Release Notes for Cisco ASDM, 7.14(x)

Release Notes for Cisco ASDM, 7.14(x)

This document contains release information for Cisco ASDM Version 7.14(x) for the Cisco ASA series.

Important Notes

- **ASDM signed-image support in 9.14(4.14)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. (CSCwb05291, CSCwb05264)
- **ASDM Cisco.com Upgrade Wizard failure on Firepower 1000 and 2100 in Appliance mode**—The ASDM Cisco.com Upgrade Wizard does not work for upgrading to 9.14 (**Tools > Check for ASA/ASDM Updates**). The wizard can upgrade ASDM from 7.13 to 7.14, but the ASA image upgrade is grayed out. (CSCvt72183) As a workaround, use one of the following methods:
  - Use **Tools > Upgrade Software from Local Computer** for both ASA and ASDM. Note that the ASDM image (7.14(1)) in the 9.14(1) bundle also has the bug CSCvt72183; you should download the newer 7.14(1.46) image to enable correct functioning of the wizard.
  - Use **Tools > Check for ASA/ASDM Updates** to upgrade to ASDM 7.14 (the version will be 7.14(1.46); then use the new ASDM to upgrade the ASA image. Note that you may see a **Fatal Installation Error**; in this case, click **OK**. You must then set the boot image manually on the **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** screen. Save the configuration and reload the ASA.
- **For Failover pairs in 9.14(1)+, the ASA no longer shares SNMP client engine data with its peer.**
- **No support in ASA 9.14(1)+ for cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs (**CSCvy22526**).**
- **No support in ASA 9.13(1) and later for the ASA 5512-X, ASA 5515-X, ASA 5585-X, and the ASASM**—ASA 9.12(x) is the last supported version. For the ASA 5515-X and ASA 5585-X FirePOWER module, the last supported version is 6.4.

  Note: ASDM 7.13(1) and ASDM 7.14(1) also did not support these models; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.
- **ASAv requires 2GB memory in 9.13(1) and later**—Beginning with 9.13(1), the minimum memory requirement for the ASAv is 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version. You must adjust the memory size before upgrading. See the ASAv Getting Started Guide for information about the resource allocations (vCPU and memory) supported in version 9.13(1).
- **Downgrade issue for the Firepower 2100 in Platform mode from 9.13/9.14 to 9.12 or earlier**—For a Firepower 2100 with a fresh installation of 9.13 or 9.14 that you converted to Platform mode: If you

downgrade to 9.12 or earlier, you will not be able to configure new interfaces or edit existing interfaces in FXOS (note that 9.12 and earlier only supports Platform mode). You either need to restore your version to 9.13 or later, or you need to clear your configuration using the FXOS erase configuration command. This problem does not occur if you originally upgraded to 9.13 or 9.14 from an earlier release; only fresh installations are affected, such as a new device or a re-imaged device. (CSCvr19755)

- **Cluster control link MTU change in 9.13(1)**—Starting in 9.13(1), many cluster control packets are larger than they were in previous releases. The recommended MTU for the cluster control link has always been 1600 or greater, and this value is appropriate. However, if you set the MTU to 1600 but then failed to match the MTU on connecting switches (for example, you left the MTU as 1500 on the switch), then you will start seeing the effects of this mismatch with dropped cluster control packets. Be sure to set all devices on the cluster control link to the same MTU, specifically 1600 or higher.

- **Upgrade ROMMON for ASA 5506-X, 5508-X, and 5516-X to Version 1.1.15 or later**—There is a new ROMMON version for these ASA models (May 15, 2019); we highly recommend that you upgrade to the latest version. To upgrade, see the instructions in the ASA configuration guide.

  Caution: The ROMMON upgrade for 1.1.15 takes twice as long as previous ROMMON versions, approximately 15 minutes. **Do not** power cycle the device during the upgrade. If the upgrade is not complete within 30 minutes or it fails, contact Cisco technical support; **do not** power cycle or reset the device.

