Release Notes for Cisco ASDM, 7.12(x)

Release Notes for Cisco ASDM, 7.12(x)

This document contains release information for Cisco ASDM Version 7.12(x) for the Cisco ASA series.

Important Notes

- **ASDM signed-image support in 9.12(4.50)/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)
- **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.
- **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.
- **SSH security improvements and new defaults in 9.12(1)**—See the following SSH security improvements:
  - SSH version 1 is no longer supported; only version 2 is supported. The **ssh version 1** command will be migrated to **ssh version 2**.
  - Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default (**ssh key-exchange group dh-group14-sha256**). The former default was Group 1 SHA1. Make sure that your SSH client supports Diffie-Hellman Group 14 SHA256. If it does not, you may see an

error such as "Couldn't agree on a key exchange algorithm." For example, OpenSSH supports Diffie-Hellman Group 14 SHA256.

- HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha2-256 only as defined by the **ssh cipher integrity high** command). The former default was the medium set.

- **Diffie-Hellman Group 1 Removal in 9.12(1)**— Diffie-Hellman Group 1 used by the ASA IKE and IPsec modules is considered insecure and has been removed.

  IKEv1: The following subcommands were removed:

  - **crypto ikev1 policy** *priority*:
    - **group 1**

  IKEv2: The following subcommands were removed:

  - **crypto ikev2 policy** *priority*
    - **group 1**

  IPsec: The following subcommands were removed:

  - **crypto ipsec profile** ***name***
    - **set pfs group1**

  SSL: The following commands were removed:

  - **ssl dh-group group1**

  Crypto Map: The following commands were removed:

  - **crypto map** *name sequence* **set pfs group1**
  - **crypto dynamic-map** *name sequence* **set pfs group1**
  - **crypto map** *name sequence* **set ikev1 phase1-mode aggressive group1**

- **No support in 9.10(1) and later 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) or later, 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.

- **The NULL-SHA TLSv1 cipher is deprecated and removed in 9.12(1)**—Because NULL-SHA doesn't offer encryption and is no longer considered secure against modern threats, it will be removed when listing supported ciphers for TLSv1 in the output of **tls-proxy** mode commands/options and **show ssl ciphers all**. The **ssl cipher tlsv1 all** and **ssl cipher tlsv1 custom NULL-SHA** commands will also be deprecated and removed.

- **Local CA server is deprecated in 9.12(1), and will be removed in a later release**—When ASA is configured as local CA server, it is enabled to issue digital certificates, publish Certificate Revocation Lists (CRLs), and securely revoke issued certificates. This feature has become obsolete and hence the **crypto ca server** command is deprecated.
- **The default trustpool is removed in 9.12(1)**—In order to comply with PSB requirement, SEC-AUT-DEFROOT, the "default" trusted CA bundle is removed from the ASA image. As a result, **crypto ca trustpool import default** and **crypto ca trustpool import clean default** commands are also removed along with other related logic. However, in existing deployments, certificates that were previously imported using these command will remain in place.
- **The ssl encryption command is removed in 9.12(1)**—In 9.3(2) the deprecation was announced and replaced by **ssl cipher**. In 9.12(1), **ssl encryption** is removed and no longer supported.

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.

