



Release Notes for Cisco ASDM, Version 7.2(x)

Released: April 24, 2014

Updated: July 8, 2016

This document contains release information for Cisco ASDM Version 7.2(x) for the Cisco ASA series. This document includes the following sections:

- [Important Notes, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 9](#)
- [Upgrading the Software, page 14](#)
- [Open Caveats, page 14](#)
- [Resolved Caveats, page 16](#)
- [End-User License Agreement, page 16](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation and Submitting a Service Request, page 17](#)

Important Notes

- Upgrade impact for ASDM login when upgrading from a pre-9.2(2.4) release to 9.2(2.4) or later—If you upgrade from a pre-9.2(2.4) release to ASA Version 9.2(2.4) or later and you use command authorization and ASDM-defined user roles, users with Read Only access will not be able to log in to ASDM. You must change the **more** command either before or after you upgrade to be at privilege level 5; only Admin level users can make this change. Note that ASDM version 7.3(2) and later includes the **more** command at level 5 for defined user roles, but preexisting configurations need to be fixed manually.

ASDM:

- a. Choose **Configuration > Device Management > Users/AAA > AAA Access > Authorization**, and click **Configure Command Privileges**.
- b. Select **more**, and click **Edit**.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

monitor-interface	exec	show	15
more	exec	cmd	15
mount	configure	clear	15

c. Change the **Privilege Level** to 5, and click **OK**.

d. Click **OK**, and then **Apply**.

CLI:

```
ciscoasa(config)# privilege cmd level 5 mode exec command more
```

- WinNT AAA server to be deprecated—In ASA Version 9.3, the WinNT AAA server will no longer be supported. If you use WinNT, you should start planning alternative server types.

System Requirements

- [ASDM Client Operating System and Browser Requirements, page 2](#)
- [Java and Browser Compatibility, page 3](#)
- [Installing an Identity Certificate for ASDM, page 7](#)
- [ASA and ASDM Compatibility, page 7](#)
- [VPN Compatibility, page 7](#)
- [Maximum Configuration Size in ASDM, page 7](#)

ASDM Client Operating System and Browser Requirements

Table 1 lists the supported and recommended client operating systems and Java for ASDM.

Table 1 Operating System and Browser Requirements

Operating System	Browser				Java SE Plug-in
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): <ul style="list-style-type: none"> • 8 • 7 • Vista • 2008 Server • XP 	6 through 10. Version 11 or later is not supported.	1.5 or later	No support	18 or later	6 or later
Apple OS X 10.4 and later	No support	1.5 or later	2 or later	18 or later	6 or later
Red Hat Enterprise Linux 5 (GNOME or KDE): <ul style="list-style-type: none"> • Desktop • Desktop with Workstation 	N/A	1.5 or later	N/A	18 or later	6 or later

Java and Browser Compatibility

Table 2 lists compatibility caveats for Java, ASDM, and browser compatibility.

Table 2 Caveats for ASDM Compatibility

Java Version	Conditions	Notes
7 update 51	ASDM Launcher requires trusted certificate	<p>To continue using the Launcher, do one of the following:</p> <ul style="list-style-type: none"> • Install a trusted certificate on the ASA from a known CA. • Install a self-signed certificate and register it with Java. See the ASDM certificate procedure in this document. • Downgrade Java to 7 update 45 or earlier. • Alternatively use Java Web Start. <p>Note ASDM 7.1(5) and earlier are not supported with Java 7 update 51. If you already upgraded Java, and can no longer launch ASDM in order to upgrade it to Version 7.2, then you can either use the CLI to upgrade ASDM, or you can add a security exception in the Java Control Panel for each ASA you want to manage with ASDM. See the “Workaround” section at:</p> <p>http://java.com/en/download/help/java_blocked.xml</p> <p>After adding the security exception, launch the older ASDM and then upgrade to 7.2.</p>
	In rare cases, online help does not load when using Java Web Start	<p>In rare cases, when launching online help, the browser window loads, but the content fails to appear. The browser reports an error: “Unable to connect”.</p> <p>Workaround:</p> <ul style="list-style-type: none"> • Use the ASDM Launcher <p>Or:</p> <ul style="list-style-type: none"> • Clear the -Djava.net.preferIPv6Addresses=true parameter in Java Runtime Parameters: <ol style="list-style-type: none"> a. Launch the Java Control Panel. b. Click the Java tab. c. Click View. d. Clear this parameter: -Djava.net.preferIPv6Addresses=true e. Click OK, then Apply, then OK again.

