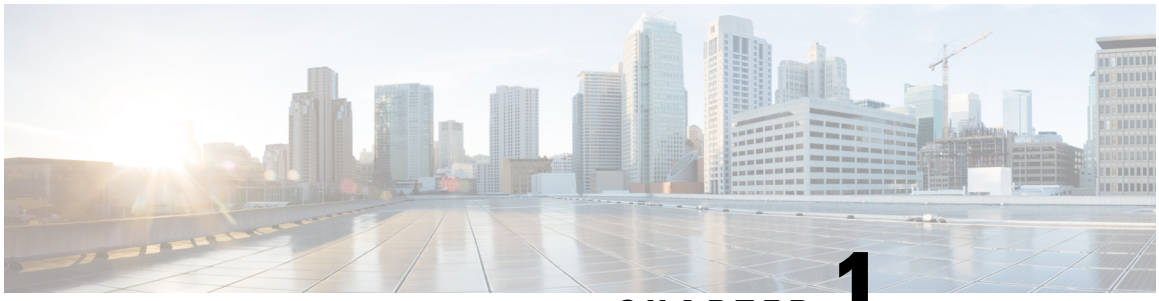
Cisco ASA Quick Start Guide for APIC Integration, 1.2(11)

First Published: 2018-09-10

Last Modified: 2018-09-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Introduction

Overview

The Cisco Application Policy Infrastructure Controller (APIC) is a single point of control for centralized functions on the Cisco Application Centric Infrastructure (ACI). The APIC can automate the insertion of services such as a Cisco Adaptive Security Appliance (ASA) northbound between applications, also called endpoint groups (EPGs). The APIC uses northbound Application Programming Interfaces (APIs) for configuring the network and services. You use these APIs to create, delete, and modify a configuration using managed objects.

To configure and monitor service devices, the APIC requires software running on the device known as a device package. The device package manages a class of service device and provides the APIC with information about the device so that the APIC knows what the device can do. By using a device package, you can insert and configure network service functions on a service device such as an ASA.

This document describes how to integrate an ASA with the ACI and configure the APIC to utilize capabilities of the ASA.

Note If you try to create a configuration that is not supported on your current ASA version, an error similar to the following could appear on the APIC:

```
*Major script error: Configuration error: …. ERROR: % Invalid input detected at '^' marker.
```

See your ASA version documentation for supported features.

Service Function Insertion

When a service function is inserted in the service graph between applications, traffic from these applications is classified by the APIC and identified using a tag in the overlay network. Service functions use the tag to apply policies to the traffic. For the ASA integration with the APIC, the service function forwards traffic using either routed or transparent firewall operation.

Available APIC Products

Starting with release 1.2(7.8), there are two versions of the Cisco ASA Device Package software for ACI:

- Cisco ASA Device Package—Policy Orchestration with Fabric Insertion. This version allows you to configure many important features of the ASA from the APIC, including (but not limited to) the following:
  - Interface
  - Routing
  - Access-list
  - NAT
  - TrustSec
  - Application inspection
  - NetFlow
  - High availability
  - Site-to-site VPN
- Cisco ASA Device Package—Fabric Insertion. This version contains the following subset of features of the original version:
  - Interface
  - Dynamic routing
  - Static routing

Supported Versions

Cisco ASA Device Package software supports only the version of APIC that it is shipped with.

The following table lists the supported versions of the Cisco ASA software for each of the supported platforms.

Platform	Software Version
Cisco ASA 5500-X (5512 through 5555)	ASA 8.4(x) and newer
Cisco ASA 5585-X (SSP 10 through SSP 60)	

Platform	Software Version
Cisco Firepower 9300 Security Appliance	ASA 9.6(1) and newer
Cisco Firepower 41xx Security Appliance	
Cisco Firepower 21xx Security Appliance	ASA 9.8(1) and newer
Cisco ASAv	ASA 9.2(x) and newer (Cisco ASA and APIC Compatibility Matrix)