- **Upgrade ROMMON for the ISA 3000 to Version 1.0.5 or later**——There is a new ROMMON version for the ISA 3000 (May 15, 2019); we highly recommend that you upgrade to the latest version. To upgrade, see the instructions in the ASA configuration guide.

  Caution: The ROMMON upgrade for 1.0.5 takes twice as long as previous ROMMON versions, approximately 15 minutes. **Do not** power cycle the device during the upgrade. If the upgrade is not complete within 30 minutes or it fails, contact Cisco technical support; **do not** power cycle or reset the device.

- **The tls-proxy keyword, and support for SCCP/Skinny encrypted inspection, was removed** from the **inspect skinny** command.

- **ASDM Upgrade Wizard**—Due to an internal change, the wizard is only supported using ASDM 7.10(1) and later; also, due to an image naming change, you must use ASDM 7.12(1) or later to upgrade to ASA 9.10(1) and later. Because ASDM is backwards compatible with earlier ASA releases, you can upgrade ASDM no matter which ASA version you are running. Note that ASDM 7.13 and 7.14 did not support the ASA 5512-X, 5515-X, 5585-X, or ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.

- **Windows DNS Client Optimization Limitation**—Because of a limitation in Windows 8 and above, we have observed that certain name resolutions, such as nslookup, fail for FQDNs by not matching any split-DNS domains. The workaround is to disable Windows DNS client optimization with the following changes:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
Value:DisableParallelAandAAA Data: 1
Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient Value:
DisableSmartNameResolution Data: 1
```

System Requirements

This section lists the system requirements to run this release.

ASDM Java Requirements

You can install ASDM using Oracle JRE 8.0 (**asdm-*version*.bin**) or OpenJRE 1.8.x (**asdm-openjre-*version*.bin**).

Note ASDM is not tested on Linux.

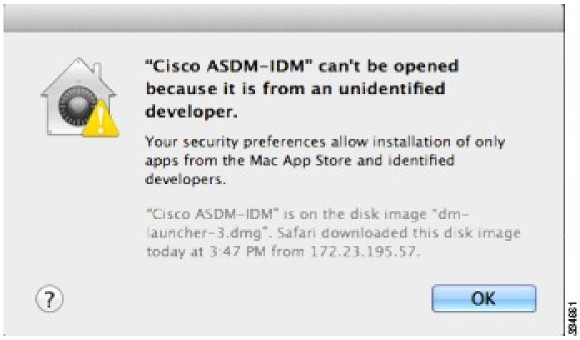
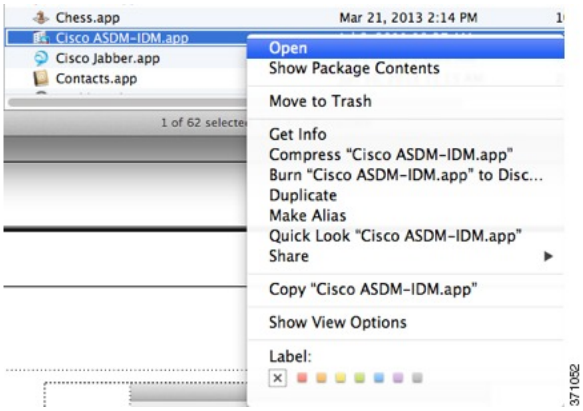
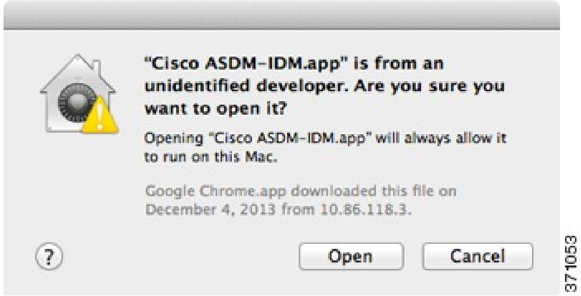
Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): • 10 **Note** See Windows 10 in ASDM Compatibility Notes, on page 3 if you have problems with the ASDM shortcut. • 8 • 7 • Server 2016 and Server 2019 (ASA management only; ASDM management of the FirePOWER module is not supported. You can alternatively use the FMC to manage the FirePOWER module when using ASDM for ASA management.) • Server 2012 R2 • Server 2012 • Server 2008	Yes	No support	Yes	8.0 version 8u261 or later	1.8 **Note** No support for Windows 7 32-bit
Apple OS X 10.4 and later	Yes	Yes	Yes (64-bit version only)	8.0 version 8u261 or later	1.8

ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
