

Release Notes for Cisco ASDM, 7.6(x)

First Published: 2016-03-21

Last Modified: 2016-10-24

Release Notes for Cisco ASDM, 7.6(x)

This document contains release information for Cisco ASDM Version 7.6(x) for the Cisco ASA series.

Important Notes

- Potential Traffic Outage (9.6(2.1) through 9.6(3))—Due to bug [CSCvd78303](#), the ASA may stop passing traffic after 213 days of uptime. The effect on each network will be different, but it could range from an issue of limited connectivity to something more extensive like an outage. You must upgrade to a new version without this bug, when available. In the meantime, you can reboot the ASA to gain another 213 days of uptime. Other workarounds may be available. See Field Notice [FN-64291](#) for affected versions and more information.
- The ASA 9.5.2(200) features, including Microsoft Azure support, are not available in 9.6(1). They are available in 9.6(2).
- ASDM 7.6(2) supports AnyConnect Client profiles in multiple context mode. This feature requires AnyConnect Version 4.2.00748 or 4.3.03013 and later.
- (ASA 9.6.2) Upgrade impact when using multiple-mode configuration—When upgrading from 9.5.2 to 9.6.1 and then subsequently to 9.6.2, any existing RAVPN for multiple-mode configuration will stop working. Post upgrade to the 9.6.2 image, a reconfiguration to give each context a storage space and to get new AnyConnect images in all of the contexts is required.
- (ASA 9.6(2)) Upgrade impact when using SSH public key authentication—Due to updates to SSH authentication, additional configuration is required to enable SSH public key authentication; as a result, existing SSH configurations using public key authentication no longer work after upgrading. Public key authentication is the default for the ASA on Amazon Web Services (AWS), so AWS users will see this issue. To avoid loss of SSH connectivity, you can update your configuration *before* you upgrade. Or you can use ASDM after you upgrade (if you enabled ASDM access) to fix the configuration.

Sample original configuration for a username "admin":

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

To use the **ssh authentication** command, before you upgrade, enter the following commands:

```
aaa authentication ssh console LOCAL
```

```
username admin password <password> privilege 15
```

We recommend setting a password for the username as opposed to keeping the **nopassword** keyword, if present. The **nopassword** keyword means that *any* password can be entered, not that *no* password can be entered. Prior to 9.6(2), the **aaa** command was not required for SSH public key authentication, so the **nopassword** keyword was not triggered. Now that the **aaa** command is required, it automatically also allows regular password authentication for a **username** if the **password** (or **nopassword**) keyword is present.

After you upgrade, the **username** command no longer requires the **password** or **nopassword** keyword; you can require that a user cannot enter a password. Therefore, to force public key authentication only, re-enter the **username** command:

```
username admin privilege 15
```

- Upgrade impact when upgrading the ASA on the Firepower 9300— Due to license entitlement naming changes on the back-end, when you upgrade to ASA 9.6(1)/FXOS 1.1.4, the startup configuration may not parse correctly upon the initial reload; configuration that corresponds to add-on entitlements is rejected.

For a standalone ASA, after the unit reloads with the new version, wait until all the entitlements are processed and are in an "Authorized" state (**Monitoring > Properties > Smart License**), and simply reload again (**Tools > System Reload**) *without* saving the configuration. After the reload, the startup configuration will be parsed correctly.

For a failover pair if you have any add-on entitlements, follow the upgrade procedure in the FXOS release notes, but reset failover after you reload each unit (**Monitoring > Properties > Failover > Status, Monitoring > Failover > System, or Monitoring > Failover > Failover Group**, and then click **Reset Failover**).

For a cluster, follow the upgrade procedure in the FXOS release notes; no additional action is required.

- ASA 5508-X and 5516-X upgrade issue when upgrading to 9.5(x) or later—Before you upgrade to ASA Version 9.5(x) or later, if you never enabled jumbo frame reservation then you must check the maximum memory footprint. Due to a manufacturing defect, an incorrect software memory limit might have been applied. If you upgrade to 9.5(x) or later before performing the below fix, then your device will crash on bootup; in this case, you must downgrade to 9.4 using ROMMON ([Load an Image for the ASA 5500-X Series Using ROMMON](#)), perform the below procedure, and then upgrade again.

1. Enter the following command to check for the failure condition:

```
ciscoasa# show memory detail | include Max memory footprint
Max memory footprint      =    456384512
Max memory footprint      =           0
Max memory footprint      =    456384512
```

If a value less than **456,384,512** is returned for “Max memory footprint,” then the failure condition is present, and you must complete the remaining steps before you upgrade. If the memory shown is 456,384,512 or greater, then you can skip the rest of this procedure and upgrade as normal.