Supported Features

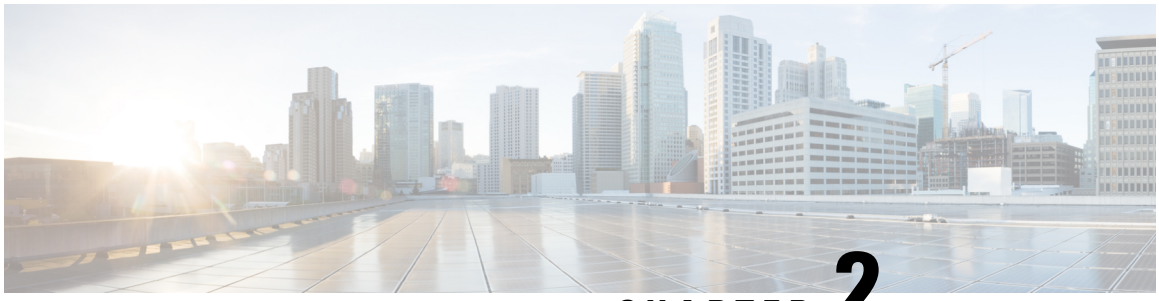
The following table lists the supported features for the ASAv and the ASA 5585-X. For releases that support BGP and OSPF, see the Cisco ASA Device Package Software, Version 1.2(1) Release Notes.

Feature	ASAv Support	ASA 5500-X/5585-X Support
Access lists and access groups	Yes	Yes
Application inspection	Yes	Yes
BGP	Yes	Yes
Clustering	No	Yes
Connection limits	Yes	Yes
DNS clients	Yes	Yes
EtherChannels	No	Yes
High availability (active/active, active/standby)	Active/standby only	Active/standby only
Interface configuration	Yes	Yes
Interface description	Yes	Yes
IP audit	Yes	Yes
IPv6	Yes	Yes
Logging	Yes	Yes
Message of the day	Yes	Yes
Multiple contexts	No	Yes
NAT and Twice NAT	Yes	Yes
Netflow	Yes	Yes

Feature	ASAv Support	ASA 5500-X/5585-X Support
Network and service objects and groups	Yes	Yes
NTP	Yes	Yes
OSPF	Yes	Yes
Protocol timeouts	Yes	Yes
Service policies	Yes	Yes
Shared AnyConnect premium licenses	No	Yes
Site-to-site VPN	Yes	Yes
Smart Call Home enable	Yes	Yes
SNMPv3	Yes	Yes
Static routing	Yes	Yes
TCP Intercept (embryonic connection limits)	Yes	Yes
Threat detection	Yes	Yes
TrustSec	Yes	Yes

Related Documentation

- Cisco ACI Fundamentals
- Cisco ACI Security Solution
- Cisco APIC Layer 4 to Layer 7 Services Deployment Guide
- Cisco APIC Product Support
- Cisco ASA Series Roadmap
- Cisco Firepower Management Center



CHAPTER 2

Deploy and Install

Deploy the ASA

To deploy an ASA 5585-X, see the Cisco ASA 5585-X Quick Start Guide for installation procedures:

http://www.cisco.com/go/asa5585x-quick

To deploy an ASAv, see the Cisco Adaptive Security Virtual Appliance Quick Start Guide for installation procedures:

http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/products-installation-guides-list.html

Note During an ASAv deployment, you must define the value of the nameif property for the management interface as **management**. If you define the interface name as anything other than **management**, the device cluster will be stuck in AuditRequested/AuditPending state, and the fault will indicate that the read operation timed out. The management interface and default gateway configuration are deleted from the ASAv, and the interface is shut down.

Install the ASA Device Package

Each service node type must provide a device package, which includes two parts: a device specification and a device script. Service nodes of the same type are bound to a single device package.

The ASA device package enables you to configure an ASA and register the ASA with the APIC.

Before you begin

Review the prerequisites in the Overview and Prerequisites chapters of the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

Step 1 Download the ASA device package, a .zip file available at http://www.cisco.com/go/asa-software, and save it onto your local drive. Do not unzip the file.