Windows 10	"**This app can't run on your PC**" error message. When you install the ASDM Launcher, Windows 10 might replace the ASDM shortcut target with the Windows Scripting Host path, which causes this error. To fix the shortcut target: **1.** Choose **Start** > **Cisco ASDM-IDM Launcher**, and right-click the **Cisco ASDM-IDM Launcher** application. **2.** Choose **More** > **Open file location**. Windows opens the directory with the shortcut icon. **3.** Right click the shortcut icon, and choose **Properties**. **4.** Change the **Target** to: **C:\Windows\System32\wscript.exe invisible.vbs run.bat** **5.** Click **OK**.
OS X	On OS X, you may be prompted to install Java the first time you run ASDM; follow the prompts as necessary. ASDM will launch after the installation completes.

Conditions	Notes
OS X 10.8 and later	You need to allow ASDM to run because it is not signed with an Apple Developer ID. If you do not change your security preferences, you see an error screen.  **"Cisco ASDM-IDM" can't be opened because it is from an unidentified developer.** Your security preferences allow installation of only apps from the Mac App Store and identified developers. "Cisco ASDM-IDM" is on the disk image "dm-launcher-3.dmg". Safari downloaded this disk image today at 3:47 PM from 172.23.195.57. 1. To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose **Open**.  Chess.app Mar 21, 2013 2:14 PM Cisco ASDM-IDM.app Cisco Jabber.app Contacts.app 1 of 62 selecte Open Show Package Contents Move to Trash Get Info Compress "Cisco ASDM-IDM.app" Burn "Cisco ASDM-IDM.app" to Disc... Duplicate Make Alias Quick Look "Cisco ASDM-IDM.app" Share Copy "Cisco ASDM-IDM.app" Show View Options Label: 371052 2. You see a similar error screen; however, you can open ASDM from this screen. Click **Open**. The ASDM-IDM Launcher opens.  **"Cisco ASDM-IDM.app" is from an unidentified developer. Are you sure you want to open it?** Opening "Cisco ASDM-IDM.app" will always allow it to run on this Mac. Google Chrome.app downloaded this file on December 4, 2013 from 10.86.118.3.

Conditions	Notes
Requires Strong Encryption license (3DES/AES) on ASA **Note** Smart licensing models allow initial access with ASDM without the Strong Encryption license.	ASDM requires an SSL connection to the ASA. You can request a 3DES license from Cisco: **1.** Go to www.cisco.com/go/license. **2.** Click **Continue to Product License Registration**. **3.** In the Licensing Portal, click **Get Other Licenses** next to the text field. **4.** Choose **IPS, Crypto, Other...** from the drop-down list. **5.** Type **ASA** in to the **Search by Keyword** field. **6.** Select **Cisco ASA 3DES/AES License** in the **Product** list, and click **Next**. **7.** Enter the serial number of the ASA, and follow the prompts to request a 3DES/AES license for the ASA.
• Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari	When the ASA uses a self-signed certificate or an untrusted certificate, Firefox and Safari are unable to add security exceptions when browsing using HTTPS over IPv6. See https://bugzilla.mozilla.org/show_bug.cgi?id=633001. This caveat affects all SSL connections originating from Firefox or Safari to the ASA (including ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority.
• SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome. • Chrome	If you change the SSL encryption on the ASA to exclude both RC4-MD5 and RC4-SHA1 algorithms (these algorithms are enabled by default), then Chrome cannot launch ASDM due to the Chrome "SSL false start" feature. We suggest re-enabling one of these algorithms (see the **Configuration** > **Device Management** > **Advanced** > **SSL Settings** pane); or you can disable SSL false start in Chrome using the **--disable-ssl-false-start** flag according to Run Chromium with flags.

Install an Identity Certificate for ASDM

When using Java 7 update 51 and later, the ASDM Launcher requires a trusted certificate. An easy approach to fulfill the certificate requirements is to install a self-signed identity certificate. You can use Java Web Start to launch ASDM until you install a certificate.

See Install an Identity Certificate for ASDM to install a self-signed identity certificate on the ASA for use with ASDM, and to register the certificate with Java.

Increase the ASDM Configuration Memory

ASDM supports a maximum configuration size of 512 KB. If you exceed this amount you may experience performance issues. For example, when you load the configuration, the status dialog box shows the percentage of the configuration that is complete, yet with large configurations it stops incrementing and appears to suspend operation, even though ASDM might still be processing the configuration. If this situation occurs, we recommend that you consider increasing the ASDM system heap memory.

Increase the ASDM Configuration Memory in Windows

To increase the ASDM heap memory size, edit the **run.bat** file by performing the following procedure.

Procedure

Step 1 Go to the ASDM installation directory, for example C:\Program Files (x86)\Cisco Systems\ASDM.

Step 2 Edit the **run.bat** file with any text editor.

Step 3 In the line that starts with “start javaw.exe”, change the argument prefixed with “-Xmx” to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.

Step 4 Save the **run.bat** file.

Increase the ASDM Configuration Memory in Mac OS

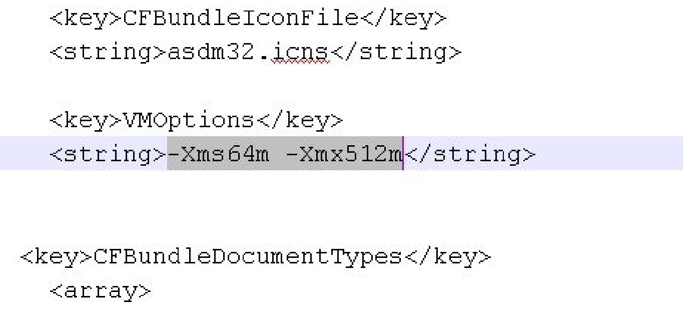
To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

Procedure

Step 1 Right-click the **Cisco ASDM-IDM** icon, and choose **Show Package Contents**.

Step 2 In the **Contents** folder, double-click the **Info.plist** file. If you have Developer tools installed, it opens in the **Property List Editor**. Otherwise, it opens in **TextEdit**.

Step 3 Under **Java** > **VMOptions**, change the string prefixed with “-Xmx” to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.

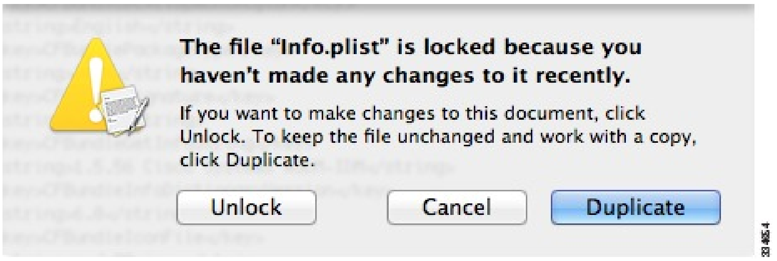


