

# Release Notes for Cisco ASDM, 7.15(x)

---

**First Published:** 2020-11-02

**Last Modified:** 2019-05-24

## Release Notes for Cisco ASDM, 7.15(x)

This document contains release information for Cisco ASDM Version 7.15(x) for the Cisco ASA series.

### Important Notes

- **No support in ASA 9.15(1) and later for the ASA 5525-X, ASA 5545-X, and ASA 5555-X**—ASA 9.14(x) is the last supported version. For the ASA FirePOWER module, the last supported version is 6.6.
  - **Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1)**—Limited support will continue on releases prior to 9.17(1).
  - **For the Firepower 1010, invalid VLAN IDs can cause problems**—Before you upgrade to 9.15(1), make sure you are not using a VLAN for switch ports in the range 3968 to 4047. These IDs are for internal use only, and 9.15(1) includes a check to make sure you are not using these IDs. For example, if these IDs are in use after upgrading a failover pair, the failover pair will go into a suspended state. See [CSCvw33057](#) for more information.
  - **ASDM Cisco.com Upgrade Wizard failure on Firepower 1000 and 2100 in Appliance mode in 9.13**—The ASDM Cisco.com Upgrade Wizard does not work for upgrading from 9.13 (**Tools > Check for ASA/ASDM Updates**). The wizard can upgrade ASDM from 7.13, but the ASA image upgrade is grayed out. ([CSCvt72183](#)) As a workaround, use one of the following methods:
    - Use **Tools > Upgrade Software from Local Computer** for both ASA and ASDM.
    - Use **Tools > Check for ASA/ASDM Updates** to upgrade ASDM; then use the new ASDM to upgrade the ASA image. Note that you may see a **Fatal Installation Error**; in this case, click **OK**. You must then set the boot image manually on the **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration** screen. Save the configuration and reload the ASA.
  - **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.

- **SAMLv1 feature deprecation**—Support for SAMLv1 is deprecated.
- **Low-Security Cipher Removal in ASA 9.15(1)**—Support for the following less secure ciphers used by IKE and IPsec have been removed:
  - Diffie-Hellman groups: 2 and 24
  - Encryption algorithms: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256, NULL, ESP-3DES, ESP-DES, ESP-MD5-HMAC
  - Hash algorithms: MD5




---

**Note** Low-security SSH and SSL ciphers have not yet been removed.

---

Before you upgrade from an earlier version of ASA to Version 9.15(1), you must update your VPN configuration to use the ciphers supported in 9.15(1), or else the old configuration will be rejected. When the configuration is rejected, one of the following actions will occur, depending on the command:

- The command will use the default cipher.
- The command will be removed.

Fixing your configuration before upgrading is especially important for clustering or failover deployments. For example, if the secondary unit is upgraded to 9.15(1), and the removed ciphers are synced to this unit from the primary, then the secondary unit will reject the configuration. This rejection might cause unexpected behavior, like failure to join the cluster.

**IKEv1:** The following subcommands are removed:

- **crypto ikev1 policy *priority*:**
  - **hash md5**
  - **encryption 3des**
  - **encryption des**
  - **group 2**

**IKEv2:** The following subcommands are removed:

- **crypto ikev2 policy *priority*:**
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**

- **encryption 3des**
- **encryption des**
- **encryption null**

**IPsec:** The following subcommands are removed:

- **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 group24**

**Crypto Map:** The following subcommands are removed:

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **Re-introduction of CRL Distribution Point configuration**—The static CDP URL configuration option, that was removed in 9.13(1), was re-introduced in the **match-certificate** command.
- **Restoration of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was restored.

The following subcommands were restored:

- **revocation-check crl none**
- **revocation-check ocsp none**
- **revocation-check crl ocsp none**
- **revocation-check ocsp crl none**

## System Requirements

ASDM requires a computer with a CPU with at least 4 cores. Fewer cores can result in high memory usage.

