

Release Notes for the Cisco ASA Device Package Software, Version 1.2(9) for ACI

Release Notes for the Cisco ASA Device Package for ACI 2

Available APIC Products 2

Supported Versions 2

Important Notes 3

Running APIC 1.2(x) with ASA 9.3(1) 3

Policy Manager Locks Up When the Configuration for BGP Peering for the Service Appliance is Incomplete 3

Manually Re-Sync the APIC if You Changed the Version of ASA After It Was Registered with the APIC 4

ASA Configuration Not Rolled Back on Changing Concrete Interfaces 4

Second Graph Pushes Incorrect Configuration to ASA in Bridged Mode 4

Download the Software 5

Install the Software 5

Bug Search 5

Resolved Enhancement Requests in Version 1.2(9) 5

Resolved Caveats in Version 1.2(9) 5

Related Documentation 6

Revised: March 25, 2025

Release Notes for the Cisco ASA Device Package for ACI

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)	
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

Platform	Software Version
Cisco ASAv	ASA 9.2(x) and newer (Cisco ASA and APIC Compatibility Matrix)

Important Notes

- The ASAv does not support multiple context mode.
- ACE with dynamic EPG requires ASA image 9.3.2 or newer.

Running APIC 1.2(x) with ASA 9.3(1)

If you're running APIC 1.2(x) with ASA 9.3(1), which has a default SSL configuration, you'll see the following error:

```
*Major script error : Connection error :
[SSL:SSLV3_ALERT_HANDSHAKE_FAILURE] sslv3 alert handshake failure(_ssl.c:581)*
```

The workaround is to have **ssl encryption aes128-sha1** configured on the ASA or to upgrade the ASA to version 9.3(2) or newer.

Policy Manager Locks Up When the Configuration for BGP Peering for the Service Appliance is Incomplete

Use this workaround for caveat CSCuw0342:

Symptom: The Policy Manager crashes when the l3Out that is used for BGP peering for the service appliance has an incomplete configuration (CSCuw03425).

Conditions: The l3Out used for BGP peering for the service appliance is missing l3extRsNodeL3OutAtt.

Workaround: Make sure that the l3Out contains l3extRsNodeL3OutAtt. This problem will be fixed in a subsequent release.

The following shows the BGP XML example with l3extRsNodeL3OutAtt:

```
<polUni>
<fvTenant name="tenant1">
<l3extOut name="StaticExternal">
<l3extLNodeP name="bLeaf-101">
<l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="190.0.0.11">
<ipRouteP ip="50.50.50.0/24">
<ipNexthopP nhAddr="40.40.40.102/32"/>
</ipRouteP>
</l3extRsNodeL3OutAtt>
<l3extLIfP name="portIf">
<l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/15]" ifInstT="ext-svi" encap="vlan-3843"
addr="40.40.40.100/28" mtu="1500"/>
</l3extLIfP>
</l3extLNodeP>
<l3extInstP name="ExtInstP">
<l3extSubnet ip="50.50.50.0/24" scope="export-rtctrl"/>
</l3extInstP>
<l3extRsEctx tnFvCtxName="tenant1ctx1"/>
</l3extOut>
```

```
</fvTenant>
</polUni>
```

Manually Re-Sync the APIC if You Changed the Version of ASA After It Was Registered with the APIC

Use this workaround for caveat CSCva89163:

Symptom: Some commands don't work. For example, the information for the **network** and **neighbor** commands is not displayed (CSCva89163).

Conditions: If you're using a version of the ASA that is different from the version that is registered with the APIC, it doesn't automatically re-register with the APIC. Therefore, if you're using an older version of ASA, some commands may not be supported.

Workaround: Manually re-sync the APIC with the ASA by completing the following procedure:

Procedure

Step 1 On the **Tenants** tab of the APIC GUI, expand **L4-L7 Services** in the left pane.

Step 2 Expand **L4-L7 Devices**.

Step 3 Expand the firewall that is running the APIC.

Step 4 Right-click the device that is running the APIC, and select **Re-Query for Device Validation**.

ASA Configuration Not Rolled Back on Changing Concrete Interfaces

Use this workaround for caveat CSCvd65130:

Symptom: When cluster interfaces are changed under lif configuration for a deployed graph in bridge mode, the new interface might not get updated correctly on the ASA.

Conditions: When changes are made to the ASA device cluster interface configuration.

Workaround: Detach the graph from the contract before making any device changes and then attach it.

Second Graph Pushes Incorrect Configuration to ASA in Bridged Mode

Use this workaround for caveat CSCvd68860:

Symptom: When a second or subsequent graph is deployed on a new set of cluster interfaces in an ASA in bridged mode, the user might see cluster interfaces not configured under the correct bridge-group. This results in a configuration issue which creates a conflict with existing cluster interfaces using the default names in the ASA.

Conditions: Graph deployment using a new set of cluster interfaces with default interface names in an ASA in bridged mode.

Workaround: Rename the cluster interface name under **Interface Related Configuration** in graph parameters while configuring the graph.

Download the Software

Use your Cisco.com login credentials to obtain the Cisco ASA Device Package software image from:

https://software.cisco.com/download/release.html?mdfid=283123066&flowid=22661&softwareid=286279676

Install the Software

For instructions on how to install the device package, see the respective version of the Cisco ASA Quick Start Guide for APIC Integration hyperlinked on the Software Download page.

Note To upgrade from an older to a newer version, you do not need to remove the previous software package if your APIC release has the fix for CSCuv4353. Otherwise, remove the older version from the APIC before installing the newer version.

Bug Search

As a registered Cisco.com user, sign in to view more information about each bug or caveat using the Cisco Bug Search Tool.

Resolved Enhancement Requests in Version 1.2(9)

Table 1: Enhancement Requests Resolved in the Cisco ASA Device Package, Version 1.2(9)

Request/Caveat	Description
CSCuq96567	ASA device package needs to support site-to-site VPN.
CSCve93631	Add dynamic EPGs to the ASA FI device package.
CSCvf07594	ASA-DP: Support Firepower 21xx.

Resolved Caveats in Version 1.2(9)

Table 2: Caveats Resolved in the Cisco ASA Device Package, Version 1.2(9)

Caveat	Description
CSCve12665	Dynamic EPG network object-groups are deleted and re-added during APIC upgrade.
CSCve85459	F0324 is raised after changing Application Inspection parameter to **disable**.
CSCvf58335	ASA device package trying to delete existing port-channels.

Caveat	Description
CSCvf59620	ASA device package needs to support **bgp graceful-restart**.

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

© 2017 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.