Release Notes for Cisco ASDM, 7.10(x)

This document contains release information for Cisco ASDM Version 7.10(x) for the Cisco ASA series.

Important Notes

- No support in 9.10(1) for the ASA FirePOWER module on the ASA 5506-X series and the ASA 5512-X—The ASA 5506-X series and 5512-X no longer support the ASA FirePOWER module in 9.10(1) and later due to memory constraints. You must remain on 9.9(x) or lower to continue using this module. Other module types are still supported. If you upgrade to 9.10(1), the ASA configuration to send traffic to the FirePOWER module will be erased; make sure to back up your configuration before you upgrade. The FirePOWER image and its configuration remains intact on the SSD. If you want to downgrade, you can copy the ASA configuration from the backup to restore functionality.

- These ciphers are currently unsupported for DTLS 1.2 in FIPS mode for the Firepower 2100:

    - DHE-RSA-AES256-SHA

    - AES256-SHA

    - DHE-RSA-AES128-SHA

    - AES128-SHA

- If you are using SAML authentication with AnyConnect 4.4 or 4.5 and you deploy ASA version 9.10(1), the defaulted SAML behavior is the embedded browser, which is not supported on AnyConnect 4.4 and 4.5. Therefore, you must enable the **saml external-browser** command in tunnel group configuration in order for AnyConnect 4.4 and 4.5 clients to authenticate with SAML using the external (native) browser.

    Note   The **saml external-browser** command is for migration purposes for those upgrading to AnyConnect 4.6 or later. Because of security limitations, use this solution only as part of a temporary migration while upgrading AnyConnect software. The command itself will be depreciated in the future.

- New ROMMON Version 1.1.12 for the ASA 5506-X, 5508-X, and 5516-X—We recommend that you upgrade your ROMMON for several crucial fixes. See https://www.cisco.com/go/asa-firepower-sw, choose your *model* > ASA Rommon Software > 1.1.12. Refer to the release notes on the software download page for more information. To upgrade the ROMMON, see Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X). Note that the ASA running Firepower Threat Defense does not yet support upgrading to this ROMMON version; you can, however, successfully upgrade it in ASA and then reimage to Firepower Threat Defense.

- The RSA toolkit version used in ASA 9.x is different from what was used in ASA 8.4, which causes differences in PKI behavior between these two versions.

  For example, ASAs running 9.x software allow you to import certificates with an Organizational Name Value (OU) field length of 73 characters. ASAs running 8.4 software allow you to import certificates with an OU field name of 60 characters. Because of this difference, certificates that can be imported in ASA 9.x will fail to be imported to ASA 8.4. If you try to import an ASA 9.x certificate to an ASA running version 8.4, you will likely receive the error, "ERROR: Import PKCS12 operation failed.

System Requirements

This section lists the system requirements to run this release.

ASDM Client Operating System and Browser Requirements

The following table lists the supported client operating systems and Java for ASDM when managing both the ASA and the ASA FirePOWER module.
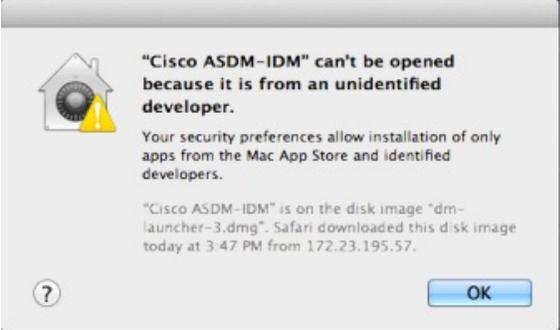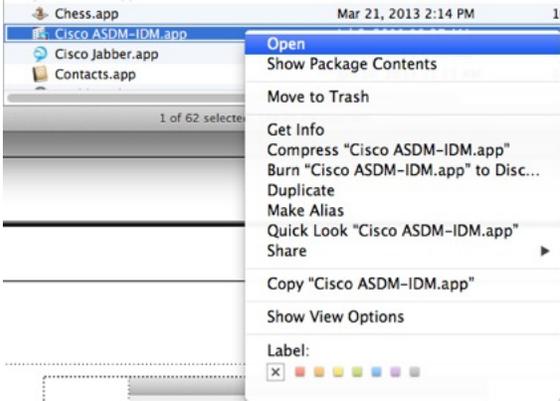
Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

