



Cisco Nexus 9k Switch with APIC/ACI

Common Criteria Configuration Guide

Version 1.0

April 12, 2018

Table of Contents

1	Introduction.....	7
1.1	Audience	7
1.2	Purpose.....	7
1.3	Document References.....	7
1.4	Supported Hardware and Software.....	9
1.5	Assumptions.....	10
1.5.1	Enabling Fabric Secure Mode	11
1.6	Operational Environment.....	11
1.6.1	Supported non-TOE Hardware/ Software/ Firmware.....	11
1.7	Excluded Functionality.....	12
2	Secure Acceptance of the TOE.....	13
3	Secure Installation and Configuration.....	16
3.1	Physical Installation.....	16
3.2	Initial Setup via Direct Console Connection.....	16
3.2.1	Options to be chosen during the initial setup of the APIC.....	16
3.2.2	Options to be chosen during the initial setup of the ACI Fabric.....	18
3.2.3	Tenant Setup.....	19
3.2.4	Create VRF.....	22
3.2.5	Create Bridge Domain	24
3.2.6	Create Subnet.....	26
3.2.7	Configuring FIPS mode	28
3.2.8	Ensuring all Keys and Passwords are Encrypted.....	29
3.2.9	Administrator Configuration and Credentials	31
3.2.10	Access Banner	32
3.2.11	Deleting an Administrator User.....	33
3.3	Network Protocols and Cryptographic Settings.....	35
3.3.1	Remote Administration Protocols.....	35
3.3.2	TLS Server Configuration:.....	38
3.3.3	Logging Configuration.....	39
3.3.4	Vitual Port Channel Operations.....	41

3.3.5	Routing Protocols	42
3.3.6	Non-Approved Algorithms and Protocols	42
4	Secure Management	43
4.1	Configuring Management Access to APIC.....	43
4.1.1	Configuring Static In-Band Management Access Using the GUI.....	43
4.2	APIC User Roles	45
4.2.1	User Account Creation.....	46
4.2.2	RADIUS/TACACS+.....	49
4.3	Clock Management.....	51
4.4	Identification and Authentication.....	52
4.4.1	Login Banners	52
4.5	Information Flow Policies.....	53
4.5.1	Policies, Filters, and Contracts	54
5	Auditing.....	82
5.1	Deleting Audit Records	82
5.2	Audit Records Description.....	82
6	Modes of Operation.....	84
6.1	Module States.....	85
6.2	Self-Tests	86
7	Security Measures for the Operational Environment.....	88
8	Related Documentation	89
8.1	World Wide Web.....	89
8.2	Ordering Documentation	89
8.3	Documentation Feedback.....	89
9	Obtaining Technical Assistance.....	90

List of Tables

Table 1: Acronyms.....	5
Table 2 Cisco Documentation	7
Table 3: Operational Environment Components	11
Table 4 Excluded Functionality.....	12
Table 5 Evaluated Software Images	14
Table 6 Roles and Privileges	45
Table 7 Module States.....	86
Table 8 Redundancy Modes: for Supervisor.....	86
Table 9 Operational Environment Security Measures	88

List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 1: Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CI	Configuration Item
FIPS	Federal Information Processing Standards
EAL	Evaluation Assurance Level
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial In User Service
SFP	Security Function Policy
SSHv2	Secure Shell (version 2)
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transport Control Protocol
TOE	Target of Evaluation

DOCUMENT INTRODUCTION

Prepared By:

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

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the APIC and Nexus 9k Switch (9k). 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. All administrative actions that are relevant to the Common Criteria (CC) Evaluation and claimed Protection Profile(s) are described within this document. This document will include pointers to the official Cisco documentation in order to aid the administrator in easily identifying the CC relevant administrative commands, including subcommands, scripts (if relevant), and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in the APIC and 9k that are necessary to enforce the requirements claimed.

1 Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Nexus 9k Switch (9k) in ACI mode, the TOE, as it was certified under Common Criteria. The Nexus 9k Switch (9k) may be referenced below by the model number series related acronym ex. 9k, TOE, Nexus 9000 Series, or simply switch. All of the instructions pertain specifically to the switch except for the instructions specifically noted with APIC. The APIC and ACI mode switches as well as the FEX and network connections that make up the ACI fabric must be installed in one physically protected data center.

1.1 Audience

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

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. 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 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 section lists the Cisco Systems documentation that is also the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 2. Throughout this document, the guides will be referred to by the “#”, such as [4]. Note: The guides below that reference 7.x and 11 apply also to the Nexus 9k in ACI mode. Note: Only a subset of the Nexus commands for Nexus stand-alone mode are in the Nexus ACI mode, so not all of the commands in the Nexus command reference guides that are not specific to ACI mode will work. These guides are listed for completeness. See the APIC specific guides for APIC and ACI mode for specific commands.

Table 2 Cisco Documentation

#	Title	Link
[1]	Cisco Nexus 9k Switch Security Target, (Current Version)	https://www.niap-ccevs.org/CCEVS_Products/vpl.cfm
[2]	Cisco Nexus 9000 Series NX-OS System Management Configuration Guide	Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 7.x
[3]	Cisco Nexus 9000 Series NX-OS Security Configuration Guide	Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 7.x

#	Title	Link
[4]	Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide	Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 7.x
[5]	Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands)	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/command_reference/config_612I22/b_n9k_command_ref.html
[6]	Cisco Nexus 9000 Series NX-OS Command Reference (Show Commands)	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/command_reference/show_612I22/b_n9k_show_command_ref.html
[7]	Cisco Nexus Mode Switch Hardware Installation Guides	Cisco Nexus 9332PQ NX-OS-Mode Switch Hardware Installation Guide Cisco Nexus 9372PX NX-OS-Mode Switch Hardware Installation Guide Cisco Nexus 9372TX NX-OS-Mode Switch Hardware Installation Guide Cisco Nexus 9396PX NX-OS-Mode Switch Hardware Installation Guide Cisco Nexus 9396TX NX-OS-Mode Switch Hardware Installation Guide Cisco Nexus 93120TX NX-OS-Mode Switch Hardware Installation Guide Cisco Nexus 93128TX NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9504 NX-OS Mode Switch Hardware Installation Guide Cisco Nexus 9508 ACI-Mode Switch Hardware Installation Guide Cisco Nexus 9516 NX-OS Mode Switch Hardware Installation Guide
[8]	Cisco Nexus 9000 Series NX-OS System Messages Reference	Cisco Nexus 9000 Series NX-OS System Messages Reference, Release 7.0(3)I1(2)
[9]	Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/interfaces/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Interfaces_Configuration_Guide_7x.pdf
[10]	Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/unicast/configuration/guide/13_cli_nxos.pdf
[11]	Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/layer2/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_7x.html
[12]	Cisco APIC Getting Started Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/getting-started/b_APIC_Getting_Started_Guide.html
[13]	Operating Cisco Application Centric Infrastructure	http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/Operating_ACI/Cisco_OperatingApplicationCentricInfrastructure.pdf

#	Title	Link
[14]	Cisco APIC Layer 4 to Layer 7 Services Deployment Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-L7_Services_Deployment/guide/b_L4L7_Deploy.html
[15]	Cisco Application Centric Infrastructure Fundamentals	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals.pdf
[16]	Cisco APIC Command-Line Interface User Guide	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/cli/nx/cr231/b_APIC_NXOS_CLI_Cmd_Reference_231.pdf
[17]	Cisco ACI Switch Command Reference, NX-OS Release 11.0	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/nxos/cli/b_inxos_command_ref.html
[18]	Cisco APIC REST API Configuration Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide.html
[19]	Cisco APIC Basic Configuration Guide, Release 2.x	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/basic_config/b_APIC_Basic_Config_Guide_2_x.html
[20]	Cisco Application Centric Infrastructure Best Practices Guide	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/ACI_Best_Practices/b_ACI_Best_Practices/b_ACI_Best_Practices_chapter_010000.html
[21]	Connecting Application Centric Infrastructure (ACI) to Outside Layer 2 and 3 Networks Version 1.0	https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c07-732033.pdf
[22]	Cisco APIC Troubleshooting Guide	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/troubleshooting/b_APIC_Troubleshooting.pdf

1.4 Supported Hardware and Software

Only the hardware and software listed in section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The TOE is a hardware and software solution that makes up the switch models as follows: 9300, 9500. The network, on which they reside, is considered part of the environment. The software is comprised of the Cisco ACI mode software image Release 12.3, APIC v2.3. When the Nexus 9k is configured for ACI mode, the APIC is used for remote management of the switch images and some configuration. The APIC is the authorized administrator's centralized management interface for all devices in the fabric. From the APIC, the authorized administrator can attach to the switch over SSHv2 to make specific configuration changes.

Example

The following example shows how to use the attach command to connect the leaf1 node:

```
admin@apic1:aci> attach leaf1
# Executing command: ssh leaf1
Warning: Permanently added 'leaf1,10.0.75.31' (RSA) to the list of known hosts.
```

admin@leaf1's password:
admin@leaf1:~>

For more information on the **attach** command see the [16] *APIC Command-Line Interface User Guide*.

1.5 Assumptions

Assumption	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that 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.
A.FIREWALL	A firewall located between the ACI fabric and external networks to protect against malicious or unauthorized traffic from entering the ACI fabric.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation.
A.REMOTE_SERVERS	When remote servers are used, such as NTP server and optionally remote authentication servers and syslog servers, the administrator will ensure the session between the TOE and remote server(s) is secured.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

In order to ensure that the TOE and Nexus 9k switches that make up the ACI Fabric are secure the above assumptions have been made. More specifically, all Nexus 9k switches that make up the fabric are installed in a physically secure datacenter. There is limited access to the datacenter. For example, only authorized badged personnel can enter the building and the raised floor datacenter. All administrators are considered to be trusted so for example if an unauthorized device was installed on the ACI fabric, it could not communicate with the Fabric or other switches because:

1. Any device added to the ACI Fabric must be authorized by a trusted administrator via the APIC GUI before being allowed access to the ACI Fabric once the Fabric Security has been enabled. See section 1.5.1 below.
2. In addition, the device must have a valid X.509 certificate issued by Cisco and installed on the switch during the manufacturing process by Cisco.

In addition, all administrators follow the recommended guidance for configuring the Nexus 9k Switches and APIC as stated in this document. For example for best practices, an administrator should not configure an EPG to EPG with any to any data flow. Only specific data flows from one EPG to another should be configured to ensure that only allowed protocols from one EPG to another EPG will be configured. When configuring the contracts and EPGs in order for the ACI Fabric to have external connectivity, a separate EPG specifically for external traffic must be configured. See Figure 55 below. See section 4.5.1.3 and the *Cisco Application Centric Infrastructure Best Practices Guide* [20] for more information.

1.5.1 Enabling Fabric Secure Mode

By default the Fabric Secure Mode is not enabled. Fabric secure mode prevents parties with physical access to the fabric equipment from adding a switch or APIC controller to the fabric without manual authorization by an administrator. The firmware checks that switches and controllers in the fabric have valid serial numbers associated with a valid Cisco digitally signed certificate. To configure Fabric Secure mode go to > Admin > Fabric Security > Enable

Fabric Security

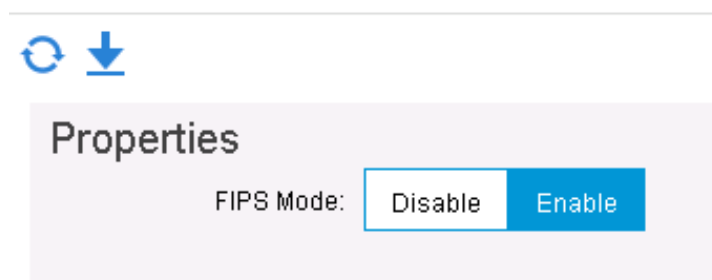


Figure 1 Fabric Security

1.6 Operational Environment

1.6.1 Supported non-TOE Hardware/ Software/ Firmware

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

Table 3: Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Firewall	Yes	This includes a firewall that must be placed between the ACI fabric and an external network.
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.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.1 and above with the supported ciphersuites may be used.
NTP Server	Yes	The TOE supports communications with an NTP server.
Syslog Server	No	This includes any syslog server to which the TOE would transmit syslog messages.
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. The TOE correctly leverages the services provided by this RADIUS or TACACS+ AAA server to provide single-use authentication to administrators.

1.7 Excluded Functionality

Table 4 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet passes authentication credentials in clear text. SSHv2 is to be used instead.
SNMP	SNMP is disabled in the evaluated configuration.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the claimed security functions. FIPS configuration is described in section 3.2.7 Telnet is disabled by default. SNMP is disabled by default.

2 Secure Acceptance of the TOE

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

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

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

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

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

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

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

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). To further ensure proper and secure delivery of the 9k TOE, the recipient must check the models received against the list of TOE component hardware models listed in Table 5 of the Security Target

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. Software images are available from Cisco.com at the following: <http://www.cisco.com/cisco/software/navigator.html>.

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 hash by comparing the SHA512 hash that is listed on the Cisco web site and in Table 5 Evaluated Software Images below or by using the show file command on the Nexus 9k. The "show file *filename* shasum" command on the Nexus 9k can be used to verify the SHA512 hash. Refer to section "Displaying File Checksums" in [4]. If the SHA512 hashes do not match, contact Cisco Technical Assistance Center (TAC) <http://tools.cisco.com/ServiceRequestTool/create/launch.do>.

Step 9 Install the downloaded and verified software image onto your APIC as described in section “Setting Up the APIC” of chapter Initial Setup and in chapter “Switch Discovery with the APIC” in the *Cisco APIC Getting Started Guide* [12]. Start your APIC as described in [4]. Confirm that your APIC loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console. The APIC has the images for the ACI mode switches in the fabric also. First you will bring up the APIC and then the ACI switches.

Table 5 Evaluated Software Images

Model	Software Version	Image Name	SHA512 hash
Cisco 9300 models			
9332PQ	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
9336PQ	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
9372PX	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
C9372PX-E	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
9372TX	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
9396PX	12.3(1f)	aci-n9000-dk9.12.3.1e.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
9396TX	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
93128TX	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
C93180L-C-EX	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
93180YC-EX	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
93108TC-EX	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
Cisco 9500 models			

Model	Software Version	Image Name	SHA512 hash
9504	12.3(1f)	N/A	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
9508	12.3(1f)	N/A	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
9516	12.3(1f)	N/A	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
Supervisor A	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
Supervisor B	12.3(1f)	aci-n9000-dk9.12.3.1f.bin	e47955081622287fda8c9603dd512828c07e76cba925f583ba654526b5aaac4cd521237fd9ce1d0d9c3e977fe5238f2b8e39e76af8367441f470f38b46336ce9
System Controller	12.3(1f)	N/A	N/A
APIC	2.3(1f)	aci-apic-dk9.2.3.1e.iso	4acf11b92ead3ba7498bbdcac310002206b6738643913f9d64fcb54efe455504c1837a6c6cb2865d5dd7727a67359f2bd9be17346dacd5a897377f9b9cd957ad
2000 Series Fabric Extenders			
Cisco Nexus 2348UPQ	12.3(1f)	N/A	N/A
Cisco Nexus 2248TP-1GE	12.3(1f)	N/A	N/A
Cisco Nexus 2248TP-E	12.3(1f)	N/A	N/A
Cisco Nexus 2232PP-10GE	12.3(1f)	N/A	N/A
Cisco Nexus 2248PQ-10GE	12.3(1f)	N/A	N/A
Cisco Nexus 2232TM-E	12.3(1f)	N/A	N/A

3 Secure Installation and Configuration

3.1 Physical Installation

Follow the Cisco Nexus 9000 Series Hardware Installation and Reference Guides [7] for hardware installation instructions. Follow these directions for connecting all 9k models. All of the Nexus 9k APIC and ACI models installed to make up the ACI fabric must be installed in a single datacenter within a physically secure facility. For example a raised floor that has badge readers for access that is located within a secured building with external door badge readers and building security.

3.2 Initial Setup via Direct Console Connection

Once the Nexus 9k switches and APIC have been racked and powered, the APIC needs to be set up. The first device that will be configured will be the APIC since it acts as the central management interface for the switches and the entire ACI. See the [12] *Cisco APIC Getting Started Guide*, "Setting up the APIC" section.

3.2.1 Options to be chosen during the initial setup of the APIC

A console and keyboard can be directly connected into the APIC. The first step is to change the default BIOS password. The Entering Setup message displays as it accesses the setup menu.

Step 1 During the BIOS boot process, when the screen displays Press <F2> Setup, press F2. The Entering Setup message displays as it accesses the setup menu.

Step 2 At the Enter Password dialog box, enter the current password.

The default is 'password' which must be changes to a pasword that meets the password quality parameters described in section **Error! Reference source not found.**below.

Step 3 In the Setup Utility, choose the Security tab, and choose Set Administrator Password.

Step 4 In the Enter Current Password dialog box, enter the current password.

Step 5 In the Create New Password dialog box, enter the new password.

Step 6 In the Confirm New Password dialog box, re-enter the new password.

Step 7 Choose the Save & Exit tab.

Step 8 In the Save & Exit Setup dialog box, choose Yes.

Step 9 Wait for the reboot process to complete.

The updated BIOS password is effective.

After the APIC boots, the initial setup screen will be displayed.


```

Cluster configuration ...
Enter the fabric name [ACI Fabric1 #1]:
Enter the number of controllers in the fabric (1-16) [3]:
Enter the controller ID (1-3) [2]:
Enter the controller name [apic2]:
Enter address pool for TEP addresses [10.0.0.0/16]:
Enter the VLAN ID for infra network (1-4094) []: <<< This is for the physical APIC
Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
Enter the IP address for out-of-band management: 192.168.10.2/24
Enter the IP address of the default gateway [None]: 192.168.10.254
Enter the interface speed/duplex mode [auto]:

Administrator user configuration...
Enable strong passwords? [Y]
Enter the password for admin:

```

Fabric Name:

The first thing it asks for is the fabric name. This is somewhat arbitrary, but if you have multiple ACI fabrics an administrator may want to make sure a recognizable name that will help recognize the fabric.

Number of Controllers:

Usually there will have be controllers for redundancy. If you have a larger environment, more APICs may be necessary.

Controller ID:

Each APIC must be configured in order. The first APIC must be configured with a Controller ID of 1. An administrator cannot configure the APICs out of order for the first time. An administrator must boot them and set them up in order. After they are all set up it doesn't matter what boot order is used use later on.

Controller Name:

This is the name that will identify each APIC. The administrator may want to specify that it's APIC1 or something indicating that it's the first controller to match the controller ID configured above.

TEP Address Pool:

A TEP is a Tunnel End Point. This is used for VXLAN traffic and an administrator must have TEPs to send traffic over the VXLANs. The ACI fabric uses VXLAN exclusively within the infrastructure space, or the space between the spine and leaf switches. This pool will assign each TEP an IP address on the leaf and spine switches.

VLAN ID for Infra Network:

Again the Infra Network (or Infrastructure Network) is the space between the leaf and spine switches. We only need to use one VLAN ID because it will use VXLAN to allow it to scale. In the image above it uses 4093 as 4094 is reserved for other communication. However, if you're using UCS within your environment you may want to take care not to use VLANs 3968-4047 as this range of VLANs is also reserved.

Admin User Configuration:

Choose Y for Yes for enabling strong passwords. When entering the new admin password, make sure it follows the strong password rules.

Choose a strong password according to the guidelines in section 3.2.9

Make sure the CIMC default password is changed. A strong password should be used. The password for the CIMC is separate than the APIC password. The default username is admin and password is password.

3.2.2 Options to be chosen during the initial setup of the ACI Fabric

The Cisco ACI fabric is inherently secure because it uses a zero-trust models and relies on many layers of security. Before any controller or leaf or spine switch becomes a member of the Cisco ACI fabric, it **must** be authenticated and admitted by the fabric administrator. After that, it becomes an operational component of the fabric.

All devices (the APIC and Cisco Nexus 9000 Series leaf and spine switches) use a hardware-based secure key store. The controller uses a Trusted Platform Module (TPM) hardware cryptographic module to store digitally signed certificates. The TPM is enabled by default. The Cisco Nexus 9000 Series leaf and spine switches in the Cisco ACI fabric use the Anti-Counterfeit Technology 2 (ACT-2) hardware security module (HSM) embedded on the motherboard to store digitally signed certificates.

Cisco ACI security starts at the time of manufacture with the installation of keys in the hardware-based secure key store. The controller's TPM chip is programmed with the Cisco ACI platform's public key. The Cisco Nexus 9000 Series leaf and spine switches use an ACT-2 chip programmed with three keys: a development key, a release key, and a revocation key. All certificates in TPM and ACT-2 chips are unique, digitally signed, and encrypted at the time of manufacture. During Cisco ACI fabric activation or while adding a new device to an existing Cisco ACI fabric, all devices are authenticated based on their digitally signed certificates and identity information. If someone adds a rogue Cisco Nexus 9000 Series switch or APIC device to the Cisco ACI fabric, the certificate authentication will fail, and the infrastructure VLAN on the switch will not even open. As a result, the rogue device will not be added to the fabric and will not have any access to Cisco ACI resources.

All configuration is done via the APIC GUI. Although an authorized administrator can login individually to the switches, it is only for troubleshooting purposes. In the APIC, you have to click the Fabric and then Fabric Membership to setup the ACI fabric. Click on the first listed Node

Note: The alert on the screen is because there is only once APIC in use.

