

Release Notes for the Cisco ASA Device Package Software, Version 1.2(8) for ACI

This document contains information for the release of Cisco ASA Device Package software, Version 1.2(8) for ACI.

Cisco Systems, Inc.
www.cisco.com

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 software for ACI - Same as the original version that was available with version 1.2(6) and older. This version allows you to configure many important features of ASA from the APIC, including, but not limited to, the following:
  - Interface
  - Routing
  - Access-list
  - NAT
  - TrustSec
  - Application inspection
  - NetFlow
  - High availability
- Cisco ASA Device Package Fabric Insertion software for ACI - This version contains the following subset of the 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 1.2.8.9 has been qualified with APIC 2.2(2e) and 2.3(1e).

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 ASAv	See the “ASA and ASDM Compatibility” section of the *Cisco ASA 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 are running APIC 1.2(x) with ASA 9.3(1), which has a default SSL configuration, you will 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 do not work. For example, the information for the **network** and **neighbor** commands is not displayed (CSCva89163).

Conditions If you are using a version of the ASA that is different from the version that is registered with APIC, it does not automatically re-register with the APIC. Therefore, if you are 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:

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

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.

For instructions on how to install the Cisco ASA Device Package software, see *Cisco ASA Quick Start Guide for APIC Integration, Version 1.2.x*.

Bug Search

If you're registered on Cisco.com, view more information about each caveat using the Bug Search tool:

https://tools.cisco.com/bugsearch

Resolved Enhancement Requests in the Cisco ASA Device Package, Version 1.2(8.9)

The following table lists the enhancement requests resolved in the Cisco ASA Device Package, Version 1.2(8.9):

Request/Caveat	Description
CSCvb24699	ASA DP: AAA Cut-through Proxy Authentication Support
CSCvc20334	ASA DevPak: support for icmp permit configuration

Resolved Caveats in the Cisco ASA Device Package, Version 1.2(8.9)

The following table lists the caveats resolved in the Cisco ASA Device Package, Version 1.2(8.9):

Caveat	Description
CSCvb67004	ASA device in auditfailed state but no faults and health is 100%
CSCvb77538	nat source dynamic is not configured on the ASA device
CSCvb88784	nat source static command is not present on the ASA device
CSCvb95956	nat source static any any command is on the ASA device
CSCvc91248	ASA device in modifyfailed state with faults
CSCvd66331	ASA DP unable to delete logging host command on ASA 9.7.1

Open Caveats in the Cisco ASA Device Package, Version 1.2(8.9)

The following table lists the open caveats (severity 1 to 3) in the Cisco ASA Device Package, Version 1.2(8.9):

Caveat	Description
CSCvd68007	Cannot delete NAT commands in TFW mode
CSCvd72334	OSPF fails with APIC 2.2(1n) when both IPv4 and IPv6 OSPF configs are sent
CSCvd72493	OSPF configuration fails to be sent to ASA with APIC 2.2(1n)
CSCvd92354	BGP test case failing with APIC, no serviceModify being called

Related Documentation

For additional information about the Cisco ASA, see *Navigating the Cisco ASA Series Documentation*.

For additional information about the Cisco APIC, see APIC Documentation and Cisco Application Centric Infrastructure Security Solution.

Additional Information

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2017 Cisco Systems, Inc. All rights reserved.