Step 2 Install the ASA device package. See the Importing a Device Package chapter of the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

Step 3 Register the ASA with the APIC. See the Configuring a Device Cluster and Configuring Connectivity to a Device Cluster chapters of the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

Migrate from 1.2(x) to 1.3(x)

To migrate your existing Cisco ASA device package deployment from software version 1.2(x) to 1.3(x), complete the following steps:

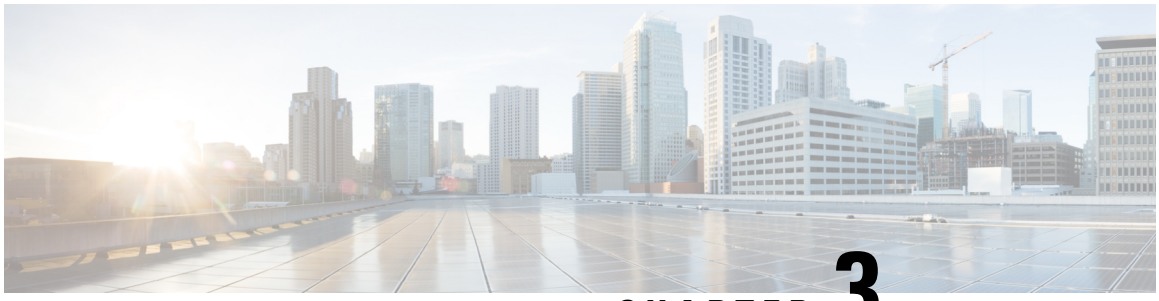
Step 1 Install the ASA device package software version 1.3(x) onto the APIC.

Step 2 From your existing deployment, download the configuration from the tenant.

Step 3 Replace the top-level `<imdata>` tag with `<polUni>` in the configuration.

Step 4 Globally, replace `mDev-CISCO-ASA-1.2` with `mDev-CISCO-ASA-1.3` in the configuration.

Step 5 Upload the modified configuration back onto the APIC.



CHAPTER 3

Configure

Background

The ACI fabric provides for integration of L4-L7 services as an integral part of an application. This is accomplished through the use of an APIC-managed service graph, which requires a L4-L7 device package. The imported device package exposes configuration parameters in APIC, and allows it to orchestrate a given configuration onto the device.

To install the L4-L7 service graph, register a L4-L7 device with the APIC, add its configuration as part of a Function Profile or L4-L7 Service Parameters, and link those two with a service graph. Once you apply this L4-L7 service graph to a contract, the APIC renders it in the fabric by tagging device interfaces and stitching them to appropriate consumer and provider EPGs. The APIC then applies a given configuration to the registered device in an automated fashion. Once all of the configuration is applied to the ACI fabric and the L4-L7 device, the ACI fabric directs traffic defined by the contract to a given device for inspection. The ACI also allows you to chain multiple services together under a single service graph.

Configure Management Access to the ASA

Configure management access to the ASA so that the APIC can manage the ASA.

- To configure management access to an ASAv, see the respective Quick Start Guide:

  http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/products-installation-guides-list.html

- To configure management access to an ASA 5585-X, follow the steps in this section.

Step 1 Remove any existing configuration.

```
ciscoasa(config)# clear configure all
```

Step 2 (Optional) Set the firewall mode to transparent firewall mode.

```
ciscoasa(config)# firewall transparent
```

Step 3 Configure the IP address and subnet mask on the management interface. The ASA needs to be on the same subnet as the APIC.

```
ciscoasa(config)# interface management {0/0 | 0/1}
ciscoasa(config-subif)# ip address ip_address subnet_mask
```

Step 4 Name the interface "management."

```
ciscoasa(config-subif)# nameif management
```

Step 5 Enable the interface.

```
ciscoasa(config-subif)# no shutdown
```

Step 6 Enable the ASA HTTPS server.

```
ciscoasa(config)# http server enable
```

Step 7 Enable an APIC to access the ASA. Repeat this step for each APIC in the APIC cluster.

```
ciscoasa(config)# http apic_address 255.255.255.255 management
```

Step 8 Create the user which the APIC uses to access the ASA. The user is not required to be the management user. Any user is acceptable.

```
ciscoasa(config)# username username password password privilege 15
```