2. Enter global configuration mode:

```
ciscoasa# configure terminal
```

```
ciscoasa(config)#
```

3. Temporarily enable jumbo frame reservation:

```
ciscoasa(config)# jumbo-frame reservation
WARNING: This command will take effect after the running-config
is saved and the system has been rebooted. Command accepted.
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```



Note Do not reload the ASA.

4. Save the configuration:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. Disable jumbo frame reservation:

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```



Note Do not reload the ASA.

6. Save the configuration again:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. You can now upgrade to Version 9.5(x) or later.

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

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

System Requirements

This section lists the system requirements to run this release.

ASDM Java Requirements

You can install ASDM using Oracle JRE 8.0. OpenJRE is not supported.

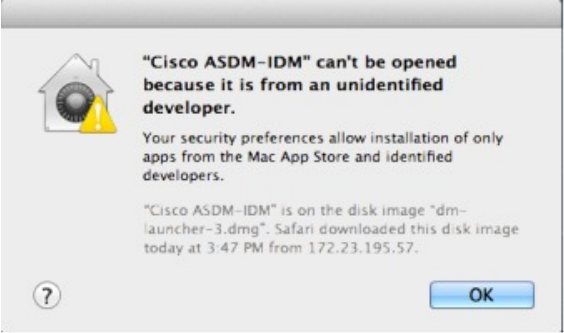
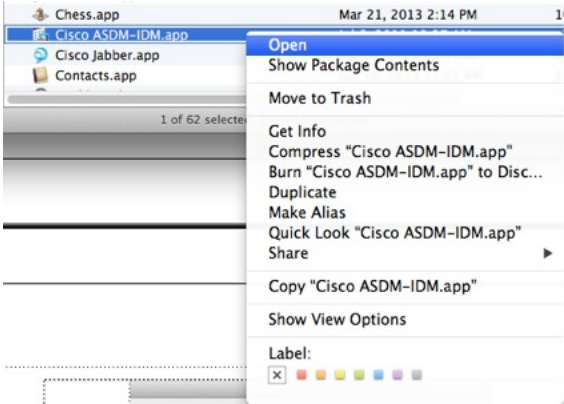

Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

Operating System	Browser				Oracle JRE
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): 8 7 Server 2012 R2 Server 2012 Server 2008	Yes	Yes	No support	Yes	8.0
Apple OS X 10.4 and later	No support	Yes	Yes	Yes (64-bit version only)	8.0
Ubuntu Linux 14.04 Debian Linux 7	N/A	Yes	N/A	Yes	8.0

ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
<p>Requires Strong Encryption license (3DES/AES) on ASA</p> <p>Note Smart licensing models allow initial access with ASDM without the Strong Encryption license.</p>	<p>ASDM requires an SSL connection to the ASA. You can request a 3DES license from Cisco:</p> <ol style="list-style-type: none"> 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.
<ul style="list-style-type: none"> • Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari 	<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 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.</p>
<ul style="list-style-type: none"> • SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome. • Chrome 	<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 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.</p>
IE9 for servers	<p>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.</p>
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 Open.</p>  <p>2. You see a similar error screen; however, you can open ASDM from this screen. Click Open. The ASDM-IDM Launcher opens.</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"> 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.

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

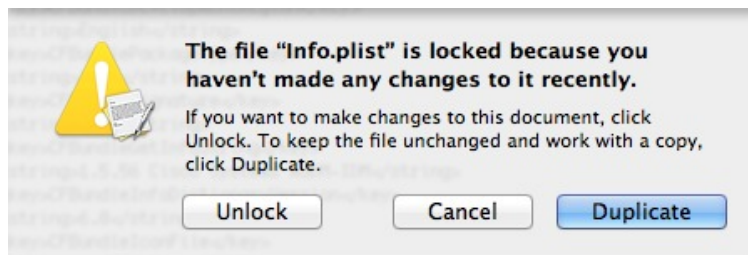
- Step 1** Right-click the **Cisco ASDM-IDM** icon, and choose **Show Package Contents**.
- Step 2** In the **Contents** folder, double-click the **Info.plist** file. If you have Developer tools installed, it opens in the **Property List Editor**. Otherwise, it opens in **TextEdit**.
- Step 3** Under **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 ASA 9.6(4)/ASDM 7.9(1)

Released: December 13, 2017

There are no new features in this release.

New Features in ASA 9.6(3.1)/ASDM 7.7(1)

Released: April 3, 2017



Note Version 9.6(3) was removed from Cisco.com due to bug [CSCvd78303](#).

Feature	Description
AAA Features	
Separate authentication for users with SSH public key authentication and users with passwords	In releases prior to 9.6(2), you could enable SSH public key authentication (ssh authentication) without also explicitly enabling AAA SSH authentication with the Local user database (aaa authentication ssh console LOCAL). In 9.6(2), the ASA required you to explicitly enable AAA SSH authentication. In this release, you no longer have to explicitly enable AAA SSH authentication; when you configure the ssh authentication command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for for usernames with <i>passwords</i> , and you can use any AAA server type (aaa authentication ssh console radius_1 , for example). For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS. We did not modify any screens.

New Features in ASDM 7.6(2.150)

Released: October 12, 2016

There are no new features in this release.

New Features in ASA 9.6(2)/ASDM 7.6(2)**Released: August 24, 2016**

Feature	Description
Platform Features	
ASA for the Firepower 4150	<p>We introduced the ASA for the Firepower 4150.</p> <p>Requires FXOS 2.0.1.</p> <p>We did not add or modify any screens.</p>
Hot Plug Interfaces on the ASAv	<p>You can add and remove Virtio virtual interfaces on the ASAv while the system is active. When you add a new interface to the ASAv, the virtual machine detects and provisions the interface. When you remove an existing interface, the virtual machine releases any resource associated with the interface. Hot plug interfaces are limited to Virtio virtual interfaces on the Kernel-based Virtual Machine (KVM) hypervisor.</p>