```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>


  <key>CFBundleDocumentTypes</key>
    <array>
```

Step 4 If this file is locked, you see an error such as the following:



The file "Info.plist" is locked because you haven't made any changes to it recently.

If you want to make changes to this document, click Unlock. To keep the file unchanged and work with a copy, click Duplicate.

Step 5 Click **Unlock** and save the file.

If you do not see the **Unlock** dialog box, exit the editor, right-click the **Cisco ASDM-IDM** icon, choose **Copy Cisco ASDM-IDM**, and paste it to a location where you have write permissions, such as the Desktop. Then change the heap size from this copy.

ASA and ASDM Compatibility

For information about ASA/ASDM software and hardware requirements and compatibility, including module compatibility, see Cisco ASA Compatibility.

VPN Compatibility

For VPN compatibility, see Supported VPN Platforms, Cisco ASA 5500 Series.

New Features

This section lists new features for each release.

Note New, changed, and deprecated syslog messages are listed in the syslog message guide.

New Features in ASA 9.14(4)/ASDM 7.17(1)

Released: February 2, 2022

There are no new features in this release.

New Features in ASA 9.14(3)/ASDM 7.15(1.150)

Released: June 15, 2021

There are no new features in this release.

New Features in ASA 9.14(2)

Released: November 9, 2020

Feature	Description
SNMP Features	
SNMP polling over site-to-site VPN	For secure SNMP polling over a site-to-site VPN, include the IP address of the outside interface in the crypto map access-list as part of the VPN configuration.

New Features in ASA 9.14(1.30)

Released: September 23, 2020

Feature	Description
Licensing Features	
ASAv100 permanent license reservation	The ASAv100 now supports permanent license reservation using product ID L-ASAV100SR-K9=. **Note:** Not all accounts are approved for permanent license reservation.

New Features in ASDM 7.14(1.48)

Released: April 30, 2020

Feature	Description
Platform Features	
Restore support for the ASA 5512-X, 5515-X, 5585-X, and ASASM for ASA 9.12 and earlier	This ASDM release restores support for the ASA 5512-X, 5515-X, 5585-X, and ASASM when they are running 9.12 or earlier. The final ASA version for these models is 9.12. The original 7.13(1) and 7.14(1) releases blocked backwards compatibility with these models; this version has restored compatibility.

New Features in ASAv 9.14(1.6)

Released: April 30, 2020

Note This release is only supported on the ASAv.

Feature	Description
Platform Features	

Feature	Description
ASAv100 platform	The ASAv virtual platform has added the ASAv100, a high-end performance model that provides 20 Gbps Firewall throughput levels. The ASAv100 is a subscription-based license, available in terms of 1 year, 3 years, or 5 years. The ASAv100 is supported on VMware ESXi and KVM only.

New Features in ASA 9.14(1)/ASDM 7.14(1)

Released: April 6, 2020

Feature	Description
Platform Features	
ASA for the Firepower 4112	We introduced the ASA for the Firepower 4112. No modified screens. **Note** Requires FXOS 2.8(1).
Firewall Features	
Ability to see port numbers in show access-list output.	The **show access-list** command now has the numeric keyword. You can use this to view port numbers in the access control entries rather than names, for example, 80 instead of www.
The **object-group icmp-type** command is deprecated.	Although the command remains supported in this release, the **object-group icmp-type** command is deprecated and might be removed in a future release. Please change all ICMP-type objects to service object groups (**object-group service**) and specify **service icmp** within the object.
Kerberos Key Distribution Center (KDC) authentication.	You can import a keytab file from a Kerberos Key Distribution Center (KDC), and the system can authenticate that the Kerberos server is not being spoofed before using it to authenticate users. To accomplish KDC authentication, you must set up a **host**/*ASA_hostname* service principal name (SPN) on the Kerberos KDC, then export a keytab for that SPN. You then must upload the keytab to the ASA, and configure the Kerberos AAA server group to validate the KDC. New/Modified screens: **Configuration** > **Device Management** > **Users/AAA** > **AAA Kerberos**, **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups** Add/Edit dialog box for Kerberos server groups.
High Availability and Scalability Features	
