. In this method, the certification revocation status is limited by the peer's ability to reach an OCSP responder through the cloud or by the certificate sender's performance in retrieving the certificate revocation-information.

When the remote syslog server shares the certificate which has an OCSP responder URL, the client sends the server certificate to an external OCSP responder (CA) server. The CA server validates this certificate and confirms if it is a valid or a revoked certificate. In this case, the client does not have to maintain the revoked certificate list locally.

4. Secure Management

Cisco NX-OS devices perform authentication using the local database.

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 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations. An authorized administrator can also limit access to specific VLANs, virtual routing and forwarding instances (VRFs), and interfaces.

The Cisco NX-OS software provides default user roles as follows:

- network-admin - Complete read-and-write access to the entire Cisco NX-OS device
- network-operator - Complete read access to the entire Cisco NX-OS device

An authorized user cannot change these default roles and their associated privileges. NX-OS does allow for custom roles to be created. Chapter 8 "Configuring User Accounts and RBAC", section "Creating User Roles and Rules" in the **[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 section "User Roles" in chapter 8 of **[3]** Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Cisco Nexus 3000 Series NX-OS Security Configuration Guide and **[6]** Cisco Nexus 9000 Series NX-OS Security Command Reference, Cisco Nexus 3000 Series NX-OS Security Command Reference.

4.2 Local Passwords

The password complexity is enforced by the switch using the "**password strength-check**" command, see "Enabling Password-Strength Checking" in **[3]**.

```
Switch# conf t
Switch (config)# password strength-check
Switch (config)# exit
Switch# copy run start
```

When an authorized administrator enables password-strength checking, the Cisco NX-OS software only allows an administrator to create strong passwords. Only strong passwords based on the following characteristics will be allowed to be created:

- 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

For the evaluated configuration passwords must be a **minimum length of 15 characters** and composed of any combination of upper and lower case letters, numbers, and the following special characters: *[*"<", ",", ">", ".", ":", ";", "/", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")",*[no other characters]*];

Administrative passwords, including any "enable" password that may be set for any privilege level, must be stored in non-plaintext form.

4.3 Clock Management

Clock management is restricted to the privileged administrator.

For instructions to set the timezone for the clock, refer to section "Configuring the Time Zone" in **[4]**.
To manually set the clock see section "Manually Setting the Device Clock" in **[4]**.

Switch# **clock set** *time day month year*

For Example:
Switch# clock set 15:00:00 30 May 2008 Fri May 30 15:14:00 PDT 2008

To set the clock manager, see section "Setting the Clock Manager" in **[4]**.

Switch# **clock protocol none**

For Example: Switch# **clock protocol** *none*

4.4 Identification and Authentication

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

The Nexus 3K and 9K can be configured to use Local authentication (password or SSH public key authentication) as described in Sections 3.2, 3.3, 4.1 and 4.2 of this document.

4.5 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 "This is a banner" use the command. See **[5]** *Cisco Nexus 3000 Series NX-OS Command Reference (Configuration Commands), Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands)*

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

4.6 Authentication failure

Administrator account access is to be restricted to a specified number of authentication attempts before the

administrator account in question is locked out. The account then requires unlocking after an authorized administrator predefined time period before it can be used again.

The evaluated configuration requires that the lockout occurs after a specified threshold for unsuccessful authentication attempts.

Switch (config) # **ssh login-attempts** <*number*>

Example
Switch (config) # **ssh login-attempts** *3*

Where number of failures is the number of consecutive failures that will trigger locking of the account. For the evaluated configuration this should be configured to between 1 – 3 failure attempts.

To configure the evaluated configuration to block failed authentication attempts for a period of time, the following commands are used.

Switch (config) #**aaa authentication rejected <***attempts* **in** *seconds* **ban** *seconds*>

Example
Switch #**aaa authentication rejected** *2* **in** *60* **ban** *100*

The example shows how to configure the switch to enter a 100-second quiet period if 2 failed login attempts are exceeded within 60 seconds. After this command is entered, all login attempts made through SSH are denied during the quiet period.

Note: Both commands must be used in conjunction.

Configuration of these settings is limited to the privileged administrator (see Section 4.1).

4.7 Product Updates

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

5. Security Relevant Events

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server.

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above. The details for configuration of these settings are covered in Section 3.2.2 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 Descriptions

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

The local audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. The audit fields in each audit event will contain at a minimum the following:

Example Audit Event: 2016 Feb 4 16:27:31 N9k %$ VDC-1 %$ %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:reload (REDIRECT)
Date: 2016 Feb 4
Time: 16:27:31
Type of event: %AAA-6-AAA_ACCOUNTING_MESSAGE

Subject identity: admin

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.

2016 Feb 4 16:27:37 N9k %$ VDC-1 %$ %SYSMGR-6-SUBPROC_SUCCESS_EXIT: "System Manager (core-server)" (PID 10361) has successfully exited with exit code

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 11 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 startup of the switch. Below just shows the audit event for stopping sending logs to remote syslog server. **Shutdown:** *Aug 11 16:00:39 nexus3k.example.com : 2021 Aug 11 17:59:24 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:Rebooting the switch* *Aug 11 16:00:39 nexus3k.example.com : 2021 Aug 11 17:59:24 EST: %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface* **Start up** *Aug 11 16:03:10 nexus3k.example.com : 2021 Aug 11 18:01:54 EST: %ASCII-CFG-2-CONF_CONTROL: System ready* *Aug 11 16:04:06 nexus3k.example.com : 2021 Aug 11 18:02:51 EST: %USER-2-SYSTEM_MSG: Switch is now running in FIPS mode - security* **Nexus9k** **Shutdown:** *Jun 3 19:06:11 nexus9k.example.com : 2021 Jun 3 18:05:37 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:Rebooting the switch* *Jun 3 19:06:11 nexus9k.example.com : 2021 Jun 3 18:05:37 EST: %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface* **Start up:** *Jun 3 19:09:39 nexus9k.example.com : 2021 Jun 3 18:09:04 EST: %ASCII-CFG-2-CONF_CONTROL: System ready* *Jun 3 19:10:09 nexus9k.example.com : 2021 Jun 3 18:09:34 EST: %USER-2-SYSTEM_MSG: Switch is now running in FIPS mode - securityd*