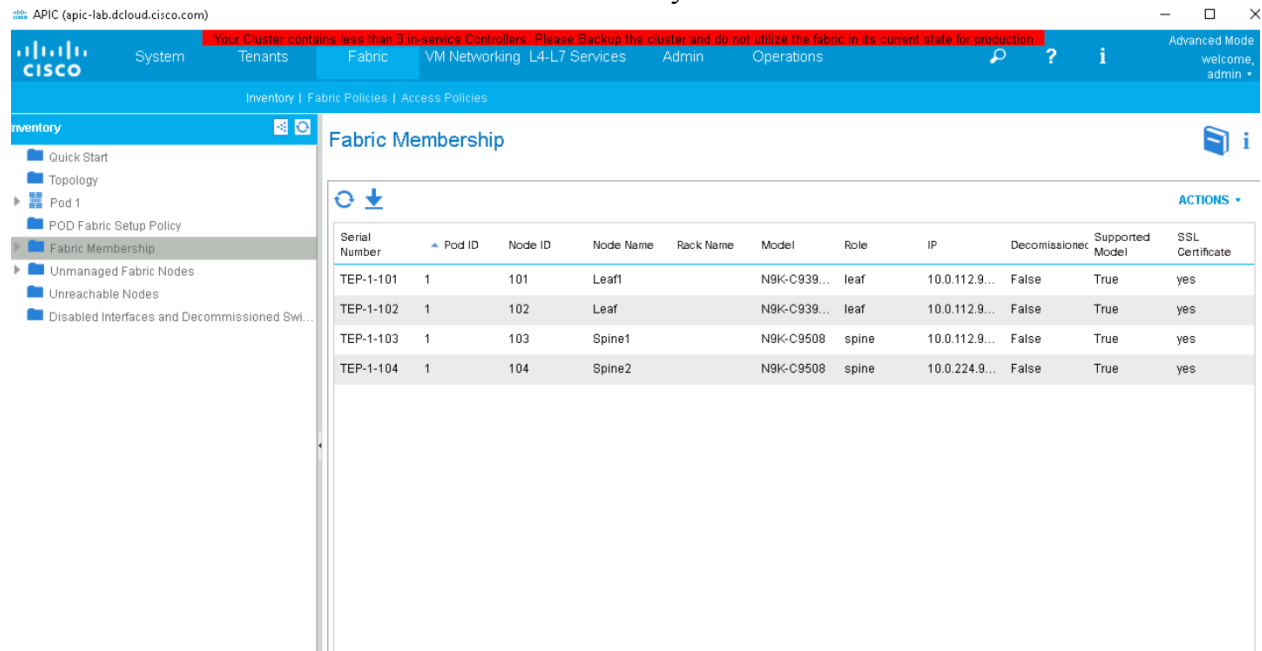


Figure 2 Node ID and Name

Click on the first node give it a Node ID 101 and a Name Leaf1 – Click Update. The IP address will automatically be assigned. Do the same for any other switches on the Fabric.

Fabric Membership

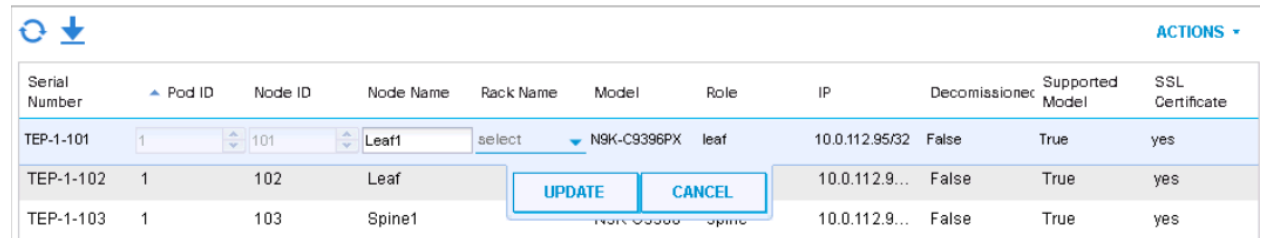



Figure 3

Once the first fabric switch is registered then the other leaf switches and then spine switches in the fabric will be discovered. You may have to click the refresh button  to see the other switches be registered. Give them IDs and Names as described in Figures 1 and 2 above and click Update.

3.2.3 Tenant Setup

Once your Fabric nodes are setup, an authorized administrator can configure the Tenants. Tenants further break down into contexts which are private Layer 3 (Private-L3) networks. Contexts directly relate to a Virtual Route Forwarding (VRF) instance or separate IP space. Each tenant may have one or more private Layer 3 networks depending on their business needs. Private Layer 3 networks provide a way to further separate the organizational and forwarding requirements below a given tenant. Because contexts use separate forwarding instances, IP addressing can be duplicated in separate contexts (VRF) for the purpose of multitenancy.

A bridge domain is defined as a Layer 2 address space. Each bridge domain must be linked to a VRF.

A tenant is a logical container or a folder for application policies. It can represent an actual tenant, an organization, or a domain, or can just be used for the convenience of organizing information. A normal tenant represents a unit of isolation from a policy perspective, but it does not represent a private network. A special tenant named "common" has sharable policies that can be used by all tenants.

A "context" is a representation of a private Layer 3 network such as a VRF. It is a unit of isolation in the Cisco ACI framework. A tenant can be configured with several contexts or VRFs to provide private layer 3 networks. Contexts can be configured within a single tenant (contained by the tenant) or can be shared across multiple tenants in the "common" tenant. This approach provides both multiple private Layer 3 networks per tenant and shared Layer 3 networks used by multiple tenants.

Logical Model Overview

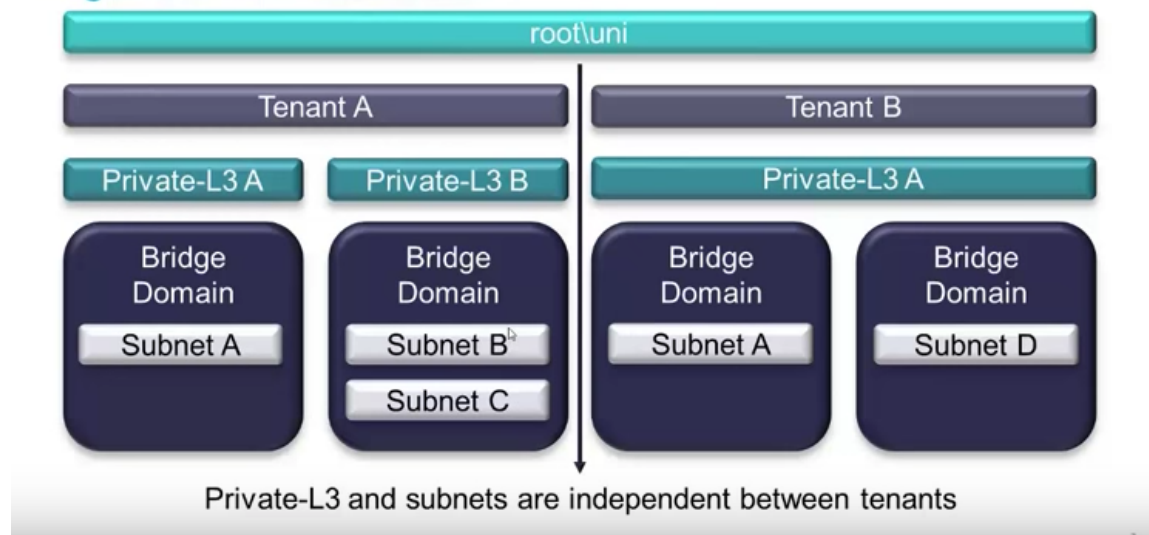


Figure 4 Logical Model Overview

Tenant Logical Hierarchy

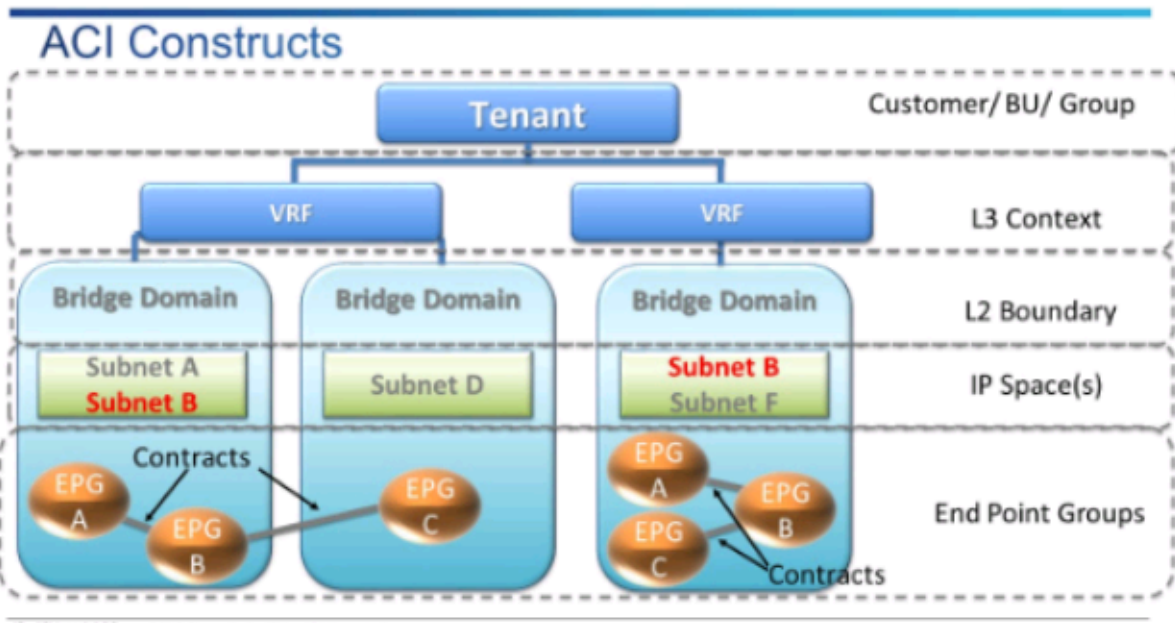


Figure 5 Setup Tenants

Click Tenants.

APIC (apic-lab.dcloud.cisco.com)

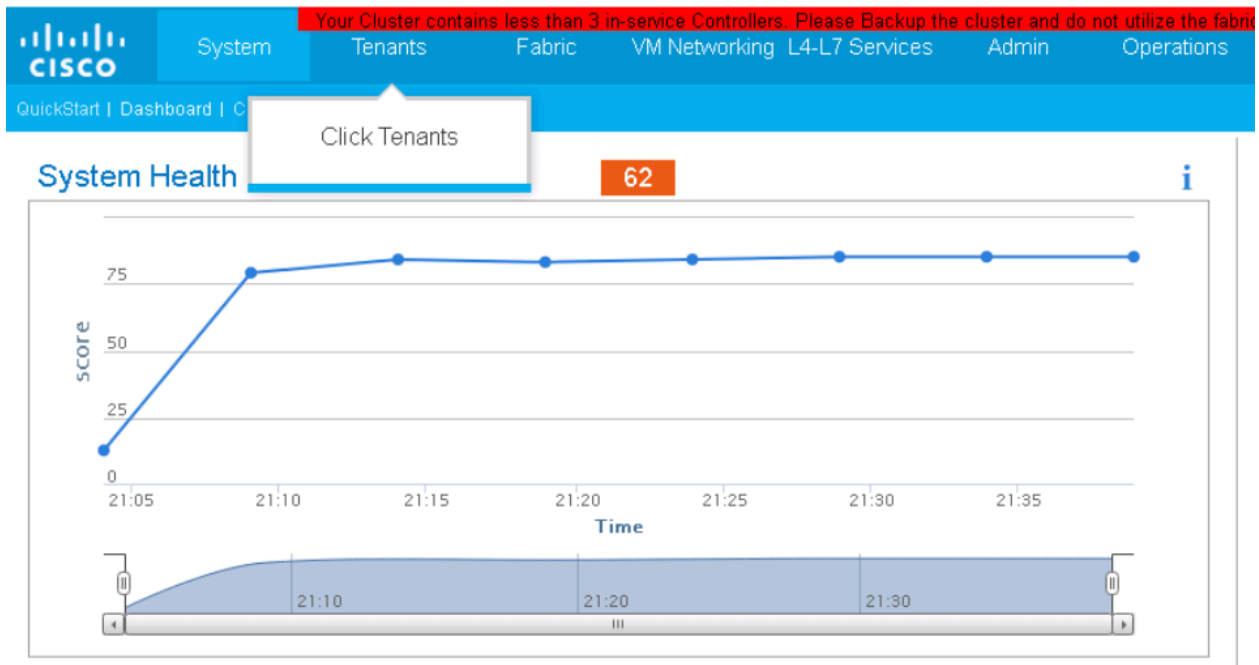


Figure 6 Tenant in APIC

Click Add Tenant

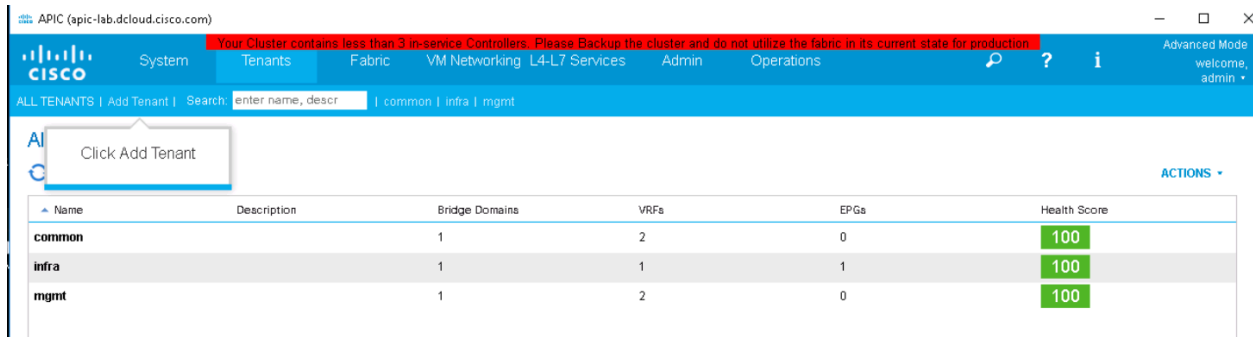


Figure 7 Add Tenant

Create Tenant

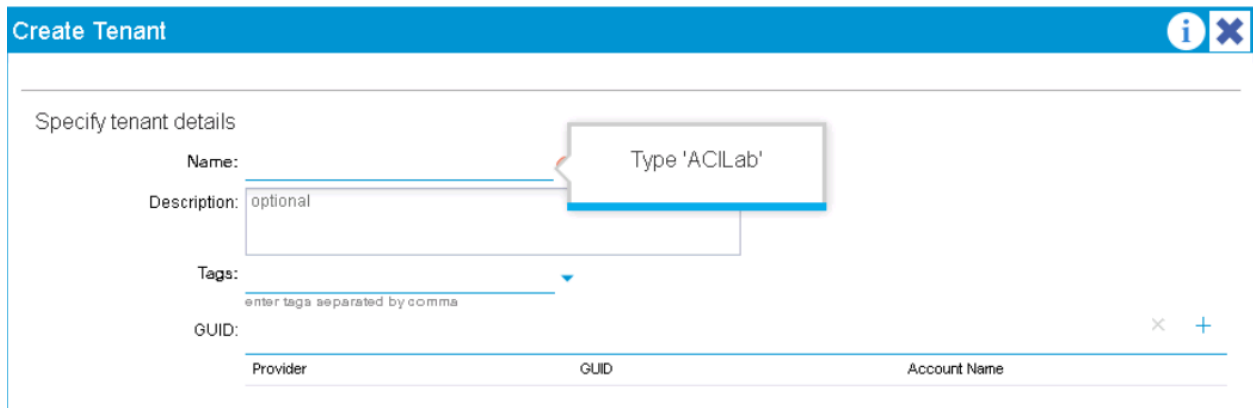


Figure 8 Create Tenant - Name

Once you have named the tenant, you can click submit.

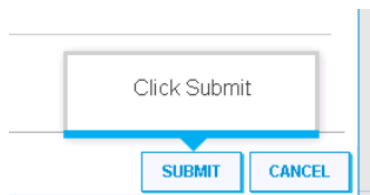


Figure 9 Create Tenant – Submit

3.2.4 Create VRF

A tenant can contain one or more virtual routing and forwarding (VRF) instances or contexts; each context can be associated with multiple bridge domains.

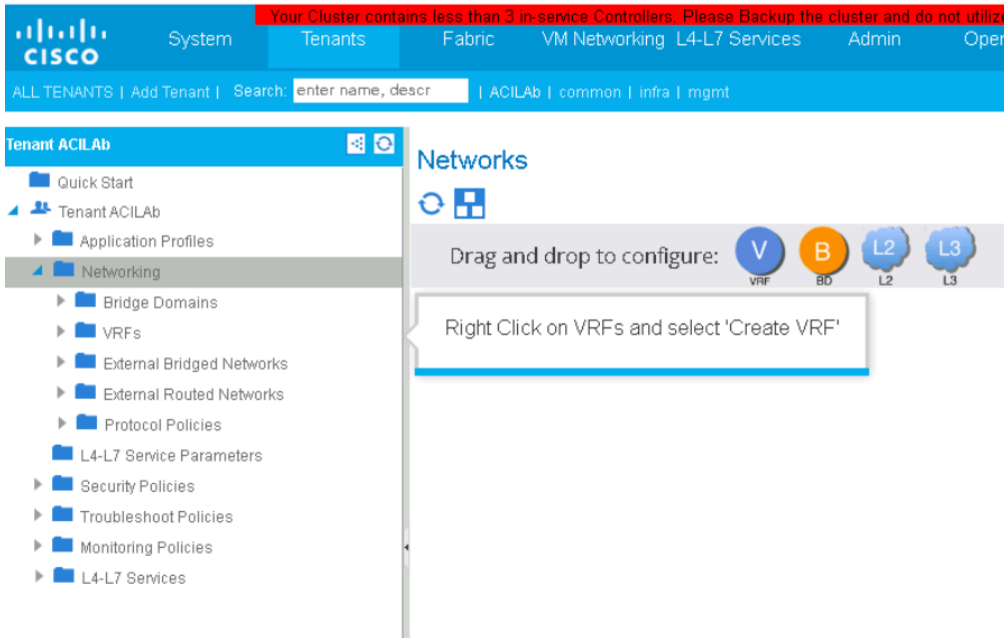


Figure 10 Right click create VRF

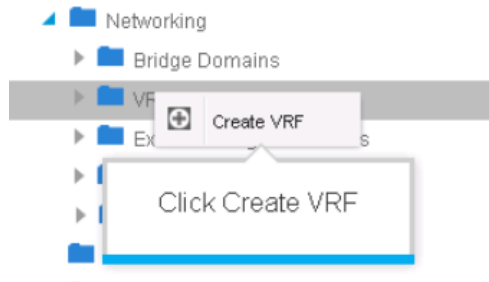


Figure 11 Create VRF

What is a VRF?

A Virtual Routing & Forwarding instance is a L3 boundary within an ACI tenant. This is also known as a Private Network or Context. A Tenant can contain one or more VRFs. In turn, a VRF will contain one or more Bridge Domains (BDs). A BD can only belong to one VRF.

For purposes of Tenant usage, the VRF allows various IP subnets to exist without impacting subnets from other VRFs. This includes re-using IP address space across VRFs.

A common use case for a Tenant having multiple VRFs might be create one VRF for Dev/Test and another for Prod. This would allow users to develop applications in a separate routing space and eliminate the need to re-address endpoints when they move from development into production.

Specify Tenant VRF

The screenshot shows a configuration form for a VRF. The 'Name' field is highlighted with a callout box that says 'Enter: ACILab_VRF' and 'This steps creates the first VRF (Private Network) for our Tenant.' Below the name field is a 'Description' field with the placeholder text 'optional'. The 'Policy Control Enforcement Preference' has two buttons: 'Enforced' (selected) and 'Unenforced'. The 'Policy Control Enforcement Direction' has two buttons: 'Egress' and 'Ingress' (selected). The 'End Point Retention Policy' is a dropdown menu with 'select a value' and a note 'This policy only applies to remote L3 entries'. The 'Monitoring Policy' is another dropdown menu with 'select a value'. The 'DNS Labels' field has a placeholder 'enter names separated by comma'. The 'Route Tag Policy' is a dropdown menu with 'select a value'. At the bottom, there are four checkboxes: 'Create A Bridge Domain' (checked), 'Configure BGP Policies', 'Configure OSPF Policies', and 'Configure EIGRP Policies'.

Figure 12 Enter Name for VRF

Next Name the VRF for example, ACILab_VRF and click NEXT.

3.2.5 Create Bridge Domain

The Bridge Domain provides a Layer 2 forwarding domain. Enter the Bridge Domain Name and click Finish.

What is a Bridge Domain?

A Bridge Domain (BD) represents a Layer 2 forwarding boundary within the fabric and will be assigned to a single VRF. A BD defines a unique L2 MAC address space and flood domain (if enabled).

Bridge Domains can span multiple Leaf switches and can be assigned to one or more End Point Groups (EPGs).

Specify Bridge Domain for the VRF

Name:

Description: optional

Type: fc regular

Forwarding: Optimize

Endpoint Dataplane Learning:

Limit IP Learning To Subnet:

Config BD MAC Address:

MAC Address:

Enter Name: ACILab_BD1

This creates our first Bridge Domain for our Tenant. The bridge domain defines a scope for the broadcast traffic within the tenant

Figure 13 Enter Name of Bridge Domain

Right click on Bridge Domain (BD) to create a second BD. Specify a second BD with unique name. Click on the VRF drop down of the one setup in the first step and then click NEXT.

Create Bridge Domain

STEP 1 > Main

1. Main

2. L3 Configurations

3. AC

Specify Bridge Domain for the VRF

Name: ACILab_BD2

Description: optional

Type: fc regular

VRF: select a value

Forwarding: ACILab/ACILab_VRF

End Point Retention Policy: common/copy
common/default

IGMP Snoop Policy: Create VRF

Click the dropdown
Select ACILab/ACILab_VRF

Figure 14 bridge domain setup

3.2.6 Create Subnet

Unicast Routing: Enabled

ARP Flooding: Enabled

Config BD MAC Address:

MAC Address: 00:22:BD:F8:19:FF

Subnets:

Gateway Address	Scope	Primary IP Address	Subnet
-----------------	-------	--------------------	--------

Click + to add a new subnet

Figure 15 Create Subnet

About Subnets

As mentioned previously, the IP Subnets are defined within each Bridge Domain. When we create a subnet within a Bridge Domain we are creating a Switch Virtual Interface (SVI) to act as the Gateway for the particular endpoints assigned to the bridge domain.

Subnets can be configured as:

Private: They will only exist within the tenant.

Public: They will be advertised outside of the fabric via an External L3 connection.

Shared: Allows the subnet to be exported to multiple VRFs in the same tenant or across tenants as part of a shared service. An example of a shared service is a routed connection to an EPG present in another context (VRF) or different tenant. This enables traffic to pass in both directions across VRFs.

Enter the Gateway IP, ex. 20.20.20.1/24 and select Private to VRF which ensures the subnet will not be advertised outside of the fabric.

Figure 16 Create Subnet

Click OK – NEXT – FINISH.