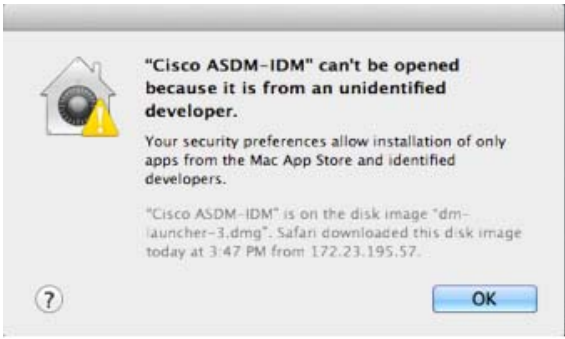
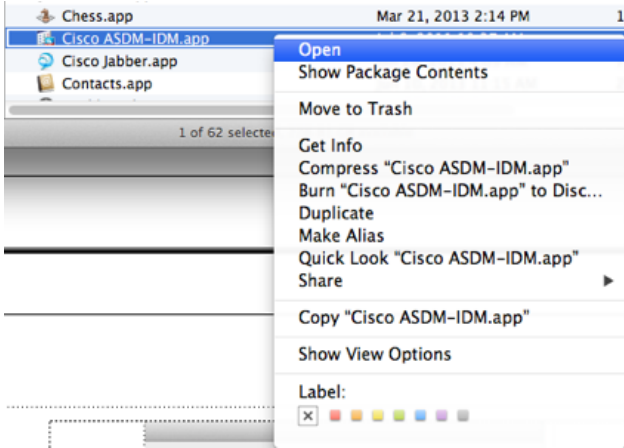

Table 2 Caveats for ASDM Compatibility

Java Version	Conditions	Notes
7 update 45	ASDM shows a yellow warning about the missing Permissions attribute when using an untrusted certificate	Due to a bug in Java, if you do not have a trusted certificate installed on the ASA, you see a yellow warning about a missing Permissions attribute in the JAR manifest. It is safe to ignore this warning ; ASDM 7.2 includes the Permissions attribute. To prevent the warning from appearing, install a trusted certificate (from a known CA); or generate a self-signed certificate on the ASA by choosing Configuration > Device Management > Certificates > Identity Certificates . Launch ASDM, and when the certificate warning is shown, check the Always trust connections to websites check box.
7	Requires strong encryption license (3DES/AES) on ASA	ASDM requires an SSL connection to the ASA. If the ASA has only the base encryption license (DES), and therefore has weak encryption ciphers for the SSL connection, you cannot launch ASDM. You must uninstall Java 7, and install Java 6 (http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html). Note that a workaround is required for weak encryption and Java 6 (see below, in this table).
6	No usernames longer than 50 characters	Due to a Java bug, ASDM does not support usernames longer than 50 characters when using Java 6. Longer usernames work correctly for Java 7.
	Requires strong encryption license (3DES/AES) on ASA <i>or</i> workaround	When you initially connect a browser to the ASA to load the ASDM splash screen, the browser attempts to make an SSL connection to the ASA. If the ASA has only the base encryption license (DES), and therefore has weak encryption ciphers for the SSL connection, you may not be able to access the ASDM splash screen; most current browsers do not support weak encryption ciphers. Therefore, without the strong encryption license (3DES/AES), use one of the following workarounds: <ul style="list-style-type: none"> • If available, use an already downloaded ASDM launcher or Java Web Start shortcut. The Launcher and Web Start shortcut work with Java 6 and weak encryption, even if the browsers do not. • For Windows Internet Explorer, you can enable DES as a workaround. See http://support.microsoft.com/kb/929708 for details. • For Firefox on any operating system, you can enable the security.ssl3.dhe_dss_des_sha setting as a workaround. See http://kb.mozillazine.org/About:config to learn how to change hidden configuration preferences.

