Release Notes for Cisco ASDM, 7.13(x)

Release Notes for Cisco ASDM, 7.13(x)

This document contains release information for Cisco ASDM Version 7.13(x) for the Cisco ASA series.

Important Notes

- **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 to 9.12 or earlier**—For a Firepower 2100 with a fresh installation of 9.13 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 you need to clear your configuration using the FXOS erase configuration command. This problem does not occur if you originally upgraded to 9.13 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.

- **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.

- **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.

- **Beginning with 9.13(1), the ASA establishes an LDAP/SSL connection only if one of the following certification criteria is satisfied**:

  - The LDAP server certificate is trusted (exists in a trustpoint or the ASA trustpool) and is valid.

  - A CA certificate from servers issuing chain is trusted (exists in a trustpoint or the ASA trustpool) and all subordinate CA certificates in the chain are complete and valid.

- **Local CA server is removed in 9.13(1)**—When the ASA is configured as local CA server, it can 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 removed.

- **Removal of CRL Distribution Point commands**—The static CDP URL configuration commands, namely **crypto-ca-trustpoint crl** and **crl url** were removed with other related logic. The CDP URL was moved to match certificate command.

> **Note** The CDP URL configuration was enhanced to allow multiple instances of the CDP override for a single map (refer CSCvu05216).

- **Removal of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was removed.

  The following subcommands are removed:

  - **revocation-check crl none**

  - **revocation-check ocsp none**

  - **revocation-check crl ocsp none**

  - **revocation-check ocsp crl none**

Thus, after an upgrade, any revocation-check command that is no longer supported will transition to the new behavior by ignoring the trailing none.

> **Note** These commands were restored later (refer CSCtb41710).

- **Low-Security Cipher Deprecation**— Several encryption ciphers used by the ASA IKE, IPsec, and SSH modules are considered insecure and have been deprecated. They will be removed in a later release.

  IKEv1: The following subcommands are deprecated:

  - **crypto ikev1 policy** *priority*:

    - **hash md5**

    - **encryption 3des**

    - **encryption des**

    - **group 2**

    - **group 5**

  IKEv2: The following subcommands are deprecated:

  - **crypto ikev2 policy** *priority*

    - **integrity md5**

    - **prf md5**

    - **group 2**

    - **group 5**

    - **group 24**

    - **encryption 3des**

    - **encryption des** (this command is still available when you have the DES encryption license only)

    - **encryption null**

  IPsec: The following commands are deprecated:

  - **crypto ipsec ikev1 transform-set** *name* **esp-3des esp-des esp-md5-hmac**

  - **crypto ipsec ikev2 ipsec-proposal** *name*

    - **protocol esp integrity md5**

    - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**

  - **crypto ipsec profile** *name*

    - **set pfs group2 group5 group24**

SSH: The following commands are deprecated:

- **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**

- **ssh key-exchange group dh-group1-sha1**

SSL: The following commands are deprecated:

- **ssl dh-group group2**

- **ssl dh-group group5**

- **ssl dh-group group24**

Crypto Map: The following commands are deprecated:

- **crypto map** *name sequence* **set pfs group2**

- **crypto map** *name sequence* **set pfs group5**

- **crypto map** *name sequence* **set pfs group24**

- **crypto map** *name sequence* **set ikev1 phase1-mode aggressive group2**

- **crypto map** *name sequence* **set ikev1 phase1-mode aggressive group5**

- **In 9.13(1), Diffie-Hellman Group 14 is now the default** for the **group** command under **crypto ikev1 policy**, **ssl dh-group**, and **crypto ikev2 policy** for IPsec PFS using **crypto map set pfs**, **crypto ipsec profile**, **crypto dynamic-map set pfs**, and **crypto map set ikev1 phase1-mode**. The former default Diffie-Hellman group was Group 2.