FCS_SSHS_EXT.1	Failure to establish an SSH Session.	Reason for failure.	**Nexus3k:** *Oct 26 16:45:20 nexus3k.example.com : 2020 Oct 26 16:18:57 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 57990: no matching cipher found. Their offer: aes128-cbc [preauth] - dcos_sshd[4021]* *Oct 26 18:17:11 nexus3k.example.com : 2020 Oct 26 17:50:51 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 60794: no matching host key type found. Their offer: ecdsa-sha2-nistp256 [preauth] - dcos_sshd[25256]* *Oct 27 00:44:14 nexus3k.example.com : 2020 Oct 27 00:18:05 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 37840: no matching MAC found. Their offer: hmac-sha1-96 [preauth] - dcos_sshd[16812]* *Oct 27 00:50:50 nexus3k.example.com : 2020 Oct 27 00:24:41 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 39070: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c [preauth] - dcos_sshd[18426]* **Nexus9k**: *Oct 26 19:54:51 nexus9k.example.com : 2020 Oct 26 18:52:27 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 48552: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth] - dcos_sshd[9310]* *Oct 27 00:47:02 nexus9k.example.com : 2020 Oct 26 23:44:38 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 51348: no matching MAC found. Their offer: hmac-md5 [preauth] - dcos_sshd[16220]* *Oct 27 00:51:41 nexus9k.example.com : 2020 Oct 26 23:49:17 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 52168: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c [preauth] - dcos_sshd[17574]* *Oct 26 18:12:34 nexus9k.example.com : 2020 Oct 26 17:10:10 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 44392: no matching cipher found. Their offer: aes128-cbc [preauth] - dcos_sshd[16148]*

FCS_TLSC_EXT.1	Failure to establish an TLS session	Reason for failure.	**Nexus3k:** *May 7 10:47:52 nexus3k.example.com : 2021 May 7 11:57:01 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] – syslogd* *May 7 10:46:19 nexus3k.example.com : 2021 May 7 11:55:27 EST: %SYSLOG-5-SYSTEM_MSG: Subject Name validation Failed for SSL connection to 192.168.144.254:6514 in [vrf: management] - syslogd* *Oct 26 18:11:43 nexus3k.example.com : 2020 Oct 26 17:45:23 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 59526: no matching cipher found. Their offer: aes256-cbc [preauth] - dcos_sshd[23883]* *Apr 9 17:06:35 nexus3k.example.com : 2021 Apr 9 17:56:03 EST: %USER-2-SYSTEM_MSG: TLS certificate verification: Error, certificate signature failure - syslogd* *Nov 23 17:51:59 nexus3k.example.com : 2020 Nov 23 18:06:55 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, self signed certificate in certificate chain - syslogd* *Nov 19 12:33:10 nexus3k.example.com : 2020 Nov 19 12:45:05 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, unsupported certificate purpose - syslogd* *Apr 9 16:55:37 nexus3k.example.com : 2021 Apr 9 17:45:04 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error] -syslogd* *Apr 9 16:07:41 nexus3k.example.com : 2021 Apr 9 16:57:07 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib] – syslogd* *Aug 11 16:51:33 nexus3k.example.com : 2021 Aug 11 18:50:20 EST: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type - syslogd*

			Aug 11 16:57:02 nexus3k.example.com : 2021 Aug 11 18:55:48 EST: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned - syslogd *Aug 11 17:02:27 nexus3k.example.com : 2021 Aug 11 19:01:13 EST: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1409210A:SSL routines:ssl3_get_server_hello:wrong ssl version - syslogd* **Nexus9k:** *Dec 1 22:47:57 nexus9k.example.com : 2020 Dec 1 22:47:52 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] - syslogd* *Dec 2 16:55:19 nexus9k.example.com : 2020 Dec 2 16:55:14 EST: %SYSLOG-5-SYSTEM_MSG: Subject Name validation Failed for SSL connection to 192.168.144.254:6514 in [vrf: management] - syslogd* *Dec 1 23:56:45 nexus9k.example.com : 2020 Dec 1 23:56:40 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, unsupported certificate purpose - syslogd* *Dec 3 15:36:20 nexus9k.example.com : 2020 Dec 3 15:36:14 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error] - syslogd* *Dec 3 15:40:46 nexus9k.example.com : 2020 Dec 3 15:40:40 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, certificate signature failure - syslogd* *Dec 8 19:17:48 nexus9k.example.com : 2020 Dec 8 19:17:41 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib] – syslogd* *Aug 11 17:15:33 nexus9k.example.com : 2021 Aug 11 16:14:43 EST: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1409210A:SSL routines:ssl3_get_server_hello:wrong ssl version - syslogd*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			Aug 11 17:20:36 nexus9k.example.com : 2021 Aug 11 16:19:46 EST: %SYSLOG-4-SYSTEM_MSG: SSL_connect: SSL_get_error() = 1 SSL_connect error: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned - syslogd *Aug 11 17:24:18 nexus9k.example.com : 2021 Aug 11 16:23:28 EST: %SYSLOG-4-SYSTEM_MSG:SSL_connect: SSL_get_error() = 1 SSL_connect error: error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type - syslogd*
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).	**Nexus3k:** *Oct 28 18:30:33 nexus3k.example.com : 2020 Oct 28 18:05:38 UTC: %DAEMON-3-SYSTEM_MSG: error: maximum authentication attempts exceeded for admin from 192.168.144.253 port 54676 ssh2 [preauth] - dcos_sshd[28086]* *Oct 28 18:30:33 nexus3k.example.com : 2020 Oct 28 18:05:38 UTC: %DAEMON-6-SYSTEM_MSG: Disconnecting authenticating user admin 192.168.144.253 port 54676: Too many authentication failures [preauth] - dcos_sshd[28086]* **Nexus9k:** *Nov 23 15:50:20 nexus9k.example.com : 2020 Nov 23 15:50:16 EST: %DAEMON-3-SYSTEM_MSG: error: maximum authentication attempts exceeded for admin from 192.168.144.254 port 49924 ssh2 [preauth] - dcos_sshd[5056]* *Nov 23 15:50:20 nexus9k.example.com : 2020 Nov 23 15:50:16 EST: %DAEMON-6-SYSTEM_MSG: Disconnecting authenticating user admin 192.168.144.254 port 49924: Too many authentication failures [preauth] - dcos_sshd[5056]*

FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**Nexus 3k:** **SSH Password Success** *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %DAEMON-7-SYSTEM_MSG: Got user name <admin> - dcos_sshd[28889]* *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %DAEMON-7-SYSTEM_MSG: remote host: 192.168.144.254 - dcos_sshd[28889]* *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %DAEMON-7-SYSTEM_MSG: user admin authenticated - dcos_sshd[28889]* *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %DAEMON-7-SYSTEM_MSG: result->context->protocol 11 - dcos_sshd[28889]* *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %DAEMON-6-SYSTEM_MSG: Accepted keyboard-interactive/pam for admin from 192.168.144.254 port 56974 ssh2 - dcos_sshd[28887]* *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session opened for user admin by (uid=0) - dcos_sshd[28887]* **SSH Password failure** *Oct 26 16:07:09 nexus3k.example.com : 2020 Oct 26 15:40:45 UTC: %DAEMON-3-SYSTEM_MSG: error: PAM: Authentication failure for admin from 192.168.144.254 - dcos_sshd[26924]* **SSH Public Key Success** *Nov 2 16:43:16 nexus3k.example.com : 2020 Nov 2 16:43:18 EST: %DAEMON-6-SYSTEM_MSG: Accepted publickey for admin from 192.168.144.254 port 46964 ssh2: ECDSA SHA256:kPXBg+5BLcJGbqI7XFEka7Js6gEUdjSSkdhNNQRL7Xw - dcos_sshd[27165]* *Nov 2 16:43:16 nexus3k.example.com : 2020 Nov 2 16:43:18 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session opened for user admin by (uid=0) - dcos_sshd[27165]* **SSH Public Key Failure:** *Oct 26 19:55:15 nexus3k.example.com : 2020 Oct 26 19:28:57 UTC: %DAEMON-6-SYSTEM_MSG: FIPS mode initialized - dcos_sshd[15320]* *Oct 26 19:55:16 nexus3k.example.com : 2020 Oct 26 19:28:58 UTC: %DAEMON-6-SYSTEM_MSG: Postponed*

			keyboard-interactive for admin from 192.168.144.254 port 36028 ssh2 [preauth] - dcos_sshd[15320] *Oct 26 19:55:16 nexus3k.example.com : 2020 Oct 26 19:28:58 UTC: %DAEMON-6-SYSTEM_MSG: Connection closed by authenticating user admin 192.168.144.254 port 36028 [preauth] - dcos_sshd[15320]* **Local Success** *Feb 10 16:51:43 nexus3k.example.com : 2021 Feb 10 18:00:03 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_aaa:Authentication success for user admin from console – login* **Local Failure** *Feb 10 16:54:44 nexus3k.example.com : 2021 Feb 10 18:03:04 EST: %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from console - login* *Feb 10 16:54:44 nexus3k.example.com : 2021 Feb 10 18:03:04 EST: %AUTHPRIV-5-SYSTEM_MSG: Login failed for user admin – login* **Nexus9k:** **SSH Password Success** *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %DAEMON-7-SYSTEM_MSG: Got user name <admin> - dcos_sshd[19415]* *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %DAEMON-7-SYSTEM_MSG: remote host: 192.168.144.254 - dcos_sshd[19415]* *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %DAEMON-7-SYSTEM_MSG: user admin authenticated - dcos_sshd[19415]* *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %DAEMON-7-SYSTEM_MSG: result->context->protocol 11 - dcos_sshd[19415]* *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %DAEMON-6-SYSTEM_MSG: Accepted keyboard-interactive/pam for admin from 192.168.144.254 port 41514 ssh2 - dcos_sshd[19412]* *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session opened for user admin by (uid=0) - dcos_sshd[19412]* **SSH Password Failure** *Oct 26 16:07:33 nexus9k.example.com : 2020 Oct 26 15:05:09 UTC: %DAEMON-3-SYSTEM_MSG: error:*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			PAM: Authentication failure for admin from 192.168.144.254 - dcos_sshd[17645] **SSH Public Key Success** *Nov 2 16:53:28 nexus9k.example.com : 2020 Nov 2 16:53:28 EST: %DAEMON-6-SYSTEM_MSG: Accepted publickey for admin from 192.168.144.254 port 36486 ssh2: ECDSA SHA256:kPXBg+5BLcJGbqI7XFEka7Js6gEUdjSSkdhNNQRL7Xw - dcos_sshd[31389]* **SSH Public Key Failure** *Aug 12 10:51:12 nexus9k.example.com : 2021 Aug 12 09:50:21 EST: %DAEMON-6-SYSTEM_MSG: FIPS mode initialized - dcos_sshd[20249]* *Aug 12 10:51:12 nexus9k.example.com : 2021 Aug 12 09:50:22 EST: %DAEMON-6-SYSTEM_MSG: Postponed keyboard-interactive for admin from 192.168.144.254 port 50192 ssh2 [preauth] - dcos_sshd[20249]* *Aug 12 10:51:12 nexus9k.example.com : 2021 Aug 12 09:50:22 EST: %DAEMON-6-SYSTEM_MSG: Connection closed by authenticating user admin 192.168.144.254 port 50192 [preauth] - dcos_sshd[20249]* **Local Success** *Feb 10 16:51:49 nexus9k.example.com : 2021 Feb 10 16:51:36 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_aaa:Authentication success for user admin from console – login* **Local Failure** *Feb 10 16:54:57 nexus9k.example.com : 2021 Feb 10 16:54:44 EST: %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from console - login* *Feb 10 16:54:57 nexus9k.example.com : 2021 Feb 10 16:54:44 EST: %AUTHPRIV-5-SYSTEM_MSG: Login failed for user admin – login*
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

FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure	**Nexus3k** *Dec 4 19:47:04 nexus3k.example.com : 2020 Dec 4 20:09:52 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] – syslogd* *Apr 12 16:54:37 nexus3k.example.com : 2021 Apr 12 17:46:12 EST: %USER-2-SYSTEM_MSG: TLS certificate verification: Error, invalid CA certificate - syslogd* *Dec 4 19:47:04 nexus3k.example.com : 2020 Dec 4 20:09:52 EST: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP certificate is revoked! - syslogd* *Dec 4 20:10:05 nexus3k.example.com : 2020 Dec 4 20:32:53 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error] - syslogd* *Dec 4 20:25:27 nexus3k.example.com : 2020 Dec 4 20:48:15 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, self signed certificate in certificate chain - syslogd* *Dec 7 15:54:50 nexus3k.example.com : 2020 Dec 7 16:19:38 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, certificate signature failure - syslogd* *Dec 7 15:54:50 nexus3k.example.com : 2020 Dec 7 16:19:38 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib] – syslogd* *Dec 2 19:35:27 nexus3k.example.com : 2020 Dec 2 19:56:49 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, certificate has expired - syslogd* *Jun 8 17:17:23 nexus3k.example.com : 2021 Jun 8 18:49:23 EST: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP certificate is revoked! - syslogd* **Nexus9k** *Dec 7 11:07:56 nexus9k.example.com : 2020 Dec 7 11:07:51 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] – syslogd* *Dec 3 15:53:54 nexus9k.example.com : 2020 Dec 3 15:53:48*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, invalid CA certificate - syslogd *Dec 7 11:07:56 nexus9k.example.com : 2020 Dec 7 11:07:51 EST: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP certificate is revoked! - syslogd* *Dec 7 11:16:42 nexus9k.example.com : 2020 Dec 7 11:16:36 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error] – syslogd* *Dec 7 11:20:46 nexus9k.example.com : 2020 Dec 7 11:20:40 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, self signed certificate in certificate chain - syslogd* *Dec 8 19:17:48 nexus9k.example.com : 2020 Dec 8 19:17:41 EST: %SYSLOG-4-SYSTEM_MSG: TLS certificate verification: Error, certificate signature failure - syslogd* *Dec 8 19:17:48 nexus9k.example.com : 2020 Dec 8 19:17:41 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib] - syslogd* *Apr 13 16:10:56 nexus9k.example.com : 2021 Apr 13 15:10:33 EST: %USER-2-SYSTEM_MSG: TLS certificate verification: Error, certificate has expired - syslogd* *Jun 8 17:18:24 nexus9k.example.com : 2021 Jun 8 16:17:48 EST: %SYSLOG-4-SYSTEM_MSG: tls_verify_cb: OCSP certificate is revoked! - syslogd*
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.	See FPT_TUD_EXT.1
FMT_MTD.1/CoreData	Management of cryptographic keys	None.	See FMT_SMF.1

FMT_SMF.1	All management activities of TSF data.	None.	**Reset Password** **Nexus3K** *Jun 9 11:24:49 nexus3k.example.com : 2021 Jun 9 12:57:21 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/0:admin:configure terminal ; username gossamer password 5 ******** role network-admin (SUCCESS)* *Nov 23 23:32:34 nexus3k.example.com : 2020 Nov 23 23:47:39 EST: %AUTHPRIV-6-SYSTEM_MSG: changed password expiry for test admin - chage[25423]* *Jun 23 03:39:11 nexus3k.example.com : 2021 Jun 23 05:21:24 EST: %AUTHPRIV-6-SYSTEM_MSG: change user 'testadmin' password - usermod[15231]* ***Nexus9K*** *Jun 23 10:44:31 nexus9k.example.com : 2021 Jun 23 09:43:52 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; username testadmin password ******** (SUCCESS)* *Oct 27 20:41:14 nexus9k.example.com : 2020 Oct 27 19:38:50 UTC: %AUTHPRIV-6-SYSTEM_MSG: changed password expiry for testadmin - chage[18125]* *Oct 27 20:41:14 nexus9k.example.com : 2020 Oct 27 19:38:50 UTC: %AUTHPRIV-6-SYSTEM_MSG: change user 'testadmin' password - usermod[18146]* **Generate/Import/change/Delete Cryptographic Key** **Nexus 3k** *Jun 3 14:14:07 nexus3k.example.com : 2021 Jun 3 15:42:29 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/0:admin:configure terminal ; no ssh key rsa (SUCCESS)* *Jun 3 14:03:47 nexus3k.example.com : 2021 Jun 3 15:32:09 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update::}user:rsa key cleared* *Thu Jun 3 15:42:47 2021:type=update:id=:}:user=rsa key created with size:cmd=2048* *Thu Jun 3 15:42:47 2021:type=update:id=192.168.144.254@pts/0:user=admin:cmd=configure terminal ; ssh key rsa 2048 (SUCCESS)* *Jun 3 14:14:25 nexus3k.example.com : 2021 Jun 3 15:42:47 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE:*

			update:192.168.144.254@pts/0:admin:configure terminal ; ssh key rsa 2048 (SUCCESS) *Jun 3 14:16:25 nexus3k.example.com : 2021 Jun 3 15:44:47 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/0:admin:configure terminal ; ssh key rsa 2048 force (SUCCESS)* **Nexus 9k** *Jun 3 18:13:32 nexus9k.example.com : 2021 Jun 3 17:12:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update::}user:rsa key cleared* *Jun 3 18:13:32 nexus9k.example.com : 2021 Jun 3 17:12:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no ssh key rsa (SUCCESS* *Jun 3 18:18:05 nexus9k.example.com : 2021 Jun 3 17:17:31 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:generated RSA keypair Nexus9k* *Jun 3 18:18:05 nexus9k.example.com : 2021 Jun 3 17:17:31 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto key generate rsa modulus 2048 (SUCCESS)* *Jun 3 18:20:19 nexus9k.example.com : 2021 Jun 3 17:19:45 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh key rsa 2048 (SUCCESS)* *Jun 3 18:15:15 nexus9k.example.com : 2021 Jun 3 17:14:41 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update::}user:rsa key created with size:2048* *Jun 3 18:15:15 nexus9k.example.com : 2021 Jun 3 17:14:41 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; ssh key rsa 2048 force (SUCCESS)* **Configure Access banner** **Nexus3k** *Feb 15 12:05:00 nexus3k.example.com : 2021 Feb 15 13:16:44 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no banner motd (SUCCESS)* *Feb 15 12:44:54 nexus3k.example.com : 2021 Feb 15 13:56:40 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; banner motd #CC Test Login Banner!# (SUCCESS)* **Nexus 9k**