Step 9 Create an AAA authentication that allows APIC to have access to the HTTP console using LOCAL authentication.

```
ciscoasa(config)# aaa authentication http console LOCAL
```

Step 10 Verify that there is crypto key. If it doesn't exist, generate one using:

```
ciscoasa(config)# show crypto key mypubkey rsa
ciscoasa(config)# crypto key generate rsa
```

Step 11 Verify that Encryption-DES and Encryption-3DES-AES are enabled. If they're disabled, generate a new license.

```
ciscoasa(config)# show version
```

Configure Jumbo Frame Support

To use Ethernet packets larger than 1500 bytes, configure jumbo frame support.

Step 1 Enable jumbo frames.

```
ciscoasa(config)# jumbo-frame reservation
```

Step 2 Save the running configuration.

```
ciscoasa(config)# write memory
```

Step 3 Reboot the ASA.

```
ciscoasa(config)# reload
```

Configure Multiple Context Mode

To configure multi-context mode, see the High Availability and Scalability chapter in the Cisco ASA Series General Operations CLI Configuration Guide for instructions.

The instructions describe how to configure interfaces in system mode, assign them to contexts, and configure the interfaces in each context. Those are all steps that will be done by the device package.

The device package is responsible for allocating and configuring interfaces used in each service graph in multi-context mode. However, the system administrator is responsible for provisioning a multi-context ASA before registering it to the APIC.

Step 1 Create the required user contexts. The device package does not create or delete any context.

Step 2 For each context, make the provisioning similar to that for a single-context ASA.

a. Allocate a management interface to it from the admin context. For example:

```
context tenant
allocate-interface Management0/1
config-url disk0:/tenant1.cfg
```

b. In the user context, configure the management interface with **nameif** as **management** and specify a static IP address. For example:

```
interface management 0/1
nameif management
ip address 10.1.1.1 255.255.255.0
security-level 100
```

c. In the user context, enable HTTPS access to the management interface. For example:

```
http server enable
http 0.0.0.0 0.0.0.0 management
```

d. Set user credentials, and create an AAA authentication that allows APIC to have access to the HTTP console using LOCAL authentication.

```
username username password password privilege 15
aaa authentication http console LOCAL
```

e. Set up the management route.

f. Verify that there is crypto key. If it doesn't exist, generate one using:

```
show crypto key mypubkey rsa
crypto key generate rsa
```

Configure an ASA Cluster

ASA clustering lets you group multiple ASAs together as a single, logical device. A cluster provides all the management convenience of a single device, while achieving the increased throughput and redundancy of multiple devices. For more information, see the ASA Cluster chapter of the Cisco ASA Series General Operations CLI Configuration Guide.

By default, the APIC does not touch ASA cluster configuration. You have the option to configure it out-of-band by using the CLI, ASDM, or CSM.

This release of the ASA device package introduces support for configuring ASA clusters using the APIC. The advantages of doing it this way include:

- Configure cluster parameters on the LDev rather than every CDev. So you only have to enter the parameters once rather than repeating them on every unit. This prevents parameter mismatches between cluster units. The ASA device package can control the order in which to set up or remove the ASA cluster configuration from cluster units when you make such changes from the APIC.
- The ASA device package auto generates some parameters, such as unit-label, priority, and the management IP address pool. This minimizes the number of configuration tasks by the user to help avoid user error.

Note We do not recommend using this to work with an existing ASA cluster setup and its configuration.