When you upgrade from a pre-9.13(1) release, if you need to use the old default (Diffie-Hellman Group 2), then you must *manually* configure the DH group as **group 2** or else your tunnels will default to Group 14. Because group 2 will be removed in a future release, you should move your tunnels to group 14 as soon as possible.

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**).
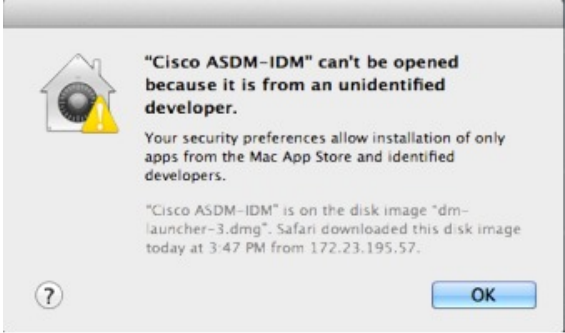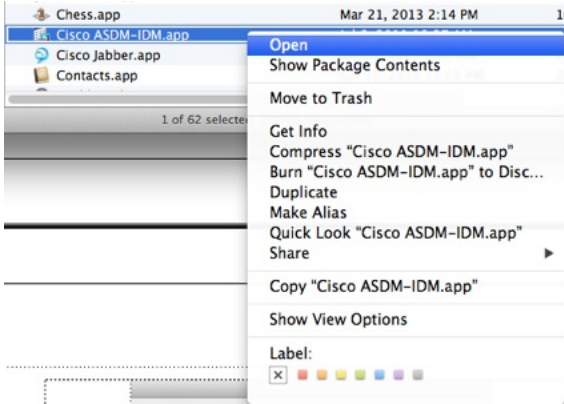
Note ASDM is not tested on Linux.

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

Operating System	Browser				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
• Microsoft Windows (English and Japanese): • 10 **Note** See Windows 10 in ASDM Compatibility Notes, on page 5 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 Firepower Management Center to manage the FirePOWER module when using ASDM for ASA management.) • Server 2012 R2 • Server 2012 • Server 2008	Yes	Yes	No support	Yes	8.0	1.8 **Note** No support for Windows 7 32-bit
Apple OS X 10.4 and later	No support	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.

OK

1. To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose **Open**.

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 |

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.
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.

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:

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 ASDM 7.13(1.101)

Released: May 7, 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 ASA 9.13(1)/ASDM 7.13(1)

Released: September 25, 2019

Feature	Description
Platform Features	
ASA for the Firepower 1010	We introduced the ASA for the Firepower 1010. This desktop model includes a built-in hardware switch and Power-Over-Ethernet+ (PoE+) support. New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Edit** > **Switch Port** • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Edit** > **Power Over Ethernet** • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add VLAN Interface** • **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** • **Configuration** > **Device Setup** > **System Time** > **Clock** • **Monitoring** > **Interfaces** > **L2 Switching** • **Monitoring** > **Interfaces** > **Power Over Ethernet**
ASA for the Firepower 1120, 1140, and 1150	We introduced the ASA for the Firepower 1120, 1140, and 1150. New/Modified screens: • **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** • **Configuration** > **Device Setup** > **System Time** > **Clock**
Firepower 2100 Appliance mode	The Firepower 2100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). You can run the Firepower 2100 in the following modes: • Appliance mode (now the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI. • Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Firepower Chassis Manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI. If you are upgrading to 9.13(1), the mode will remain in Platform mode. New/Modified screens: • **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** • **Configuration** > **Device Setup** > **System Time** > **Clock**