Microsoft Azure support on the ASAv10	<p>Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. The ASAv runs as a guest in the Microsoft Azure environment of the Hyper V Hypervisor. The ASAv on Microsoft Azure supports one instance type, the Standard D3, which supports four vCPUs, 14 GB, and four interfaces.</p> <p><i>Also in 9.5(2.200).</i></p>
Through traffic support on the Management 0/0 interface for the ASAv	<p>You can now allow through traffic on the Management 0/0 interface on the ASAv. Previously, only the ASAv on Microsoft Azure supported through traffic; now all ASAvs support through traffic. You can optionally configure this interface to be management-only, but it is not configured by default.</p>
Common Criteria Certification	<p>The ASA was updated to comply with the Common Criteria requirements. See the rows in this table for the following features that were added for this certification:</p> <ul style="list-style-type: none"> • ASA SSL Server mode matching for ASDM • SSL client RFC 6125 support: <ul style="list-style-type: none"> • Reference Identities for Secure Syslog Server connections and Smart Licensing connections • ASA client checks Extended Key Usage in server certificates • Mutual authentication when ASA acts as a TLS client for TLS1.1 and 1.2 • PKI debug messages • Crypto Key Zeroization verification • IPsec/ESP Transport Mode Support for IKEv2 • New syslog messages
Firewall Features	

Feature	Description
DNS over TCP inspection	<p>You can now inspect DNS over TCP traffic (TCP/53).</p> <p>We modified the following page: Configuration > Firewall > Objects > Inspection Maps > DNS Add/Edit dialog box</p>
MTP3 User Adaptation (M3UA) inspection	<p>You can now inspect M3UA traffic and also apply actions based on point code, service indicator, and message class and type.</p> <p>We added or modified the following pages: Configuration > Firewall > Objects > Inspection Maps > M3UA; the Rule Action > Protocol Inspection tab for service policy rules</p>
Session Traversal Utilities for NAT (STUN) inspection	<p>You can now inspect STUN traffic for WebRTC applications including Cisco Spark. Inspection opens pinholes required for return traffic.</p> <p>We added an option to the Rule Actions > Protocol Inspection tab of the Add/Edit Service Policy dialog box</p>
Application layer health checking for Cisco Cloud Web Security	<p>You can now configure Cisco Cloud Web Security to check the health of the Cloud Web Security application when determining if the server is healthy. By checking application health, the system can fail over to the backup server when the primary server responds to the TCP three-way handshake but cannot process requests. This ensures a more reliable system.</p> <p>We modified the following screen: Configuration > Device Management > Cloud Web Security</p>
Connection holddown timeout for route convergence.	<p>You can now configure how long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. You can reduce the holddown timer to make route convergence happen more quickly. However, the 15 second default is appropriate for most networks to prevent route flapping.</p> <p>We modified the following screen: Configuration > Firewall > Advanced > Global Timeouts <i>Also in 9.4(3).</i></p>
Changes in TCP option handling	<p>You can now specify actions for the TCP MSS and MD5 options in a packet's TCP header when configuring a TCP map. In addition, the default handling of the MSS, timestamp, window-size, and selective-ack options has changed. Previously, these options were allowed, even if there were more than one option of a given type in the header. Now, packets are dropped by default if they contain more than one option of a given type. For example, previously a packet with 2 timestamp options would be allowed, now it will be dropped.</p> <p>You can configure a TCP map to allow multiple options of the same type for MD5, MSS, selective-ack, timestamp, and window-size. For the MD5 option, the previous default was to clear the option, whereas the default now is to allow it. You can also drop packets that contain the MD5 option. For the MSS option, you can set the maximum segment size in the TCP map (per traffic class). The default for all other TCP options remains the same: they are cleared.</p> <p>We modified the following screen: Configuration > Firewall > Objects > TCP Maps Add/Edit dialog box</p>
Transparent mode maximum interfaces per bridge group increased to 64	<p>The maximum interfaces per bridge group was increased from 4 to 64.</p> <p>We did not modify any screens.</p>

Feature	Description
Flow offload support for multicast connections in transparent mode.	<p>You can now offload multicast connections to be switched directly in the NIC on transparent mode Firepower 4100 and 9300 series devices. Multicast offload is available for bridge groups that contain two and only two interfaces.</p> <p>There are no new commands or ASDM screens for this feature.</p>
Customizable ARP rate limiting	<p>You can set the maximum number of ARP packets allowed per second. The default value depends on your ASA model. You can customize this value to prevent an ARP storm attack.</p> <p>We modified the following screen: Configuration > Device Management > Advanced > ARP > ARP Static Table</p>