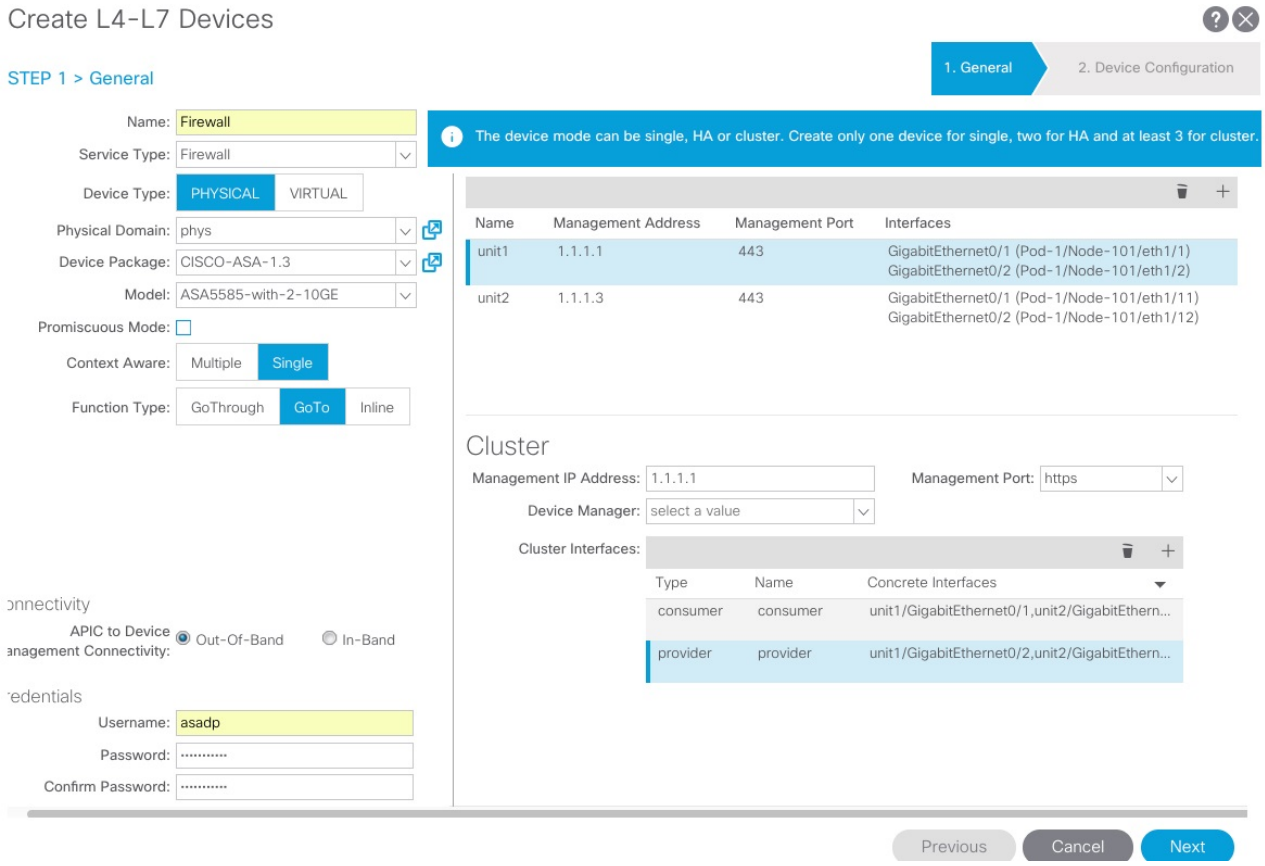
Before you begin

- You must use physical ASA units. The virtual ASA does not support clustering.
- You must have at least two ASA units of the same model running the same software image version and in the same mode (transparent or routed, all in single-context mode or all in multiple-context mode). Do not mix.
- You must have at least one hardware interface from each ASA designated as a cluster control link.
- In the ASA, ensure that there is no data interface configured when setting up or removing an ASA cluster.
- In the APIC, you must remove all service graphs before creating or deleting a cluster configuration.

Step 1 In the APIC, register all the ASA units in the cluster as CDevs (concrete devices) under an LDev (logical device).

Note The management IP addresses of the ASA units must be contiguous, so that once the ASA cluster is formed, the APIC does not lose connectivity with them. For example, if you have two ASA units, and the first ASA has an IP address of 1.1.1.1, the second ASA must be addressed 1.1.1.3, so that once the ASA cluster is formed, 1.1.1.1 becomes the virtual IP address of the ASA cluster, 1.1.1.2 becomes the local IP address of the first ASA, and 1.1.1.3 remains the local IP address of the second ASA.