3.2.7 Configuring FIPS mode

When FIPS is enabled, it is applied across all the tenants managed by the APIC and across all of the switches in the ACI fabric.

Go to Admin > Fabric Security > Enable > SUBMIT

A reboot of the APIC and all the ACI mode switches on the ACI Fabric must be rebooted in order for the FIPS mode to be implemented.

See the following for more information on configuring FIPS mode:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/KB/b_Cisco_APIC_and_FIPS.html

Note: All of the FIPS approved algorithms and key sizes are automatically configured when FIPS mode is Enabled.

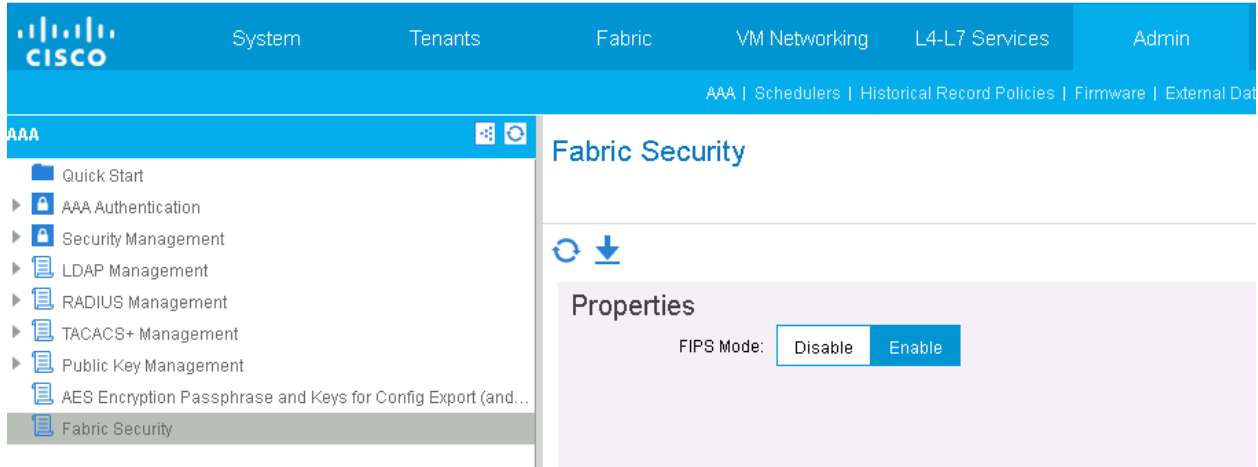


Figure 17 FIPS Mode Config

In order to have the APIC run in FIPS mode an Administrator needs to follow the steps outlined below and in the [18] REST API Configuration Guide.

Follow these guidelines and limitations:

- When FIPS is enabled, it is applied across Cisco APIC.
- Make your passwords a minimum of eight characters in length. This is enforced by setting the password strength check
- Disable Telnet. Note: Telnet is disabled by default. Users should log in using SSH only.
- Delete all SSH Server RSA1 keypairs.
- Disable remote authentication through RADIUS/TACACS+. Only local and LDAP users can be authenticated.
- SNMP is disabled by default.

Configuring FIPS for Cisco APIC Using REST API

Procedure:

Configure FIPS for all tenants.

Example:

`https://apic1.cisco.com/api/node/mo/uni/userext.xml`

`<aaaFabricSec fipsMode="enable" />`

You must reboot to complete the configuration. Anytime you change the mode, you must reboot to complete the configuration.

3.2.8 Ensuring all Keys and Passwords are Encrypted

To ensure all keys and passwords are encrypted in all configuration files:

Admin > AES Encryption Passphrases and Keys for Config Export > Global AES Encryption Settings for all Configuration Import and Export > Select Enable Encryption and enter a minimum 16 character password > Click Submit > Submit Changes

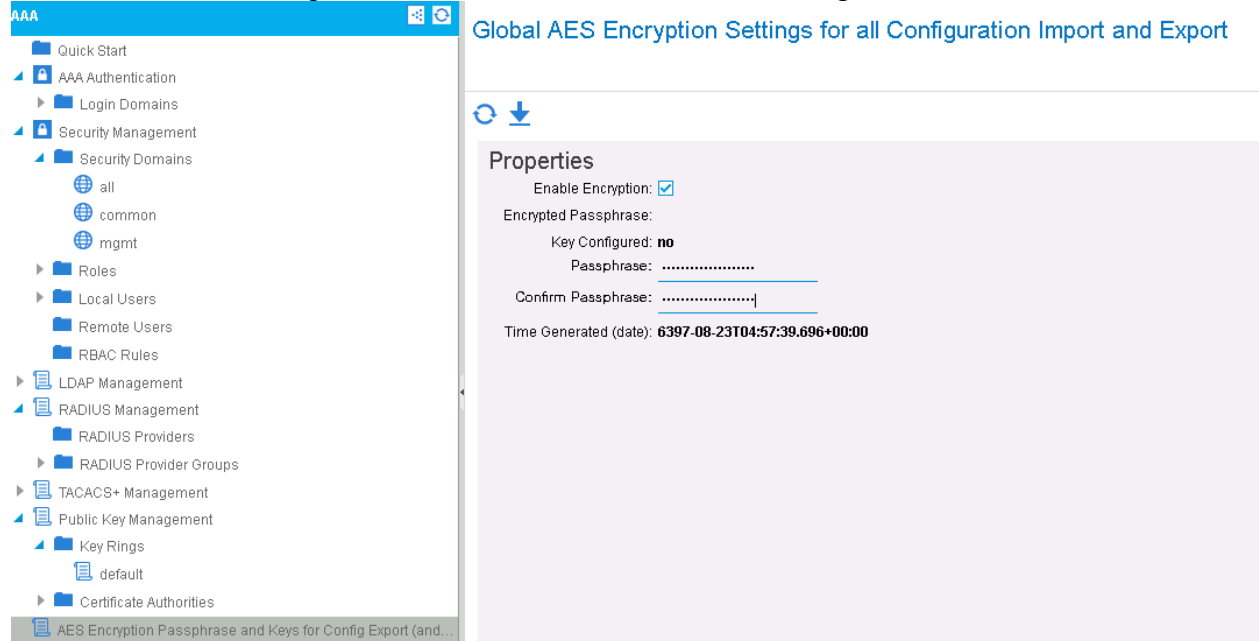


Figure 18 Create AES Key

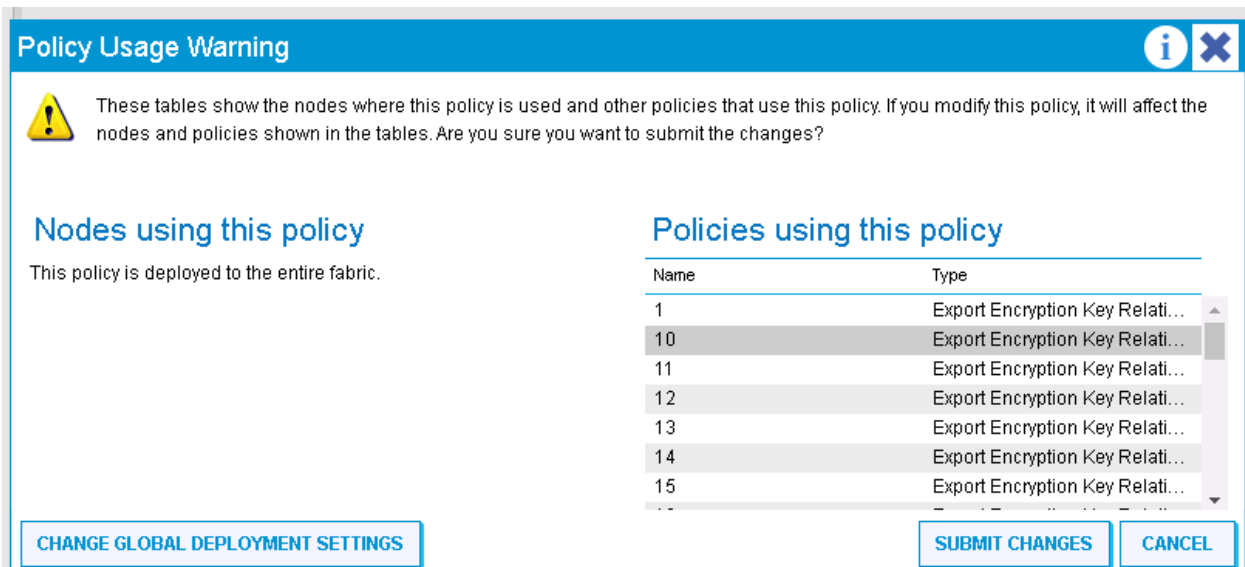


Figure 19 AES Key - Submit Changes

Ensure all passwords are stored encrypted by using the following listed commands. See [5] *Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands)* for the following commands:

3.2.8.1 CLI Configuration Steps:

```
apic1(config)#configure
apic1(config)# crypto aes
apic1(config-aes)# passphrase "thisismypassphrase"
```

apic1(config-aes)# encryption >> enables encryption

3.2.9 Administrator Configuration and Credentials

To setup the Administrator password Go To Admin > Security Management > Select Password Strength Check ‘Yes’

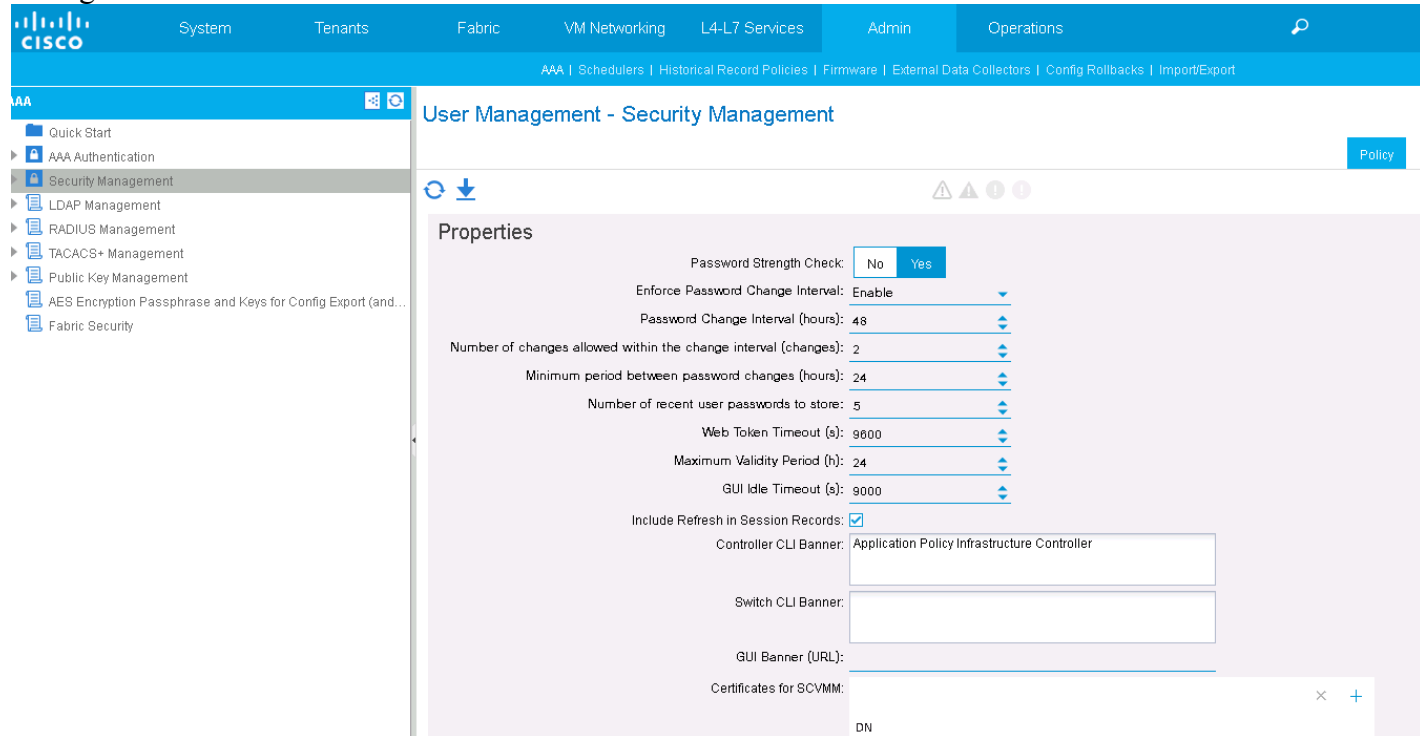


Figure 20 Password Policy

Selecting Yes for Password Strength Check which will enforce a strong password meeting the following characteristics:

- Minimum password length is 8 characters.
- Maximum password length is 64 characters.
- Has fewer than three consecutive repeated characters.
- Must have characters from at least three of the following characters types: lowercase, uppercase, digit, symbol.
- Does not use easily guessed passwords.
- Cannot be the username or the reverse of the username. Cannot be any variation of cisco, isco or any permutation of these characters or variants obtained by changing the capitalization of letters therein.

3.2.9.1 APIC Password Change via CLI

To change the password on the APIC , use the password command. The following example shows how to use the password command:

```
admin@apic1:aci> passwd
Changing password for user admin.
(current) password:
New password:
Retype new password:
Password for user admin is changed successfully.
admin@apic1:aci>
Password for user admin is changed successfully.
To change the admin password via the GUI see below:
```

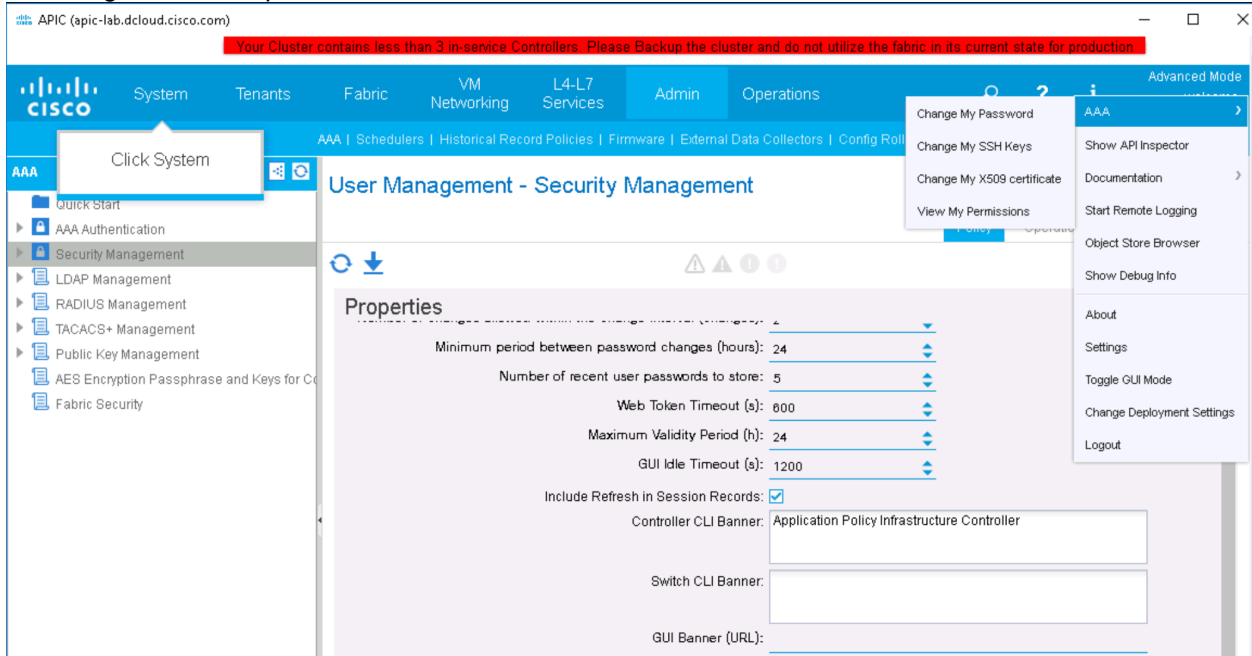


Figure 21 Change own admin password

3.2.10 Access Banner

In the APIC Go To Admin > Security Management > Properties >

- Controller CLI Banner
- Switch CLI Banner
- GUI Banner

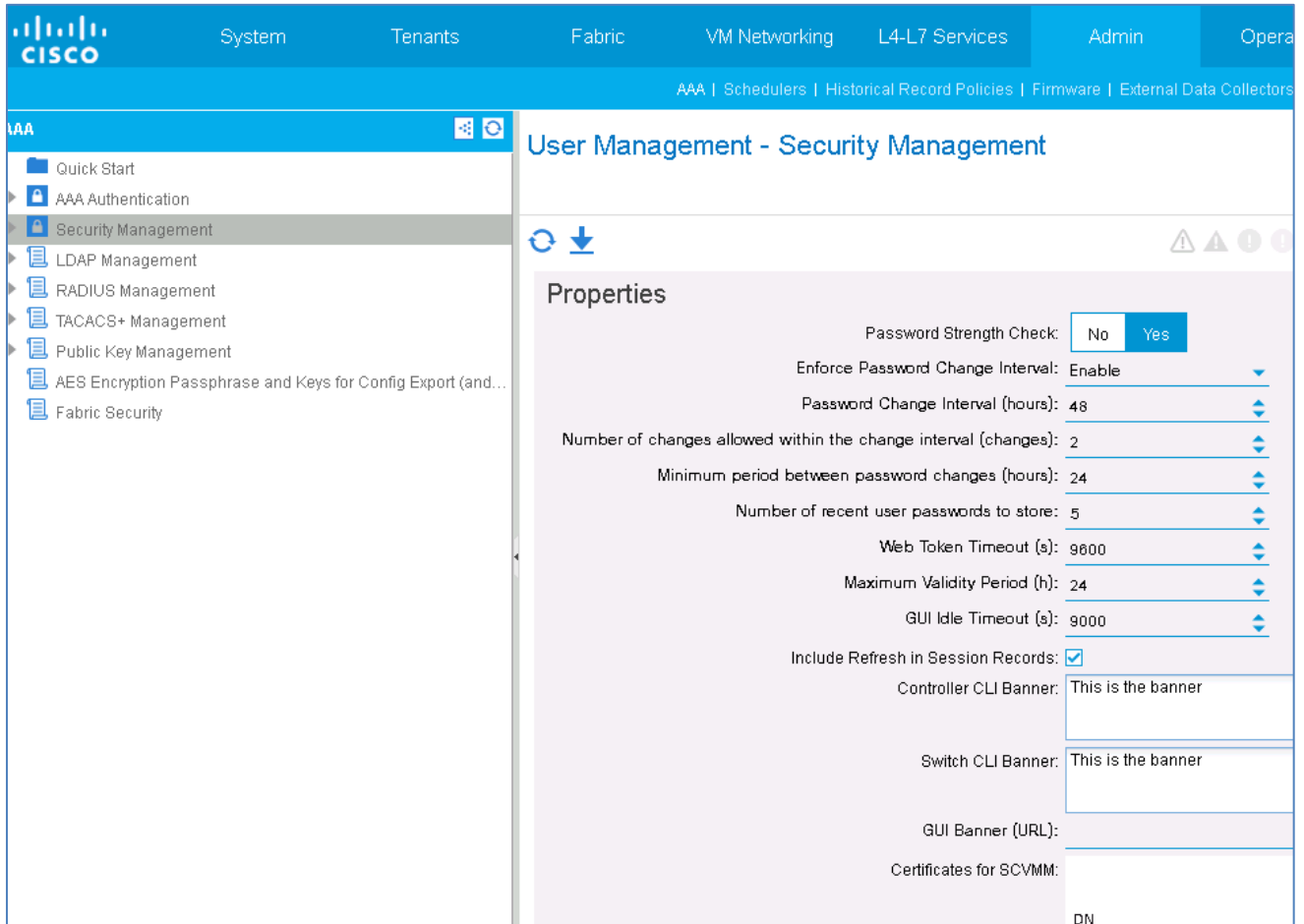


Figure 22 Banner Config

3.2.11 Deleting an Administrator User

To remove an Administrator's access, an administrator user can be deleted following the below steps. Note: There must be two or more administrator accounts in order to delete one administrator account. The default admin account cannot be deleted. The admin account should only be used during initial installation and configuration. Additional Administrator accounts should be created for each individual Administrator with the assigned administrator roles and access permissions.

GUI Configuration Steps to delete an Administrator User:

Administrator first performs the removal of user to be deleted.

Go to Admin Tab / AAA / Local Users / Select User to be deleted / Right Click Delete

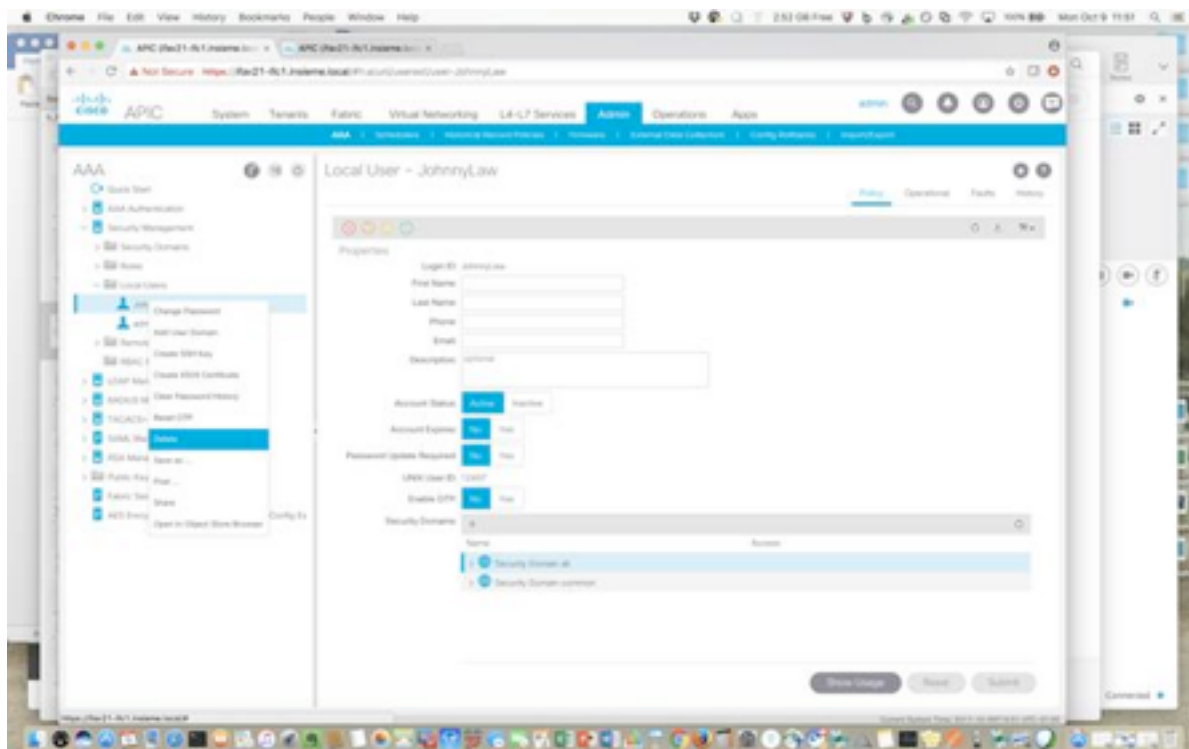


Figure 23 Delete User

Note: By default there is a 600 second timer before the user account times out and is removed from the APIC GUI. In order to ensure the user session is locked out immediately follow the instructions in the Clear User session after deletion section below.

