

Release Notes for the Cisco ASA Device Package Software, Version 1.2(11) for ACI

Release Notes for the Cisco ASA Device Package for ACI 2

Download the Software 2

Available APIC Products 2

Supported Versions 2

Install the Software 3

Bug Search 3

Resolved Enhancement Requests in Version 1.2(11) 3

Resolved Caveats in Version 1.2(11) 4

Important Notes 4

Policy Manager Locks Up When the Configuration for BGP Peering for the Service Appliance is Incomplete 4

Manually Re-Sync the APIC if You Changed the Version of ASA After It Was Registered with the APIC 5

ASA Configuration Not Rolled Back on Changing Concrete Interfaces 5

Second Graph Pushes Incorrect Configuration to ASA in Bridged Mode 5

Restore Out-of-Band Configuration 6

Related Documentation 8

Revised: September 11, 2025

Release Notes for the Cisco ASA Device Package for ACI

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

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

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(11)

Table 1: Enhancement Requests Resolved in the Cisco ASA Device Package, Version 1.2(11)

Request/Caveat	Description
CSCvf74631	Support ASA cluster configuration.
CSCvi63894	Support configuration of cluster-pool for data interface IP address.
CSCvj75339	CLI 'mac-address-table' command in ASA device package.
CSCvk42308	Support port-channel span-cluster.

Resolved Caveats in Version 1.2(11)

Table 2: Caveats Resolved in the Cisco ASA Device Package, Version 1.2(11)

Caveat	Description
CSCvh95888	ASA DP needs to support access-group and security-level for BVI for IRB deployment.
CSCvi23896	ASA DP missing function profile for IPv4 and IPv6.
CSCvi80770	ASA multi-context feature with overlapping mgmt IPs, needs a solution with APIC.
CSCvj87694	Cannot assign bridge-group to interface.
CSCvj97862	ASA DP needs a function profile for mixed-mode IRB.
CSCvk44096	ASA DP unable to upload FI device package to APIC.
CSCvn10162	ASA DP treats 9.10 as less than 9.3 in which some BGP test cases fail.

Important Notes

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

Restore Out-of-Band Configuration

Use this enhancement feature for caveat CSCvb90258:

Symptom: The ASA Fabic Insertion (FI) Device Package (DP) does not support saving configuration out-of-band.