			Jun 2 15:03:36 nexus9k.example.com : 2021 Jun 2 14:03:02 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/2:admin:configure terminal ; no banner motd (SUCCESS) *Jun 2 15:03:53 nexus9k.example.com : 2021 Jun 2 14:03:19 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/2:admin:configure terminal ; banner motd #CC Test Banner!# (SUCCESS)* **Configure session inactivity** **Nexus 3k** *Jun 2 15:26:41 nexus3k.example.com : 2021 Jun 2 16:54:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/1:admin:configure terminal ; ssh idle-timeout 60 (SUCCESS)* **Nexus 9k** *Jun 2 15:14:28 nexus9k.example.com : 2021 Jun 2 14:13:54 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/2:admin:configure terminal ; ssh idle-timeout 60 (SUCCESS)* **Update TOE** **Nexus 3k** *May 11 17:00:49 nexus3k.example.com : 2021 May 11 18:12:59 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:copy* *scp://192.168.144.254/nexus/nxos.9.3.7.18.bin bootflash:/ (SUCCESS)* *May 11 17:03:45 nexus3k.example.com : 2021 May 11 18:15:55 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin sha512sum (SUCCESS)* *May 11 17:04:20 nexus3k.example.com : 2021 May 11 18:16:30 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin md5sum (SUCCESS)* *May 11 17:36:48 nexus3k.example.com : 2021 May 11 18:48:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:::NXOS Image set to bootflash:/nxos.9.3.7.18.bin* *May 11 17:36:48 nexus3k.example.com : 2021 May 11 18:48:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:vsh.bin.32099:root:configure terminal ; boot nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS)* *May 11 17:39:20 nexus3k.example.com : 2021 May 11 18:51:30 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE:*

			update:console0:admin:install all nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS) **Nexus 9k** *May 11 17:00:26 nexus9k.example.com : 2021 May 11 15:59:57 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:copy scp://192.168.144.254/nexus/nxos.9.3.7.18.bin bootflash:/ (SUCCESS)* *May 11 17:03:27 nexus9k.example.com : 2021 May 11 16:02:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin sha512sum (SUCCESS)* *May 11 17:04:24 nexus9k.example.com : 2021 May 11 16:03:55 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin md5sum (SUCCESS)* *May 11 17:36:52 nexus9k.example.com : 2021 May 11 16:36:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:::NXOS Image set to bootflash:/nxos.9.3.7.18.bin* *May 11 17:36:52 nexus9k.example.com : 2021 May 11 16:36:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:vsh.bin.31954:root:configure terminal ; boot nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS)* *May 11 17:39:22 nexus9k.example.com : 2021 May 11 16:38:53 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:install all nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS)* **Configure authentication failure parameters** **Nexus 3k** *Oct 30 17:01:47 nexus3k.example.com : 2020 Oct 30 16:38:15 UTC: %DAEMON-3-SYSTEM_MSG: error: maximum authentication attempts exceeded for testadmin from 192.168.144.253 port 53607 ssh2 [preauth] - dcos_sshd[22693]* *Oct 30 17:01:47 nexus3k.example.com : 2020 Oct 30 16:38:15 UTC: %DAEMON-6-SYSTEM_MSG: Disconnecting authenticating user testadmin 192.168.144.253 port 53607: Too many authentication failures [preauth] - dcos_sshd[22693]* *Jun 3 14:46:44 nexus3k.example.com : 2021 Jun 3 16:15:07 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/0:admin:configure terminal ; aaa authentication rejected 3 in 60 ban 60 (SUCCESS)* **Nexus 9k**

			Oct 27 21:04:55 nexus9k.example.com : 2020 Oct 27 20:02:31 UTC: %DAEMON-3-SYSTEM_MSG: error: maximum authentication attempts exceeded for testadmin from 192.168.144.253 port 62972 ssh2 [preauth] - dcos_sshd[24342] *Oct 27 21:04:55 nexus9k.example.com : 2020 Oct 27 20:02:31 UTC: %DAEMON-6-SYSTEM_MSG: Disconnecting authenticating user testadmin 192.168.144.253 port 62972: Too many authentication failures [preauth] - dcos_sshd[24342]* *Jun 4 12:26:07 nexus9k.example.com : 2021 Jun 4 11:25:32 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; aaa authentication rejected 5 in 120 ban 60 (SUCCESS)* **Configure Audit behavior** **Nexus 3k** *Jun 4 15:45:23 nexus3k.example.com : 2021 Jun 4 17:14:30 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to configure logging server with: hostname/IP 172.16.16.150,severity 5,port 514,facility local7 - syslogd* *Jun 4 15:45:24 nexus3k.example.com : 2021 Jun 4 17:14:31 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging server 172.16.16.150 (SUCCESS)* *Jun 4 15:45:28 nexus3k.example.com : 2021 Jun 4 17:14:35 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to deconfigure logging server with hostname/IP 172.16.16.150 - syslogd* *Jun 4 15:45:29 nexus3k.example.com : 2021 Jun 4 17:14:36 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no logging server 172.16.16.150 (SUCCESS)* *Jun 4 15:45:50 nexus3k.example.com : 2021 Jun 4 17:14:57 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging logfile testlog 7 (SUCCESS)* *Jun 4 15:46:05 nexus3k.example.com : 2021 Jun 4 17:15:12 EST: %AAA-6-* *AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no logging logfile testlog 7 (SUCCESS)* *May 11 17:26:28 nexus3k.example.com : 2021 May 11 18:38:37 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to modify the logging level of local7 from 3 to 3 – syslogd* *Jun 2 18:01:01 nexus3k.example.com : 2021 Jun 2 19:28:47 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/1:admin:configure terminal ;*

			no logging server tl35-16x.example.com 7 port 6514 secure use-vrf management facility syslog (SUCCESS) *Jun 2 18:02:13 nexus3k.example.com : 2021 Jun 2 19:29:59 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to configure logging server with: hostname/IP tl35-16x.example.com,severity 7,port 6514,facility syslog - syslogd* *Jun 2 18:02:14 nexus3k.example.com : 2021 Jun 2 19:30:00 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/1:admin:configure terminal ; logging server tl35-16x.example.com 7 port 6514 secure use-vrf management facility syslog (SUCCESS)* **Nexus 9k** *Jun 4 15:43:00 nexus9k.example.com : 2021 Jun 4 14:42:25 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging logfile testlog 7 (SUCCESS)* *Jun 4 15:43:10 nexus9k.example.com : 2021 Jun 4 14:42:35 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no logging logfile testlog 7 (SUCCESS)* *Jun 4 15:43:57 nexus9k.example.com : 2021 Jun 4 14:43:22 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to configure logging server with: hostname/IP 172.16.16.150,severity 5,port 514,facility local7 - syslogd* *Jun 4 15:43:58 nexus9k.example.com : 2021 Jun 4 14:43:23 EST: %AAA-6-* *AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging server 172.16.16.150 (SUCCESS)* *Jun 4 15:44:29 nexus9k.example.com : 2021 Jun 4 14:43:53 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to deconfigure logging server with hostname/IP 172.16.16.150 - syslogd* *Jun 4 15:44:30 nexus9k.example.com : 2021 Jun 4 14:43:54 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no logging server 172.16.16.150 (SUCCESS)* *Jun 3 19:09:37 nexus9k.example.com : 2021 Jun 3 18:09:03 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to modify the logging level of authpriv from 7 to 7 – syslogd* *Jun 2 18:05:18 nexus9k.example.com : 2021 Jun 2 17:04:44 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/2:admin:show accounting log | include 'no logging server' (SUCCESS)* *Jun 2 12:27:06 nexus9k.example.com : 2021 Jun 2 11:26:32 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to configure*

