



Introduction

- [Overview, on page 1](#)
- [Service Function Insertion, on page 2](#)
- [Available APIC Products, on page 2](#)
- [Supported Versions, on page 2](#)
- [Supported Features, on page 3](#)
- [Related Documentation, on page 4](#)

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.

Cisco ASA Device Package 1.3(x) with cloud orchestrator mode is a superset of Cisco ASA Device Package 1.2(x). Customers who want to use cloud orchestrator mode should use Cisco ASA Device Package 1.3(x) and APIC 3.1(x) or newer. Customers who *do not* want to use cloud orchestrator mode should use Cisco ASA Device Package 1.2(x) and APIC 3.0(x) or older.

When using ASA 9.12(x) and newer, use Cisco ASA Device Package 1.3(12.x) (with cloud orchestrator mode) or 1.2(12.x) (no cloud orchestrator mode) and newer. Otherwise, it will fail because of [CSCvo59053](#).

The following table lists the supported versions of 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)	
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

Feature	ASAv Support	ASA 5500-X/5585-X Support
NAT and Twice NAT	Yes	Yes
Netflow	Yes	Yes
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](#)