CLI Configuration Steps to delete an Administrator User:

```
TOE-common-criteria# conf t
TOE-common-criteria (config)# no username <userid>
TOE-common-criteria (config)# exit
TOE-common-criteria# copy run start
```

REST API to delete an Administrator User:

```
<aaaUser unixUserId="13982" rbacString="" pwdUpdateRequired="no" pwdLifeTime="no-password-expire" phone="" ownerTag="" ownerKey="" otpkey="DISABLEDDISABLED"
otpenable="no" nameAlias="" name="test-admin" lastName="" firstName="" expires="yes"
expiration="2017-02-10T10:41:13.000-08:00" email="" dn="uni/userext/user-test-admin"
descr="" clearPwdHistory="no" accountStatus="active"/>
```

```
<aaaUser unixUserId="15166" rbacString="" pwdUpdateRequired="no" pwdLifeTime="no-password-expire" phone="" ownerTag="" ownerKey="" otpkey="DISABLEDDISABLED"
otpenable="no" nameAlias="" name="prestige-admin" lastName="" firstName="" expires="no"
expiration="never" email="" dn="uni/userext/user-prestige-admin" descr=""
clearPwdHistory="no" accountStatus="active"/>
```

Clear User session after deletion

The APIC GUI must be rebooted in order to force the user immediately off the session. To ensure that the deleted user is forced off session with the APIC GUI immediately all APICs must be rebooted. Follow the below steps to reboot all the APIC GUIs. See the Troubleshooting Guide [22], section “Shutting Down the APIC Controller Using the GUI.”

This document describes how to reload the APIC controller (not the entire APIC system) using the GUI.

Reload the APIC controller as follows:

- 1 In the menu bar, click System .
- 2 In the submenu bar, click Controllers .
- 3 Under Controllers, click the APIC node that you would like to reload, for example, apic1 (Node-1).
- 4 In the right window pane, at the top of the screen, click the General tab.
- 6 Select Reload from the pull-down menu to immediately reload the APIC controller.
7. Follow the above steps 1-6 to reload the APIC2 and finally APIC3 to ensure the deleted user’s session is immediately ended.

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 in ACI mode only supports SSHv2. 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.

SSH Server Configuration Using APIC:

Go to Admin > Local Users > Right click on the username and select ‘Create SSH Key.’

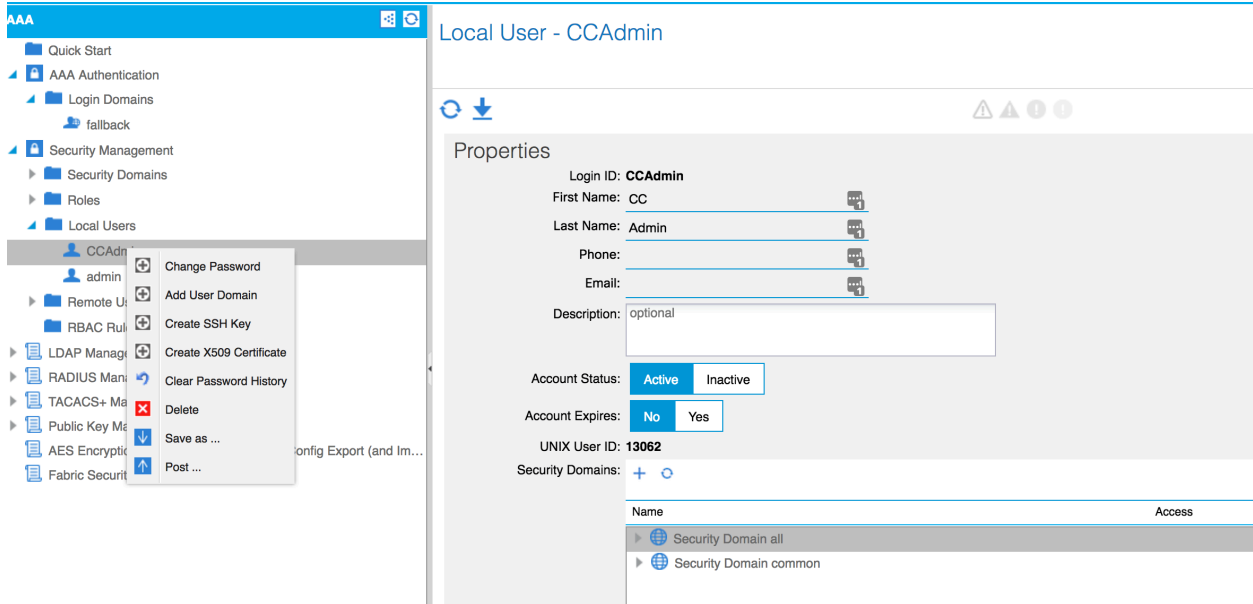


Figure 24 User Login Menu

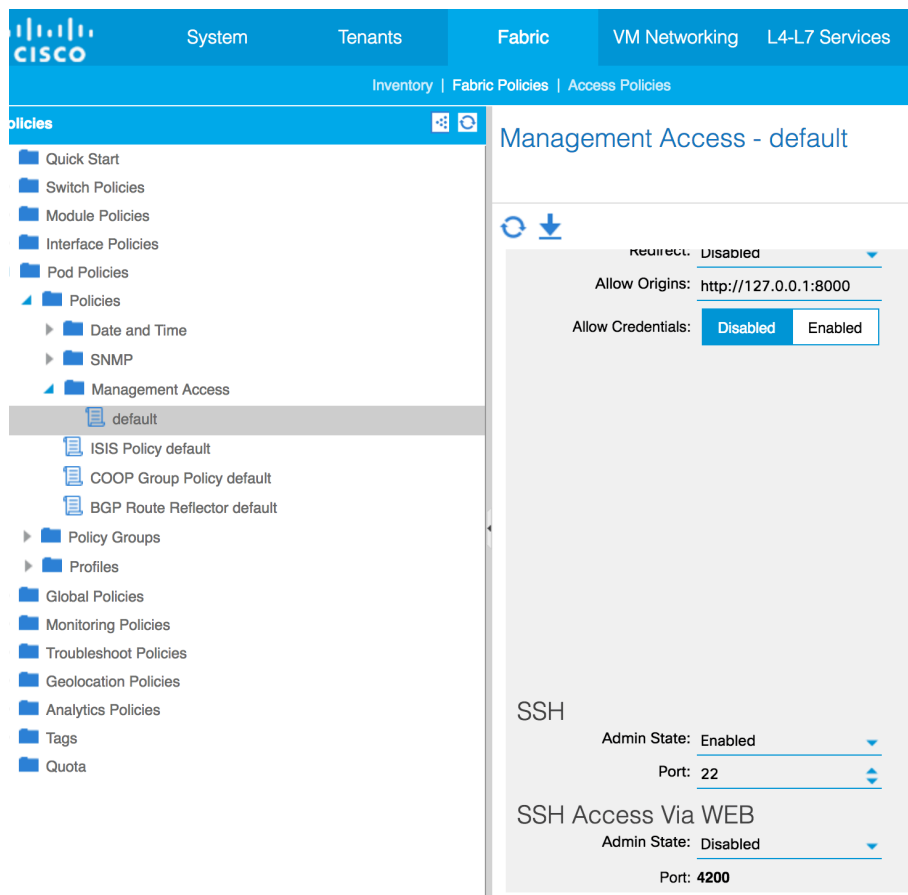
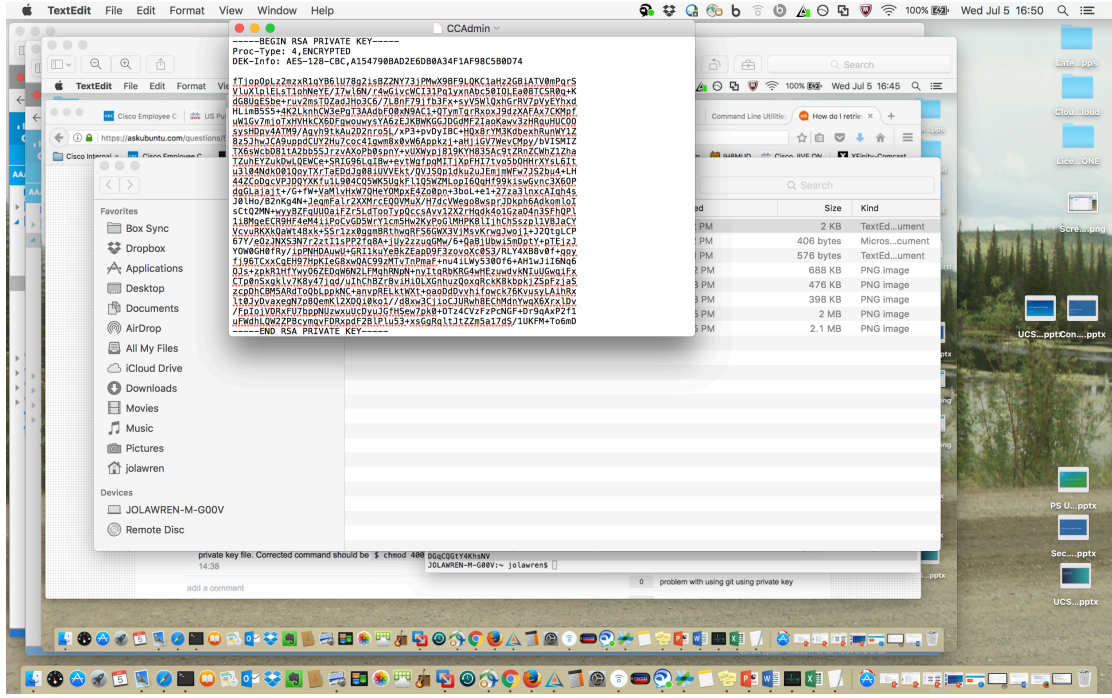
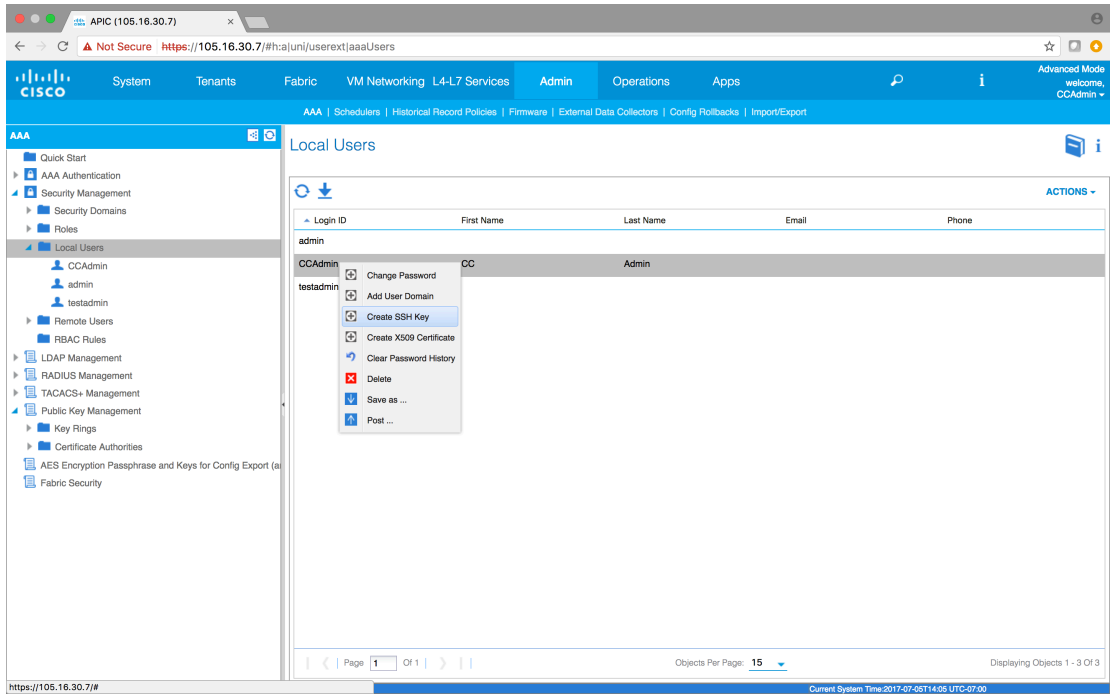


Figure 25 SSH Admin State: Enabled

A SSH key pair can be generated for a particular user to authenticate.



SSH Server Configuration Using CLI:

Note: To SSH to the APIC: #ssh admin@apic1

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

```

apic1# config
apic1(config)# username testadmin
apic1(config-username)#password
Password: Ke%y^&*(t@#!s_123
Retype password:
apic1(config-username)#ssh-key testadminkey
apic1(config-ssh-key)# Note: Copy and paste the public key

```

3.3.1.1 To Configure SSHv2 on the mgmt0 port on the APIC:

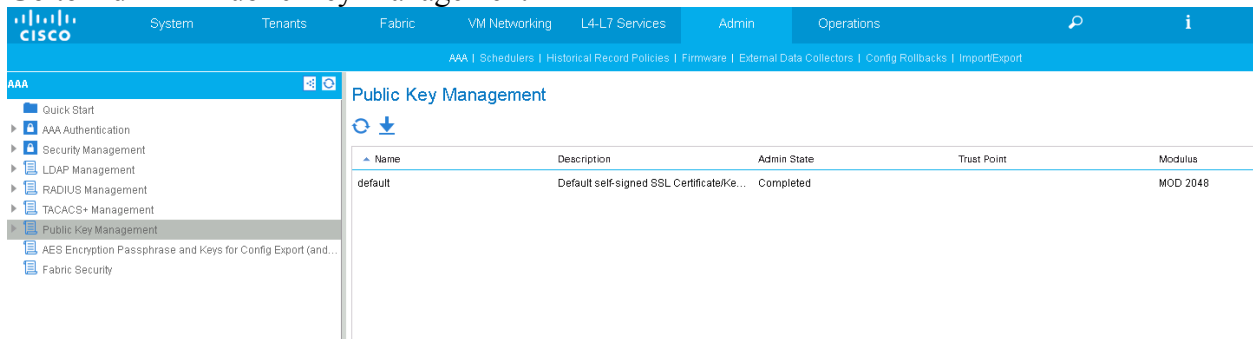
```

apic1# configure
apic1(config)# switch 101
apic1(config-switch)# interface inband-mgmt0
apic1(config-switch-if)# ip address 10.13.1.1/24 gateway 10.13.1.254
apic1(config-switch-if)# exit apic1(config-switch)# exit

```

3.3.2 TLS Server Configuration:

By default a self-signed TLS certificate is installed.
Go to Admin > Public Key Management



By default TLSv1.0 is disabled, but to ensure this go to Fabric > Fabric Policies > Pod Policies > Policies > Management Access > default.

Both TLSv1.1 and TLSv1.2 can be enabled and DH Param must be selected as 2048. These settings can be configured by:

Fabric > Fabric Policies > Pod Policies > Policies > Management Access > default. HTTP is disabled to ensure that only HTTPS is used for accessing the APIC remotely

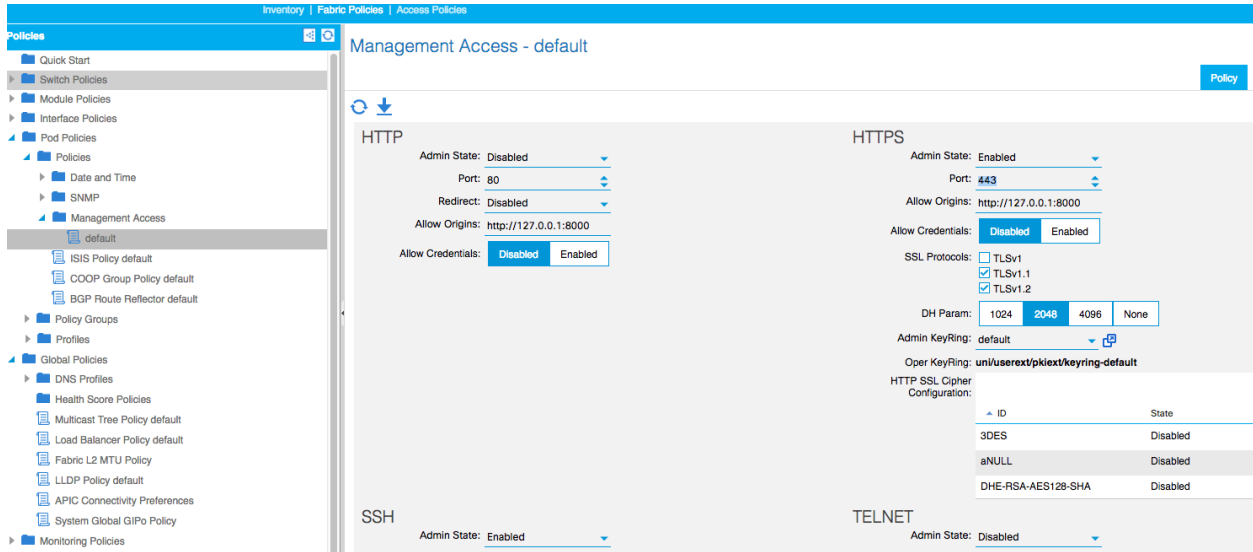


Figure 26 TLS Configuration

3.3.3 Logging Configuration

3.3.3.1 Nexus 9k in ACI mode

Configuration of the Audit Logging is covered in section "User Login Menu Options" in the *Cisco Application Centric Infrastructure Fundamentals Guide*. The Nexus 9k Switch supports local logging of events which are referred to as system messages in the Cisco 9k Documentation. All logs are stored in a local database except for the debug logs. Debug logs can be run for troubleshooting. The device scripts can generate debug logs through the ACI logging framework. The logs are written to a circular file called debug.log under the logs directory.

By default logging is on for the APIC and ACI mode switches. To view the logs in the APIC GUI: System > Events. Ex. EPG contract and logged. Additional logs can be found at Fabric > Pod1 > History > Audit Log

Audit Log



Time Stamp	ID	User	Action	Affected Object
2017-06-30T11:16:19.313-07:00	8589934642	CCAdmin	creation	uni/fabric/moncommon/slsrc-common
2017-06-30T10:58:30.125-07:00	8589934641	CCAdmin	modification	uni/userext/fabricsec
2017-06-30T10:58:24.437-07:00	8589934640	CCAdmin	modification	uni/userext/fabricsec
2017-06-30T10:50:56.464-07:00	8589934639	CCAdmin	modification	uni/userext/fabricsec
2017-06-28T09:47:41.672-07:00	12884901896	admin	modification	topology/pod-1/node-1
2017-06-28T09:00:26.115-07:00	8589934638	admin	creation	uni/backupst/snapshots-[uni/fabric/confi DailyAutoBackup]/snapshot-run-2017-0
2017-06-28T01:00:20.478-07:00	8589934637	admin	creation	uni/backupst/snapshots-[uni/fabric/confi DailyAutoBackup]/snapshot-run-2017-0
2017-06-27T17:00:15.555-07:00	8589934636	admin	creation	uni/backupst/snapshots-[uni/fabric/confi DailyAutoBackup]/snapshot-run-2017-0
2017-06-27T12:42:42.978-07:00	12884901893	admin	creation	uni/userext/user-CCAdmin/userdomain-
2017-06-27T12:42:42.978-07:00	12884901894	admin	creation	uni/userext/user-CCAdmin/userdomain-
2017-06-27T12:42:42.978-07:00	12884901890	admin	creation	uni/userext/user-CCAdmin/userdomain-
2017-06-27T12:42:42.978-07:00	12884901889	admin	creation	uni/userext/user-CCAdmin/userdata
2017-06-27T12:42:42.978-07:00	12884901892	admin	creation	uni/userext/user-CCAdmin/userdomain-

Figure 27 Audit Log

Events



Severity	Affected Object	Code	Cause	Creation Time	Description
1	uni/backupst/jobs-[uni/fabric/configexp-DailyAutoBackup]/run-2017-06-30T09-00-12	E4204965	backup-finish	2017-06-30T09:40:43.813-07:00	Configuration import/export job 2017-06-30T09-00-12 finished with status: failed
1	uni/backupst/jobs-[uni/fabric/configexp-DailyAutoBackup]/run-2017-06-30T09-00-12	E4208481	transition	2017-06-30T09:00:12.772-07:00	Job 2017-06-30T09-00-12 created
1	uni/backupst/jobs-[uni/fabric/configexp-DailyAutoBackup]/run-2017-06-28T17-00-04	E4208483	transition	2017-06-30T09:00:12.772-07:00	Job 2017-06-28T17-00-04 deleted

Figure 28 Audit Events

CLI Commands for Configuring Logging

```
configure
  syslog common
    logging audit
    logging event
    logging fault
    logging session
    logging severity information
  logging server-group sysloghost
  logfile severity information
  server 172.31.208.160
show accounting log
show audits
```


show sessions

In logflash, the maximum file size is 4MB on final images, while it is 10MB on GDB images. To display the system messages that are logged in the file, use the **show logging EXEC** command. The first message displayed is the oldest message in the buffer. To clear the current contents of the buffer, use the **clear debug-logfile** command.

Changing the default configuration of the logging levels can be made. See section "Configuring System Message Logging to Terminal Sessions" and "Logging System Messages to a File" in [2] *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*. By default, audit events are logged to the log:messages file in DRAM.