Table 2 **Caveats for ASDM Compatibility**

Java Version	Conditions	Notes
All	<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 4 and later 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 <i>or</i> 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 http://www.chromium.org/developers/how-tos/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>

Table 2 *Caveats for ASDM Compatibility*

Java Version	Conditions	Notes
All	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>  <ol style="list-style-type: none"> To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose Open.  <ol style="list-style-type: none"> You see a similar error screen; however, you can open ASDM from this screen. Click Open. The ASDM-IDM Launcher opens. 

Installing an Identity Certificate for ASDM

When using the current Java version, the ASDM Launcher requires a trusted certificate. An easy approach to fulfill the certificate requirements is to generate a self-signed identity certificate and to configure the ASA to use it when establishing an SSL connection. After you generate the identity certificate and configure the ASA, you need to register it with the Java Control Panel on your computer. You can use Java Web Start to launch ASDM until you install a certificate.

See the following document to install a self-signed identity certificate on the ASA for use with ASDM, and to register the certificate with Java.

<http://www.cisco.com/go/asdm-certificate>

ASA and ASDM Compatibility

For information about ASA/ASDM requirements and compatibility, see *Cisco ASA Compatibility*:

<http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrix.html>

VPN Compatibility

For VPN compatibility, see the *Supported VPN Platforms, Cisco ASA 5500 Series*:

<http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asa-vpn-compatibility.html>

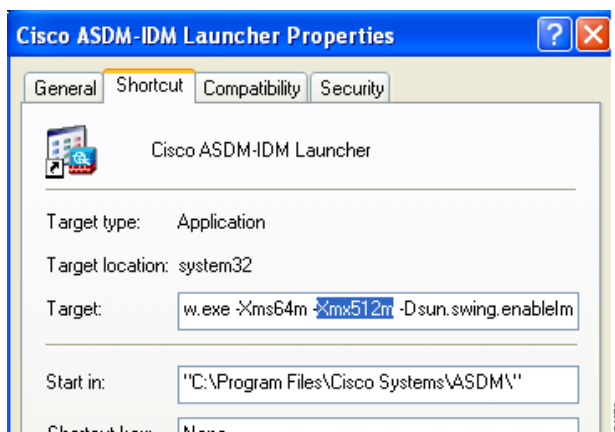
Maximum Configuration Size in ASDM

- 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 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 increase the ASDM heap memory size, download the ASDM-IDM Launcher, and then modify the ASDM-IDM Launcher shortcut by performing the following steps.

Windows:

- a. Right-click the shortcut for the Cisco ASDM-IDM Launcher, and choose **Properties**.
- b. Click the **Shortcut** tab.
- c. In the Target field, 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.



Macintosh:

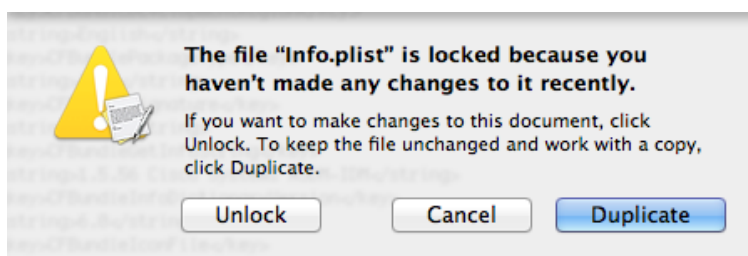
- a. Right-click the **Cisco ASDM-IDM** icon, and choose **Show Package Contents**.
- b. In the Contents folder, double-click the Info.plist file. If you have Developer tools installed, it opens in the Property List Editor. Otherwise, it opens in TextEdit.
- c. Under Java > VMOptions, change the string 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>
    