Ethertype rule support for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address.	<p>You can now write Ethertype access control rules for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address. Because of this addition, the bpdu keyword no longer matches the intended traffic. Rewrite bpdu rules for dsap 0x42.</p> <p>We modified the following screen: Configuration > Firewall > EtherType Rules.</p>
Remote Access Features	
Pre-fill/Username-from-cert feature for multiple context mode	<p>AnyConnect SSL support is extended, allowing pre-fill/username-from-certificate feature CLIs, previously available only in single mode, to be enabled in multiple context mode as well.</p> <p>We did not modify any screens.</p>
Flash Virtualization for Remote Access VPN	<p>Remote access VPN in multiple context mode now supports flash virtualization. Each context can have a private storage space and a shared storage place based on the total flash that is available:</p> <ul style="list-style-type: none"> • Private storage—Store files associated only with that user and specific to the content that you want for that user. • Shared storage—Upload files to this space and have it accessible to any user context for read/write access once you enable it. <p>We modified the following screens: Configuration > Context Management > Resource Class > Add Resource Class Configuration > Context Management > Security Contexts</p>
AnyConnect client profiles supported in multiple context mode	<p>AnyConnect client profiles are supported in multiple context mode. To add a new profile using ASDM, you must have the AnyConnect Secure Mobility Client release 4.2.00748 or 4.3.03013 and later.</p>
Stateful failover for AnyConnect connections in multiple context mode	<p>Stateful failover is now supported for AnyConnect connections in multiple context mode.</p> <p>We did not modify any screens.</p>
Remote Access VPN Dynamic Access Policy (DAP) is supported in multiple context mode	<p>You can now configure DAP per context in multiple context mode.</p> <p>We did not modify any screens.</p>

Feature	Description
Remote Access VPN CoA (Change of Authorization) is supported in multiple context mode	You can now configure CoA per context in multiple context mode. We did not modify any screens.
Remote Access VPN localization is supported in multiple context mode	Localization is supported globally. There is only one set of localization files that are shared across different contexts. We did not modify any screens.
Umbrella Roaming Security module support	You can choose to configure the AnyConnect Secure Mobility Client's Umbrella Roaming Security module for additional DNS-layer security when no VPN is active. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.
IPsec/ESP Transport Mode Support for IKEv2	Transport mode is now supported for ASA IKEv2 negotiation. It can be used in place of tunnel (default) mode. Tunnel mode encapsulates the entire IP packet. Transport mode encapsulates only the upper-layer protocols of an IP packet. Transport mode requires that both the source and destination hosts support IPsec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IPsec Proposals (Transform Sets) > IKEv2 proposals > Add/Edit
Per-packet routing lookups for IPsec inner packets	By default, per-packet adjacency lookups are done for outer ESP packets; lookups are not done for packets sent through the IPsec tunnel. In some network topologies, when a routing update has altered the inner packet's path, but the local IPsec tunnel is still up, packets through the tunnel may not be routed correctly and fail to reach their destination. To prevent this, use the new option to enable per-packet routing lookups for the IPsec inner packets. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps adding the Enable IPsec Inner Routing Lookup checkbox.
Certificate and Secure Connection Features	
ASA client checks Extended Key Usage in server certificates	Syslog and Smart licensing Server Certificates must contain "ServerAuth" in the Extended Key Usage field. If not, the connection fails.
Mutual authentication when ASA acts as a TLS client for TLS1.1 and 1.2	If the server requests a client certificate from the ASA for authentication, the ASA will send the client identity certificate configured for that interface. The certificate is configured by the ssl trust-point command.
PKI debug messages	The ASA PKI module makes connections to CA servers such as SCEP enrollment, revocation checking using HTTP, etc. All of these ASA PKI exchanges will be logged as debug traces under debug crypto ca message 5.
ASA SSL Server mode matching for ASDM	For an ASDM user who authenticates with a certificate, you can now require the certificate to match a certificate map. We modified the following screen: Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Feature	Description
Reference Identities for Secure Syslog Server connections and Smart Licensing connections	<p>TLS client processing now supports rules for verification of a server identity defined in RFC 6125, Section 6. Identity verification will be done during PKI validation for TLS connections to the Syslog Server and the Smart Licensing server only. If the presented identity cannot be matched against the configured reference identity, the connection is not established.</p> <p>We modified the following screens:</p> <p>Configuration > Remote Access VPN > Advanced</p> <p>Configuration > Device Management > Logging > Syslog Servers > Add/Edit</p> <p>Configuration > Device Management > Smart Call Home</p>