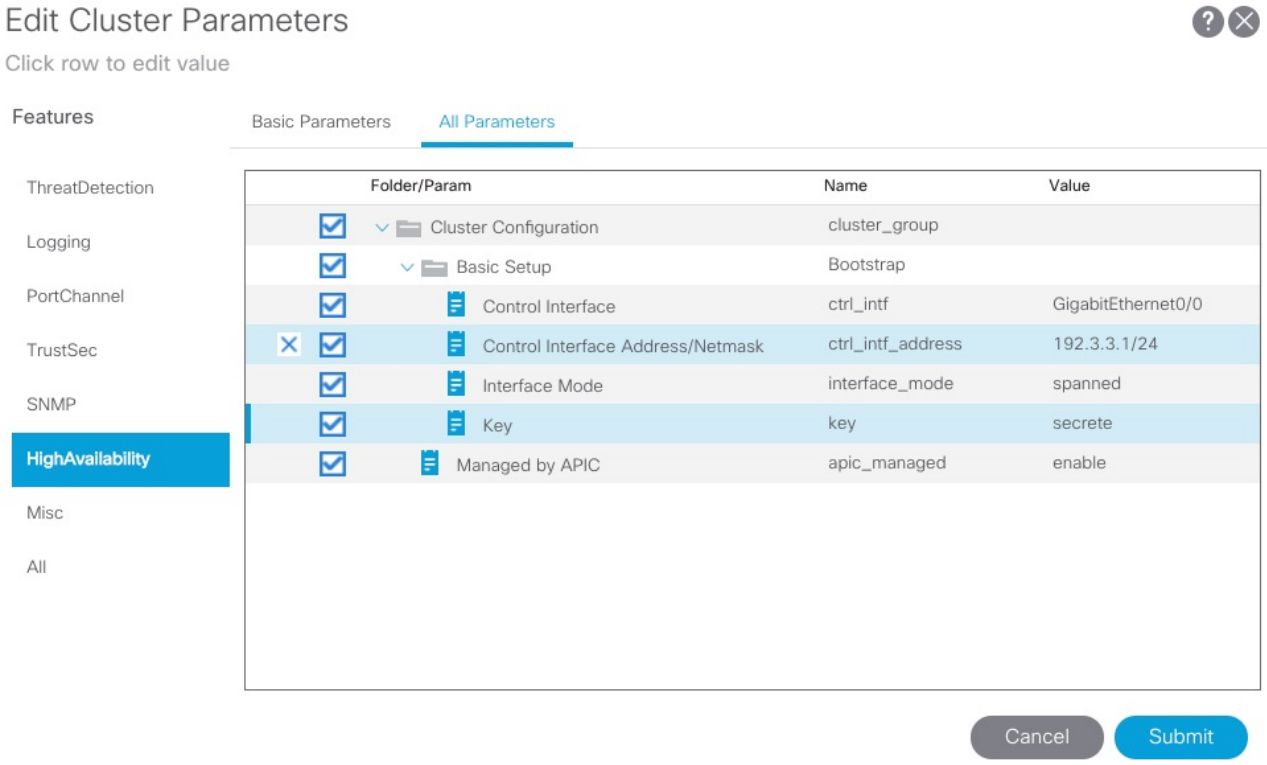
For example:



Step 2 Configure the LDev.

Note Wait up to 2 minutes for the ASA cluster to be formed. Avoid making any configuration changes until after you can successfully ping the management IP addresses of the cluster units.