```

- d. If this file is locked, you see an error such as the following:



- e. 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.

New Features

- [New Features in Version 7.2\(2\), page 9](#)
- [New Features in Version 7.2\(1\), page 9](#)

New Features in Version 7.2(2)

Released: August 12, 2014

[Table 3](#) lists the new features for ASA Version 9.2(2.4)/ASDM Version 7.2(2).



Note

Version 9.2(2) was removed from Cisco.com due to build issues; please upgrade to Version 9.2(2.4) or later.

Table 3 *New Features for ASA Version 9.2(2.4)/ASDM Version 7.2(2)*

Feature	Description
Platform Features	
<p>ASA 5585-X (all models) support for the matching ASA FirePOWER SSP hardware module.</p> <p>ASA 5512-X through ASA 5555-X support for the ASA FirePOWER software module.</p>	<p>The ASA FirePOWER module supplies next-generation firewall services, including Next-Generation IPS (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP). You can use the module in single or multiple context mode, and in routed or transparent mode.</p> <p>We introduced the following screens:</p> <p>Home > ASA FirePOWER Status Wizards > Startup Wizard > ASA FirePOWER Basic Configuration Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA FirePOWER Inspection</p>
Remote Access Features	
<p>Internet Explorer 11 browser support on Windows 8.1 and Windows 7 for clientless SSL VPN</p>	<p>We added support for Internet Explorer 11 with Windows 7 and Windows 8.1 for clientless SSL VPN..</p> <p>We did not modify any screens.</p>

New Features in Version 7.2(1)

Released: April 24, 2014

[Table 4](#) lists the new features for ASA Version 9.2(1)/ASDM Version 7.2(1).



Note

The ASA 5510, ASA 5520, ASA 5540, ASA 5550, and ASA 5580 are not supported in this release or later. ASA Version 9.1 was the final release for these models.

Table 4 *New Features for ASA Version 9.2(1)/ASDM Version 7.2(1)*

Feature	Description
Platform Features	
The Cisco Adaptive Security Virtual Appliance (ASAv) has been added as a new platform to the ASA series.	The ASAv brings full firewall functionality to virtualized environments to secure data center traffic and multi-tenant environments. The ASAv runs on VMware vSphere. You can manage and monitor the ASAv using ASDM or the CLI.
Routing Features	
BGP Support	<p>We now support the Border Gateway Protocol (BGP). BGP is an inter autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).</p> <p>We introduced the following screens: Configuration > Device Setup > Routing > BGP Monitoring > Routing > BGP Neighbors, Monitoring > Routing > BGP Routes</p> <p>We modified the following screens: Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route Configuration > Device Setup > Routing > Route Maps> Add > Add Route Map</p>
Static route for Null0 interface	<p>Sending traffic to a Null0 interface results in dropping the packets destined to the specified network. This feature is useful in configuring Remotely Triggered Black Hole (RTBH) for BGP.</p> <p>We modified the following screen: Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route</p>
OSPF support for Fast Hellos	<p>OSPF supports the Fast Hello Packets feature, resulting in a configuration that results in faster convergence in an OSPF network.</p> <p>We modified the following screen: Configuration > Device Setup > Routing > OSPF > Interface > Edit OSPF Interface Advanced properties</p>
New OSPF Timers	<p>New OSPF timers were added; old ones were deprecated.</p> <p>We modified the following screen: Configuration > Device Setup > Routing > OSPF > Setup > Edit OSPF Process Advanced Properties</p>
OSPF Route filtering using ACL	<p>Route filtering using ACL is now supported.</p> <p>We introduced the following screen: Configuration > Device Setup > Routing > OSPF > Filtering Rules > Add Filter Rules</p>
OSPF Monitoring enhancements	<p>Additional OSPF monitoring information was added.</p> <p>We modified the following commands: show ospf events, show ospf rib, show ospf statistics, show ospf border-routers [detail], show ospf interface brief</p>

Table 4 **New Features for ASA Version 9.2(1)/ASDM Version 7.2(1) (continued)**

Feature	Description
OSPF redistribute BGP	<p>OSPF redistribution feature was added.</p> <p>We added the following screen: Configuration > Device Setup > Routing > OSPF > Redistribution</p>
EIGRP Auto- Summary	<p>For EIGRP, the Auto-Summary field is now disabled by default.</p> <p>We modified the following screen: Configuration > Device Setup > Routing > EIGRP > Setup > Edit EIGRP Process Advanced Properties</p>
High Availability Features	