Feature	Description
DHCP reservation	The ASA DHCP server now supports DHCP reservation. You can assign a static IP address from the defined address pool to a DHCP client based on the client's MAC address. No modified screens.
ASAv minimum memory requirement	The minimum memory requirement for the ASAv is now 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version without increasing the memory of your ASAv VM. You can also redeploy a new ASAv VM with version 9.13(1). No modified screens.
ASAv MSLA Support	The ASAv supports Cisco's Managed Service License Agreement (MSLA) program, which is a software licensing and consumption framework designed for Cisco customers and partners who offer managed software services to third parties. MSLA is a new form of Smart Licensing where the licensing Smart Agent keeps track of the usage of licensing entitlements in units of time. New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
ASAv Flexible Licensing	Flexible Licensing is a new form of Smart Licensing where any ASAv license now can be used on any supported ASAv vCPU/memory configuration. Session limits for AnyConnect and TLS proxy will be determined by the ASAv platform entitlement installed rather than a platform limit tied to a model type. New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
ASAv for AWS support for the C5 instance; expanded support for C4, C3, and M4 instances	The ASAv on the AWS Public Cloud now supports the C5 instance (c5.large, c5.xlarge, and c5.2xlarge). In addition, support has been expanded for the C4 instance (c4.2xlarge and c4.4xlarge); C3 instance (c3.2xlarge, c3.4xlarge, and c3.8xlarge); and M4 instance (m4.2xlarge and m4.4xlarge). No modified screens.
ASAv for Microsoft Azure support for more Azure virtual machine sizes	The ASAv on the Microsoft Azure Public Cloud now supports more Linux virtual machine sizes: • Standard_D4, Standard_D4_v2 • Standard_D8_v3 • Standard_DS3, Standard_DS3_v2 • Standard_DS4, Standard_DS4_v2 • Standard_F4, Standard_F4s • Standard_F8, Standard_F8s Earlier releases only supported the Standard_D3 and Standard_D3_v2 sizes. No modified screens.

Feature	Description
ASAv enhanced support for DPDK	The ASAv supports enhancements to the Data Plane Development Kit (DPDK) to enable support for multiple NIC queues, which allow multi-core CPUs to concurrently and efficiently service network interfaces. This applies to all ASAv hypervisors except Microsoft Azure and Hyper-V. **Note** DPDK support was introduced in release ASA 9.10(1)/ASDM 7.13(1). No modified screens.
ASAv support for VMware ESXi 6.7	The ASAv virtual platform supports hosts running on VMware ESXi 6.7. New VMware hardware versions have been added to the *vi.ovf* and *esxi.ovf* files to enable optimal performance and usability of the ASAv on ESXi 6.7. No modified screens.
Increased VLANs for the ISA 3000	The maximum VLANs for the ISA 3000 with the Security Plus license increased from 25 to 100.
Firewall Features	
Location logging for mobile stations (GTP inspection).	You can configure GTP inspection to log the initial location of a mobile station and subsequent changes to the location. Tracking location changes can help you identify possibly fraudulent roaming charges. New/Modified screens: **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **GTP**.
GTPv2 and GTPv1 release 15 support.	The system now supports GTPv2 3GPP 29.274 V15.5.0. For GTPv1, support is up to 3GPP 29.060 V15.2.0. The new support includes recognition of 2 additional messages and 53 information elements. No modified screens.
Mapping Address and Port-Translation (MAP-T)	Mapping Address and Port (MAP) is primarily a feature for use in service provider (SP) networks. The service provider can operate an IPv6-only network, the MAP domain, while supporting IPv4-only subscribers and their need to communicate with IPv4-only sites on the public Internet. MAP is defined in RFC7597, RFC7598, and RFC7599. New/Modified commands: **Configuration** > **Device Setup** > **CGNAT Map**, **Monitoring** > **Properties** > **MAP Domains**.
Increased limits for AAA server groups and servers per group.	You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4). In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged. We modified the AAA screens to accept these new limits.
TLS proxy deprecated for SCCP (Skinny) inspection.	The **tls-proxy** keyword, and support for SCCP/Skinny encrypted inspection, was deprecated. The keyword will be removed from the **inspect skinny** command in a future release.
VPN Features	