Crypto Key Zeroization verification	<p>The ASA crypto system has been updated to comply with new key zeroization requirements. Keys must be overwritten with all zeros and then the data must be read to verify that the write was successful.</p>
SSH public key authentication improvements	<p>In earlier releases, you could enable SSH public key authentication without also enabling AAA SSH authentication with the Local user database . The configuration is now fixed so that you must explicitly enable AAA SSH authentication. To disallow users from using a password instead of the private key, you can now create a username without any password defined.</p> <p>We modified the following screens:</p> <p>Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH</p> <p>Configuration > Device Management > Users/AAA > User Accounts > Add/Edit User Account</p>
Interface Features	
Increased MTU size for the ASA on the Firepower 4100/9300 chassis	<p>You can set the maximum MTU to 9188 bytes on the Firepower 4100 and 9300; formerly, the maximum was 9000 bytes. This MTU is supported with FXOS 2.0.1.68 and later.</p> <p>We modified the following screen: Configuration > Device Setup > Interface Settings > Interfaces > Advanced</p>
Routing Features	
Bidirectional Forwarding Detection (BFD) Support	<p>The ASA now supports the BFD routing protocol. Support was added for configuring BFD templates, interfaces, and maps. Support for BGP routing protocol to use BFD was also added.</p> <p>We added or modified the following screens:</p> <p>Configuration > Device Setup > Routing > BFD > Template</p> <p>Configuration > Device Setup > Routing > BFD > Interface</p> <p>Configuration > Device Setup > Routing > BFD > Map</p> <p>Configuration > Device Setup > Routing > BGP > IPv6 Family > Neighbors</p>

Feature	Description
IPv6 DHCP	<p>The ASA now supports the following features for IPv6 addressing:</p> <ul style="list-style-type: none"> • DHCPv6 Address client—The ASA obtains an IPv6 global address and optional default route from the DHCPv6 server. • DHCPv6 Prefix Delegation client—The ASA obtains delegated prefix(es) from a DHCPv6 server. The ASA can then use these prefixes to configure other ASA interface addresses so that StateLess Address Auto Configuration (SLAAC) clients can autoconfigure IPv6 addresses on the same network. • BGP router advertisement for delegated prefixes • DHCPv6 stateless server—The ASA provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. <p>We added or modified the following screens:</p> <p>Configuration > Device Setup > Interface Settings > Interfaces > Add Interface > IPv6</p> <p>Configuration > Device Management > DHCP > DHCP Pool</p> <p>Configuration > Device Setup > Routing > BGP > IPv6 Family > Networks</p> <p>Monitoring > interfaces > DHCP</p>
High Availability and Scalability Features	
Improved sync time for dynamic ACLs from AnyConnect when using Active/Standby failover	<p>When you use AnyConnect on a failover pair, then the sync time for the associated dynamic ACLs (dACLs) to the standby unit is now improved. Previously, with large dACLs, the sync time could take hours during which time the standby unit is busy syncing instead of providing high availability backup.</p> <p>We did not modify any screens.</p>
Licensing Features	
Permanent License Reservation for the ASAv	<p>For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASAv. In 9.6(2), we also added support for this feature for the ASAv on Amazon Web Services. This feature is not supported for Microsoft Azure.</p> <p>Note Not all accounts are approved for permanent license reservation. Make sure you have approval from Cisco for this feature before you attempt to configure it.</p> <p>We introduced the following commands: license smart reservation, license smart reservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return</p> <p>No ASDM support.</p> <p><i>Also in 9.5(2.200).</i></p>

Feature	Description
Satellite Server support for the ASAv	<p>If your devices cannot access the internet for security reasons, you can optionally install a local Smart Software Manager satellite server as a virtual machine (VM).</p> <p>We did not modify any screens.</p>
Permanent License Reservation for the ASAv Short String enhancement	<p>Due to an update to the Smart Agent (to 1.6.4), the request and authorization codes now use shorter strings.</p> <p>We did not modify any screens.</p>
Permanent License Reservation for the ASA on the Firepower 4100/9300 chassis	<p>For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASA on the Firepower 9300 and Firepower 4100. All available license entitlements are included in the permanent license, including the Standard Tier, Strong Encryption (if qualified), Security Contexts, and Carrier licenses. Requires FXOS 2.0.1.</p> <p>All configuration is performed on the Firepower 4100/9300 chassis; no configuration is required on the ASA.</p>