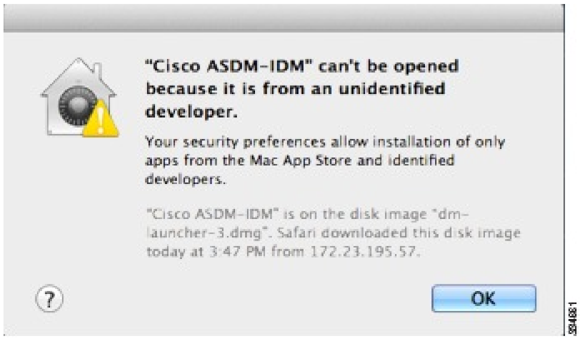
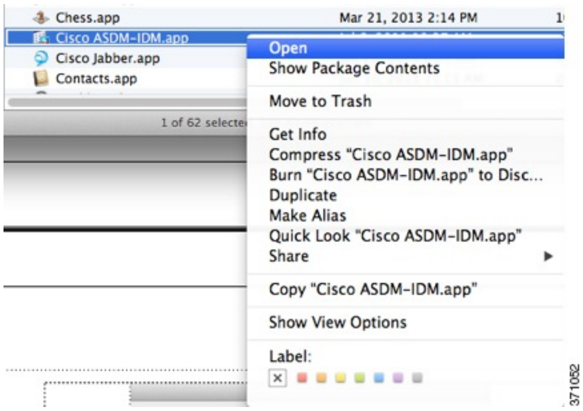
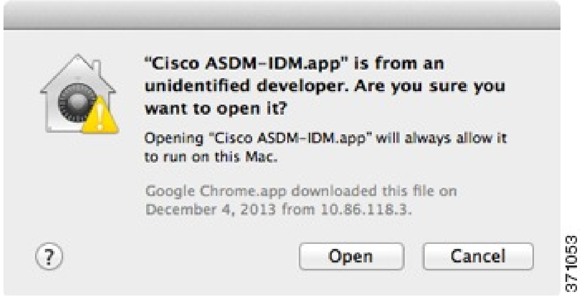
Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

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 4 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	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	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

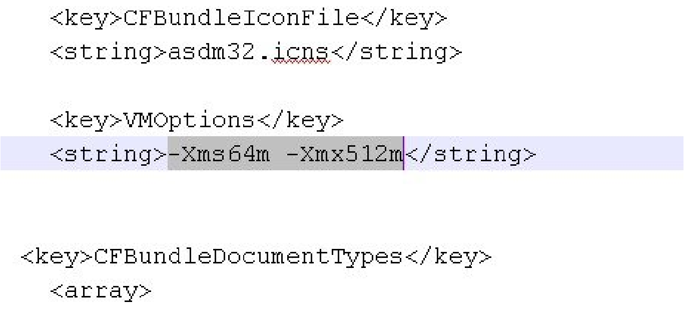
To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

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.