### ASDM Java Requirements

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

The Oracle version of ASDM is included in the ASA package; if you want to use the OpenJRE version, you will need to copy it to the ASA and configure the ASA to use that version of ASDM.



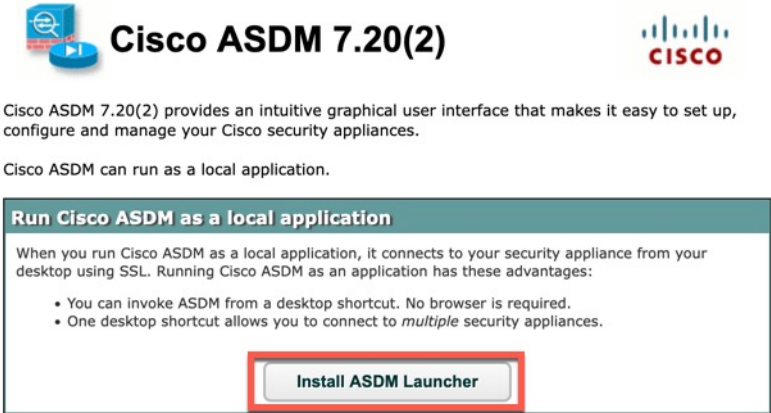
**Note** ASDM is not supported on Linux.

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

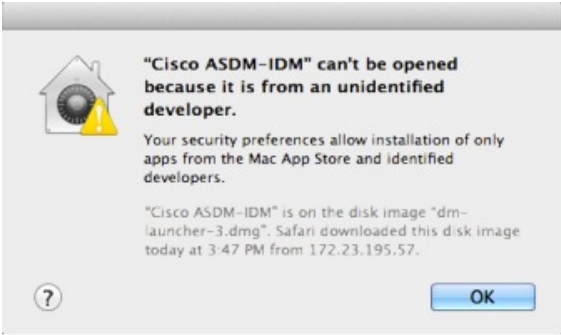
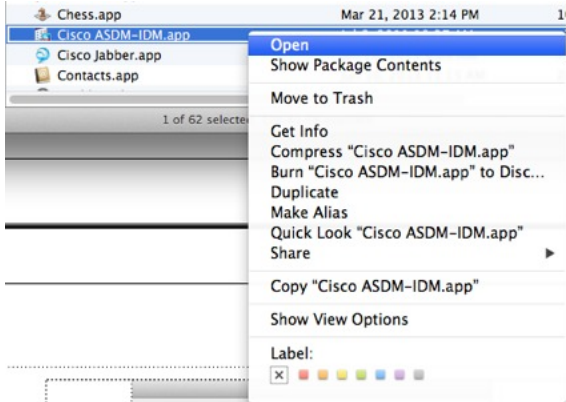

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): <ul style="list-style-type: none"> <li>10</li> </ul> <p><b>Note</b> See Windows 10 in <a href="#">ASDM Compatibility Notes, on page 4</a> if you have problems with the ASDM shortcut.</p> <ul style="list-style-type: none"> <li>8</li> <li>7</li> <li>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.)</li> <li>Server 2012 R2</li> <li>Server 2012</li> <li>Server 2008</li> </ul>	Yes	No support	Yes	8.0 version 8u261 or later	1.8  <p><b>Note</b> No support for Windows 7 or 10 32-bit</p>
Apple OS X 10.4 and later	Yes	Yes	Yes (64-bit version only)	8.0 version 8u261 or later	1.8

## ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
ASDM Launcher compatibility with ASDM version	<p>"Unable to Launch Device Manager" error message.</p> <p>If you upgrade to a new ASDM version and then get this error, you may need to re-install the latest Launcher.</p> <ol style="list-style-type: none"> <li>1. Open the ASDM web page on the ASA: <a href="https://&lt;asa_ip_address&gt;">https://&lt;asa_ip_address&gt;</a>.</li> <li>2. Click <b>Install ASDM Launcher</b>.</li> </ol> <p><i>Figure 1: Install ASDM Launcher</i></p>  <p>Copyright © 2006-2022 Cisco Systems, Inc. All rights reserved.</p> <ol style="list-style-type: none"> <li>3. Leave the username and password fields empty (for a new installation), and click <b>OK</b>.</li> </ol> <p>With no HTTPS authentication configured, you can gain access to ASDM with no username and the <b>enable</b> password, which is blank by default. When you enter the <b>enable</b> command at the CLI for the first time, you are prompted to change the password; this behavior is not enforced when you log into ASDM. We suggest that you change the enable password as soon as possible so that it does not remain blank. <b>Note:</b> If you enabled HTTPS authentication, enter your username and associated password. Even without authentication, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.</p>
Windows Active Directory directory access	<p>In some cases, Active Directory settings for Windows users may restrict access to program file locations needed to successfully launch ASDM on Windows. Access is needed to the following directories:</p> <ul style="list-style-type: none"> <li>• Desktop folder</li> <li>• C:\Windows\System32\Users\&lt;username&gt;\.asdm</li> <li>• C:\Program Files (x86)\Cisco Systems</li> </ul> <p>If your Active Directory is restricting directory access, you need to request access from your Active Directory administrator.</p>

Conditions	Notes
Windows 10	<p>"This app can't run on your PC" error message.</p> <p>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:</p> <ol style="list-style-type: none"> <li>1. Choose <b>Start &gt; Cisco ASDM-IDM Launcher</b>, and right-click the <b>Cisco ASDM-IDM Launcher</b> application.</li> <li>2. Choose <b>More &gt; Open file location</b>. Windows opens the directory with the shortcut icon.</li> <li>3. Right click the shortcut icon, and choose <b>Properties</b>.</li> <li>4. Change the <b>Target</b> to: <b>C:\Windows\System32\wscript.exe invisible.vbs run.bat</b></li> <li>5. Click <b>OK</b>.</li> </ol>
OS X	<p>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.</p>

Conditions	Notes
OS X 10.8 and later	<p>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.</p>  <p>1. To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose <b>Open</b>.</p>  <p>2. You see a similar error screen; however, you can open ASDM from this screen. Click <b>Open</b>. The ASDM-IDM Launcher opens.</p> 

Conditions	Notes
<p>(ASA 5500 and ISA 3000) Requires Strong Encryption license (3DES/AES) on ASA</p> <p><b>Note</b> Smart licensing models allow access with ASDM without the Strong Encryption license.</p>	<p>ASDM requires an SSL connection to the ASA. You can request a 3DES PAK license from Cisco:</p> <ol style="list-style-type: none"> <li>1. Go to <a href="https://www.cisco.com/go/license">https://www.cisco.com/go/license</a>.</li> <li>2. Under <b>Traditional Licenses</b>, click <b>Access LRP</b>.</li> <li>3. Click <b>Get Licenses</b> and then choose <b>IPS, Crypto, Other...</b> from the drop-down list.</li> <li>4. Type <b>ASA</b> in to the <b>Search by Keyword</b> field.</li> <li>5. Select <b>Cisco ASA 3DES/AES License</b> in the <b>Product</b> list, and click <b>Next</b>.</li> <li>6. Enter the serial number of the ASA, and follow the prompts to request a 3DES/AES license for the ASA.</li> </ol>
<ul style="list-style-type: none"> <li>• Self-signed certificate or an untrusted certificate</li> <li>• IPv6</li> <li>• Firefox and Safari</li> </ul>	<p>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 <a href="https://bugzilla.mozilla.org/show_bug.cgi?id=633001">https://bugzilla.mozilla.org/show_bug.cgi?id=633001</a>. 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.</p>
<ul style="list-style-type: none"> <li>• SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome.</li> <li>• Chrome</li> </ul>	<p>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 <b>Configuration &gt; Device Management &gt; Advanced &gt; SSL Settings</b> pane); or you can disable SSL false start in Chrome using the <b>--disable-ssl-false-start</b> flag according to <a href="#">Run Chromium with flags</a>.</p>

## 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.

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. To confirm that you are experiencing memory exhaustion, monitor the Java console for the "java.lang.OutOfMemoryError" message.