Authentication and authorization events are maintained in the local accounting log. See chapter "Configuring AAA", section "Monitoring and Clearing the Local AAA Accounting Log" of [3] for information on viewing and clearing these logs. In addition, for more information on configuring system logging see [2], section "Configuring System Message Logging". The accounting log for Authentication, Authorization, and Accounting (AAA) and local, allows us to see all the config commands run on the devices from any user. In order to enable logging of all commands use the **terminal log-all** command.

#TOE-common-criteria (config)# **terminal log-all**

To view the audit events for Authentication, Authorization, and Accounting (AAA) and local:

#TOE-common-criteria (config)# **show accounting log all**

To enable Login Authentication Failure Messages:

#aaa authentication login error-enable

System events are maintained by default in the file "logflash:" filesystem. This file can be viewed and the settings for it can be modified as indicated in chapter "Configuring System Message Logging" and sections "Logging System Messages to a File" and "Displaying and Clearing Log Files" of [2] *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

TOE-common-criteria (config)# **dir logflash:**

If the logflash filesystem is not mounted, try to manually mount it:

TOE-common-criteria (config)# **mount logflash:**

TOE-common-criteria (config)# **show logging nvram** [last number-lines]

TOE-common-criteria (config)# **clear logging nvram**

3.3.3.2 APIC

From the APIC, an audit log summary can be viewed without directly having to attach to the 9k switch to view the logs. To display an audit summary for a given node, module, or interface, use the **auditlog** command. Using the auditlog command includes auditing information such as login and logout times. The **eventlog** command will display an event summary for a given switch or another APIC controller. The eventlog command can show the events such as for an interface or port.

To display the logging settings on the APIC, use the **loglevel** command.

3.3.4 Virtual Port Channel Operations

Information related to the Virtual Port Channel Operations can be found in section "Configuring vPCs" [9] *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.

3.3.5 Routing Protocols

The routing protocols are used to maintain routing tables. The routing tables can also be configured and maintained manually. Refer to the applicable sections in [10] *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide* for configuration of the routing protocols.

The following routing protocols are used on all of the TOE models:

- Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4) and 3 (IPv6)
- Intermediate System-to-Intermediate System (IS-IS) Protocol for IPv4
- Border Gateway Protocol (BGP) for IPv4 and IPv6
- Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and IPv6
- Routing Information Protocol Version 2 (RIPv2)
- Protocol Independent Multicast (PIM)

3.3.6 Non-Approved Algorithms and Protocols

This section details the algorithms and protocols that were not evaluated. These algorithms and protocols are supported by the TOE and are disabled by default. They will not be configured for use in the evaluated configuration.

- DES
- 3DES
- HMAC MD5
- MD5
- NDRNG
- RC4
- ftp
- telnet
- GRE
- PMTUD
- LLDP
- NX-API

4 Secure Management

Cisco APIC and NX-OS devices support Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) protocols. Based on the user ID and password combination that an authorized administrator provides, Cisco NX-OS devices perform authentication using the local database or remote authentication using one or more AAA (RADIUS or TACACS+) servers. A pre-shared secret key provides security for communication between the Cisco NX-OS device and AAA servers. An authorized administrator can configure a common secret key for all AAA servers or for only a specific AAA server. See [3] section "AAA Security Services" for more information.

4.1 Configuring Management Access to APIC

Follow the procedures in section "Configuring In-Band Management Access Using the CLI" in the *Cisco APIC Getting Started Guide* [12]. To configure SSH on the inbound mgmt0 see section 3.3.1.1 A management EPG will be configured to ensure that only In-Bound Management Access is allowed within the ACI Fabric.

4.1.1 Configuring Static In-Band Management Access Using the GUI

First VLAN IDs will be allocated for the internal inband management EPG (VLAN 100) and for the user facing EPG (VLAN 99). Both of these VLANs will be put into a VLAN Pool.

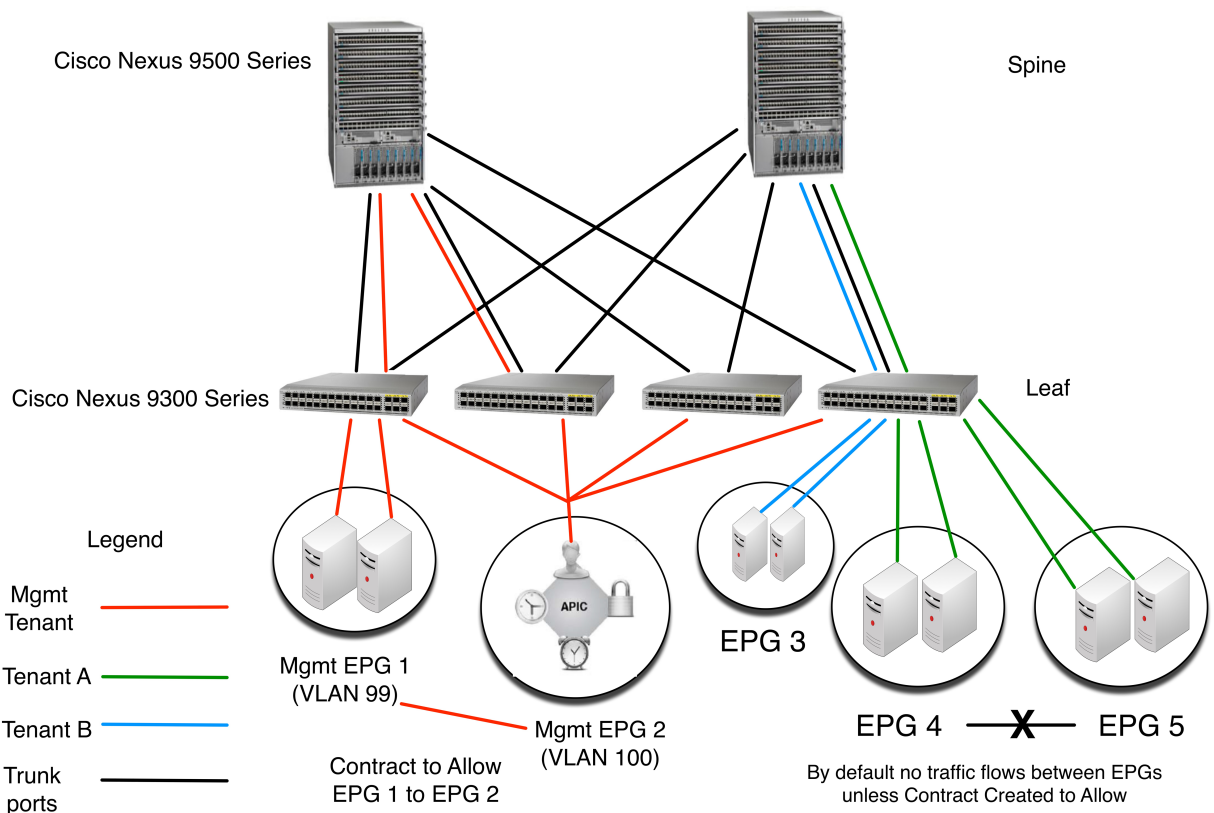


Figure 29 In-Band Tenant Management

The mgmt Tenant

As shown in Figure 29, separate tenants ensure traffic is isolated for a specific tenant. Traffic can only flow between different EPGs once a specific contract is configured for what traffic is allowed to flow. By configuring an **In-band EPG**, management traffic will be separate from the regular user data traffic. This will have to be done before assigning the static addresses for the APIC, Leaves, and Spines. See the APIC Basic Configuration Guide, section “*Configuring In-Band Management Access Using the Basic GUI*” [19] for more information.

Step 1 Login to the Basic Mode in the APIC GUI, and on the menu bar, click System > In Band & Out Of Band.

Step 2 In the Navigation pane, choose InBand Management Configuration.

Step 3 (Optional) In the Encap field, enter a new value to change the default VLAN that is used for in-band management, if desired.

Step 4 Expand Nodes and perform the following actions:

a) In the Nodes field, choose the appropriate node to associate the in-band address.

b) In the IP address field, enter the desired IPv4 or IPv6 address.

c) In the Gateway field, enter the desired IPv4 or IPv6 gateway address. Click Submit.

Note: The default gateway IP address will be the pervasive gateway of the ACI fabric on the VRF for the inband management.

Step 5 Click the L2 Connectivity tab, expand Ports, and perform the following actions:

a) In the Path field, from the drop-down list, choose the port that is connected to a server for management or to the outside.

b) In the Encap field, specify a VLAN to use on this port.

Step 6 Expand Gateway IP Address for External Connectivity and in the IP address fields, list the desired gateway

IPv4 and Pv6 address for external connectivity.

Step 7 Expand ACLs, and add the desired ports that you want to connect to the inband management network. Click Submit.

Procedure

Step 1 Assign a VLAN for the APIC inband management, as shown in the following example:

Example:

```
apic1(config)#
apic1(config)# vlan-domain inband-mgmt
apic1(config-vlan) vlan 10
apic1(config-vlan) exit
```

Step 2 Provide external connectivity to the inband management ports, as shown in the following

Example:

Note: In this step, the controller is connected to a port on a leaf switch. You must add a VLAN domain member on that port. In this example, in leaf 101, the port ethernet 1/2 is connected to controller 1. You are configuring the VLAN domain member "inband management". This is one part of the connection. The other part is that the management station is connected to leaf 102, interface ethernet

1/3. A controller is one machine connected one port on the leaf switch, which in this case is leaf 102. The machine is trying to connect to the controller from the outside (ethernet 1/3).

```

apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf) internet ethernet 1/2
apic1(config-leaf-if)# vlan-domain member inband-mgmt
apic1(config-leaf-if)# exit
apic1(config)# leaf 102
apic1(config-leaf) internet ethernet 1/3
apic1(config-leaf-if)# vlan-domain member inband-mgmt
apic1(config-leaf-if)# switchport trunk allowed vlan
apic1(config-leaf-if)# exit

```

Configure in-band management access the default management connectivity mode for the APIC server using the following CLI command sequence:

```

apic1# configure
apic1(config)# mgmt_connectivity pref inband

```

4.2 APIC User Roles

Role-Based Access Control (RBAC) allows you to control user permissions by creating roles with a set of permissions and assigning them to users. RBAC allows you to apply permission to a user by assigning a role rather than directly configuring permissions. See the [18] *APIC REST API Guide* section “AAA RBAC Roles and Privileges”.

Table 6 Roles and Privileges

Role	Operations
<i>aaa</i>	<i>Used for configuring authentication, authorization, accounting, and import/export policies.</i>
<i>admin</i>	<i>read, write operations for all security attributes defined within administratively configured ACLs policy rules and IP Source Guard/Traffic Storm Inspection.</i> <i>read, write operations for all security attributes defined within administratively configured ACLs policy rules IP Source Guard/Traffic Storm Inspection policies. .</i>
<i>access-admin</i>	<i>Layer 1, Layer 2, Layer 3 configuration under infra. Fabric wide policies for NTP, DNS, and image management. Management infra policies</i>
<i>fabric-admin</i>	<i>Layer 1, Layer 2, Layer 3 configuration under fabric. Fabric wide policies for NTP, DNS, and image management. Management fabric policies</i>
<i>nw-svc-admin</i>	<i>managing Layer 4 to Layer 7 service devices, shared service devices, orchestration</i>
<i>nw-svc-params</i>	<i>managing Layer 4 to Layer 7 service policies.</i>
<i>ops</i>	<i>Used for operational policies including monitoring and troubleshooting policies such as atomic counter, SPAN, TSW, tech support, traceroute, analytics, and core policies.</i>
<i>read-all</i>	<i>Read only for infra and fabric policies and ops</i>

Role	Operations
<i>tenant-admin</i>	<i>Layer 1, Layer 2, Layer 3 configuration under infra and fabric. Fabric wide policies for NTP, DNS, and image management. Management infra and fabric policies for their assigned tenant</i>
<i>tenant-ext-admin</i>	<i>Used for managing network policies that affect the external to the tenant network. Layer 1, 2, and 3 protocols such as Used for managing tenant external Layer 3 protocols such as BGP, OSPF, PIM, and IGMP</i>
<i>vmm-admin</i>	<i>Read all objects in APIC's VMM and managing VMM policies.</i>
<i>Administrator defined role(s)</i>	<i>read, write operations consistent with the role definitions.</i>

To Configure the User Roles via the APIC:

Go To Admin > Security Management > Roles

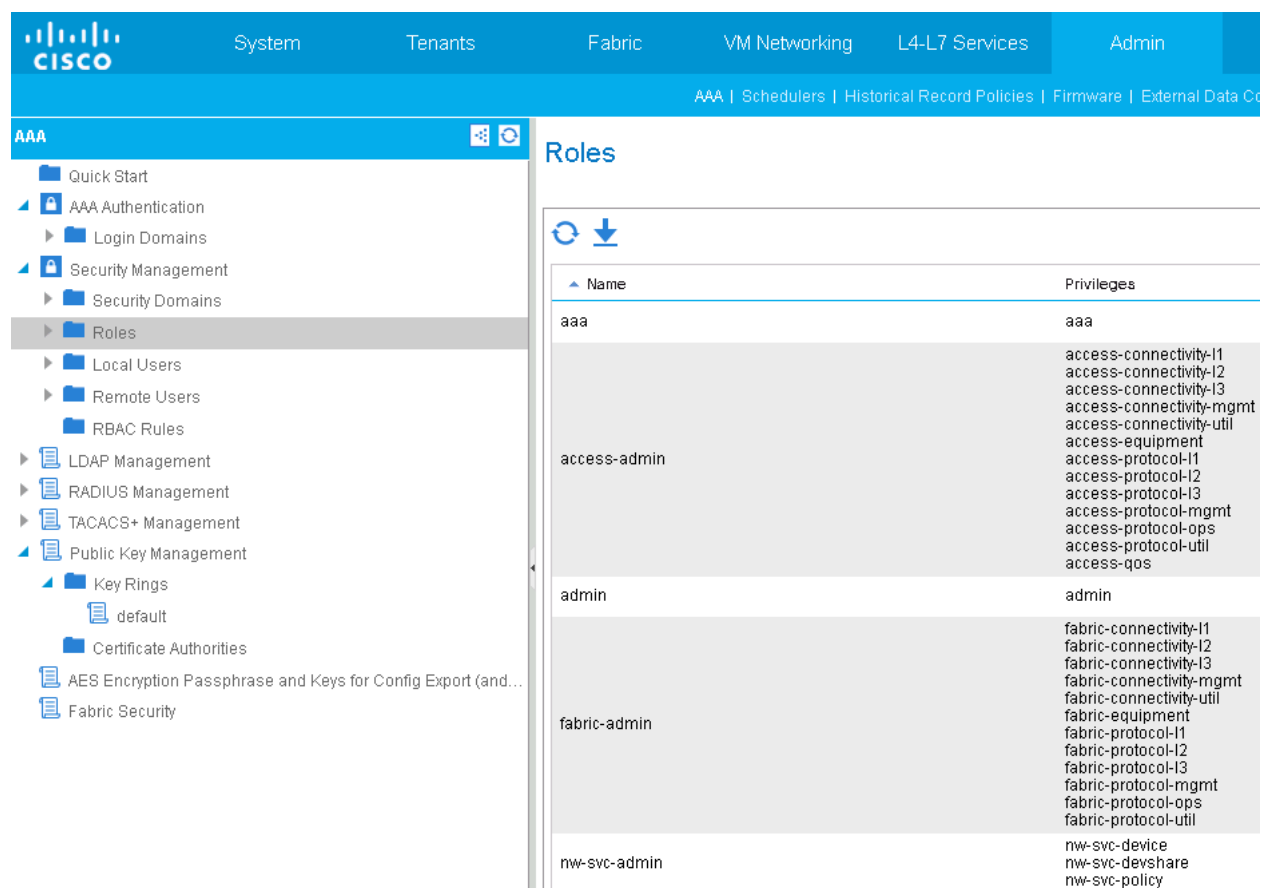


Figure 30 RBAC

4.2.1 User Account Creation

4.2.1.1 Configuring a Local User via GUI

Go To Admin > Local Users (Right Click) > Select Security Domain > NEXT > Roles (Select) > NEXT > User Identity

Create Local User i X

STEP 1 > Security 1. Security 2. User Identity

Enter the Security Information for this User

Security Domain: 🔄 +

Select	Name	Description
<input type="checkbox"/>	all	
<input checked="" type="checkbox"/>	common	
<input type="checkbox"/>	mgmt	

User Certificates: ✕ +

Name	Certificate


SSH Keys: ✕ +

Name	Key

NEXT CANCEL

Figure 31 Create Local User

Specify the User Identity

Login ID: 

Password:

Confirm Password:

First Name:

Last Name:

Phone:

Email:

Description:

Account Status: Active Inactive

Account Expires: No Yes

FINISH

CANCEL

Figure 32 User Identity

4.2.1.2 Configuring a Local User Using CLI

Step 1 In the CLI, change the directory to /aci.

Example:

```
admin@apic1:~> cd /aci
```

Step 2 Create a local user.

Example:

```
admin@apic1:aci> cd admin/aaa/security-management/  
admin@apic1:security-management> cd local-users/  
admin@apic1:local-users> mcreate operations  
admin@apic1:local-users> moconfig commit  
Committed mo 'admin/aaa/security-management/local-users/operations'
```

All mos committed successfully.

```
admin@apic1:local-users> cd operations/  
admin@apic1:operations> moset password  
Password:
```


Verify:

password is set and committed.

```
admin@apic1:operations> moconfig commit
```

```
admin@apic1:operations>
```

4.2.1.3 AV Pair on the External Authentication Server

An administrator can add a Cisco attribute/value (AV) pair to the existing user record to propagate the user privileges to the APIC controller. The Cisco AV pair is a single string that can specify the Role-Based Access Control (RBAC) roles and privileges for an APIC user. An example configuration for an open RADIUS server (/etc/raddb/users) is as follows:

```
aaa-network-admin Cleartext-Password := "<password>"
Cisco-avpair = "shell:domains = all/aaa/read-all(16001)"
```

4.2.2 RADIUS/TACACS+

To configure RADIUS via the APIC, follow the below steps from [18] REST API Configuration Guide.

To configure users on RADIUS servers, the APIC administrator must configure the required attributes (shell:domains) using the cisco-av-pair attribute. The default user role is network-operator. "

Configuring APIC for RADIUS Access

See [19] for more information on configuring the APIC for RADIUS *Cisco APIC Basic Configuration Guide, Release 2.x*.

Step 1 In the APIC, create the RADIUS provider.

a) On the menu bar, choose Admin > AAA .

b) In the Navigation pane, choose RADIUS Management > RADIUS Providers (Right Click to add server).

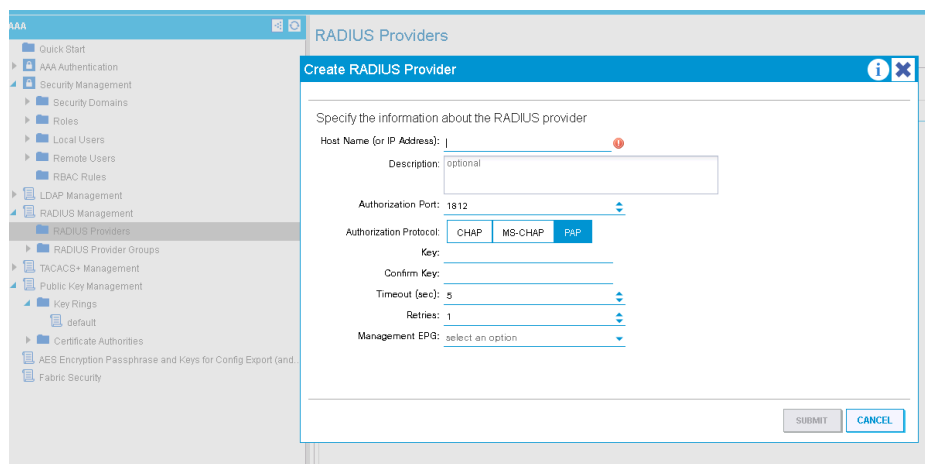


Figure 33 RADIUS Config

c) In the Work pane, choose Actions > Create RADIUS Provider .

d) Specify the RADIUS host name (or IP address), port, protocol, and management endpoint group.

Note:

If the APIC is configured for in-band management connectivity, choosing an out-of-band management endpoint group for RADIUS access does not take effect. Alternatively, an out-of-band over an in-band management endpoint group can connect a RADIUS server but requires configuring a static route for the RADIUS server. The Cisco ACS sample configuration procedure below uses an APIC in-band IP address.

Step 2 Create the RADIUS provider group.

- a) In the Navigation pane, choose RADIUS Management > RADIUS Provider Groups .
- b) In the Work pane, choose Actions > Create RADIUS Provider Group .
- c) Specify the RADIUS Provider Group name, description, and providers as appropriate.

Step 3 Create the login domain for RADIUS.

- a) In the Navigation pane, choose AAA Authentication > Login Domains .
- b) In the Work pane, choose Actions > Create Login Domain .
- c) Specify the login domain name, description, realm, and provider group as appropriate.

To configure the local console to work with a RADIUS or TACACS+ server see section "Configuring Console Login Authentication Methods" in [3].

If using RADIUS:

```
TOE-common-criteria# conf t
TOE-common-criteria (config)# aaa authentication login console group radius
TOE-common-criteria (config)# exit
TOE-common-criteria# copy run start
```

If using TACACS+:

```
TOE-common-criteria# conf t
TOE-common-criteria (config)# feature tacacs+
TOE-common-criteria (config)# exit
TOE-common-criteria# copy run start
```

4.2.2.1 User Authorization (Roles) To Be Handled by RADIUS/TACACS

Configuring authentication and authorization methods for console logins, use the '**aaa authentication login console**' command. This example shows how to configure the authorization authentication console login methods:

```
switch# configure terminal
```

```
switch(config)# aaa authentication login console group [radius tacacs+]1
```

¹ [6] aaa authentication login console

To configure default AAA authorization methods for all EXEC commands, use the `aaa authorization commands default` command. This command allows for all authorization (role) data to be sent to the TACACS+ Server automatically when user accounts are created:

```
switch# configure terminal  
switch(config)# aaa authorization config-commands default group TacGroup local
```

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for authorization, use the `aaa authorization cts default group` command.