Feature	Description
HSTS Support for WebVPN as Client	A new CLI mode under WebVPN mode called http-headers was added so that WebVPN could transform HTTP references to HTTPS references for hosts that are HSTS. Configures whether the user agent should allow the embedding of resources when sending this header for WebVPN connections from the ASA to browsers. New/Modified screens: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Proxies**.
Diffie-Hellman groups 15 and 16 added for key exchange	To add support for Diffie-Hellman groups 15 and 16, we modified few **crypto** commands to accept these new limits. **crypto ikev2 policy <index> group <number>** and **crypto map <map-name> <map-index> set pfs <group>.**
show asp table vpn-context enhancement to output	To enhance debug capability, these vpn context counters were added to the output: Lock Err, No SA, IP Ver Err, and Tun Down. New/Modified commands: **show asp table vpn-context** (output only).
Immediate session establishment when the maximum remote access VPN session limit is reached.	When a user reaches the maximum session (login) limit, the system deletes the user's oldest session and waits for the deletion to complete before establishing the new session. This can prevent the user from successfully connecting on the first attempt. You can remove this delay and have the system establish the new connection without waiting for the deletion to complete. New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** Add/Edit dialog box, **General** tab.
High Availability and Scalability Features	
Initiator and responder information for Dead Connection Detection (DCD), and DCD support in a cluster.	If you enable Dead Connection Detection (DCD), you can use the **show conn detail** command to get information about the initiator and responder. Dead Connection Detection allows you to maintain an inactive connection, and the **show conn** output tells you how often the endpoints have been probed. In addition, DCD is now supported in a cluster. No modified screens.

Monitor the traffic load for a cluster	You can now monitor the traffic load for cluster members, including total connection count, CPU and memory usage, and buffer drops. If the load is too high, you can choose to manually disable clustering on the unit if the remaining units can handle the load, or adjust the load balancing on the external switch. This feature is enabled by default.
	
	New/Modified screens:
	
	  • **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Enable Cluster Load Monitor** check box
	
	  • **Monitoring** > **ASA Cluster** > **Cluster Load-Monitoring**

Feature	Description
Accelerated cluster joining	When a data unit has the same configuration as the control unit, it will skip syncing the configuration and will join faster. This feature is enabled by default. This feature is configured on each unit, and is not replicated from the control unit to the data unit. **Note** Some configuration commands are not compatible with accelerated cluster joining; if these commands are present on the unit, even if accelerated cluster joining is enabled, configuration syncing will always occur. You must remove the incompatible configuration for accelerated cluster joining to work. Use the **show cluster info unit-join-acceleration incompatible-config** to view incompatible configuration. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Enable config sync accelleration** check box
Routing Features	
SMTP configuration enhancement	You can optionally configure the SMTP server with primary and backup interface names to enable ASA for identifying the routing table to be used for logging—management routing table or data routing table. If no interface is provided, ASA would refer to management routing table lookup, and if no proper route entry is present, it would look at the data routing table.
Support to set NSF wait timer	OSPF routers are expected to set the RS-bit in the EO-TLV attached to a Hello packet when it is not known whether all neighbors are listed in the packet, and the restarting router require to preserve their adjacencies. However, the RS-bit value must not be longer than the RouterDeadInterval seconds. The **timers nsf wait** command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds.
Support to set tftp blocksize	The typical blocksize fixed for tftp file transfer is 512-octets. A new command, **tftp blocksize**, is introduced to configure a larger blocksize and thereby enhance the tftp file transfer speed. You can set a blocksize varying from 513 to 8192 octets. The new default blocksize is 1456 octets. The **no** form of this command will reset the blocksize to the older default value—512 octets. The **timers nsf wait** command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds.
Certificate Features	
Support to view FIPS status	The **show running-configuration fips** command displayed the FIPS status only when fips was enabled. In order to know the operational state, the **show fips** command was introduced where, it displays the fips status when an user enables or disables fips that is in disabled or enabled state. This command also displays the status for rebooting the device after an enable or disable action.
CRL cache size increased	To prevent failure of large CRL downloads, the cache size was increased, and the limit on the number of entries in an individual CRL was removed. • Increased the total CRL cache size to 16 MB per context for multi-context mode. • Increased the total CRL cache size to 128 MB for single-context mode.