Operating System	Browser				Java SE Plug-in
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): 10 8 7 Server 2012 R2 Server 2012 Server 2008	Yes	Yes	No support	Yes	8.0
Apple OS X 10.4 and later	No support	Yes	Yes	Yes (64-bit version only)	8.0
Ubuntu Linux 14.04 Debian Linux 7	N/A	Yes	N/A	Yes	8.0 (Oracle only; OpenJDK is not supported)

Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
Requires strong encryption license (3DES/AES) on ASA	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.
IE9 for servers	For Internet Explorer 9.0 for servers, the "**Do not save encrypted pages to disk**" option is enabled by default (See **Tools** > **Internet Options** > **Advanced**). This option causes the initial ASDM download to fail. Be sure to disable this option to allow ASDM to download.
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. [OK] **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 — Open Cisco Jabber.app — Show Package Contents Contacts.app Move to Trash 1 of 62 selected 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: **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. [Open] [Cancel]
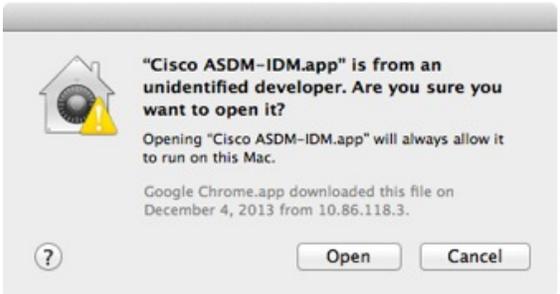
Install an Identity Certificate for ASDM

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.

Unlock   Cancel   **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 9.10(1)/ASDM 7.10(1)

Released: October 25, 2018

Feature	Description
Platform Features	
ASAv VHD custom images for Azure	You can now create your own custom ASAv images on Azure using a compressed VHD image available from Cisco. To deploy using a VHD image, you upload the VHD image to your Azure storage account. Then, you can create a managed image using the uploaded disk image and an Azure Resource Manager template. Azure templates are JSON files that contain resource descriptions and parameter definitions.
ISA 3000 support for FirePOWER module Version 6.3	The previous supported version was FirePOWER 5.4.
Firewall Features	

Feature	Description
Cisco Umbrella support	You can configure the device to redirect DNS requests to Cisco Umbrella, so that your Enterprise Security policy defined in Cisco Umbrella can be applied to user connections. You can allow or block connections based on FQDN, or for suspicious FQDNs, you can redirect the user to the Cisco Umbrella intelligent proxy, which can perform URL filtering. The Umbrella configuration is part of the DNS inspection policy.
	New/Modified screens:
	Configuration > **Firewall** > **Objects** > **Umbrella**, **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **DNS**
GTP inspection enhancements for MSISDN and Selection Mode filtering, anti-replay, and user spoofing protection	You can now configure GTP inspection to drop Create PDP Context messages based on Mobile Station International Subscriber Directory Number (MSISDN) or Selection Mode. You can also implement anti-replay and user spoofing protection.
	New/Modified screens:
	Configuration > **Firewall** > **Objects** > **Inspection Maps** > **GTP** > **Add/Edit** dialog box
Default idle timeout for TCP state bypass	The default idle timeout for TCP state bypass connections is now 2 minutes instead of 1 hour.
Support for removing the logout button from the cut-through proxy login page	If you configure the cut-through proxy to obtain user identity information (the AAA authentication listener), you can now remove the logout button from the page. This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address.
	New/Modified commands: **aaa authentication listener no-logout-button**
	No ASDM support.
	Also in 9.8(3).
Trustsec SXP connection configurable delete hold down timer	The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds.
	New/Modified commands: **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections**
	No ASDM support.
	Also in 9.8(3).
Support for offloading NAT'ed flows in transparent mode.	If you are using flow offload (the **flow-offload enable** and **set connection advanced-options flow-offload** commands), offloaded flows can now include flows that require NAT in transparent mode.
Support for transparent mode deployment for a Firepower 4100/9300 ASA logical device	You can now specify transparent or routed mode when you deploy the ASA on a Firepower 4100/9300.
	New/Modified Firepower Chassis Manager screens:
	Logical Devices > **Add Device** > **Settings**
	New/Modified options: **Firewall Mode** drop-down list
VPN Features	