			logging server with: hostname/IP tl35-16x.example.com,severity 7,port 6514,facility syslog - syslogd *Jun 2 12:27:07 nexus9k.example.com : 2021 Jun 2 11:26:33 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/2:admin:configure terminal ; logging server tl35-16x.example.com 7 port 6514 secure use-vrf management facility syslog (SUCCESS)* **Configure Crypto functionality** **Nexus 3k** *Apr 8 11:27:53 nexus3k.example.com : 2021 Apr 8 12:16:29 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE:* *update:console0:admin:configure terminal ; crypto ca trustpoint testca (SUCCESS)* *Apr 7 14:07:29 nexus3k.example.com : 2021 Apr 7 14:55:27 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint testca ; revocation-check none (SUCCESS)* *Apr 8 11:28:03 nexus3k.example.com : 2021 Apr 8 12:16:39 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint testca ; revocation-check ocsp (SUCCESS)* *Apr 8 11:37:49 nexus3k.example.com : 2021 Apr 8 12:26:25 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show crypto ca certificates (SUCCESS)* *Jun 3 18:18:05 nexus9k.example.com : 2021 Jun 3 17:17:31 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto key generate rsa modulus 2048 (SUCCESS)* *Jun 3 18:12:03 nexus9k.example.com : 2021 Jun 3 17:11:29 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show crypto key mypubkey rsa (SUCCESS)* *Jun 4 15:10:49 nexus3k.example.com : 2021 Jun 4 16:39:55 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint newca ; ocsp url http://192.168.144.241:7799 (FAILURE)* *Jun 4 15:08:41 nexus3k.example.com : 2021 Jun 4 16:37:47 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint newca (SUCCESS)* *Jun 4 15:09:17 nexus3k.example.com : 2021 Jun 4 16:38:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint newca ; enrollment terminal (SUCCESS)*

			Jun 4 15:22:16 nexus3k.example.com : 2021 Jun 4 16:51:23 EST: %AAA-6- *AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca import newca certificate (FAILURE)* *Jun 4 15:23:39 nexus3k.example.com : 2021 Jun 4 16:52:45 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no crypto ca trustpoint newca (SUCCESS)* **Nexus 9k** *May 5 14:53:18 nexus9k.example.com : 2021 May 5 13:52:50 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show crypto ca certificates (SUCCESS)* *Jun 3 18:12:03 nexus9k.example.com : 2021 Jun 3 17:11:29 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show crypto key mypubkey rsa (SUCCESS)* *Jun 3 18:18:05 nexus9k.example.com : 2021 Jun 3 17:17:31 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto key generate rsa modulus 2048 (SUCCESS)* *Apr 7 14:07:29 nexus3k.example.com : 2021 Apr 7 14:55:27 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint testca ; revocation-check none (SUCCESS)* *Apr 8 11:28:03 nexus3k.example.com : 2021 Apr 8 12:16:39 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint testca ; revocation-check ocsp (SUCCESS)* *Jun 4 15:03:57 nexus9k.example.com : 2021 Jun 4 14:03:22 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint newca (SUCCESS)* *Jun 4 15:04:39 nexus9k.example.com : 2021 Jun 4 14:04:04 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ;* *crypto ca trustpoint newca ; enrollment terminal (SUCCESS)* *Jun 4 15:10:49 nexus3k.example.com : 2021 Jun 4 16:39:55 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint newca ; ocsp url http://192.168.144.241:7799 (FAILURE)* *Jun 4 15:22:16 nexus3k.example.com : 2021 Jun 4 16:51:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE:*

			update:console0:admin:configure terminal ; crypto ca import newca certificate (FAILURE) *Jun 4 15:09:17 nexus3k.example.com : 2021 Jun 4 16:38:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint newca ; enrollment terminal (SUCCESS)* *Jun 4 15:23:39 nexus3k.example.com : 2021 Jun 4 16:52:45 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no crypto ca trustpoint newca (SUCCESS)* **Configure SSH rekey threshold** **Nexus 3k** *Jun 2 16:25:22 nexus3k.example.com : 2021 Jun 2 17:53:06 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/1:admin:configure terminal ; ssh rekey max-data 1g max-time 60m (SUCCESS)* **Nexus 9k** *Jun 2 16:28:21 nexus9k.example.com : 2021 Jun 2 15:27:47 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/2:admin:configure terminal ; ssh rekey max-data 1g max-time 60m (SUCCESS)* **Configure Time** **Nexus 3k** *Oct 30 17:34:03 nexus3k.example.com : 2020 Oct 30 17:34:00 EST: %AUTHPRIV-* *7-SYSTEM_MSG: Old time: Fri Oct 30 13:10:32 2020 - vsh.bin[31186]* *Oct 30 17:34:03 nexus3k.example.com : 2020 Oct 30 17:34:00 EST: %AUTHPRIV-7-SYSTEM_MSG: New time: Fri Oct 30 17:34:00 2020 - vsh.bin[31186]* **Nexus9k:** *Oct 30 17:37:01 nexus9k.example.com : 2020 Oct 30 17:37:00 EST: %AUTHPRIV-7-SYSTEM_MSG: Old time: Fri Oct 30 12:34:36 2020 - vsh.bin[1245]* *Oct 30 17:37:01 nexus9k.example.com : 2020 Oct 30 17:37:00 EST: %AUTHPRIV-7-SYSTEM_MSG: New time: Fri Oct 30 17:37:00 2020 - vsh.bin[1245]* **Configure Reference identifier** **Nexus 3k** *Jun 2 18:02:13 nexus3k.example.com : 2021 Jun 2 19:29:59 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to configure*