Feature	Description
Modifications to the CRL Distribution Point commands	The static CDP URL configuration commands are removed and moved to the match certificate command. New/Modified screens: **Configuration** > **Device Management** > **Certificate Management** > **CA Certificates** The static CDP URL was re-introduced in 9.13(1)12 to the match certificate command.
Administrative and Troubleshooting Features	
Management access when the Firepower 1000, Firepower 2100 Appliance mode is in licensing evaluation mode	The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager. **Note** If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature. No modified screens.
Additional NTP authentication algorithms	Formerly, only MD5 was supported for NTP authentication. The ASA now supports the following algorithms: • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC New/Modified screens: **Configuration** > **Device Setup** > **System Time** > **NTP** > **Add** button **> Add NTP Server Configuration** dialog box **> Key Algorithm** drop-down list
ASA Security Service Exchange (SSE) Telemetry Support for the Firepower 4100/9300	With Cisco Success Network enabled in your network, device usage information and statistics are provided to Cisco which is used to optimize technical support. The telemetry data that is collected on your ASA devices includes CPU, memory, disk, or bandwidth usage, license usage, configured feature list, cluster/failover information and the like. New/Modified screens: • **Configuration** > **Device Management** > **Telemetry** • **Monitoring** > **Properties** > **Telemetry**

Feature	Description
SSH encryption ciphers are now listed in order from highest to lowest security for pre-defined lists	SSH encryption ciphers are now listed in order from highest security to lowest security for pre-defined lists (such as medium or high). In earlier releases, they were listed from lowest to highest, which meant that a low security cipher would be proposed before a high security cipher. New/Modified screens: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**
show tech-support includes additional output	The output of **show tech-support** is enhanced to display the output of the following: **show flow-offload info detail** **show flow-offload statistics** **show asp table socket** New/Modified commands: **show tech-support** (output only).
Enhancement to **show-capture asp_drop** output to include drop location information	While troubleshooting using ASP drop counters, the exact location of the drop is unknown, especially when the same ASP drop reason is used in many different places. This information is critical in finding root cause of the drop. With this enhancement, the ASP drop details such as the build target, ASA release number, hardware model, and ASLR memory text region (to facilitate the decode of drop location) are shown. New/Modified commands: **show-capture asp_drop**
Modifications to **debug crypto ca**	The **debug crypto ca transactions** and **debug crypto ca messages** options are consolidated to provide all applicable content into the **debug crypto ca** command itself. Also, the number of available debugging levels are reduced to 14. New/Modified commands: **debug crypto ca**
FXOS Features for the Firepower 1000 and 2100	
Secure Erase	The secure erase feature erases all data on the SSDs so that data cannot be recovered even by using special tools on the SSD itself. You should perform a secure erase in FXOS when decomissioning the device. New/Modified FXOS commands: **erase secure** (local-mgmt) Supported models: Firepower 1000 and 2100
Configurable HTTPS protocol	You can set the SSL/TLS versions for FXOS HTTPS acccess. New/Modified FXOS commands: **set https access-protocols** Supported models: Firepower 2100 in Platform Mode