Feature	Description
Support for legacy SAML authentication	If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6 (or later). This option will be deprecated in the near future. New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles** page **> Connection Profiles** area **> Add** button **> Add AnyConnect Connection Profile** dialog box **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** > page **> Connection Profiles** area **> Add** button **> Add Clientless SSL VPN Connection Profile** dialog box New/Modified options: **SAML External Browser** check box *Also in 9.8(3).*
DTLS 1.2 support for AnyConnect VPN remote access connections.	DTLS 1.2, as defined in RFC- 6347, is now supported for AnyConnect remote access in addition to the currently supported DTLS 1.0 (1.1 version number is not used for DTLS.) This applies to all ASA models except the 5506; and applies when the ASA is acting as a server only, not a client. DTLS 1.2 supports additional ciphers, as well as all current TLS/DTLS cyphers, and a larger cookie size. New/Modified screens: **Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings**
High Availability and Scalability Features	
Cluster control link customizable IP Address for the Firepower 4100/9300	By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id.slot_id*. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. New/Modified Firepower Chassis Manager screens: **Logical Devices** > **Add Device** > **Cluster Information** New/Modified options: **CCL Subnet IP** field
Parallel joining of cluster units per Firepower 9300 chassis	For the Firepower 9300, this feature ensures that the security modules in a chassis join the cluster simultaneously, so that traffic is evenly distributed between the modules. If a module joins very much in advance of other modules, it can receive more traffic than desired, because the other modules cannot yet share the load. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** New/Modified options: **Parallel Join of Units Per Chassis** area

Feature	Description
Cluster interface debounce time now applies to interfaces changing from a down state to an up state	When an interface status update occurs, the ASA waits the number of milliseconds specified in the **health-check monitor-interface debounce-time** command or the ASDM **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** screen before marking the interface as failed and the unit is removed from the cluster. This feature now applies to interfaces changing from a down state to an up state. For example, in the case of an EtherChannel that transitions from a down state to an up state (for example, the switch reloaded, or the switch enabled an EtherChannel), a longer debounce time can prevent the interface from appearing to be failed on a cluster unit just because another cluster unit was faster at bundling the ports. We did not modify any screens.
Active/Backup High Availability for ASAv on Microsoft Azure Government Cloud	The stateless Active/Backup solution that allows for a failure of the active ASAv to trigger an automatic failover of the system to the backup ASAv in the Microsoft Azure public cloud is now available in the Azure Government Cloud. New or modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** **Monitoring** > **Properties** > **Failover** > **Status** **Monitoring** > **Properties** > **Failover** > **History**
Interface Features	
show interface ip brief and **show ipv6 interface** output enhancement to show the supervisor association for the Firepower 2100/4100/9300	For the Firepower 2100/4100/9300, the output of the command is enhanced to indicate the supervisor association status of the interfaces. New/Modified commands: **show interface ip brief**, **show ipv6 interface**
The **set lacp-mode** command was changed to **set port-channel-mode** on the Firepower 2100	The **set lacp-mode** command was changed to **set port-channel-mode** to match the command usage in the Firepower 4100/9300. New/Modified FXOS commands: **set port-channel-mode**
Administrative and Troubleshooting Features	
Support for NTP Authentication on the Firepower 2100	You can now configure SHA1 NTP server authentication in FXOS. New/Modified FXOS commands: **enable ntp-authentication, set ntp-sha1-key-id, set ntp-sha1-key-string** New/Modified Firepower Chassis Manager screens: **Platform Settings** > **NTP** New/Modified options: **NTP Server Authentication: Enable** check box, **Authentication Key** field, **Authentication Value** field
Packet capture support for matching IPv6 traffic without using an ACL	If you use the **match** keyword for the **capture** command, the **any** keyword only matches IPv4 traffic. You can now specify **any4** and **any6** keywords to capture either IPv4 or IPv6 traffic. The **any** keyword continues to match only IPv4 traffic. New/Modified commands: **capture match** No ASDM support.