Configuration sync to data units in parallel	The control unit now syncs configuration changes with data units in parallel by default. Formerly, synching occurred sequentially. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Enable parallel configuration replicate** check box

Feature	Description
Messages for cluster join failure or eviction added to **show cluster history**	New messages were added to the **show cluster history** command for when a cluster unit either fails to join the cluster or leaves the cluster. New/Modified commands: **show cluster history** No modified screens.
Interface Features	
Speed auto-negotation can be disabled on 1GB fiber interfaces on the Firepower 1000 and 2100	You can now configure a Firepower 1100 or 2100 SFP interface to disable auto-negotiation. For 10GB interfaces, you can configure the speed down to 1GB without auto-negotiation; you cannot disable auto-negotiation for an interface with the speed set to 10GB. New/Modified screens: **Configuration** > **Device Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties** > **Speed**
Administrative and Troubleshooting Features	
New **connection-data-rate** command	The **connection-data-rate** command was introduced to provide an overview on data rate of individual connections on the ASA. When this command is enabled, per-flow data rate along with the existing connection information are provided. This information helps to identify and block unwanted connections with high data rates, thereby, ensuring an optimized CPU utilization. New/Modified commands: **conn data-rate**,**show conn data-rate**, **show conn detail**, **clear conn data-rate** No modified screens.
HTTPS idle timeout setting	You can now set the idle timeout for all HTTPS connections to the ASA, including ASDM, WebVPN, and other clients. Formerly, using the **http server idle-timeout** command, you could only set the ASDM idle timeout. If you set both timeouts, the new command takes precendence. New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** > **HTTP Settings** > **Connection Idle Timeout** check box.
NTPv4 support	The ASA now supports NTPv4. No modified screens.
New **clear logging counter** command	The **show logging** command provides statistics of messages logged for each logging category configured on the ASA. The **clear logging counter** command was introduced to clear the logged counters and statistics. New/Modified commands: **clear logging counter** No modified screens.
Debug command changes for FXOS on the Firepower 1000 and 2100 in Appliance mode	The **debug fxos_parser** command has been simplified to provide commonly-used troubleshooting messages about FXOS. Other FXOS debug commands have been moved under the **debug menu fxos_parser** command. New/Modified commands: **debug fxos_parser**, **debug menu fxos_parser** No modified screens.

Feature	Description
show tech-support command enhanced	The **show ssl objects** and **show ssl errors** command was added to the output of the **show tech-support** command. New/Modified commands: **show tech-support** No modified screens. *Also in 9.12(4).*
Monitoring Features	
Net-SNMP version 5.8 Support	The ASA is using Net-SNMP, a suite of applications used to implement SNMP v1, SNMP v2c, and SNMP v3 using both IPv4 and IPv6. New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **SNMP**
SNMP OIDs and MIBs	The ASA enhances support for the CISCO-REMOTE-ACCESS-MONITOR-MIB to track rejected/failed authentications from RADIUS over SNMP. This feature implements three SNMP OIDs: • crasNumTotalFailures (total failures) • crasNumSetupFailInsufResources (AAA and other internal failures) • crasNumAbortedSessions (aborted sessions) objects The ASA provides support for the Advanced Encryption Standard (AES) Cipher Algorithm. This feature implements the following SNMP OIDs: • usmAesCfb128Protocol • usmNoPrivProtocol
SNMPv3 Authentication	You can now use SHA-256 HMAC for user authentication. New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **SNMP**
debug telemetry command.	You can use the **debug telemetry** command, debug messages related to telemetry are displayed. The debugs help to identify the cause for errors when generating the telemetry report. No modified screens.
VPN Features	
DHCP Relay Server Support on VTI	You can now configure DHCP relay server to forward DHCP messages through VTI tunnel interface. New/Modified screens: **Configuration** > **Device Management** > **DHCP** > **DHCP Relay**