Support for cluster members at different geographical locations (inter-site) for transparent mode	<p>You can now place cluster members at different geographical locations when using Spanned EtherChannel mode in transparent firewall mode. Inter-site clustering with spanned EtherChannels in routed firewall mode is not supported.</p> <p>We did not modify any ASDM screens.</p>
Static LACP port priority support for clustering	<p>Some switches do not support dynamic port priority with LACP (active and standby links). You can now disable dynamic port priority to provide better compatibility with spanned EtherChannels. You should also follow these guidelines:</p> <ul style="list-style-type: none"> • Network elements on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped. • Port-channel bundling downtime should not exceed the configured keepalive interval. <p>We modified the following screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster</p>
Support for 32 active links in a spanned EtherChannel for clustering	<p>ASA EtherChannels now support up to 16 active links. With <i>spanned</i> EtherChannels, that functionality is extended to support up to 32 active links across the cluster when used with two switches in a vPC and when you disable dynamic port priority. The switches must support EtherChannels with 16 active links, for example, the Cisco Nexus 7000 with with F2-Series 10 Gigabit Ethernet Module.</p> <p>For switches in a VSS or vPC that support 8 active links, you can now configure 16 active links in the spanned EtherChannel (8 connected to each switch). Previously, the spanned EtherChannel only supported 8 active links and 8 standby links, even for use with a VSS/vPC.</p> <p>Note If you want to use more than 8 active links in a spanned EtherChannel, you cannot also have standby links; the support for 9 to 32 active links requires you to disable cLACP dynamic port priority that allows the use of standby links.</p> <p>We modified the following screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster</p>
Support for 16 cluster members for the ASA 5585-X	<p>The ASA 5585-X now supports 16-unit clusters.</p> <p>We did not modify any ASDM screens.</p>

Table 4 *New Features for ASA Version 9.2(1)/ASDM Version 7.2(1) (continued)*

Feature	Description
Support for clustering with the Cisco Nexus 9300	The ASA supports clustering when connected to the Cisco Nexus 9300.
Remote Access Features	
ISE Change of Authorization	<p>The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is no longer required to apply access control lists (ACLs) for each VPN session established with the ASA.</p> <p>When an end user requests a VPN connection the ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network. An accounting start message is sent to the ISE to register the session. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA. The ISE sends a policy update to the ASA via a CoA “policy push.” This identifies a new user ACL that provides increased network access privileges. Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates.</p> <p>We modified the following screen: Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups > Add/Edit AAA Server Group</p>
Improved clientless rewriter HTTP 1.1 compression handling	<p>The rewriter has been changed so that if the client supports compressed content and the content will not be rewritten, then it will accept compressed content from the server. If the content must be rewritten and it is identified as being compressed, it will be decompressed, rewritten, and if the client supports it, recompressed.</p> <p>We did not introduce or modify any ASDM screens.</p>
OpenSSL upgrade	<p>The version of OpenSSL on the ASA will be updated to version 1.0.1e.</p> <p>Note We disabled the heartbeat option, so the ASA is not vulnerable to the Heartbleed Bug.</p> <p>We did not introduce or modify any ASDM screens.</p>
Interface Features	
Support for 16 active links in an EtherChannel	<p>You can now configure up to 16 active links in an EtherChannel. Previously, you could have 8 active links and 8 standby links. Be sure your switch can support 16 active links (for example the Cisco Nexus 7000 with with F2-Series 10 Gigabit Ethernet Module).</p> <p>Note If you upgrade from an earlier ASA version, the maximum active interfaces is set to 8 for compatibility purposes.</p> <p>We modified the following screen: Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface > Advanced.</p>

Table 4 **New Features for ASA Version 9.2(1)/ASDM Version 7.2(1) (continued)**

Feature	Description