To use the `aaa authorization cts default group` command, an authorized administrator must enable the Cisco TrustSec feature using the 'feature cts' command.

```
switch# feature cts  
switch# configure terminal  
switch(config)# aaa authorization cts default group RadGroup
```

4.3 Clock Management

Clock management is restricted to the privileged administrator.

Fabric > Fabric Policies >

In the Navigation menu choose > Pod Policies > Policies > Date and Time

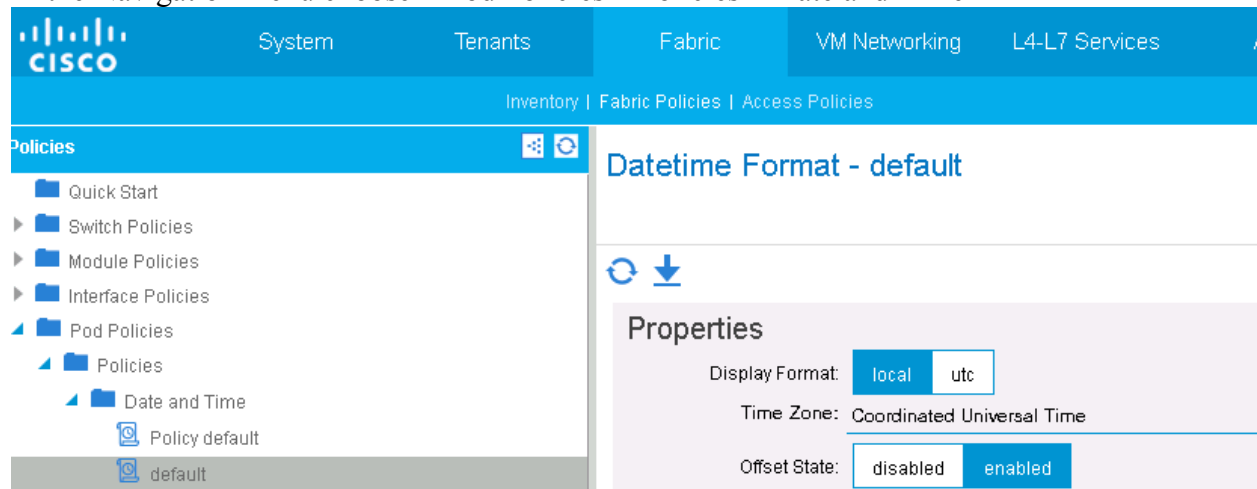


Figure 34 Clock Settings

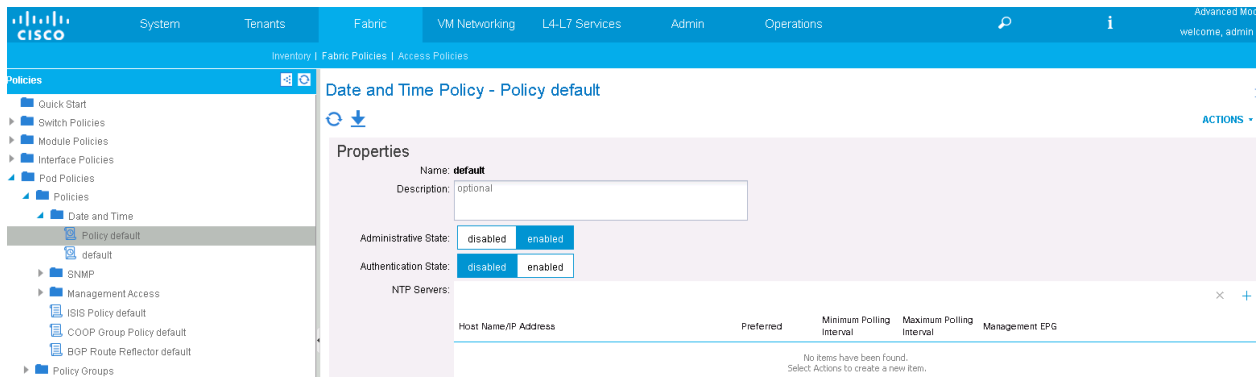


Figure 35 NTP Configuration

For instructions to set the timezone for the clock, refer to section "Configuring the Time Zone" in [16].

To manually set the clock see section "Display Format" in [16].

```
TOE-common-criteria# configure [['terminal', 't']]
TOE-common-criteria (config)# clock display-format local|utc
```

```
TOE-common-criteria # configure [['terminal', 't']]
TOE-common-criteria (config)# clock show-offset enable
```

To configure ntp using the command line:

```
# configure [['terminal', 't']]
(config)# pod <NUMBER>
(config-pod)# ntp
(config-ntp)# description <STRING>
```

4.4 Identification and Authentication

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

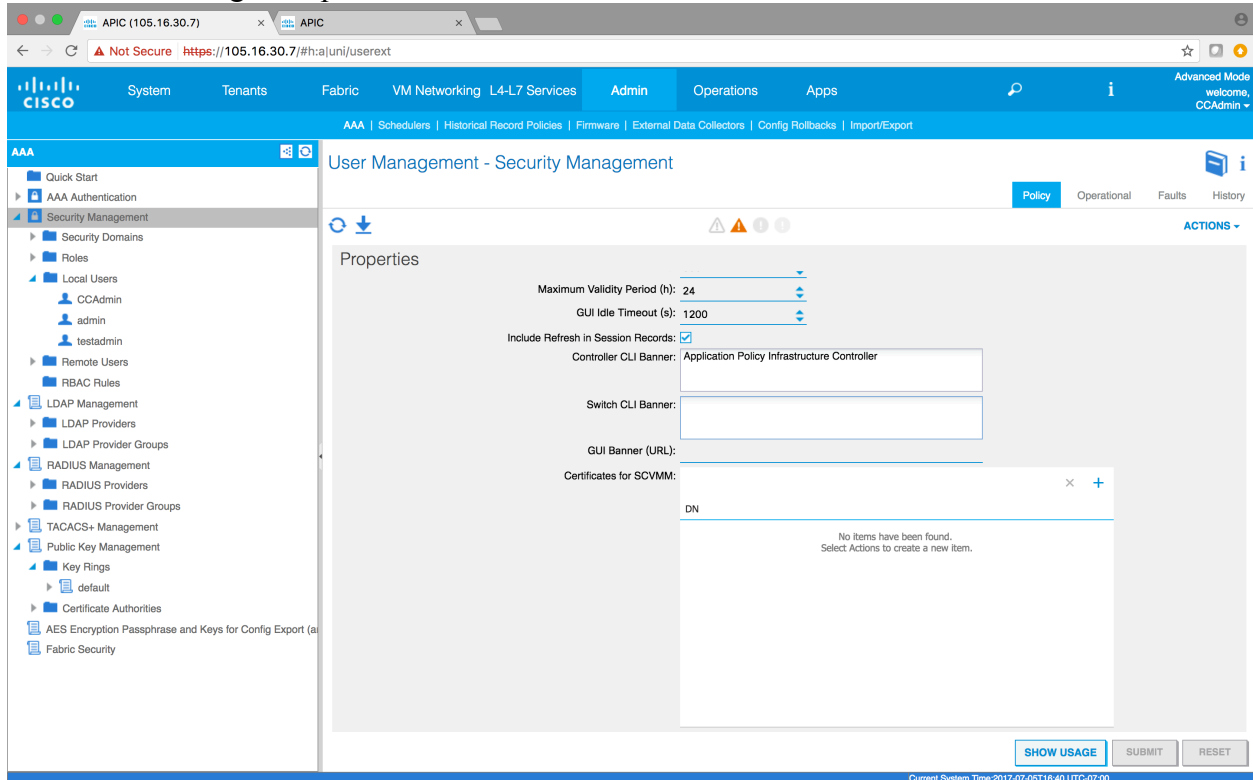
The APIC and 9k can be configured to use any of the following authentication methods:

- Remote authentication (RADIUS or TACACS+)
 - Refer to “Authentication Server Protocols” elsewhere in this document for more details.
- Local authentication (password or SSH public key authentication);
 - Note: this should only be configured for local fallback if the remote authentication server is not available.

4.4.1 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 9000 Series NX-OS Command Reference (Configuration Commands)*

In the APIC an Administrator can configure the banner under the AAA. Under the user login drop down menu > Select AAA > banner.



4.5 Information Flow Policies

The TOE may be configured by privileged administrators for information flow control using the APIC policies. Each information flow action is controlled by the supervisor (permit, drop, ignore) via the contracts which specify the subjects/filter/action of the policy rules applied to Endpoint Groups (EPGs). The network traffic is mediated via the I/O network module ports. Configuration of information flow policies is restricted to the privileged administrator. See section "Contracts" and "Labels, Filters, and Subjects Govern EPG Communications [15]."

4.5.1 Policies, Filters, and Contracts

4.5.1.1 Create Filter

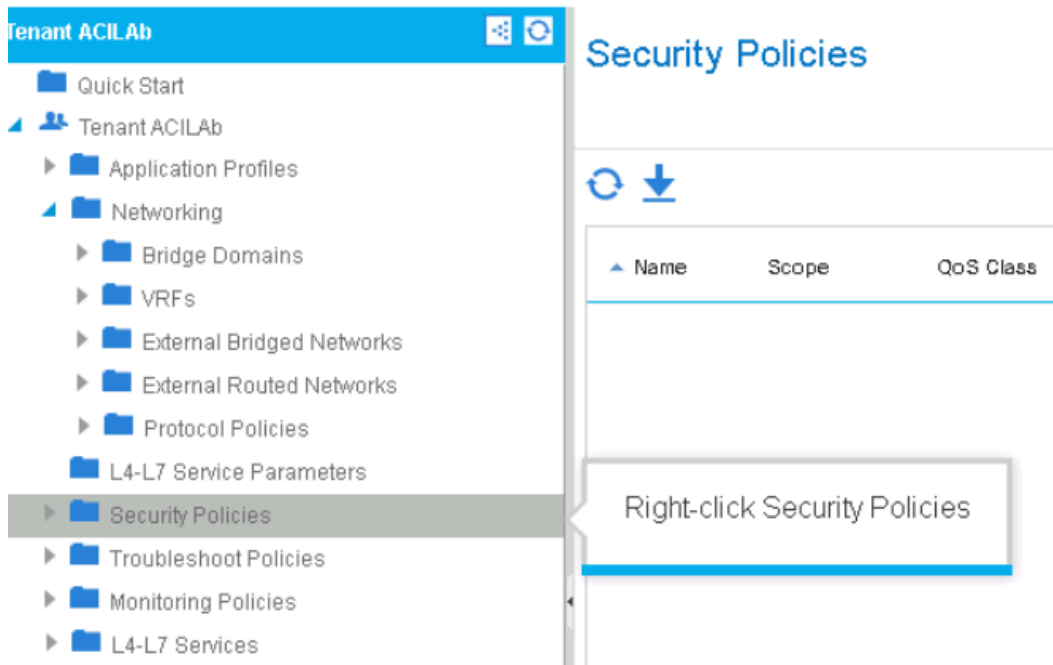


Figure 36 Security Policies

Right Click Security Policies and click Create Filter.

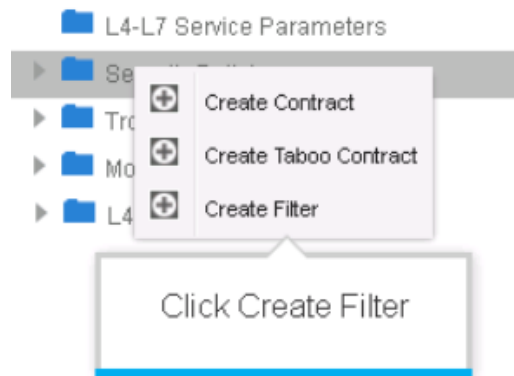


Figure 37 Create Filter

Name the Filter, ex web_filter.

Create Filter

Specify the Filter Identity

Name: ⓘ

Description: optional

Enter: web_filter

Entries:

Name	EtherType	ARP Flag	IP Protocol

Figure 38 Name the Filter

Click the + and specify the filter.

Specify the Filter Identity

Name: web_filter

Description: optional

Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source Port / Range		Destination Port / Range		TCP Session Rules
						From	To	From	To	

Click +

Figure 39 Click +

Create Filter

Specify the Filter Identity

Name: web_filter

Description: optional

Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source Port / Range		Destination Port / Range		TCP Session Rules
						From	To	From	To	
<u>web_acl</u>	Unspecified	Unspecified	Unspecified	<input type="checkbox"/>	<input type="checkbox"/>	Unspecified	Unspecified	Unspecified	Unspecified	Unspecified

Enter: web_acl

UPDATE CANCEL

Figure 40 Specify Filter

Specify the Filter Identity

Name: web_filter

Description: optional

Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source Port / Range From	To	Destination Port / Range From	To	TCP Session Rules
web_acl	Unspecified	Unspecified	Unspecified	<input type="checkbox"/>	<input type="checkbox"/>	Unspecified	Unspecified	Unspecified	Unspecified	Unspecified

Select 'IP'

UPDATE CANCEL

Figure 41 Specify Filter Identity – Ethertype IP

Create Filter i X

Specify the Filter Identity

Name: web_filter

Description: optional

Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source Port / Range From	To	Destination Port / Range From	To	TCP Session Rules
web_acl	IP	Unspecified	Unspecified	<input type="checkbox"/>	<input type="checkbox"/>	Unspecified	Unspecified	Unspecified	Unspecified	Unspecified

Select 'tcp'

UPDATE CANCEL

Figure 42 Select 'tcp'

Create Filter i X

Specify the Filter Identity

Name: web_filter

Description: optional

Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source Port / Range From	To	Destination Port / Range From	To	TCP Session Rules
web_acl	IP	Unspecified	tcp	<input type="checkbox"/>	<input type="checkbox"/>	Unspecified	Unspecified	Unspecified	Unspecified	Unspecified

Select 'http'

UPDATE CANCEL

Figure 43 Select http

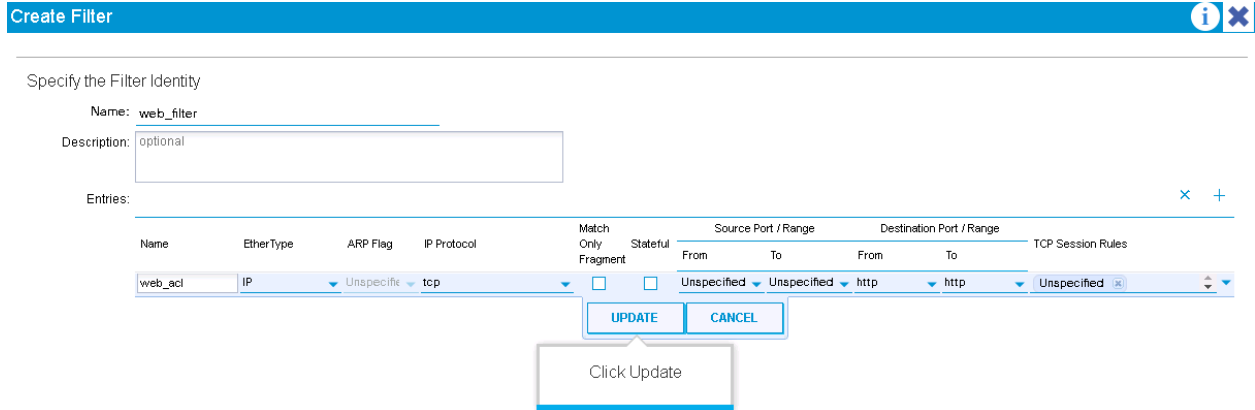


Figure 44 Click Update

About Filters

You've added your first Access Control List (ACL) entry to the web filter which will allow TCP/IP traffic from any source to any destination port 80 (http). These ACL entries are similar to what you would traditionally find any firewall.

As you can see, ACI can replace some functionality normally provided by a separate firewall device.

The top level filter can be re-used across different Contracts, but the individual ACL entries are restricted to their respective filters.

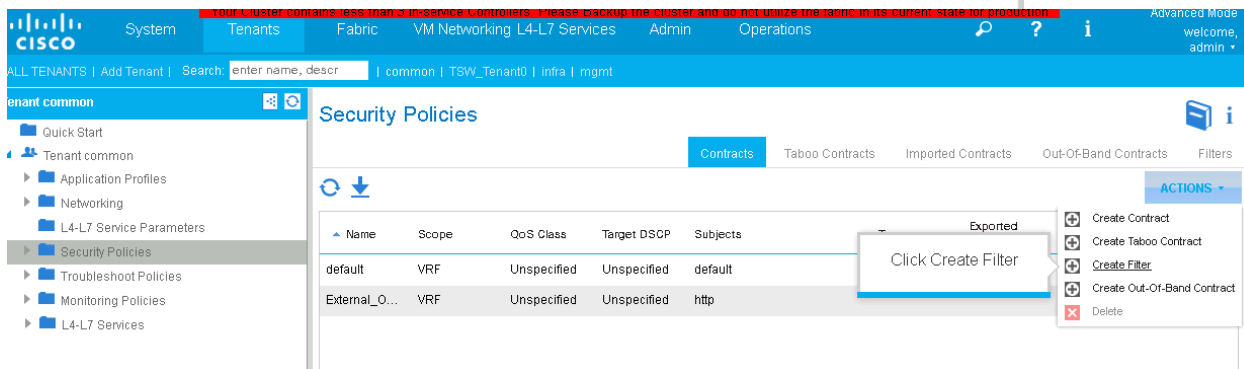


Figure 45 Create Filter

Create Filter

Specify the Filter Identity

Name:

Description:

Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source From	Source To	Destination From	Destination To	TCP Session Rules
app_acl	IP	Unspecifi	tcp	<input type="checkbox"/>	<input type="checkbox"/>	Unspecified	Unspecified	Unspecified	Unspecified	Unspecified

Erase text and replace with '1433'

Figure 46 Filter port 1433

Create Filter

Specify the Filter Identity

Name:

Description:

Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source Port / Range		Destination Port / Range		TCP Session Rules
						From	To	From	To	
app_acl	IP	Unspecifi	tcp	<input type="checkbox"/>	<input type="checkbox"/>	Unspecified	Unspecified	1433	1433	Unspecified

Click Update

Figure 47 Filter port 1433

Filter Chain

Filters

Name	Directives
common/web_filter	none

Click Update

Figure 48 Filter Chain Update – then OK

On the TOE, an authorized administrator can define the traffic rules on the box by configuring policies, contracts, filters, and endpoint groups.

The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, permit, deny, redirect, deny-and-log.

The Cisco APIC policy model is built on a series of one or more tenants that allow segregation of the network infrastructure administration and data flows. These tenants can be used for customers, business units, or groups, depending on organizational needs as described in section 3.2.3 .

Endpoint Groups (EPG)

Endpoint Groups (EPG) provide a logical grouping for objects that require similar policy. For example, an EPG could be the group of components that make up an application's web tier. Endpoints themselves are defined using NIC, vNIC, IP address, or DNS name with extensibility for future methods of identifying application components.

EPGs are also used to represent other entities such as outside networks, network services, security devices, network storage, and so on. They are collections of one or more endpoints providing a similar function. They are a logical grouping with varying use options depending on the application deployment model in use.

EPGs are designed for flexibility, allowing their use to be customized to one or more deployment models a given customer might choose. The EPGs are then used to define where policy is applied. Within the Cisco ACI fabric, policy is applied between EPGs, therefore defining how EPGs communicate with one another.

Some example uses of EPGs are as follows:

- **EPG defined by a VxLAN:** All endpoints connecting to a given VxLAN are placed in an EPG
- **EPG defined by IPs or subnet:** For example, 172.168.10.10 or 172.168.10*
- **EPG defined by DNS names or DNS ranges:** For example, example.web.networks.com or *.web.networks.com

Endpoint groups (EPG) provide a series of objects that define the application itself. An EPG is a collection of similar endpoints representing an application tier or set of services. EPGs are connected to each other via one or more policies. It is important to note that policies in this case are more than just a set of ACLs and include a collection of inbound/outbound filters, traffic quality settings, marking rules/redirection rules, and Layers 4–7 service device graphs.

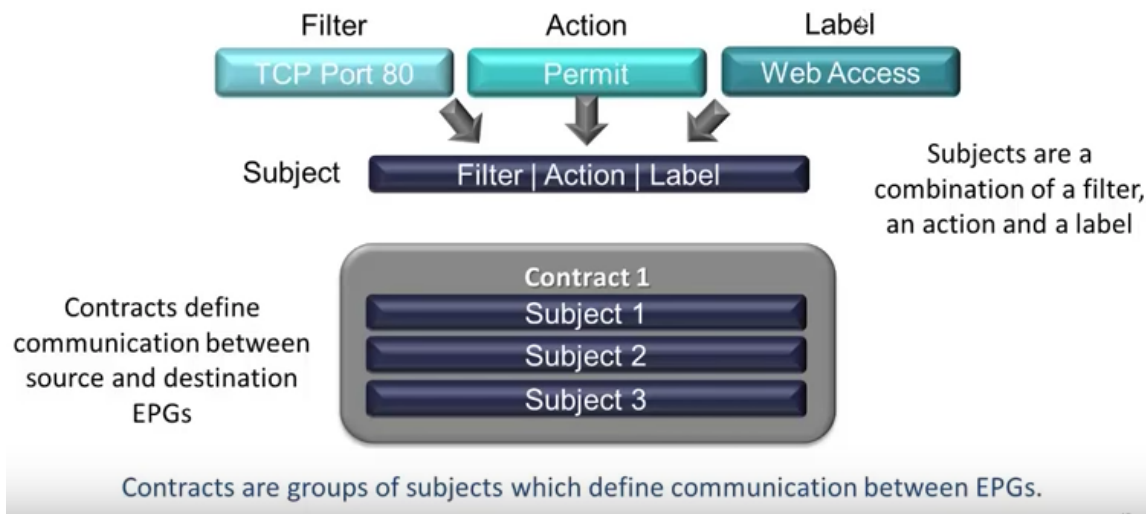
Application Network Profiles

An application network profile (ANP) within the fabric is a collection of the EPGs, their connections, and the policies that define those connections. ANPs become the logical representation of the entire application and its interdependencies on the Cisco ACI fabric.

Contracts

Contracts define inbound and outbound permits, denies, QoS, redirects, and service graphs. They allow for both simple and complex definition of how a given EPG communicates with other EPGs dependent on the requirements of a given environment.