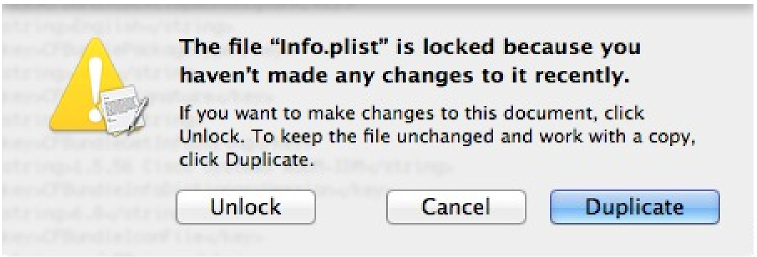


```
  <key>CFBundleIconFile</key>
  <string>asdm32.icns</string>

  <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.

334654

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 9.12(4)

Released: May 26, 2020

Feature	Description
Routing Features	
Multicast IGMP interface state limit raised from 500 to 5000	The multicast IGMP state limit per interface was raised from 500 to 5000. New/Modified commands: **igmp limit** No ASDM support.
Troubleshooting Features	

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.
VPN Features	
Support for configuring the maximum in-negotiation SAs as an absolute value	You can now configure the maximum in-negotiation SAs as an absolute value up to 15000 or a maximum value derived from the maximum device capacity; formerly, only a percentage was allowed. New/Modified commands: **crypto ikev2 limit max-in-negotiation-sa value** No ASDM support.

New Features in ASA 9.12(3)

Released: November 25, 2019

There are no new features in this release.

New Features in ASA 9.12(2)/ASDM 7.12(2)

Released: May 30, 2019

Feature	Description
Platform Features	
Firepower 9300 SM-56 support	We introduced the following security modules: SM-56. Requires FXOS 2.6.1.157 No modified screens.
Administration Features	
Setting the SSH key exchange mode is restricted to the Admin context	You must set the SSH key exchange in the Admin context; this setting is inherited by all other contexts. New/Modified screen: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** > **SSH Settings** > **DH Key Exchange**
ASDM Features	
OpenJRE version of ASDM	You can install a version of ASDM that uses OpenJRE 1.8.x instead of Oracle JRE. The filename of the OpenJRE version is **asdm-openjre-*version*.bin**.

Feature	Description
Tools > **Preferences** option to specify the ASA FirePOWER module local management file folder	You can now specify the location to install ASA FirePOWER module local management files. You must have read/write privileges to the configured location. New/Modified screen: **Tools** > **Preferences** > **SFR Location Wizard** area

New Features in ASA 9.12(1)/ASDM 7.12(1)

Released: March 13, 2019

Feature	Description
Platform Features	
ASA for the Firepower 4115, 4125, and 4145	We introduced the Firepower 4115, 4125, and 4145. Requires FXOS 2.6.1. No modified screens.
Support for ASA and FTD on separate modules of the same Firepower 9300	You can now deploy ASA and FTD logical devices on the same Firepower 9300. Requires FXOS 2.6.1. No modified screens.
Firepower 9300 SM-40 and SM-48 support	We introduced the following two security modules: SM-40 and SM-48. Requires FXOS 2.6.1. No modified screens.
Firewall Features	
GTPv1 release 10.12 support.	The system now supports GTPv1 release 10.12. Previously, the system supported release 6.1. The new support includes recognition of 25 additional GTPv1 messages and 66 information elements. In addition, there is a behavior change. Now, any unknown message IDs are allowed. Previously, unknown messages were dropped and logged. No modified screens.
Cisco Umbrella Enhancements.	You can now identify local domain names that should bypass Cisco Umbrella. DNS requests for these domains go directly to the DNS servers without Umbrella processing. You can also identify which Umbrella servers to use for resolving DNS requests. Finally, you can define the Umbrella inspection policy to fail open, so that DNS requests are not blocked if the Umbrella server is unavailable. New/Modified screens: **Configuration** > **Firewall** > **Objects** > **Umbrella**, **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **DNS**.

Feature	Description
The object group search threshold is now disabled by default.	If you enabled object group search, the feature was subject to a threshold to help prevent performance degradation. That threshold is now disabled by default. You can enable it by using the **object-group-search threshold** command. We changed the following screen: **Configuration** > **Access Rules** > **Advanced**.
Interim logging for NAT port block allocation.	When you enable port block allocation for NAT, the system generates syslog messages during port block creation and deletion. If you enable interim logging, the system generates message 305017 at the interval you specify. The messages report all active port blocks allocated at that time, including the protocol (ICMP, TCP, UDP) and source and destination interface and IP address, and the port block. New/Modified screen: **Configuration** > **Firewall** > **Advanced** > **PAT Port Block Allocation**.
VPN Features	
New **condition** option for **debug aaa**.	The **condition** option was added to the **debug aaa** command. You can use this option to filter VPN debugging based on group name, user name, or peer IP address. No modified screens.
Support for RSA SHA-1 in IKEv2	You can now generate a signature using the RSA SHA-1 hashing algorithm for IKEv2. New/Modified screens:
View the default SSL configuration for both DES and 3DES encryption licenses as well as available ciphers	You can now view the default SSL configuration with and without the 3DES encryption license. In addition, you can view all the ciphers supported on the device. New/Modified commands: **show ssl information** No modified screens.