Smart Agent Upgrade for ASAv to v1.6	<p>The smart agent was upgraded from Version 1.1 to Version 1.6. This upgrade supports permanent license reservation and also supports setting the Strong Encryption (3DES/AES) license entitlement according to the permission set in your license account.</p> <p>Note If you downgrade from Version 9.5(2.200), the ASAv does not retain the licensing registration state. You need to re-register with the Configuration > Device Management > Licensing > Smart Licensing page with the Force registration option; obtain the ID token from the Smart Software Manager.</p> <p>We did not change any screens.</p> <p><i>Also in 9.5(2.200).</i></p>
Monitoring Features	
Packet capture of type asp-drop supports ACL and match filtering	<p>When you create a packet capture of type asp-drop, you can now also specify an ACL or match option to limit the scope of the capture.</p> <p>We did not modify any screens.</p>
Forensic Analysis enhancements	<p>You can create a core dump of any process running on the ASA. The ASA also extracts the text section of the main ASA process that you can copy from the ASA for examination.</p> <p>We did not modify any screens.</p>
Tracking Packet Count on a Per-Connection Basis through NetFlow	<p>Two counters were added that allow Netflow users to see the number of Layer 4 packets being sent in both directions on a connection. You can use these counters to determine average packet rates and sizes and to better predict traffic types, anomalies, and events.</p> <p>We did not modify any screens.</p>

Feature	Description
SNMP engineID sync for Failover	<p>In a failover pair, the SNMP engineIDs of the paired ASAs are synced on both units. Three sets of engineIDs are maintained per ASA—synced engineID, native engineID and remote engineID.</p> <p>An SNMPv3 user can also specify the engineID of the ASA when creating a profile to preserve localized snmp-server user authentication and privacy options. If a user does not specify the native engineID, the show running config output will show two engineIDs per user.</p> <p>We modified the following command: snmp-server user</p> <p>No ASDM support.</p> <p><i>Also in 9.4(3).</i></p>

New Features in ASA 9.6(1)/ASDM 7.6(1)

Released: March 21, 2016



Note The ASAv 9.5.2(200) features, including Microsoft Azure support, are not available in 9.6(1). They are available in 9.6(2).

Feature	Description
Platform Features	
ASA for the Firepower 4100 series	<p>We introduced the ASA for the Firepower 4110, 4120, and 4140.</p> <p>Requires FXOS 1.1.4.</p> <p>We did not add or modify any screens.</p>
SD card support for the ISA 3000	<p>You can now use an SD card for external storage on the ISA 3000. The card appears as disk3 in the ASA file system. Note that plug and play support requires hardware version 2.1 and later. Use the show module command to check your hardware version.</p> <p>We did not add or modify any screens.</p>
Dual power supply support for the ISA 3000	<p>For dual power supplies in the ISA 3000, you can establish dual power supplies as the expected configuration in the ASA OS. If one power supply fails, the ASA issues an alarm. By default, the ASA expects a single power supply and won't issue an alarm as long as it includes one working power supply.</p> <p>No ASDM support.</p>
Firewall Features	

Feature	Description
Diameter inspection improvements	<p>You can now inspect Diameter over TCP/TLS traffic, apply strict protocol conformance checking, and inspect Diameter over SCTP in cluster mode.</p> <p>We added or modified the following screens:</p> <p>Configuration > Firewall > Objects > Inspect Maps > Diameter</p> <p>Configuration > Firewall > Service Policy add/edit wizard's Rule Actions > Protocol Inspection tab</p>
SCTP stateful inspection in cluster mode	<p>SCTP stateful inspection now works in cluster mode. You can also configure SCTP stateful inspection bypass in cluster mode.</p> <p>We did not add or modify any screens.</p>
H.323 inspection support for the H.255 FACILITY message coming before the H.225 SETUP message for H.460.18 compatibility.	<p>You can now configure an H.323 inspection policy map to allow for H.225 FACILITY messages to come before the H.225 SETUP message, which can happen when endpoints comply with H.460.18.</p> <p>We added an option to the Call Attributes tab in the H.323 inspection policy map.</p>
Cisco Trustsec support for Security Exchange Protocol (SXP) version 3.	<p>Cisco Trustsec on ASA now implements SXPv3, which enables SGT-to-subnet bindings, which are more efficient than host bindings.</p> <p>We modified the following screens: Configuration > Firewall > Identity By TrustSec and the SGT Map Setup dialog boxes.</p>
Flow off-load support for the Firepower 4100 series.	<p>You can identify flows that should be off-loaded from the ASA and switched directly in the NIC for the Firepower 4100 series.</p> <p>Requires FXOS 1.1.4.</p> <p>We did not add or modify any screens.</p>
Remote Access Features	
IKEv2 Fragmentation, RFC-7383 support	<p>The ASA now supports this standard fragmentation of IKEv2 packets. This allows interoperability with other IKEv2 implementations such as Apple, Strongswan etc. ASA continues to support the current, proprietary IKEv2 fragmentation to maintain backward compatibility with Cisco products that do not support RFC-7383, such as the AnyConnect client.</p>