In addition, we recommend reducing your configuration size if possible, for example, by removing unused objects.



## 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.
- For very large configurations, you may need to specify a heap size up to 2 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>
```

For very large configurations, you may need to specify a heap size up to 2 GB.

- 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 7.15(1.150)

**Released: February 8, 2021**

There are no new features in this release.

### New Features in ASA 9.15(1)/ASDM 7.15(1)

**Released: November 2, 2020**

Feature	Description
Platform Features	

Feature	Description
ASAv for the Public Cloud	<p>We introduced the ASAv for the following Public Cloud offerings:</p> <ul style="list-style-type: none"> <li>• Oracle Cloud Infrastructure (OCI)</li> <li>• Google Cloud Platform (GCP)</li> </ul> <p>No modified screens.</p>
ASAv support for Autoscale	<p>The ASAv now supports Autoscale for the following Public Cloud offerings:</p> <ul style="list-style-type: none"> <li>• Amazon Web Services (AWS)</li> <li>• Microsoft Azure</li> </ul> <p>Autoscaling increases or decreases the number of ASAv application instances based on capacity requirements.</p> <p>No modified screens.</p>
ASAv for Microsoft Azure support for Accelerated Networking (SR-IOV).	<p>The ASAv on the Microsoft Azure Public Cloud now supports Azure's Accelerated Networking (AN), which enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance.</p> <p>No modified screens.</p>

#### Firewall Features

Changes to PAT address allocation in clustering. The PAT pool <b>flat</b> option is now enabled by default and it is not configurable.	<p>The way PAT addresses are distributed to the members of a cluster is changed. Previously, addresses were distributed to the members of the cluster, so your PAT pool would need a minimum of one address per cluster member. Now, the master instead divides each PAT pool address into equal-sized port blocks and distributes them across cluster members. Each member has port blocks for the same PAT addresses. Thus, you can reduce the size of the PAT pool, even to as few as one IP address, depending on the amount of connections you typically need to PAT. Port blocks are allocated in 512-port blocks from the 1024-65535 range. You can optionally include the reserved ports, 1-1023, in this block allocation when you configure PAT pool rules. For example, in a 4-node cluster, each node gets 32 blocks with which it will be able to handle 16384 connections per PAT pool IP address compared to a single node handling all 65535 connections per PAT pool IP address.</p> <p>As part of this change, PAT pools for all systems, whether standalone or operating in a cluster, now use a flat port range of 1023 - 65535. Previously, you could optionally use a flat range by including the <b>flat</b> keyword in a PAT pool rule. The <b>flat</b> keyword is no longer supported: the PAT pool is now always flat. The <b>include-reserve</b> keyword, which was previously a sub-keyword to <b>flat</b>, is now an independent keyword within the PAT pool configuration. With this option, you can include the 1 - 1023 port range within the PAT pool.</p> <p>Note that if you configure port block allocation (the <b>block-allocation</b> PAT pool option), your block allocation size is used rather than the default 512-port block. In addition, you cannot configure extended PAT for a PAT pool for systems in a cluster.</p> <p>New/Modified screens: NAT PAT Pool configuration.</p>
--	--

Feature	Description
XDMCP inspection disabled by default in new installations.	Previously, XDMCP inspection was enabled by default for all traffic. Now, on new installations, which includes new systems and reimaged systems, XDMCP is off by default. If you need this inspection, please enable it. Note that on upgrades, your current settings for XDMCP inspection are retained, even if you simply had it enabled by way of the default inspection settings.
<b>High Availability and Scalability Features</b>	