Add subdomains to webVPN HSTS	Allows domain owners to submit what domains should be included in the HSTS preload list for web browsers. New/Modified screens: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Proxies** > **Enable HSTS Subdomains**field
High Availability and Scalability Features	
Per-site gratuitous ARP for clustering	The ASA now generates gratuitous ARP (GARP) packets to keep the switching infrastructure up to date: the highest priority member at each site periodically generates GARP traffic for the global MAC/IP addresses. When using per-site MAC and IP addresses, packets sourced from the cluster use a site-specific MAC address and IP address, while packets received by the cluster use a global MAC address and IP address. If traffic is not generated from the global MAC address periodically, you could experience a MAC address timeout on your switches for the global MAC address. After a timeout, traffic destined for the global MAC address will be flooded across the entire switching infrastructure, which can cause performance and security concerns. GARP is enabled by default when you set the site ID for each unit and the site MAC address for each Spanned EtherChannel. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Site Periodic GARP** field

Feature	Description
Multiple context mode HTTPS resource management	You can now set the maximum number of non-ASDM HTTPS sessions in a resource class. By default, the limit is set to 6 per context, the maximum. You can use up to 100 HTTPS sesssions across all contexts. New/Modified commands: **limit-resource http** No ASDM support.
Routing Features	
OSPF Keychain support for authentication	OSPF authenticates the neighbor and route updates using MD5 keys. In ASA, the keys that are used to generate the MD5 digest had no lifetime associated with it. Thus, user intervention was required to change the keys periodically. To overcome this limitation, OSPFv2 supports MD5 authentication with rotating keys. Based on the accept and send lifetimes of Keys in KeyChain, OSPF authenticates, accepts or rejects keys and forms adjacency. New/Modified screens: • **Configuration** > **Device Setup** > **Key Chain** • **Configuration** > **Device Setup** > **Routing** > **OSPF** > **Setup** > **Authentication** • **Configuration** > **Device Setup** > **Routing** > **OSPF** > **Setup** > **Virtual Link**
Certificate Features	
Local CA configurable FQDN for enrollment URL	To make the FQDN of the enrollment URL configurable instead of using the ASA's configured FQDN, a new CLI option is introduced. This new option is added to the **smpt** mode of **crypto ca server**. New/Modified commands: **fqdn**
Administrative, Monitoring, and Troubleshooting Features	
enable password change now required on a login	The default **enable** password is blank. When you try to access privileged EXEC mode on the ASA, you are now required to change the password to a value of 3 characters or longer. You cannot keep it blank. The **no enable password** command is no longer supported. At the CLI, you can access privileged EXEC mode using the **enable** command, the **login** command (with a user at privilege level 2+), or an SSH or Telnet session when you enable **aaa authorization exec auto-enable**. All of these methods require you to set the enable password. This password change requirement is not enforced for ASDM logins. In ASDM, by default you can log in without a username and with the **enable** password. No modified screens.

Feature	Description
Configurable limitation of admin sessions	You can configure the maximum number of aggregate, per user, and per-protocol administrative sessions. Formerly, you could configure only the aggregate number of sessions. This feature does not affect console sessions. Note that in multiple context mode, you cannot configure the number of HTTPS sessions, where the maximum is fixed at 5 sessions. The **quota management-session** command is also no longer accepted in the system configuration, and is instead available in the context configuration. The maximum aggregate sessions is now 15; if you configured 0 (unlimited) or 16+, then when you upgrade, the value is changed to 15. New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **Management Session Quota**
Notifications for administrative privilege level changes	When you authenticate for enable access (**aaa authentication enable console**) or allow privileged EXEC access directly (**aaa authorization exec auto-enable**), then the ASA now notifies users if their assigned access level has changed since their last login. New/Modified screens: **Status** bar **> Login History** icon
NTP support on IPv6	You can now specify an IPv6 address for the NTP server. New/Modified screens: **Configuration** > **Device Setup** > **System Time** > **NTP** > **Add** button **> Add NTP Server Configuration** dialog box
SSH stronger security	See the following SSH security improvements: • Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default. The former default was Group 1 SHA1. • HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha2-256 only). The former default was the medium set. New/Modified screens: • **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** • **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**