Building Contracts



In more complex application deployment environments, contracts are further broken down using *subjects*, which can be thought of as applications or subapplications. To better understand this concept, think of a web server. Although it might be classified as web, it might be producing HTTP, HTTPS, FTP, and so on, and each of these subapplications might require different policies. Within the Cisco APIC model, these separate functions or services are defined using subjects, and subjects are combined within contracts to represent the set of rules that define how an EPG communicates with other EPGs.

In the unlikely event an unauthorized switch was manually cabled to the ACI fabric, there will be a fault raised in the APIC indicating a rogue device was denied to the fabric.

4.5.1.2 Create Contract

Create Contract [i] [X]

Specify Identity Of Contract

Name: | [red error icon]

Scope: VRF [dropdown arrow]

QoS Class: Un [dropdown arrow]

Target DSCP: Un [dropdown arrow]

Description: optional [text input]

Tags: [dropdown arrow]
enter tags separated by comma

Subjects: [x] [+]

Name	Description
------	-------------

Figure 49 Create Contract

Create Contract [i] [X]

Specify Identity Of Contract

Name: Web_Con

Scope: VRF [dropdown arrow]

QoS Class: Unspecified [dropdown arrow]

Target DSCP: Unspecified [dropdown arrow]

Description: optional [text input]

Tags: [dropdown arrow]
enter tags separated by comma

Subjects: [x] [+]

Name	Description
------	-------------

[SUBMIT] [CANCEL]

Click +

Figure 50 Identity of Contract

Create Contract Subject i

Specify Identity Of Subject

Name: _____ !
Description: optional
Target DSCP: Unspecified Enter: web_subj
Apply Both Directions:
Reverse Filter Ports:

Filter Chain

Filters	
Name	Directives

L4-L7 SERVICE GRAPH
Service Graph: select an option

PRIORITY
QoS: _____

OK CANCEL

Figure 51 Create Contract Subject

Create Contract Subject i

Specify Identity Of Subject

Name: web_subj
Description: optional
Target DSCP: Unspecified
Apply Both Directions:
Reverse Filter Ports:

Filter Chain

Filters	
Name	Directives

L4-L7 SERVICE GRAPH
Service Graph: select an option

PRIORITY
QoS: _____

Click +

OK CANCEL

Figure 52 Create Contract Subject - Filter Chain

Create Contract Subject

Specify Identity Of Subject

Name:

Description:

Target DSCP:

Apply Both Directions:

Reverse Filter Ports:

Filter Chain

Filters

Name	Directives
select an option	

UPDATE CANCEL

Select web_filter

Next

L4-L7 SERVICE GRAPH

Service Graph:

PRIORITY

QoS:

Figure 53 Filter Chain

Filter Chain

Filters

Name	Directives
common/web_filter	none

UPDATE CANCEL

Click Update

Figure 54 Filter Chain Update – then OK

VLANs and Cisco ACI

Cisco ACI is designed so that the user can focus on the logical or abstracted design in terms of distributed bridge domains, distributed VRFs, and so on, and not worry about maintaining VLAN mapping information.

Networking equipment managed by Cisco ACI uses VxLAN tunnels internally to the fabric, and can use VLANs or VxLANs to communicate with external devices. The VLANs used to communicate with servers or switches have local significance on the leaf. VLANs are simply a tag on the wire to segment traffic.

4.5.1.3 IP Spoofing Prevention

An external EPG must be created for external traffic. In addition, a firewall that is properly configured must be installed as shown below which, prevents malicious and unauthorized traffic from entering the TOE. Endpoint group classification occurs when a packet arrives on the leaf. For traffic arriving from an L3Out connection, traffic is classified based on network and mask. The policy rules (scope, source class ID, dest class ID, and filter) are programmed on the leaf switches in ternary content addressable memory (TCAM).

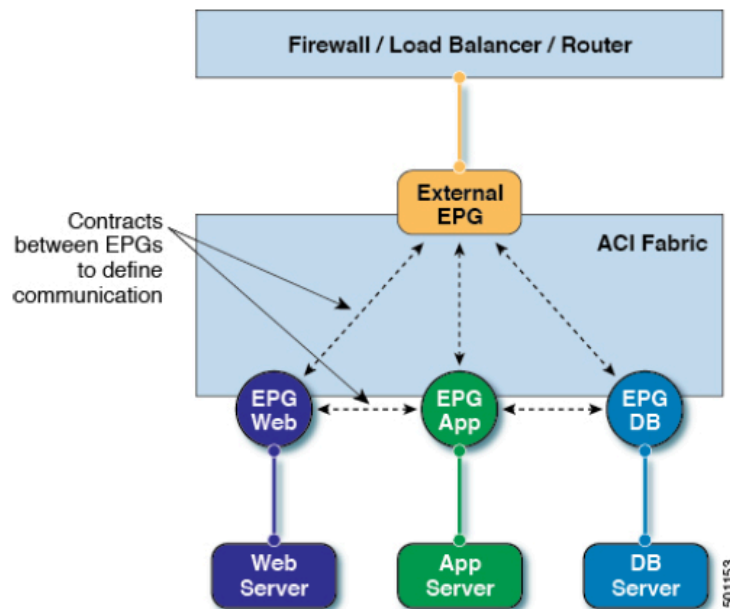


Figure 55 External EPG

4.5.1.4 Creating External EPG (Layer3)

Following is an example of creating an External EPG. For more information please refer to section “Layer 3 Outside Connection with OSPF Example” in [21] Connecting Application Centric Infrastructure (ACI) to Outside Layer 2 and 3 Networks.

1. Create a layer 3 outside connection, called "L3OUT-1", under menu Tenant>Networking>External Routed Networks. Select OSPF as the protocol, choose area ID of 100, and associate the layer 3 outside connection with the private network, ex CTX-1. See [21] *Connecting Application Centric Infrastructure (ACI) to Outside Layer 2 and 3 Networks* for more information.

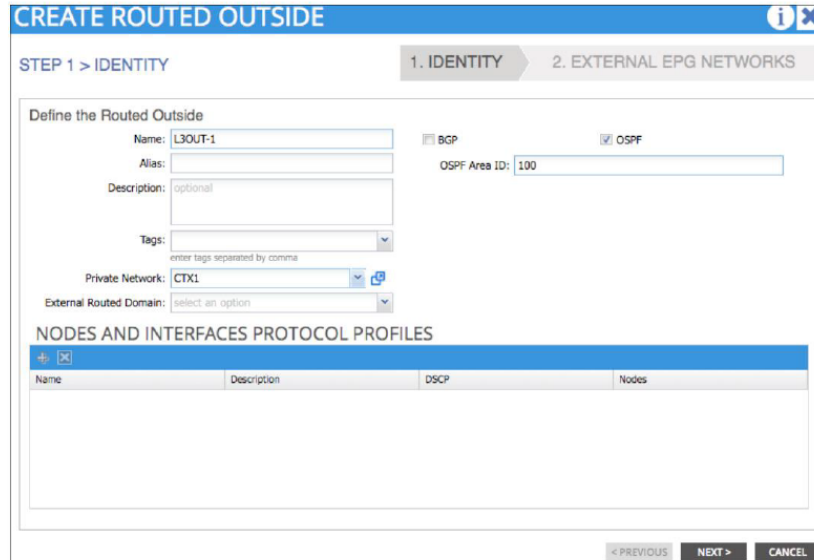


Figure 56 Start to Create L3 Outside Connection

2. Add the layer 3 border leaf node. Click the "+" sign under the "Nodes and Interface Profile Profiles" and follow the wizard to start to add border leaf node for the layer 3 outside connection.

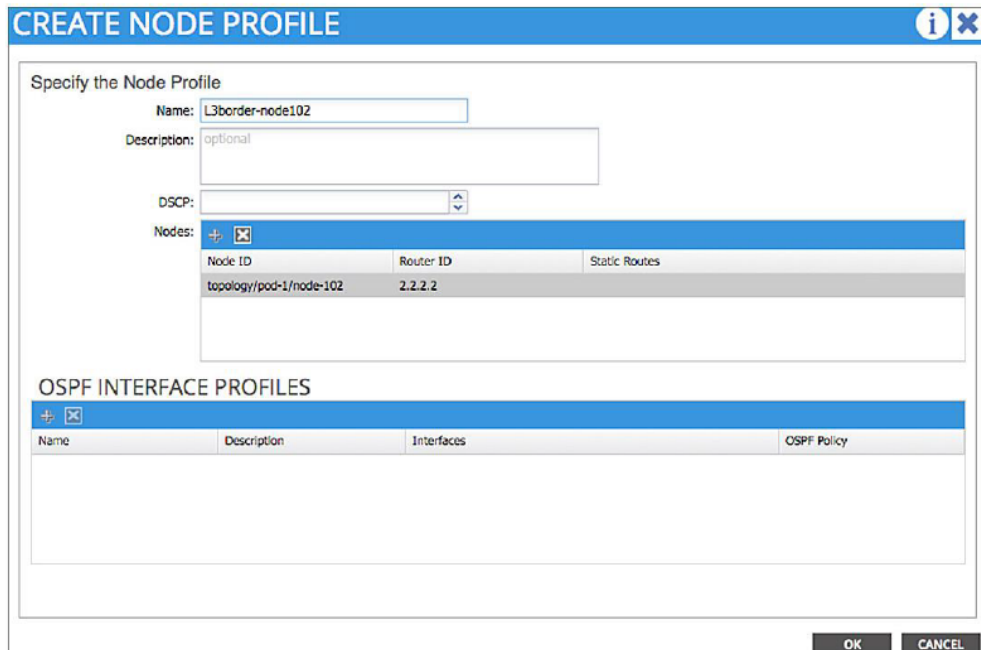


Figure 57 Adding a Layer 3 Border Leaf

3. Add layer 3 interfaces for this border leaf. Click the “+” sign under “OSPF Interface Profiles”. Figure 58 provides an example of how to add two layer 3 sub-interfaces (sub-interface for eth1/39 and eth1/40 with dot1q tag 1000) on border leaf node 102 to connect to the two Nexus 3000s. Specify the MTU to be 1500. Leave the OSPF policy empty for the time being.

CREATE INTERFACE PROFILE

Specify the Interface Profile

Name: L3Int-node102

Description: optional

OSPF PROFILE

Authentication Type: No authentication

Authentication Key:

Confirm Key:

OSPF Policy: select or type to pre-provision

INTERFACES

ROUTED INTERFACES | SVI | **ROUTED SUB-INTERFACE**

Path	Encap	IP Address	MAC Address	MTU (bytes)	Target DSCP
Node-102/eth1/39	vlan-1000	100.1.1.1/30	00:22:BD:F8:19:FF	1500	Unspecified
Node-102/eth1/40	vlan-1000	100.1.1.5/30	00:22:BD:F8:19:FF	1500	Unspecified

OK CANCEL

Figure 58 Adding Two Layer 3 Sub-Interfaces

4. Repeat steps 2 and 3 to add node 103 as a border leaf node for “L3OUT-1”. Add two sub-interfaces (eth1/39 and eth1/40 with dot1q tag 1000) for the border leaf node.

5. Click ‘Next’ to start to configure the external EPG. The ACI fabric maps external layer 3 endpoints to the external EPG by using the IP prefix and mask. One or more external EPGs can be supported for each layer 3 outside connection, depending on whether the user wants to apply a different policy for different groups of external endpoints. In this example we treat all outside endpoints equally and create only one external EPG. The ACI policy model requires an external EPG and the contract between the external EPGs and inside EPGs. Without this, all connectivity

to outside will be blocked, even if external routes are learned properly. This is part of the security model of ACI.

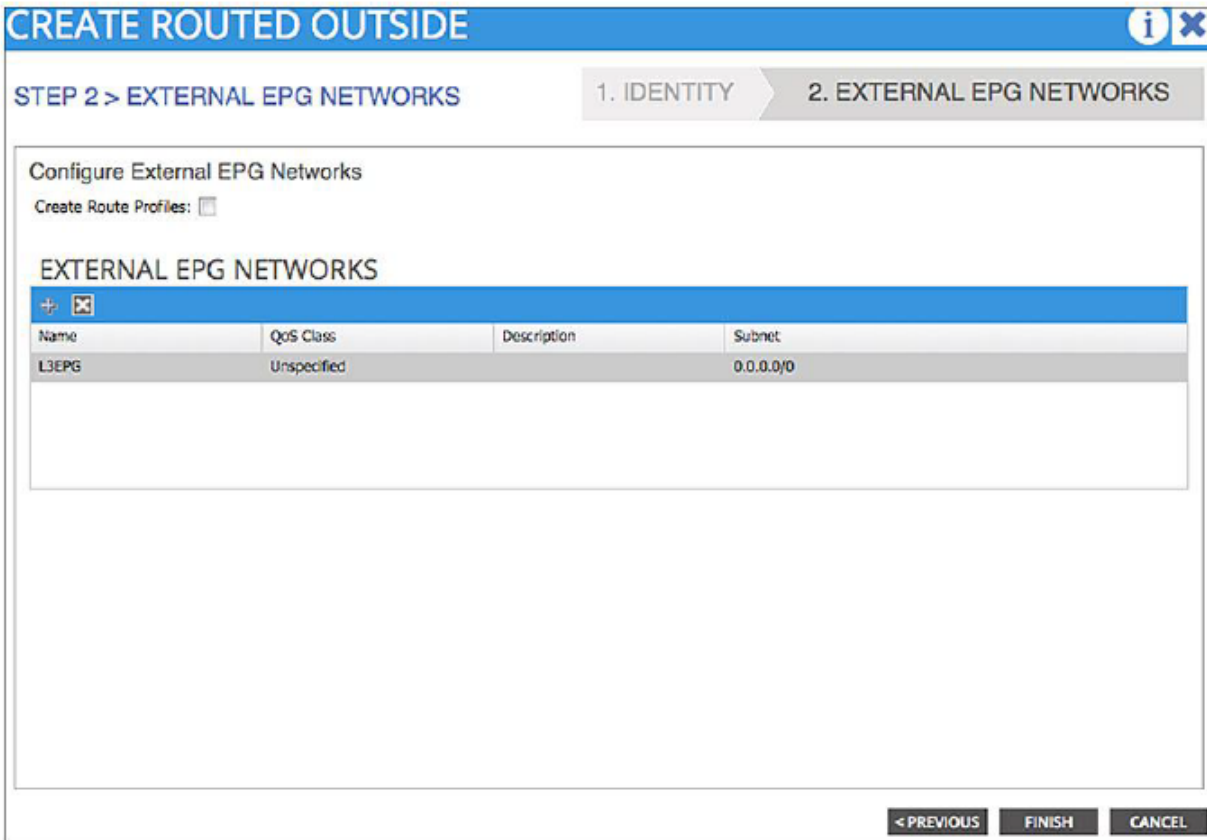


Figure 59 Configuring the External EPG

6. Configure a contract between the external and internal EPG. In this example, we specify “WEB_contract” as consumed contract for external EPG “L3EPG” (steps to configure this contract is skipped here). Click “Finish” in the previous step and go to menu Tenant>Tenant Pepsi>Networking>External Routed Networks>L3OUT-1>Networks>L3EPG. Click “+” under the section of “Consumed Contracts” to add “WEB_contract” as the consumed contract.

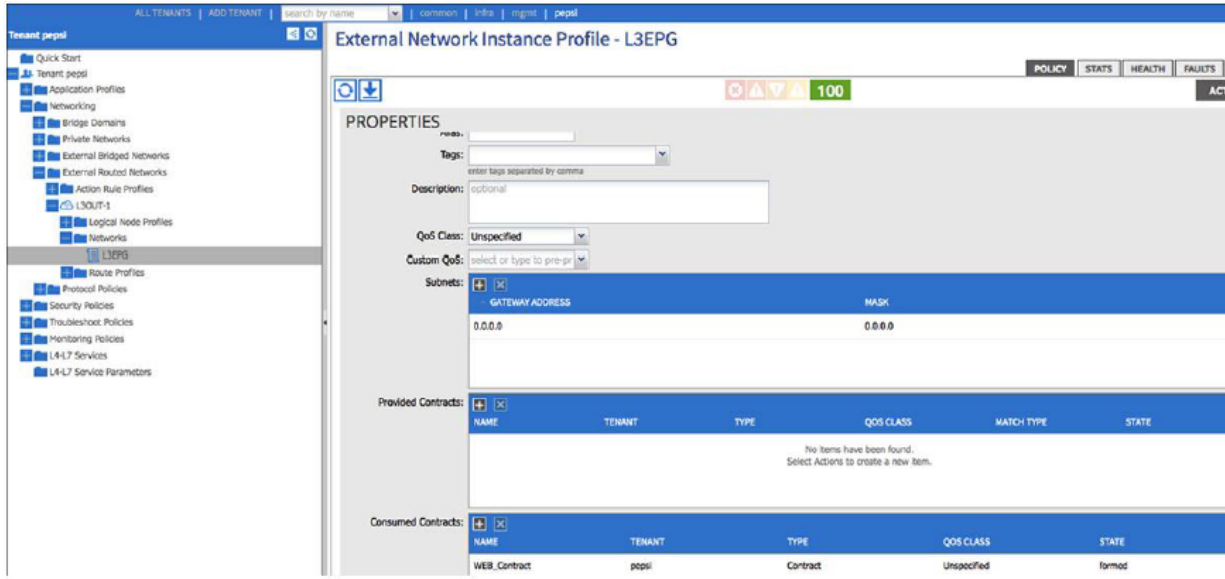


Figure 60 Configuring a Contract for External EPG

Next go to menu Application Profiles>Application1>Application EPGs>WEB EPG and add the same contract, “WEB_contract”, as the provided contract for WEB EPG. Once the consumer-provider relationship is established, check the application profile; it should look like Figure 29 on the APIC GUI. It states that communication between WEB EPG and L3EPG is regulated by policy “WEB_contract”. Note that without a contract all communications between EPGs are blocked, including the communication with external EPGs.

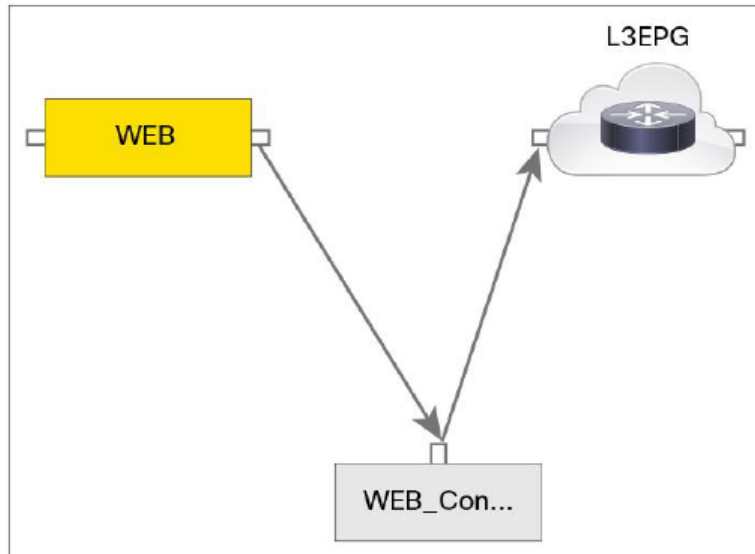


Figure 61 Contract Relationship with L3 External EPG

Create OSPF interface policy by going to menu Tenant>Networking>Protocol Policies>OSPF Interface

CREATE OSPF INTERFACE POLICY

Define OSPF Interface Policy

Name: OSPF_int_policy

Description: optional

Network Type: Broadcast
 Unspecified
 Point-to-point

Priority: 1

Cost of Interface: 10

Interface Controls: MTU ignore
 Passive Participation
 Advertise Subnet

Hello Interval (sec): 10

Dead Interval (sec): 40

Retransmit Interval (sec): 5

Transmit Delay (sec): 1

SUBMIT CANCEL

Figure 62 Creating te OSPF Interface Policy

8. Associate the OSPF interface policy with the sub-interfaces on the two border leaf switches by going to menu External Routed Networks>Logical Node Profiles>Logical Interface Profiles. You will need to repeat this step for both border leaf switches.

Interface Profile - OSPF Interface Profile

PROPERTIES

Name:

Description: optional

Authentication Key:

Authentication Key ID: 1

Authentication Type: Simple authentication
 MD5 authentication
 No authentication

Associated OSPF Interface Policy Name: OSPF_int_policy

Figure 63 Associating the OSPF Interface Policy with Sub-Interfaces

9. Configure the policy for OSPF protocol parameters and associate it with private networks This is equivalent to configuring OSPF parameters under the VRF of “router ospf”. Create the OSPF policy by going to menu Tenant>Networking>Protocol Policies>OSPF Timers.

Figure 64 OSPF Protocol Parameters Policy Configuration

Associate the policy with private network CTX1 for this tenant by going to menu Tenant>Networking>Private Networks

Figure 65 Associating Configured OSPF Protocol Policy with Private Network

10. Associate the layer 3 outside connection with bridge domain “ex. BD1” for this tenant. Repeat this step if there are multiple bridge domains for the tenant.

PROPERTIES

Name: **BD1**

Description: optional

Unknown Unicast Traffic Class ID: **16386**

Segment: **15957970**

Multicast Address: **225.0.128.16**

Network: CTX1

Custom MAC Address: 00:22:BD:F8:19:FF

L2 Unknown Unicast: Flood
 Hardware Proxy

Unknown Multicast Flooding: Flood
 Optimized Flood

ARP Flooding:

Unicast Routing:

IGMP Snoop Policy: select or type to pre-pr

End Point Retention Policy: select or type to pre-pr

L3 Out: pepsi/L3OUT-1

Route Profile: select value

Monitoring Policy: select or type to pre-pr

Figure 66 Associating Layer 3 Outside Connection with Bridge Domain

Under bridge domain “BD1” there are three subnets; two of them should be configured as public subnets. With this association, these two public subnets will be advertised to external routers by OSPF.