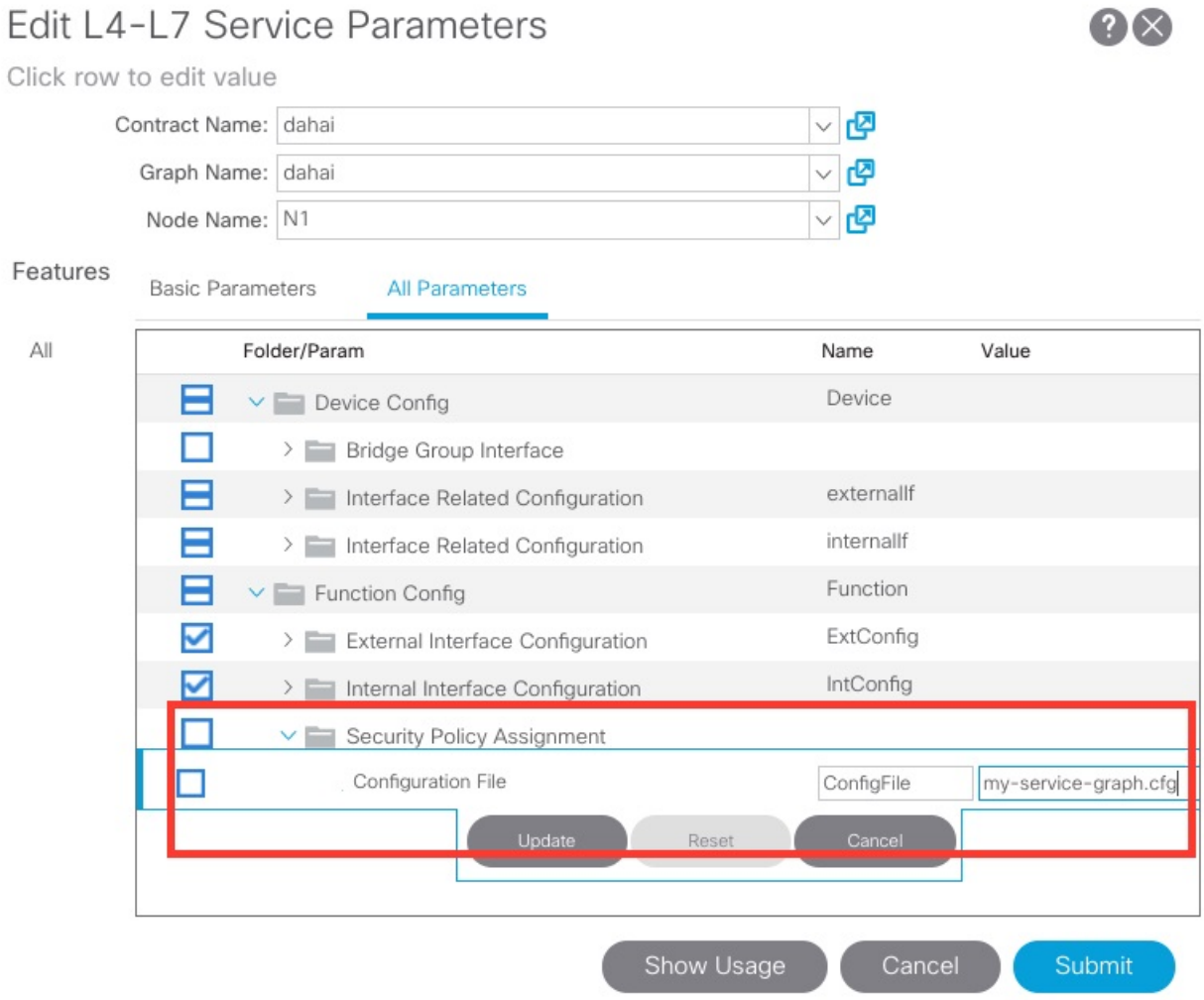
Conditions: The ASA-FI-DP only supports routing and interface configuration. It does not support the configuration of security policy binding commands, such as `access-group` and `nat`, to the service graph. To assign a security policy to a service graph, you must manually configure the setup. In the case of rerendering a service graph after removing it, you must manually reconfigure the bindings.

Solution: This enhancement feature enables you to save the security policy binding commands to a file, which the ASA-FI-DP can apply after the service graph is reattached.

XML: A folder named `SecurityPolicyAssignment` has been added under `vnsMFunc` which enables you to enter a name for the configuration that has the security policy to assign to the service graph.

```
<vnsMFunc name="Firewall">
<vnsMFolder key="ExIntfConfigRelFolder" dispLabel="External Interface Configuration"
description="A list of additional interface parameters for external connector"...>
<vnsMFolder key="InIntfConfigRelFolder" dispLabel="Internal Interface Configuration"
description="A list of additional interface parameters for internal connector" ...>
<vnsMConn name="external" ...>
<vnsMConn name="internal" ...>
 <vnsMFolder key="SecurityPolicyAssignment"
   dispLabel="Security Policy Assignment"
   description="Assign the security policy in the named file to the service-graph">
  <vnsMParam key="ConfigFile"
    dispLabel="Configuration File"
    dType="str"
    description="Specify the name of the file that contains the out of band configuration specific to the
service-graph"/>
  </vnsMFolder>
 </vnsMFunc>
```

APIC:



- If the file is on the ASA, enter the name of the file.
- If the file is on a TFTP server, enter: `tftp://<ip-address>/<filename>`
- If the file is on an FTP server, enter: `ftp://<ip-address>/<filename>`

The contents of the file should be commands that you must enter out-of-band that reference the interfaces used in the service graph. For example:

```
access-group <acl-name> [in|out] interface <nameif>
nat (<nameif>, <nameif>) …
service-policy <policy-name> interface <nameif>
crypto map <map-name> interface <nameif>
crypto ike2 enable <nameif>
```

Here's an example of such a file for a service graph with interfaces `externalInt` and `internalInt`:

```
access-group access-group external_access_acl in interface externalInt
nat (internalInt,externalInt) source static real_obj mapped_obj
nat (internalInt,externalInt) source dynamic any mapped_obj interface
```

Commands that do not reference an interface should not be part of the file because they're not removed when you remove the service graph. Examples of such commands include:

```
access-list
object network
object service
object-group network
object-group service
```

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

© 2018–2025 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.