VPN Throughput Performance Enhancements on Firepower 9300 and Firepower 4100 series	<p>The crypto engine accelerator-bias command is now supported on the ASA security module on the Firepower 9300 and Firepower 4100 series. This command lets you “bias” more crypto cores toward either IPsec or SSL.</p> <p>We did not add or modify any screens.</p>

Feature	Description
Configurable SSH encryption and HMAC algorithm.	<p>Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. You might want to change the ciphers to be more or less strict, depending on your application. Note that the performance of secure copy depends partly on the encryption cipher used. By default, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use ssh cipher encryption custom aes128-cbc, for example.</p> <p>We introduced the following screen: Configuration > Device Management > Advanced > SSH Ciphers</p> <p><i>Also available in 9.1(7), 9.4(3), and 9.5(3).</i></p>
HTTP redirect support for IPv6	<p>When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address.</p> <p>We added functionality to the following screen: Configuration > Device Management > HTTP Redirect</p> <p><i>Also available in 9.1(7) and 9.4(3).</i></p>
Routing Features	
IS-IS routing	<p>The ASA now supports the Intermediate System to Intermediate System (IS-IS) routing protocol. Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the IS-IS routing protocol.</p> <p>We introduced the following screens:</p> <p>Configuration > Device Setup > Routing > ISIS</p> <p>Monitoring > Routing > ISIS</p>
High Availability and Scalability Features	
Support for site-specific IP addresses in Routed, Spanned EtherChannel mode	<p>For inter-site clustering in routed mode with Spanned EtherChannels, you can now configure site-specific IP addresses in addition to site-specific MAC addresses. The addition of site IP addresses allows you to use ARP inspection on the Overlay Transport Virtualization (OTV) devices to prevent ARP responses from the global MAC address from traveling over the Data Center Interconnect (DCI), which can cause routing problems. ARP inspection is required for some switches that cannot use VACLs to filter MAC addresses.</p> <p>We modified the following screen: Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit EtherChannel Interface > Advanced</p>
Administrative Features	

Feature	Description
Longer password support for local username and enable passwords (up to 127 characters)	<p>You can now create local username and enable passwords up to 127 characters (the former limit was 32). When you create a password longer than 32 characters, it is stored in the configuration using a PBKDF2 (Password-Based Key Derivation Function 2) hash. Shorter passwords continue to use the MD5-based hashing method.</p> <p>We modified the following screens:</p> <p>Configuration > Device Setup > Device Name/Password > Enable Password</p> <p>Configuration > Device Management > Users/AAA > User Accounts > Add/Edit User Account > Identity</p>
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	<p>The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now supported. This is a table of memory pool monitoring entries for all physical entities on a managed system.</p> <p>Note The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and supports reporting of memory on platforms with more than 4GB of RAM.</p> <p>We did not add or modify any screens.</p> <p><i>Also available in 9.1(7) and 9.4(3).</i></p>
REST API Version 1.3.1	We added support for the REST API Version 1.3.1.

Upgrade the Software

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

ASA Upgrade Path

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

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

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

Current Version	Interim Upgrade Version	Target Version
9.5(x)	—	Any of the following: → 9.6(x) → 9.5(x)
9.4(x)	—	Any of the following: → 9.6(x) → 9.5(x) → 9.4(x)

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

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

Current Version	Interim Upgrade Version	Target Version
8.4(5+)	—	Any of the following: → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(1) through 8.4(4)	Any of the following: → 9.0(2), 9.0(3), or 9.0(4) → 8.4(6)	→ 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.3(x)	→ 8.4(6)	Any of the following: → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.2(x) and earlier	→ 8.4(6)	Any of the following: → 9.6(x) → 9.5(x) → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Upgrade Link

To complete your upgrade, see the [ASA upgrade guide](#).

Open and Resolved Bugs

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



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

For more information about the Cisco Bug Search Tool, see the [Bug Search Tool Help & FAQ](#).

Open Bugs

This section lists open bugs in each version.

Open Bugs in Version 7.6(2.150)

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

Caveat ID Number	Description