Feature	Description
Support for public key authentication for SSH to FXOS on the Firepower 2100	You can set the SSH key so you can use public key authentication instead of/as well as password authentication. New/Modified FXOS commands: **set sshkey** No Firepower Chassis Manager support.
Support for GRE and IPinIP encapsulation	When you do a packet capture on interface inside, the output of the command is enhanced to display the GRE and IPinIP encapsulation on ICMP, UDP, TCP, and others. New/Modified commands: **show capture**
Support to enable memory threshold that restricts application cache allocations	You can restrict application cache allocations on reaching certain memory threshold so that there is a reservation of memory to maintain stability and manageability of the device. New/Modified commands: **memory threshold enable, show run memory threshold,clear conf memory threshold**
Support for RFC 5424 logging timestamp	You can enable the logging timestamp as per RFC 5424 format. New/Modified command: **logging timestamp**
Support to display memory usage of TCB-IPS	Shows application level memory cache for TCB-IPS New/Modified command: **show memory app-cache**

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:

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

See the following table for the upgrade path for your version. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Current Version	Interim Upgrade Version	Target Version
9.9(x)	—	Any of the following: → **9.10(x)** → **9.9(x)**
9.8(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)**

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

Current Version	Interim Upgrade Version	Target Version
9.3(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x)
9.2(x)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x)

Current Version	Interim Upgrade Version	Target Version
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.5(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.4(5+)	—	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(1) through 8.4(4)	Any of the following: → 9.0(2), 9.0(3), or 9.0(4) → 8.4(6)	→ **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.3(x)	→ 8.4(6)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.2(x) and earlier	→ 8.4(6)	Any of the following: → **9.10(x)** → **9.9(x)** → **9.8(x)** → 9.7(x) → **9.6(x)** → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 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 in Version 7.10(1)

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

Caveat ID Number	Description
CSCvh80794	Configuring Multicast Route with interface throwing - Error : Required Validation

Resolved Bugs in Version 7.10(1)

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

Caveat ID Number	Description
CSCvh98972	hostname based URL handling while accessing the anyconnect related files in the Multi-Context Mode
CSCvi21519	ASDM 7.8(2)151 "Specified remark does not exist" when editing multiple ACL remarks
CSCvi29218	"any" option is not available for interface in the NAT Page in the VPN Wizard/AC Wizard
CSCvi38815	ASDM deletes remarks when changing log level on an ACL line
CSCvi54306	ASDM shows vxlan as udp-1 when creating an object service or object group service
CSCvi66705	ASDM in multi-context mode not able to be opened by a read-only user
CSCvi87301	ASDM:ASA cluster details not getting displayed 'Page not found' error seen instead for admin context
CSCvj37182	Not able to launch the DAP in Remote access VPN in ASDM
CSCvj46263	ASDM 7.9.2 is trying to delete wrong seq of Access-List if Logging is being used.
CSCvj91403	When editing port-channel via ASDM always asks for MIO port-channel ID
CSCvk71176	ASDM 7.9(2)152 warning "uploaded file is not a valid ASA-SM image"
CSCvm37098	ASDM Trying to edit Site to Site tunnel without making changes removes the Nat Exempt rule

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.