Subnets

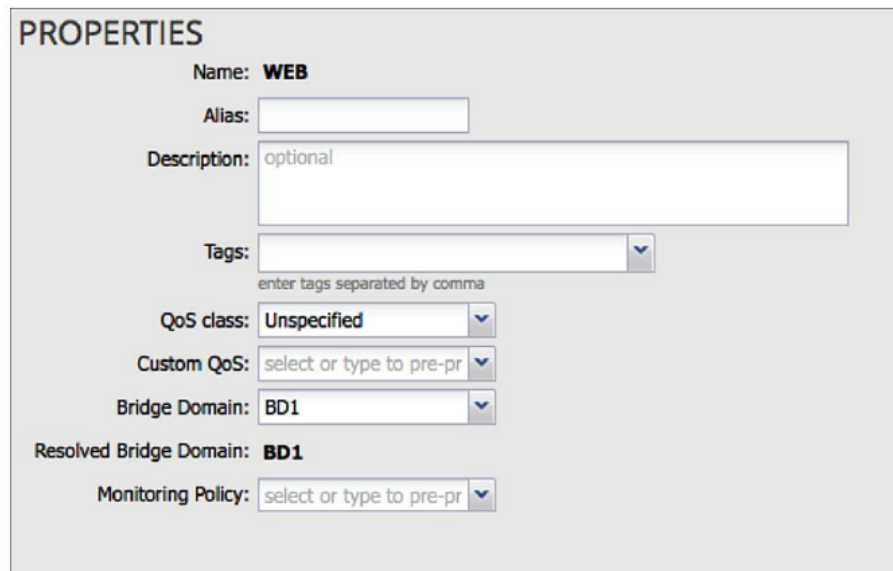
GATEWAY ADDRESS	SCOPES	SUBNET CONTROL
192.168.1.1/24	Private Subnet	
192.168.2.1/24	Public Subnet	
192.168.3.1/24	Public Subnet	

Figure 67 Subnet Scope of Bridge Domain

With above steps the Layer 3 outside connection configuration APIC GUI is complete.

4.5.1.5 Creating External EPG (Layer2)

1. Start to create a layer 2 outside connection by going to menu Tenant>Networking>External Bridged Network. Click Action to start the process of adding a layer 2 outside connection. Associate the layer 2 outside connection with bridge domain “BD1”. Also choose a VLAN ID. This VLAN needs to be configured on the external layer 2 network. This layer 2 outside connection will put this VLAN and the “BD1” of the ACI fabric under the same layer 2 domain. Also, this VLAN ID has to be in the range of the VLAN pool used for the layer 2 outside connection. The VLAN pool will be configured in step 2. See section “ Extend the Bridge Domain Out of the ACI Fabric” of [21].



PROPERTIES

Name: **WEB**

Alias:

Description: optional

Tags:
enter tags separated by comma

QoS class:

Custom QoS:

Bridge Domain:

Resolved Bridge Domain: **BD1**

Monitoring Policy:

Figure 68 EPG and Bridge Domain Relationship

CREATE BRIDGED OUTSIDE

STEP 1 > IDENTITY 1. IDENTITY 2. EXTERNAL EPG NETWORKS

Configure the Bridged Outside

Name: L2OUT-1 Bridge Domain: BD1

Alias: Encap: vlan-1000
eg, vlan-1

Description: optional

Tags: enter tags separated by comma

External Bridged Domain: select an option

NODES AND INTERFACES PROTOCOL PROFILES

Name	Description

< PREVIOUS NEXT > CANCEL

Figure 69 Start to Create a Layer 2 Outside Connection

2. Click the drop-down menu of the “External Bridged Domain” to create a layer 2 domain named “L2outdomain”. Click the drop-down menu of the VLAN Pool to create a new VLAN Pool named “L2out-VLAN-pool” with a VLAN range from 1000 to 1200. This is essentially a mechanism to specify the range of the VLAN ID that will be used for creating a layer 2 outside connection. This helps avoid overlapping the VLAN range between VLANs used for an EPG and those for a layer 2 outside connection.

CREATE LAYER 2 DOMAIN

Specify the Layer 2 Domain

Name: L2out-domain

VLAN Pool: L2out-VLAN-pool

SUBMIT CANCEL

Figure 70 Create Layer 2 Domain and VLAN Pool

3. Add a layer 2 border leaf node and layer 2 interface for a layer 2 outside connection

CREATE NODE PROFILE

Specify the Node Profile

Name: L2border

Description: optional

INTERFACE PROFILES

Name	Description	Interfaces
L2int		topology/pod-1/paths-102/pathep-[eth1/39]

OK CANCEL

Figure 71 Add Border Leaf Node to Layer 2 Outside

4. After adding a layer 2 border leaf and layer 2 interface, click “Next” to start creating a layer 2 EPG. Simply provide a name for the layer 2 EPG. All the traffic entering the ACI fabric with VLAN 1000 (the VLAN ID provided in step 1) will be classified into this layer 2 EPG.

CREATE EXTERNAL NETWORK

Define an External Network

Name: L2EPG

Alias:

Description: optional

Tags: enter tags separated by comma

QoS Class: Unspecified

OK CANCEL

Figure 72 Create External EPG for Layer 2 Outside Connection

5. Configure the contract between WEB EPG and the layer 2 external EPG. Go to menu External Bridged Networks>Networks to specify “WEB_contract” as the consumed contract. After specifying the “WEB_contract” as the provided contract for WEB EPG, the communication between this external layer 2 EPG and WEB EPG will be allowed.

PROPERTIES

Name: **L2EPG**

Alias:

Description: optional

Tags:

QoS Class: **Unspecified**

Configuration Status: **applied**

Provided Contracts:

NAME	TENANT	TYPE	QoS CLASS	MATCH TYPE	STATE
No items have been found. Select Actions to create a new item.					

Consumed Contracts:

NAME	TENANT	TYPE	QoS CLASS	STATE
WEB_Contract	pepsi	Contract	Unspecified	formed

Figure 73 Specify Contract for External EPG

6. The last step of this configuration is to create the Access Attachable Entity Profile. On a high level, this is a mechanism to instruct the APIC to allow certain VLANs on selected ports. Follow these steps to create the attachable entity profile on the APIC GUI.

6.1 Create an attached entity profile by going to menu Fabric>Access Policies>Attachable Access Entity Profile. Click Actions on the right corner to add new attachable entity profile. Click the “+” sign to associate the profile with the layer 2 external domain, called “L2out-domain” (created in step 2 above).

CREATE ATTACHABLE ACCESS ENTITY PROFILE

STEP 1 > PROFILE

1. PROFILE
2. ASSOCIATION TO INTERFACES

Specify the name, domains and infrastructure encaps

Name:

Description:

Create VxLAN Encapsulation:

Domains (VMM, Physical or External) To Be Associated To Interfaces:

Domain Profile	Encapsulation
L2 External Domain - L2out-domain	from:vlan-1000 to:vlan-1200

Figure 74 Creating an Attachable Access Entity Profile

6.2 Create an Interface Policy Group by going to menu Fabric>Access Policies>Interface Policies>Policy Groups. Associate the policy group with an attachable entity profile, called “AEP_L2out”.

CREATE ACCESS PORT POLICY GROUP

Specify the Policy Group identity

Name:

Description:

Link Level Policy:

CDP Policy:

LLDP Policy:

STP Interface Policy:

Monitoring Policy:

Attached Entity Profile:

Connectivity Filters:

Switch IDs	Interfaces
------------	------------

SUBMIT
CANCEL

Figure 75 Creating an Access Port Policy Group

6.3 Create an interface profile named “L2border_portprofile”

The screenshot shows a window titled "CREATE INTERFACE PROFILE" with a blue header bar containing an information icon and a close button. The main content area is titled "Specify the profile Identity" and contains the following fields:

- Name:** L2border_portprofile
- Description:** optional
- Interface Selectors:** A section with a blue header bar containing a "+" sign and a close button. Below it is a table with two columns: "Name" and "Type". The table is currently empty.

At the bottom right of the window, there are two buttons: "SUBMIT" and "CANCEL".

Figure 76 Creating an Interface Profile

Click the “+” sign next to Interface Selectors to add interfaces to this interface profile (Figure 65). Add interface eth1/39 and eth1/40 to the profile and select the policy group created in step 6.2 - “L2border_int” - for this profile.

CREATE ACCESS PORT SELECTOR

Specify the selector identity

Name:

Description:

Interface IDs:
valid values: All or Ranges. For Example:
1/13,1/15 or 2/22-2/24, 2/16-3/16

Interface Policy Group:

Figure 77 Add Interfaces to Port Selector

6.4 Create a switch profile by going to menu Fabric◇Access Policies◇Switch Policies◇Profiles. Under “switch selectors” add leaf nodes 102 and 103.

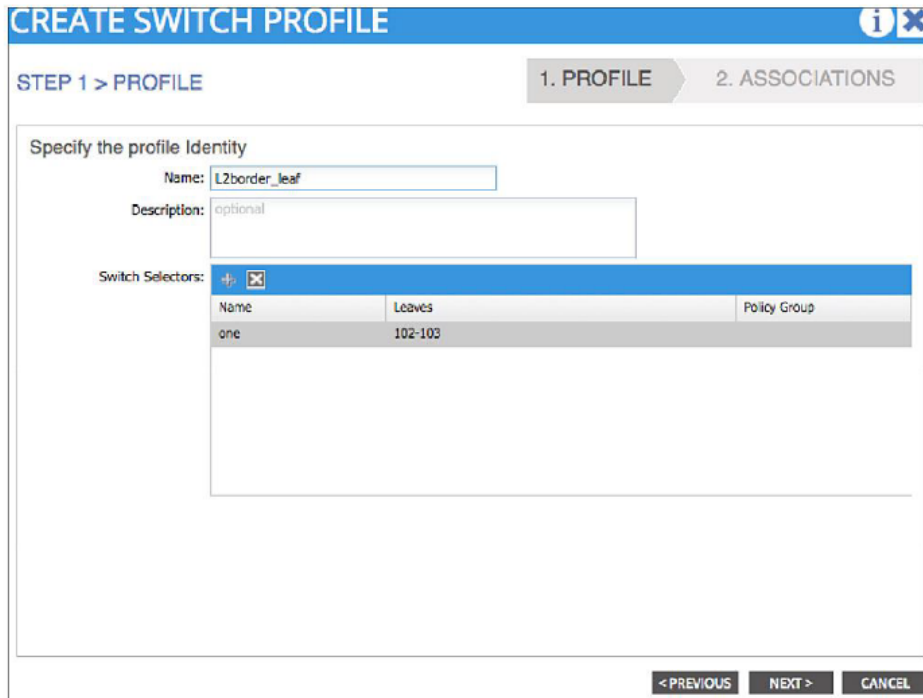


Figure 78 Creating a Switch Profile

6.5 Click Next to associate the interface profile with this switch profile (Figure 67). Select “L2border_portprofile” (created in step 6.3).

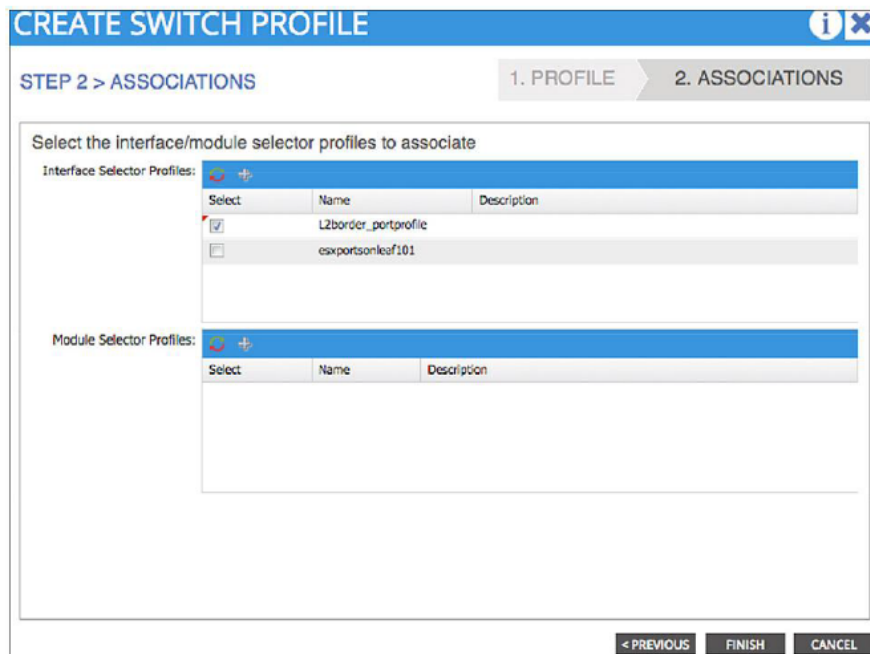


Figure 79 Associating the Interface Profile with the Switch Profile

6.6 Click “Finish” to complete the process.

4.5.1.6 User interfacing Endpoints

Any endpoint devices on the ACI fabric that have external end user interaction should be assigned to separate intra EPGs. By default, all endpoints in the same endpoint group can talk to each other without requiring a contract. Intra-endpoint group (intra-EPG) isolation prevents all endpoints in the endpoint group from talking to each other. This is a private VLAN-equivalent feature in a traditional network. Intra-EPG endpoint isolation policies provide full isolation for virtual or physical endpoints; no communication is allowed between endpoints in an EPG that is operating with isolation enforced. Isolation enforced EPGs reduce the number of EPG encapsulations required when many clients access a common service but are not allowed to communicate with each other.

This will help prevent a malicious user from being able to communicate with another device in the same EPG. See section “Intra-EPG Endpoint Isolation” in the Cisco APIC Basic Configuration Guide, Release 2.x in order to configure the Intra-EPGs.

Configuring Intra-EPG Isolation Using the GUI

The port the EPG uses must be associated with a server interface in the physical domain that is used to connect the bare metal servers directly to leaf switches.

Procedure

Step 1 In a tenant, right click on an Application Profile, and open the Create Application EPG dialog box to perform the following actions:

- a) In the Name field, add the EPG name (intra_EPG-deny).
- b) For Intra EPG Isolation, click Enforced.
- c) In the Bridge Domain field, choose the bridge domain from the drop-down list (bd1).
- d) Check the Statically Link with Leaves/Paths check box.
- e) Click Next.

Step 2 In the Leaves/Paths dialog box, perform the following actions:

- a) In the Path section, choose a path from the drop-down list (Node-107/eth1/16) in Trunk Mode.

Specify the Port Encap (vlan-102) for the secondary VLAN.

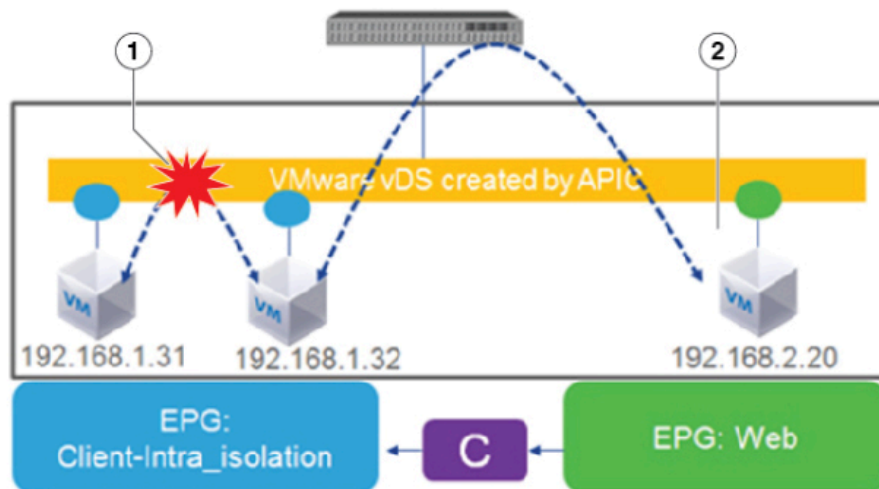
If the bare metal server is directly connected to a leaf switch, only the Port Encap secondary

VLAN is specified.

Note

Specify the Primary Encap (vlan-103) for the primary VLAN.

- b) Click Update.
- c) Click Finish.



Configure the VRF instance for ingress policy (which is the default and recommended approach). Also configure the option to disable endpoint learning on the border leaf switches. You can disable remote IP address endpoint learning on the border leaf from **Fabric>Access Policies>Global Policies>Fabric Wide Setting Policy** by selecting **Disable Remote EP Learn**.

The VRF instance for egress policy by selecting the Policy Control Enforcement Direction option Egress under **Tenants>Networking>VRFs**.

4.5.1.7 Prevent ICMP Redirect Attack

An Authorized administrator can explicitly only allow a certain categories of the ICMP packets to pass through the TOE by configuring the following steps, thus blocking the ICMP redirect packets and preventing the ICMP redirect attack.

An Authorized Administrator will need to do the following for the ipv4.

Create a filter for each type of traffic you want to permit. In this case create a filter for each type of traffic.

- 1 Filter for "Destination Unreachable"
- Another Filter for "Echo"
- Another Filter for "Echo Reply"
- Another Filter for "Source Quench"
- Another Filter for "Time Exceeded"

You will need to do the same for ipv6

Create a filter for each type of traffic you want to permit. In this case create a filter for each type of traffic you want to permit but leave redirect out of it.

- 1 Filter for "Destination Unreachable"
- Another Filter for "Echo Request"
- Another Filter for "Echo Reply"
- Another Filter for "Neighbor Advertisement"

Another Filter for “Neighbor Solicitation”
Another Filter for “Neighbor Advertisement”
Another Filter for “Time Exceeded”

5 Auditing

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

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above. The details for configuration of these settings are covered in Section 3.3.3 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 stored within the TOE.

This is done with the clear logging command.

```
TOE-common-criteria# clear logging
```

```
Clear logging buffer [confirm] <ENTER>
```

```
TOE-common-criteria# clear logging nvram
```

5.2 Audit Records Description

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

Additionally, the startup and shutdown of the audit functionality is audited.

The local audit trail consists of the individual audit records; one audit record for each event that occurred. The audit 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: 2014 May 14 13:12:40 india-29 %SECURITYD-2-
```

```
FIPS_POWERUP_SELF_TEST_STATUS: FIPS RSA power-up self-test status : PASSED
```

```
Date: 2014 May 14
```

```
Time: 13:12:40
```

```
Type of event: %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS
```

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

Wed May 14 13:23:11 2014:type=update:id=console0:user=admin:cmd=clear accounting log (SUCCESS)

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.

6 Modes of Operation

A 9k Family Switch has several modes of operation, these modes are as follows:

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

BIOS Loader Prompt – When the APIC and 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 ACI or APIC 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 APIC and ACI mode 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.

Fabric Discovery – During initial setup there is a Fabric discovery of all ACI switches.

```
User Access Verification
(none) login: admin
*****
Fabric discovery in progress, show commands are not fully functional
Logout and Login after discovery to continue to use show commands.
*****
(none) #
```

The ACI fabric uses an infrastructure space, which is securely isolated in the fabric and is where all the topology discovery, fabric management, and infrastructure addressing is performed. ACI fabric management communication within the fabric takes place in the infrastructure space through internal private IP addresses.

This addressing scheme allows the APIC to communicate with fabric nodes and other Cisco APIC controllers in the cluster. The APIC discovers the IP address and node information of other Cisco APIC controllers in the cluster using the Link Layer Discovery Protocol (LLDP)-based discovery process.

The following describes the APIC cluster discovery process:

- Each APIC in the Cisco ACI uses an internal private IP address to communicate with the ACI nodes and other APICs in the cluster. The APIC discovers the IP address of other APIC controllers in the cluster through the LLDP-based discovery process.
- APICs maintain an appliance vector (AV), which provides a mapping from an APIC ID to an APIC IP address and a universally unique identifier (UUID) of the APIC. Initially, each APIC starts with an AV filled with its local IP address, and all other APIC slots are marked as unknown.
- When a switch reboots, the policy element (PE) on the leaf gets its AV from the APIC. The switch then advertises this AV to all of its neighbors and reports any discrepancies between its local AV and neighbors' AVs to all the APICs in its local AV.
- Using this process, the APIC learns about the other APIC controllers in the ACI through switches. After validating these newly discovered APIC controllers in the cluster, the APIC controllers update their local AV and program the switches with the new AV. Switches then start advertising this new AV. This process continues until all the switches have the identical AV and all APIC controllers know the IP address of all the other APIC controllers.

Setup – The APIC and ACI 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 APIC and ACI mode images 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.

6.1 Module States

The Nexus 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 7 Module States²

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 8 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.

6.2 Self-Tests

When the system is booted up in FIPS mode, the FIPS 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 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

² Section "Verifying the Status of a Module" [7]

failure state.

All ports are blocked from moving to forwarding state during the POST³. Only when all components of all modules pass the POST is the system placed in FIPS PASS state and ports are allowed to forward data traffic.

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

- 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 Section "FIPS Self-tests" in [3]

7 Security Measures for the Operational Environment

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

Table 9 Operational Environment Security Measures

Environment Security Objective	IT Environment Security Objective Definition	Responsibility of the Administrators
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.	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 [AGD, Sect. 7]. Only the specific software images as outlined in section 2 will be installed on the APIC and ACI mode switches.
OE.FIREWALL	The operational environment of the TOE shall provide a firewall located between the ACI fabric and external networks to protect against malicious or unauthorized traffic from entering the ACI fabric.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the Firewall that is configured to prevent malicious and unauthorized traffic from entering the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. The Nexus 9k APIC and routers are intended to be deployed in the same physically protected datacenter. The ACI fabric is intended to support datacenter servers and devices, not have end users directly attach into the fabric.	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 [AGD, Sect. 7]. The APIC and ACI mode switches, FEX, and network connections deployed to create one ACI fabric must be installed in one data center with proper physical controls such as secure raised floor area with badge readers located within a secure facility with badge readers on external doors.
OE.REMOTE_SERVERS	The operational environment of the TOE shall provide NTP server and optionally remote authentication servers and syslog servers, and the administrator will ensure the session between the TOE and remote server(s) is secured.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides secure session between the TOE and remote servers.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	It is the responsibility of the authorized administrator of the TOE to ensure that the Operational

Environment Security Objective	IT Environment Security Objective Definition	Responsibility of the Administrators
		Environment provides the necessary functions, and adheres to the environment security objectives [AGD, Sect. 7] and follow all guidance in this document as well as the official Cisco documentation for the Nexus 9k APIC and ACI mode switches as described in section 1.3 of the document.

8 Related Documentation

Use this document in conjunction with the APIC and ACI mode documentation at the following location:

- <http://www.cisco.com/>

Obtaining Documentation

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

8.1 World Wide Web

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

- <http://www.cisco.com>

8.2 Ordering Documentation

Cisco documentation is available in the following ways:

Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/web/ordering/root/index.html>

Non-registered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

8.3 Documentation Feedback

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

You can 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>