Feature	Description
FQDN enforcement for IPSec and Keyrings	For FXOS, you can configure FQDN enforcement so that the FDQN of the peer needs to match the DNS Name in the X.509 Certificate presented by the peer. For IPSec, enforcement is enabled by default, except for connections created prior to 9.13(1); you must manually enable enforcement for those old connections. For keyrings, all hostnames must be FQDNs, and cannot use wild cards.
	New/Modified FXOS commands: **set dns**, **set e-mail**, **set fqdn-enforce**, **set ip**, **set ipv6**, **set remote-address**, **set remote-ike-id**
	Removed commands: **fi-a-ip**, **fi-a-ipv6**, **fi-b-ip**, **fi-b-ipv6**
	Supported models: Firepower 2100 in Platform Mode
New IPSec ciphers and algorithms	We added the following IKE and ESP ciphers and algorithms to configure an IPSec tunnel to encrypt FXOS management traffic:
	• Ciphers—aes192. Existing ciphers include: aes128, aes256, aes128gcm16.
	• Pseudo-Random Function (PRF) (IKE only)—prfsha384, prfsha512, prfsha256. Existing PRFs include: prfsha1.
	• Integrity Algorithms—sha256, sha384, sha512, sha1_160. Existing algorithms incldue: sha1.
	• Diffie-Hellman Groups—curve25519, ecp256, ecp384, ecp521,modp3072, modp4096. Existing groups include: modp2048.
	No modified FXOS commands.
	Supported models: Firepower 2100 in Platform Mode
SSH authentication enhancements	We added the following SSH server encryption algoritghms for FXOS:
	• aes128-gcm@openssh.com
	• aes256-gcm@openssh.com
	• chacha20-poly@openssh.com
	We added the following SSH server key exchange methods for FXOS:
	• diffie-hellman-group14-sha256
	• curve25519-sha256
	• curve25519-sha256@libssh.org
	• ecdh-sha2-nistp256
	• ecdh-sha2-nistp384
	• ecdh-sha2-nistp521
	New/Modified FXOS commands: **set ssh-server encrypt-algorithm**, **set ssh-server kex-algorithm**
	Supported models: Firepower 2100 in Platform Mode

Feature	Description
EDCS keys for X.509 Certificates	You can now use EDCS keys for FXOS certificates. Formerly, only RSA keys were supported.
	New/Modified FXOS commands: **set elliptic-curve**, **set keypair-type**
	Supported models: Firepower 2100 in Platform Mode
User password improvements	We added FXOS password security improvements, including the following:
	• User passwords can be up to 127 characters. The old limit was 80 characters.
	• Strong password check is enabled by default.
	• Prompt to set admin password.
	• Password expiration.
	• Limit password reuse.
	New/Modified Firepower Chassis Manager screens:
	• **System** > **User Management** > **Local Users**
	• **System** > **User Management** > **Settings**
	Supported models: Firepower 2100 in Platform Mode

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
9.12(x)	—	Any of the following: → 9.13(x)
9.10(x)	—	Any of the following: → 9.13(x) → **9.12(x)**
9.9(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x)
9.8(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x)
9.7(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**

Current Version	Interim Upgrade Version	Target Version
9.6(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.5(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.3(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

Current Version	Interim Upgrade Version	Target Version
9.2(x)	—	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(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: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 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: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.13(x) → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.5(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.2(x) and earlier	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(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 7.13(1.101)

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

Caveat ID Number	Description
CSCvo81009	WM Desktop	switchport trunk allowed vlan vlan_range not accepting ranges
CSCvq87624	ASDM: unable to create A/S or A/A HA in multi-context mode
CSCvt34517	ASDM Fails to Launch with error - invalid SHA1 signature file digest for LZMA/LzmaInputStream.class

Open Bugs in Version 7.13(1)

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

Caveat ID Number	Description
CSCvo81009	WM Desktop | switchport trunk allowed vlan vlan_range not accepting ranges
CSCvq87624	ASDM: unable to create A/S or A/A HA in multi-context mode

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.13(1.101)

There are no resolved bugs in this release.

Resolved Bugs in Version 7.13(1)

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

Caveat ID Number	Description
CSCvj24773	AC ASDM profile editore - mixes different profile settings when editing multiple profiles
CSCvn74352	ASDM Not Properly Displaying ASA Cluster Dashboard
CSCvp38825	NAT exemption rules with DM_INLINE objects should not be modified when VPN profile is deleted

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.