Release Notes for the Cisco ASA Device Package Software, Version 1.2(6) for ACI

Published: June 30 , 2016

Revised: June 30, 2016

This document contains release information for the Cisco ASA Device Package software, Version 1.2(6) for ACI, and includes the following sections:

Cisco Systems, Inc.
www.cisco.com

Supported ASA Models

The following table lists the supported ASA models.

ASA Model	Software Version
ASA 5500-X (5512 through 5555)	ASA software Version 8.4(x) and later
ASA 5585-X (SSP 10 through SSP 60)	
Firepower 9300	ASA software Version 9.6(1) and later
Firepower 41xx	
ASAv	See the "ASA and ASDM Compatibility" section of the *Cisco ASA Compatibility Matrix*.

Supported APIC Versions

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

New Features in 1.2(6)

This release includes support for the following:

- A new command is now available which enables you to add remarks or comments about entries in any access list, including extended, EtherType, IPv6, standard, and Webtype access lists. This command is used in the same way as the **access-list** *list_name* **remark** *text* command is used for the ASA. For more information about how to use the command, see the *Cisco ASA 5500 Series Command Reference*.
- In addition to being able to perform application-inspections on service connectors, you can now perform global application-inspections with the **policy-map** command. This command is used in the same way as the factory default global policy configuration on the ASA. For more information, see the *Cisco Security Appliance Command Line Configuration Guide*.
- A new command is now available which enables you to either:
  - Allow communication between interfaces with equal security levels (inter-interface)
  - Allow traffic to enter and exit the same interface (intra-interface)

  This command is used in the same way as the **same-security-traffic** command is used for the ASA. For more information about how to use the command, see the *Cisco ASA 5500 Series Command Reference*.
- A new command is now available which enables you to define the period of time which can be used in a AccessControlEntry to specify when it is active. This command is used in the same way as the **time-range** command is used for the ASA. For more information about how to use the command, see the *Cisco ASA 5500 Series Command Reference*.

Important Notes

Pay attention to the following important notes:

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

APIC 1.2(x) and 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 later.

The Policy Manager Lock Ups when the Configuration for BGP Peering for the Service Appliance is Incomplete

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>
```

Installing the Software

To upgrade, you do not need to remove the previous package if your APIC release has the fix for CSCuv4353. Otherwise, to upgrade from an older version to a newer, you need to remove the old version from APIC first, then install the new version.

To install the ASA Device Package software, see *Cisco ASA Quick Start Guide for APIC Integration, 1.2* for instructions.

Downloading the Software from Cisco.com

If you have a Cisco.com login, you can obtain the ASA Device Package image from the following website:

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

Bug Search

If you are a registered Cisco.com user, view more information about each caveat using Bug Search at the following website:

https://tools.cisco.com/bugsearch

Resolved Caveats in the ASA Device Package Version 1.2(6)

Note There are no open caveats for ASA Device Package Version.

The following table contains the resolved caveats in ASA Device Package Version 1.2(6):

Caveat	Description
CSCuz95079	Global Inspection: H.232 H.225 should be H.323 H.225 under Global Policy
CSCuz72495	asa-dp: namif of interface missing from ASA on creating service graph
CSCuy22138	ASADP CTS: AAA-server for ISE not delete after associated tenant deleted
CSCuz42674	asa-dp: serviceAudit throws exception
CSCuz50992	ACI ASA DP: Require 'standby IP' L4-L7 parameter
CSCuz56618	asa-dp: serviceAudit generates wrong CLIs for NAT
CSCuz61071	Same order number used in NAT could cause NAT to be deleted/reconfigured
CSCuy03953	IPV4 addr not validated for concrete interface in L4-L7 graph template.
CSCuz07266	Trustsec role-based sgt-map command will fail if upgraded to ASA 9.6.1
CSCuz08407	AVS BZMR2 - ASAv VMs lost access after deleting the device

Resolved Enhancement Requests in the ASA Device Package Version 1.2(6)

The following table contains the enhancement requests resolved in ASA Device Package Version 1.2(6):

Request/Caveat	Description
CSCux98269	Support for the **remark** keyword for the **access-list** command from ASA.
CSCux98266	Support for global inspections on service connectors,
CSCuy45554	Support for the **time-range** command from ASA.
N/A	Support for the **same-security-traffic** command from ASA.

Related Documentation

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

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

Obtaining Documentation and Submitting a Service Request

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.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service

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