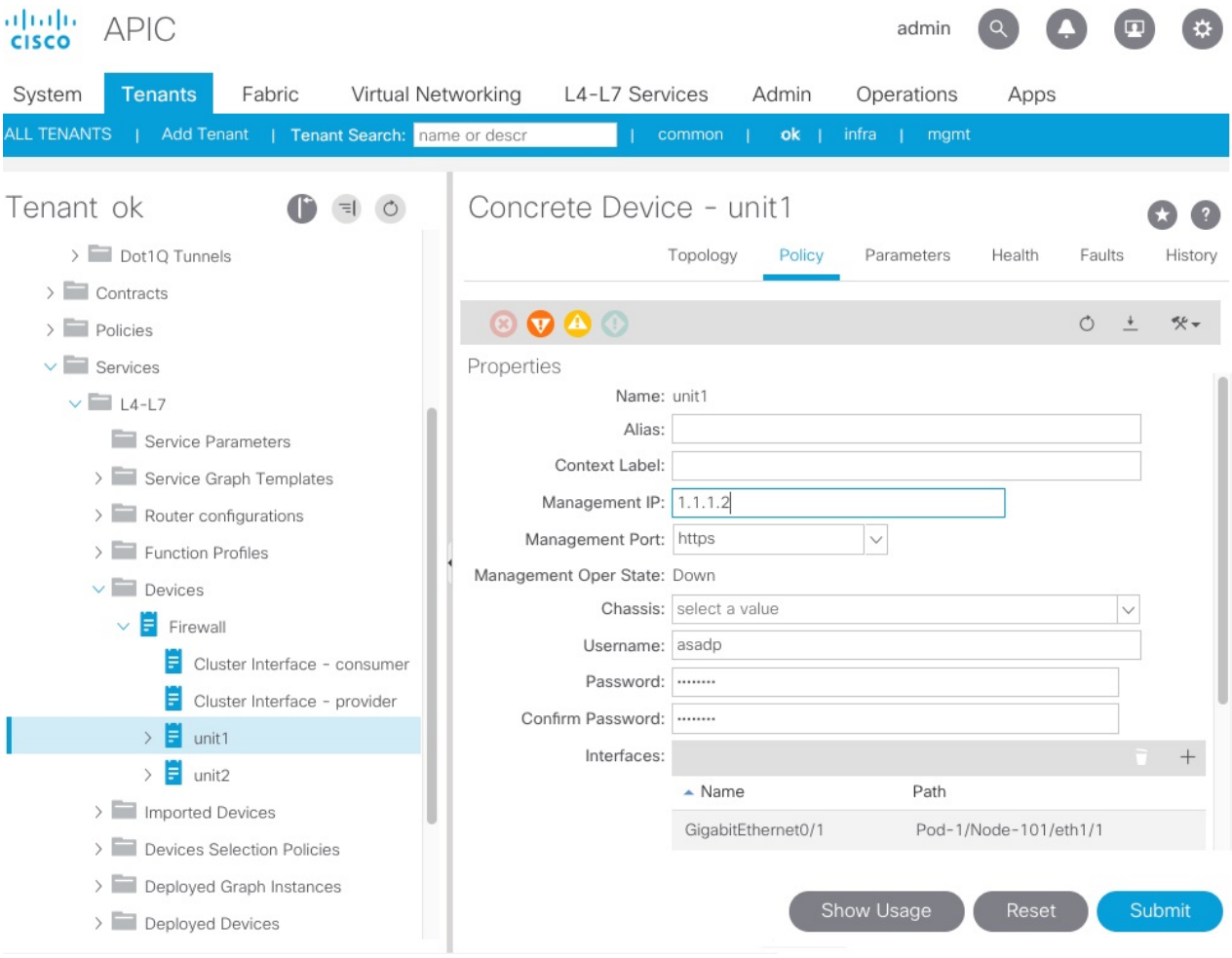
For example:



Step 3 The management IP address of the LDev becomes the virtual IP address of the ASA cluster. The primary control unit gets a separate IP address as its local IP address once the cluster is formed. Change the IP address of the CDev representing the primary control unit to the new local IP address. Otherwise, the APIC is not able to monitor the health of the primary control unit if there is a change of primary control unit such as during a failover.

Note If you remove the ASA cluster configuration, remember to restore the IP address of the primary control unit to its original value.

For example:



What to do next

To add or delete an ASA unit from the cluster, remove the cluster configuration, add or delete the ASA unit in the APIC, and configure the cluster again.

Configure the ASA From the APIC

Use the northbound API to configure the security policy, specifically for service graphs.

For information about how to use the APIC northbound APIs, see the Cisco APIC Management Information Model Reference.

Refer to the APIC documentation for more information.