IKEv2 Support for Multiple Peer Crypto Map	You can now configure IKEv2 with multi-peer crypto map—when a peer in a tunnel goes down, IKEv2 attempts to establish the SA with the next peer in the list. New/Modified screens: **Configuration** > **Site-to-Site VPN** > **Advanced** > **Crypto Maps** > **Create / Edit IPsec Rule** > **Tunnel Policy (Crypto Map) - Basic**

Feature	Description
Username Options for Multiple Certificate Authentication	In multiple certificate authentication, you can now specify from which certificate, first (machine certificate) or second (user certificate), you want the attributes to be used for aaa authentication. New/Modified screens: • **Connection Profile** > **Advanced** > **Authentication** • **Connection Profile** > **Advanced** > **Secondary Authentication**

Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

ASA Upgrade Path

To view your current version and model, use one of the following methods:

- ASDM: Choose **Home** > **Device Dashboard** > **Device Information**.
- CLI: Use the **show version** command.

This table provides upgrade paths for ASA. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Note Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage.

Note For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

Note ASA 9.12(x) was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.

ASA 9.2(x) was the final version for the ASA 5505.

ASA 9.1(x) was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

Current Version	Interim Upgrade Version	Target Version
9.13(x)	—	Any of the following: → 9.14(x)

Current Version	Interim Upgrade Version	Target Version
9.12(x)	—	Any of the following: → 9.14(x)
9.10(x)	—	Any of the following: → 9.14(x) → 9.12(x)
9.9(x)	—	Any of the following: → 9.14(x) → 9.12(x)
9.8(x)	—	Any of the following: → 9.14(x) → 9.12(x)
9.7(x)	—	Any of the following: → 9.14(x) → 9.12(x) → 9.8(x)
9.6(x)	—	Any of the following: → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	Any of the following: → 9.14(x) → 9.12(x) → 9.8(x)
9.4(x)	—	Any of the following: → 9.14(x) → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.3(x)	—	Any of the following: → 9.14(x) → 9.12(x) → 9.8(x)
9.2(x)	—	Any of the following: → 9.14(x) → 9.12(x) → 9.8(x)
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account. If you do not have a Cisco support contract, you can only look up bugs by ID; you cannot run searches.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs

This section lists open bugs in each version.

Open Bugs in Version 7.14(1.48)

The following table lists select open bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCvp26795	The wrong desktop shortcut link was created after installed the ASDM on windows10 1809.
CSCvr82737	ASDM 7.12.2 doesn't send client certificate during SSL handshake
CSCvs35014	ASDM: Copy from PC not reading local directories (Mac Catalina)
CSCvt34517	ASDM Fails to Launch with error - invalid SHA1 signature file digest for LZMA/LzmaInputStream.class

Open Bugs in Version 7.14(1.46)

The following table lists select open bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCvp26795	The wrong desktop shortcut link was created after installed the ASDM on windows10 1809.
CSCvr82737	ASDM 7.12.2 doesn't send client certificate during SSL handshake
CSCvs35014	ASDM: Copy from PC not reading local directories (Mac Catalina)

Open Bugs in Version 7.14(1)

The following table lists select open bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCvp26795	The wrong desktop shortcut link was created after installed the ASDM on windows10 1809.
CSCvr82737	ASDM 7.12.2 doesn't send client certificate during SSL handshake
CSCvs35014	ASDM: Copy from PC not reading local directories (Mac Catalina)
CSCvt72183	Upgrade from 9.131/7131 to 9141/7141 failing in Appliance mode

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.14(1.48)

There are no resolved bugs in this release.

Resolved Bugs in Version 7.14(1.46)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCvt72183	Upgrade from 9.131/7131 to 9141/7141 failing in Appliance mode

Resolved Bugs in Version 7.14(1)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCvq68530	ASDM: Issue with Cisco clientless SSL VPN and OWA and SSO.
CSCvq80097	ASDM packet tracer destination MAC not showing when switching from routed to transparent context
CSCvr15019	ASA5506 ASDM 7.12.1, a couple of pages/buttons doesn't work
CSCvr78019	Unable to Change Pre-Shared Key Using ASDM with password encryption enabled

End-User License Agreement

For information on the end-user license agreement, go to http://www.cisco.com/go/warranty.

Related Documentation

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