Allow non-browser-based HTTPS clients to access the ASA	You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed. New/Modified screens. **Configuration** > **Device Management** > **Management Access** > **HTTP Non-Browser Client Support**
Capture control plane packets only on the cluster control link	You can now capture control plane packets only on the cluster control link (and no data plane packets). This option is useful in the system in multiple context mode where you cannot match traffic using an ACL. New/Modified screens: **Wizards** > **Packet Capture Wizard** > **Cluster Option**

Feature	Description
debug conn command	The **debug conn** command was added to provide two history mechanisms that record connection processing. The first history list is a per-thread list that records the operations of the thread. The second history list is a list that records the operations into the conn-group. When a connection is enabled, processing events such as a connection lock, unlock, and delete are recorded into the two history lists. When a problem occurs, these two lists can be used to look back at the processing to determine the incorrect logic. New/Modified commands: **debug conn**
show tech-support includes additional output	The output of the **show tech-support** is enhanced to display the output of the following: • **show ipv6 interface** • **show aaa-server** • **show fragment** New/Modified commands: **show tech-support**
ASDM support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP**
Configurable graph update interval for the ASDM Home pane for the System in multiple-context mode	For the System in multiple context mode, you can now set the amount of time between updates for the graphs on the Home pane. New/Modified screens: **Tools** > **Preferences** > **Graph User time interval in System Context**

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
9.10(x)	—	Any of the following: → 9.12(x)
9.9(x)	—	Any of the following: → 9.12(x)
9.8(x)	—	Any of the following: → 9.12(x)
9.7(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.6(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.5(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.4(x)	—	Any of the following: → 9.12(x) → 9.8(x)
9.3(x)	—	Any of the following: → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.2(x)	—	Any of the following: → 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: → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → **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)

Current Version	Interim Upgrade Version	Target Version
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 7.12(2)

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

Caveat ID Number	Description
CSCvo10929	Access list Error - while uncheck RSA Signature in Site-to-Site VPN

Open Bugs in Version 7.12(1)

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

Caveat ID Number	Description
CSCvo10929	Access list Error - while uncheck RSA Signature in Site-to-Site VPN

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.12(2)

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

Caveat ID Number	Description
CSCvo26166	ASDM unable to apply external group-policy to AnyConnect / IKEv1 / IKEv2 RA tunnel-group
CSCvp01248	Interface edit button on ASDM startup wizard does not work.
CSCvp67520	ASDM 7.12.1: Editing Existing NAT rule fails to successfully push to the ASA (9.12.1)
CSCvp69678	AnyConnect images disappear from ASDM

Resolved Bugs in Version 7.12(1)

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

Caveat ID Number	Description
CSCuz09934	ASDM : Password Expiry warning message not displayed after Login
CSCvi21519	ASDM 7.8(2)151 "Specified remark does not exist" when editing multiple ACL remarks
CSCvi38815	ASDM deletes remarks when changing log level on an ACL line
CSCvi66705	ASDM in multi-context mode not able to be opened by a read-only user

Caveat ID Number	Description
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
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"
CSCvm21655	ASDM , ACL remarks are getting duplicated and showing in every sub entry
CSCvm37098	ASDM Trying to edit Site to Site tunnel without making changes removes the Nat Exempt rule
CSCvm64354	ASDM image special release with charts update frequency set to 30 seconds
CSCvm68799	ASDM restore feature performed overwriting a file of AC profile by multiple same category files
CSCvn08410	Enabling split-tunnel-all-dns from CLI doesn't reflect on ASDM. ASDM to CLI works.
CSCvn20484	ASDM throws an error when trying to diable/negate a rule action if the class-map has a single rule
CSCvn32924	Firepower tabs don't visible on ASDM on ASA v9.9 (2) with ASDM v7.9.2.X on Multi-Context Enviorment.
CSCvn38874	ASDM error when replace TCT/HTTP with IP on ACL
CSCvn72617	ASDM: Nested TCP-UDP Object Groups Not Showed as Listed nor the Child objects
CSCvo23506	ASDM in multi-context mode not able to be opened with message "show flow-offload info"

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.