Disable failover delay	<p>When you use bridge groups or IPv6 DAD, when a failover occurs the new active unit waits up to 3000 ms for the standby unit to finish networking tasks and transition to the standby state. Then the active unit can start passing traffic. To avoid this delay, you can disable the waiting time, and the active unit will start passing traffic before the standby unit transitions.</p> <p>New/Modified screens: <b>Configuration &gt; Device Management &gt; High Availability and Scalability &gt; Failover &gt; Enable switchover waiting for peer state</b></p>
<b>Routing Features</b>	
Multicast IGMP interface state limit raised from 500 to 5000	<p>The multicast IGMP state limit per interface was raised from 500 to 5000.</p> <p>New/Modified commands: <b>igmp limit</b></p> <p>No ASDM support.</p> <p><i>Also in 9.12(4).</i></p>
<b>Interface Features</b>	
ASDM support for unique MAC address generation for single context mode	<p>You can now enable unique MAC address generation for VLAN subinterfaces in single context mode in ASDM. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses. CLI support was added in ASA 9.8(3), 9.8(4), and 9.9(2) and later.</p> <p>New/Modified screen: <b>Configuration &gt; Device Setup &gt; Interface Settings &gt; Interfaces</b></p>
DDNS support for the web update method	<p>You can now configure an interface to use DDNS with the web update method.</p> <p>New/Modified screens: <b>Configuration &gt; Device Management &gt; DNS &gt; Dynamic DNS</b></p>
<b>Certificate Features</b>	
Modifications to Match Certificate commands to support static CRL Distribution Point URL	<p>The static CDP URL configuration commands allowed CDPs to be mapped uniquely to each certificate in a chain that is being validated. However, only one such mapping was supported for each certificate. This modification allows statically configured CDPs to be mapped to a chain of certificates for authentication.</p>
<b>Administrative and Troubleshooting Features</b>	
Manual import of node secret file from the RSA Authentication Manager for SDI AAA server groups.	<p>You can import the node secret file that you export from the RSA Authentication Manager for use with SDI AAA server groups.</p> <p>We added the following screen: <b>Configuration &gt; Device Management &gt; Users/AAA &gt; AAA SDI.</b></p>

Feature	Description
<b>show fragment</b> command output enhanced	The output for <b>show fragment</b> command was enhanced to include IP fragment related drops and error counters.  No modified screens
show tech-support command output enhanced	The output for <b>show tech-support</b> command was enhanced to include the bias that is configured for the crypto accelerator. The bias value can be ssl, ipsec, or balanced.  No modified screens
<b>Monitoring Features</b>	
Support to configure cplane keepalive holdtime values	Due to communication delays caused by high CPU usage, the response to the keepalive event fails to reach ASA, resulting in trigerring failover due to card failure. You can now configure the keepalive timeout period and the maximum keepalive counter value to ensure sufficient time and retries are given.  We added the following screen: <b>Configuration &gt; Device Management &gt; Service Module Settings</b> .
<b>VPN Features</b>	
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: <b>crypto ikev2 limit max-in-negotiation-sa value</b>  No ASDM support.  <i>Also in 9.12(4).</i>
Cross-Site Request Forgery (CSRF) Vulnerabilities Prevention for WebVPN Handlers	ASA provides protection against CSRF attacks for WebVPN handlers. If a CSRF attack is detected, a user is notified by warning messages. This feature is enabled by default.
Kerberos server validation for Kerberos Constrained Delegation (KCD).	When configured for KCD, the ASA initiates an AD domain join with the configured server in order to acquire Kerberos keys. These keys are required for the ASA to request service tickets on behalf of clientless SSL VPN users. You can optionally configure the ASA to validate the identity of the server during domain join.  We changed the following screens: <b>Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Advanced &gt; Microsoft KCD Server</b>

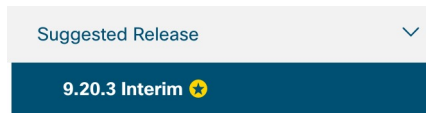
## Upgrade the Software

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

### Upgrade Path: ASA Appliances

#### What Version Should I Upgrade To?

On the Cisco Support & Download site, the suggested release is marked with a gold star. For example:

**Figure 2: Suggested Release****View Your Current Version**

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.

**Upgrade Guidelines**

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.

For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the [ASA Security Advisories](#).

**Upgrade Paths**

This table provides upgrade paths for ASA.



- Note** ASA 9.14 was the final version for the ASA 5525-X, 5545-X, and 5555-X.  
 ASA 9.12 was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.  
 ASA 9.2 was the final version for the ASA 5505.  
 ASA 9.1 was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

**Table 2: Upgrade Path**

Current Version	Interim Upgrade Version	Target Version
9.14	—	Any of the following:
9.13	—	Any of the following:
9.12	—	Any of the following:
9.10	—	Any of the following: → 9.12
9.9	—	Any of the following: → 9.12
9.8	—	Any of the following: → 9.12

Current Version	Interim Upgrade Version	Target Version
9.7	—	Any of the following: → 9.12
9.6	—	Any of the following: → 9.12
9.5	—	Any of the following: → 9.12
9.4	—	Any of the following: → 9.12
9.3	—	Any of the following: → 9.12
9.2	—	Any of the following: → 9.12
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
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.12

## 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 7.15(1.150)

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

Caveat ID Number	Description
<a href="#">CSCvu01215</a>	Appliance mode : checksum does not match issue while downloading asa image from CCO
<a href="#">CSCvu60781</a>	ASDM: Need support for MAC in Launcher 1.9.1
<a href="#">CSCvv17403</a>	Check box not available for disable delete tunnel with no delay in simultaneous connection preempt

### Open Bugs in Version 7.15(1)

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

Caveat ID Number	Description
<a href="#">CSCvu01215</a>	Appliance mode : checksum does not match issue while downloading asa image from CCO
<a href="#">CSCvu60781</a>	ASDM: Need support for MAC in Launcher 1.9.1
<a href="#">CSCvv17403</a>	Check box not available for disable delete tunnel with no delay in simultaneous connection preempt

## Resolved Bugs

This section lists resolved bugs per release.

### Resolved Bugs in Version 7.15(1.150)

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

Caveat ID Number	Description
<a href="#">CSCvv76201</a>	ASDM connection limited shows N/A in one of the contexts
<a href="#">CSCvw61817</a>	ASDM Display "n/a" for "Peak Usage (KB)" Under Tab "Context Usage" of Memory Status

### Resolved Bugs in Version 7.15(1)

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



Caveat ID Number	Description
<a href="#">CSCvq80097</a>	ASDM packet tracer destination MAC not showing when switching from routed to transparent context
<a href="#">CSCvr63410</a>	Not able to Unselect dedicate the interface to management only check box
<a href="#">CSCvr78019</a>	Unable to Change Pre-Shared Key Using ASDM with password encryption enabled
<a href="#">CSCvt34517</a>	ASDM Fails to Launch with error - invalid SHA1 signature file digest for LZMA/LzmaInputStream.class
<a href="#">CSCvu54682</a>	Power over Ethernet dialog has incorrect label for checkbox
<a href="#">CSCvu67773</a>	ASDM creates wrong outside identity NAT rule during creation of connection profile for s2s vpn
<a href="#">CSCvu69664</a>	dns-class inside of DNS Class-Map gets incorrect value
<a href="#">CSCvu82820</a>	Remove the engineID field from ASDM UI
<a href="#">CSCvu90263</a>	ASDM - ACL on management can't be added even interface configured with "no management-only"
<a href="#">CSCvv27284</a>	Unable to edit AnyConnect Custom Attribute Name value

## Cisco General Terms

The Cisco General Terms (including other related terms) governs the use of Cisco software. You can request a physical copy from Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387. Non-Cisco software purchased from Cisco is subject to applicable vendor license terms. See also: <https://cisco.com/go/generalterms>.

## Related Documentation

For additional information on the ASA, see [Navigating the Cisco ASA Series Documentation](#).

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.