			logging server with: hostname/IP tl35-16x.example.com,severity 7,port 6514,facility syslog - syslogd *Jun 2 18:02:14 nexus3k.example.com : 2021 Jun 2 19:30:00 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:192.168.144.254@pts/1:admin:configure terminal ; logging server tl35-16x.example.com 7 port 6514 secure use-vrf management facility syslog (SUCCESS)* **Nexus 9k** *Jun 4 14:59:17 nexus9k.example.com : 2021 Jun 4 13:58:42 EST: %SYSLOG-5-SYSTEM_MSG: Attempt to configure logging server with: hostname/IP tl35-16x.example.com,severity 7,port 6514,facility syslog - syslogd* *Jun 4 14:59:18 nexus9k.example.com : 2021 Jun 4 13:58:43 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; logging server tl35-16x.example.com 7* *port 6514 secure use-vrf management facility syslog (SUCCESS)* **Certificates TOE Trust Store** **Nexus 3k** *Jun 14 14:41:51 nexus3k.example.com : 2021 Jun 14 16:18:01 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint adminca ; enrollment terminal (SUCCESS)* *Jun 14 14:48:07 nexus3k.example.com : 2021 Jun 14 16:24:18 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:CA certifcate/chain configuration done for trustpoint adminca* *Jun 14 15:36:16 nexus3k.example.com : 2021 Jun 14 17:12:28 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint adminca ; delete ca-certificate (SUCCESS)* *Jun 14 15:36:52 nexus3k.example.com : 2021 Jun 14 17:13:04 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no crypto ca trustpoint adminca (SUCCESS)* **Nexus 9k** *Jun 17 19:06:39 nexus9k.example.com : 2021 Jun 17 18:06:01 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint adminca ; enrollment terminal (SUCCESS)* *Jun 17 19:09:54 nexus9k.example.com : 2021 Jun 17 18:09:16 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE:*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			update:console0:admin:CA certifcate/chain configuration done for trustpoint adminca *Jun 17 19:11:55 nexus9k.example.com : 2021 Jun 17 18:11:17 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; crypto ca trustpoint adminca ; delete ca-certificate (SUCCESS)* *Jun 17 19:13:30 nexus9k.example.com : 2021 Jun 17 18:12:52 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:configure terminal ; no crypto ca trustpoint adminca (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).	**Nexus3k**: *Oct 30 17:30:59 nexus3k.example.com : 2020 Oct 30 13:07:28 EST: %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on console0* *Oct 30 17:34:03 nexus3k.example.com : 2020 Oct 30 17:34:00 EST: %AUTHPRIV-7-SYSTEM_MSG: Old time: Fri Oct 30 13:10:32 2020 - vsh.bin[31186]* *Oct 30 17:34:03 nexus3k.example.com : 2020 Oct 30 17:34:00 EST: %AUTHPRIV-7-SYSTEM_MSG: New time: Fri Oct 30 17:34:00 2020 - vsh.bin[31186]* **Nexus9k:** *Oct 30 17:36:20 nexus9k.example.com : 2020 Oct 30 12:33:56 EST: %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on console0* *Oct 30 17:37:01 nexus9k.example.com : 2020 Oct 30 17:37:00 EST: %AUTHPRIV-7-SYSTEM_MSG: Old time: Fri Oct 30 12:34:36 2020 - vsh.bin[1245]* *Oct 30 17:37:01 nexus9k.example.com : 2020 Oct 30 17:37:00 EST: %AUTHPRIV-7-SYSTEM_MSG: New time: Fri Oct 30 17:37:00 2020 - vsh.bin[1245]*

FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success and failure)	None.	**Nexus 3k** *May 11 17:00:49 nexus3k.example.com : 2021 May 11 18:12:59 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:copy scp://192.168.144.254/nexus/nxos.9.3.7.18.bin bootflash:/ (SUCCESS)* *May 11 17:03:45 nexus3k.example.com : 2021 May 11 18:15:55 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin sha512sum (SUCCESS)* *May 11 17:04:20 nexus3k.example.com : 2021 May 11 18:16:30 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin md5sum (SUCCESS)* *May 11 17:36:48 nexus3k.example.com : 2021 May 11 18:48:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:::NXOS Image set to bootflash:/nxos.9.3.7.18.bin* *May 11 17:36:48 nexus3k.example.com : 2021 May 11 18:48:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:vsh.bin.32099:root:configure terminal ; boot nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS)* *May 11 17:39:20 nexus3k.example.com : 2021 May 11 18:51:30 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:install all nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS)* **Nexus 9k** *May 11 17:00:26 nexus9k.example.com : 2021 May 11 15:59:57 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:copy scp://192.168.144.254/nexus/nxos.9.3.7.18.bin bootflash:/ (SUCCESS)* *May 11 17:03:27 nexus9k.example.com : 2021 May 11 16:02:58 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin sha512sum (SUCCESS)* *May 11 17:04:24 nexus9k.example.com : 2021 May 11 16:03:55 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:show file bootflash:/nxos.9.3.7.18.bin md5sum (SUCCESS)* *May 11 17:36:52 nexus9k.example.com : 2021 May 11 16:36:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:::NXOS Image set to bootflash:/nxos.9.3.7.18.bin* *May 11 17:36:52 nexus9k.example.com : 2021 May 11 16:36:23 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:vsh.bin.31954:root:configure terminal ; boot nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS)*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			May 11 17:39:22 nexus9k.example.com : 2021 May 11 16:38:53 EST: %AAA-6-AAA_ACCOUNTING_MESSAGE: update:console0:admin:install all nxos bootflash:/nxos.9.3.7.18.bin (SUCCESS)
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session. Administrative Actions: Specifying the inactivity time period.	No additional information.	**The termination of a local session by the session locking mechanism** **Nexus 3k:** Nov 2 16:16:30 nexus3k.example.com : 2020 Nov 2 16:16:31 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin – login **Nexus 9k:** Feb 10 16:40:45 nexus9k.example.com : 2021 Feb 10 16:40:31 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin – login
FTA_SSL.3	The termination of a *remote* session by the session locking mechanism. Administrative Actions: Specifying the inactivity time period.	No additional information.	**Nexus3k:** *Nov 2 15:51:36 nexus3k.example.com : 2020 Nov 2 15:51:37 EST: %DAEMON-6-SYSTEM_MSG: Disconnected from user admin 192.168.144.254 port 46956 - dcos_sshd[10941]* *Nov 2 15:51:36 nexus3k.example.com : 2020 Nov 2 15:51:37 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session closed for user admin - dcos_sshd[10932]* **Nexus9k:** *Feb 10 16:46:37 nexus9k.example.com : 2021 Feb 10 16:46:24 EST: %DAEMON-6-SYSTEM_MSG: Disconnected from user admin 192.168.144.254 port 46706 - dcos_sshd[7199]* *Feb 10 16:46:37 nexus9k.example.com : 2021 Feb 10 16:46:24 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session closed for user admin - dcos_sshd[7192]*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FTA_SSL.4	The termination of an interactive session.	No additional information.	**Nexus3k:** **Local:** *Feb 10 16:44:02 nexus3k.example.com : 2021 Feb 10 17:52:21 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin - login* **Remote:** *Nov 2 15:55:16 nexus3k.example.com : 2020 Nov 2 15:55:16 EST: %DAEMON-6-SYSTEM_MSG: Received disconnect from 192.168.144.254 port 46960:11: disconnected by user - dcos_sshd[13088]* *Nov 2 15:55:16 nexus3k.example.com : 2020 Nov 2 15:55:16 EST: %DAEMON-6-SYSTEM_MSG: Disconnected from user admin 192.168.144.254 port 46960 - dcos_sshd[13088]* **Nexus9k:** **Local:** *Feb 10 16:40:45 nexus9k.example.com : 2021 Feb 10 16:40:31 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin – login* **Remote:** *Feb 10 16:46:37 nexus9k.example.com : 2021 Feb 10 16:46:24 EST: %DAEMON-6-SYSTEM_MSG: Received disconnect from 192.168.144.254 port 46706:11: disconnected by user - dcos_sshd[7199]* *Feb 10 16:46:37 nexus9k.example.com : 2021 Feb 10 16:46:24 EST: %DAEMON-6-SYSTEM_MSG: Disconnected from user admin 192.168.144.254 port 46706 - dcos_sshd[7199]* *Feb 10 16:46:37 nexus9k.example.com : 2021 Feb 10 16:46:24 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session closed for user admin - dcos_sshd[7192]*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	**Initiation** **Nexus3k** *Jun 8 18:02:13 nexus3k.example.com : 2021 Jun 8 19:34:14 EST: %SYSLOG-5-SYSTEM_MSG: Successfully established SSL connection to 192.168.144.254:6514 in [vrf: management] Protocol: TLSv1.2 Cipher: AES128-SHA - syslogd* **Nexus9k** *Nov 10 13:55:21 localhost : 2020 Nov 10 14:00:58 EST: %SYSLOG-5-SYSTEM_MSG: Successfully established SSL connection to 192.168.144.254:6514 in [vrf: management] Protocol: TLSv1.2 Cipher: AES128-SHA - syslogd* **Termination** **Nexus3k** *Jun 8 17:56:29 nexus3k.example.com : 2021 Jun 8 19:28:30 EST: %SYSLOG-5-SYSTEM_MSG: Successfully tore down SSL connection to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: AES128-SHA]. – syslogd* **Nexus9k** *Nov 10 13:55:20 localhost : 2020 Nov 10 13:58:59 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin - login* *Nov 10 13:55:20 localhost : 2020 Nov 10 13:59:00 EST: %SYSLOG-5-SYSTEM_MSG: Successfully tore down SSL connection to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: ECDHE-RSA-AES256-SHA384]. – syslogd* **Failure** **Nexus3k** *Jun 8 17:56:37 nexus3k.example.com : 2021 Jun 8 19:28:38 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown while in init] – syslogd* **Nexus9k** *Dec 1 22:47:57 nexus9k.example.com : 2020 Dec 1 22:47:52 EST: %SYSLOG-4-SYSTEM_MSG: SSL connection establishment failure to 192.168.144.254:6514 in [vrf: management] [Protocol: TLSv1.2 Cipher: 0000]. ErrorNo [0], ErrString [error:140E0197:SSL routines:SSL_shutdown:shutdown* while in init] - syslogd

FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None	**Initiation** **Nexus 3K:** *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %DAEMON-6-SYSTEM_MSG: Accepted keyboard-interactive/pam for admin from 192.168.144.254 port 56974 ssh2 - dcos_sshd[28887]* *Oct 26 16:14:57 nexus3k.example.com : 2020 Oct 26 15:48:34 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session opened for user admin by (uid=0) - dcos_sshd[28887]* **Nexus 9k:** *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %DAEMON-6-SYSTEM_MSG: Accepted keyboard-interactive/pam for admin from 192.168.144.254 port 41514 ssh2 - dcos_sshd[19412]* *Oct 26 16:15:19 nexus9k.example.com : 2020 Oct 26 15:12:55 UTC: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session opened for user admin by (uid=0) - dcos_sshd[19412]* **Termination** **Nexus 3K:** *Nov 2 15:51:36 nexus3k.example.com : 2020 Nov 2 15:51:37 EST: %DAEMON-6-SYSTEM_MSG: Disconnected from user admin 192.168.144.254 port 46956 - dcos_sshd[10941]* *Nov 2 15:51:36 nexus3k.example.com : 2020 Nov 2 15:51:37 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session closed for user admin - dcos_sshd[10932]* **Nexus 9k:** *Feb 10 16:46:37 nexus9k.example.com : 2021 Feb 10 16:46:24 EST: %DAEMON-6-SYSTEM_MSG: Disconnected from user admin 192.168.144.254 port 46706 - dcos_sshd[7199]* *Feb 10 16:46:37 nexus9k.example.com : 2021 Feb 10 16:46:24 EST: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(dcos_sshd:session): session closed for user admin - dcos_sshd[7192]* **Failure** **Nexus 3K:** *Oct 26 18:17:11 nexus3k.example.com : 2020 Oct 26 17:50:51 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 60794: no matching*

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			host key type found. Their offer: ecdsa-sha2-nistp256 [preauth] - dcos_sshd[25256] **Nexus 9k:** Oct 26 19:54:51 nexus9k.example.com : 2020 Oct 26 18:52:27 UTC: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 192.168.144.254 port 48552: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth] - dcos_sshd[9310]

6. 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 12 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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.	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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the 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 functionality. 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	Administrators must protect their access credentials where ever they may be.

	protected on any other platform on which they reside.	
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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.	Administer must follow guidance on how to securely protect sensitive residual information on equipment discarded or removed.

7. Related 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 http://www.cisco.com

8. Document Feedback

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

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

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

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

We appreciate your comments.

9. 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 anytime, 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