CSCuz92899	Prelogin Policies changes not getting saved
CSCva89785	ASDM: TCP timeout values under service-policy pushes wrong values to ASA
CSCva91507	ASDM does not allow port range from 0 to 65535

Open Bugs in Version 7.6(2)

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

Caveat ID Number	Description
CSCuz92899	Prelogin Policies changes not getting saved
CSCva89785	ASDM: TCP timeout values under service-policy pushes wrong values to ASA
CSCva91507	ASDM does not allow port range from 0 to 65535

Open Bugs in Version 7.6(1)

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

Identifier	Description
CSCuw54048	Add Windows 10 supportability ASDM with SFR module
CSCuy01413	ASDM: "Send certificate chain" under IKEv2 Conn Profile is greyed out

Identifier	Description
CSCuy15812	Can't setup multiple default routes on diff interfaces with same metric
CSCuy47135	ASDM does not change SSL trustpoint if webvpn is not enabled
CSCuy48673	DAP:endpoint.as.TrendMicroAS is misconfigured on ASDM.

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.6(2.150)

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

Caveat ID Number	Description
CSCvb16663	ASDM 7.6.2 can't display VPN sessions - stuck @ 97% loading

Resolved Bugs in Version 7.6(2)

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

Caveat ID Number	Description
CSCuy01413	ASDM: "Send certificate chain" under IKEv2 Conn Profile is greyed out
CSCuy15812	Can't setup multiple default routes on diff interfaces with same metric
CSCuy47135	ASDM does not change SSL trustpoint if webvpn is not enabled
CSCuy47429	unable to create context in ASDM ERROR: % Incomplete command
CSCuy60531	ASDM dynamic tunnel with any/any when Traffic Selection Tab selected
CSCuy73370	wrong file extension for feedback service profile
CSCuy75518	ASDM Logging filter not working with command authorization
CSCuy76658	ASDM duplicates ACL remark lines when several ACEs are edited at once
CSCuy83681	ASDM Nat-Exempt interface cannot be changed after apply
CSCuy97880	ASDM not allowing to add aes-gcm ciphers in IKEv2 policies
CSCuz01625	IKEv2 is enabled when applying group-policy where only IKEv1 is enabled
CSCuz18280	ASDM capture (managing ASA cluster) doesn't work properly.
CSCuz19708	ASDM: 'without-csd' CLI configuration is not reflected on GUI
CSCuz23820	ASDM incorrectly grouping service object definitions
CSCuz31043	ASDM - multicast igmp access group panel issue

Caveat ID Number	Description
CSCuz32502	ASDM - multicast PIM Protocol issue
CSCuz43269	ASDM not correctly indexes lines when removing multiple remarks
CSCuz47825	Duplicate error message is not coming in response
CSCuz54866	Not able to configure the interface security level using ASDM in ASA5505
CSCuz55053	ASDM modifies source port when editing and adding service object-group
CSCuz58354	ASDM Mismatching AAA Server Group after sort by alphabet
CSCuz58762	DAP rule for AV activescan matches clients that do not have AV installed
CSCuz79772	Cannot Backup Hostscan Image via ASDM
CSCuz89301	ASDM Configured servers on interfaces with nameif with (or) are missing
CSCuz99734	ASDM no option to disable max-anyconnect-premium-or-essentials-limit
CSCva31853	ASDM 7.6(1) missing "User authenticated using MSCHAP" option
CSCva32027	OnBox: ASDM connectivity to SFR lost after context switch
CSCva55292	DOC: HA: Pre-upload ASDM image in standby before set the image on active

Resolved Bugs in Version 7.6(1)

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

Identifier	Description
CSCut04399	ASDM hangs on MAC after upgrade to Java 8
CSCux20823	ASDM wrong command order when deleting objects from an object group
CSCux26490	ASDM Removes an Entire DAP Bookmark List If It Exceeds 245 Characters
CSCux33151	ASDM duplicates remarks in ACL instead of replacing
CSCux33960	ASDM fails to configure Diffie-Hellman groups above 5 in IKEv2 policy
CSCux35016	ASDM discrepancies in crypto map
CSCux37581	ASDM 7.5.2 Not displaying active anyconnect clients
CSCux39599	AnyConnect profile modification in ASDM results in access-list error
CSCux59901	Health Check option is not synced on ASDM when disabled from CLI
CSCux61213	ASDM: Missing "any6" option in AAA rule configuration using ASDM
CSCux63050	Save Running Configuration to TFTP wrong interfaces in system context.

Identifier	Description
CSCux68972	ASDM- ACL with one entry removes the crypto-map
CSCux93603	ASDM 7.6.1.11 can't display VPN sessions - stuck @ 97% loading
CSCuy01349	ASDM allows to configure IPv6 routing-type from 0-255 while CLI 2-255
CSCuy09605	ASDM: Unable to edit route-map entry for community name > 10 characters
CSCuy12402	ASDM Configuration is unnecessarily reapplied when adding a minor change
CSCuy13768	ASDM fails to re-apply ACL back to crypto map after ACL modification
CSCuy15891	Error "The Maximum AnyConnect Sessions must be between 0 and 1" on ASDM
CSCuy47429	unable to create context in ASDM ERROR: % Incomplete command

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](#).

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: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). 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)

© 2016 Cisco Systems, Inc. All rights reserved.