Maximum MTU is now 9198 bytes	<p>The maximum MTU that the ASA can use is 9198 bytes (check for your model's exact limit at the CLI help). This value does not include the Layer 2 header. Formerly, the ASA let you specify the maximum MTU as 65535 bytes, which was inaccurate and could cause problems. If your MTU was set to a value higher than 9198, then the MTU is automatically lowered when you upgrade. In some cases, this MTU change can cause an MTU mismatch; be sure to set any connecting equipment to use the new MTU value.</p> <p>We modified the following screen: Configuration > Device Setup > Interface Settings > Interfaces > Edit Interface > Advanced</p> <p><i>Also in Version 9.1(6).</i></p>
Monitoring Features	
Embedded Event Manager (EEM)	<p>The EEM feature enables you to debug problems and provides general purpose logging for troubleshooting. The EEM responds to events in the EEM system by performing actions. There are two components: events that the EEM triggers, and event manager applets that define actions. You may add multiple events to each event manager applet, which triggers it to invoke the actions that have been configured on it.</p> <p>We introduced the following screens: Configuration > Device Management > Advanced > Embedded Event Manager, Monitoring > Properties > EEM Applets.</p>
SNMP hosts, host groups, and user lists	<p>You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host.</p> <p>We modified the following screen: Configuration > Device Management > Management Access > SNMP.</p>
SNMP message size	The limit on the message size that SNMP sends has been increased to 1472 bytes.
SNMP OIDs and MIBs	<p>The ASA now supports the cpmCPUTotal5minRev OID.</p> <p>The ASAv has been added as a new product to the SNMP sysObjectID OID and entPhysicalVendorType OID.</p> <p>The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the new ASAv platform.</p>
Administrative Features	

Table 4 *New Features for ASA Version 9.2(1)/ASDM Version 7.2(1) (continued)*

Feature	Description
Improved one-time password authentication	Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once. The auto-enable option was added to the aaa authorization exec command. We modified the following screen: Configuration > Device Management > Users/AAA > AAA Access > Authorization.
Auto Update Server certificate verification enabled by default	The Auto Update Server certificate verification is now enabled by default; for new configurations, you must explicitly disable certificate verification. If you are upgrading from an earlier release, and you did not enable certificate verification, then certificate verification is not enabled, and you see the following warning: WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option. The configuration will be migrated to explicitly configure no verification. We modified the following screen: Configuration > Device Management > System/Image Configuration > Auto Update > Add Auto Update Server.

Upgrading the Software

See <http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/upgrade/upgrade92.html>.

Open Caveats

- [Open Caveats in Version 7.2\(2\), page 14](#)
- [Open Caveats in Version 7.2\(1\), page 15](#)

Open Caveats in Version 7.2(2)

Table 5 contains open caveats in ASDM software Version 7.2(2).

Registered Cisco.com users can view more information about each caveat by using Bug Search at the following website:

<https://tools.cisco.com/bugsearch>

Table 5 *Open Caveats in ASDM Version 7.2(2)*

Caveat	Description
CSCUh28694	ASDM on Mac: System font issues (font too large)
CSCUl11018	Cluster wizard fails ungracefully when CCL interface is disconnected

Table 5 *Open Caveats in ASDM Version 7.2(2) (continued)*

Caveat	Description
CSCum00219	Cannot create an IPv6 network
CSCum10167	Unable to apply regex in web type acl via ASDM
CSCum89863	ASDM is not clearing the default user group for SNMP v3
CSCun78199	ASDM unable to add subinterfaces
CSCun87045	ASDM - When IPv6 configured, startup wizard hangs on Interface Setting
CSCuo10523	ASDM 7.1 - Trustsec support is not enabled for ASA-SM in ASDM
CSCuo41545	ASDM messages displays incorrect information regarding ASAv licensing
CSCuo55691	ASDM 7.1.6 RSA key generation fail (command syntax error)
CSCuo57123	unable to config more then 3 registry check value
CSCuo62386	ASDM 7.1.6: No DNS Configuration warnings on managing GP through CP
CSCuo64879	ASDM apply button does not work when adding anyconnect xml profile
CSCuo68208	AnyConnect profiles are not rendered properly after the creation
CSCuo80011	"Enable auto-generation of MAC addresses..." checkbox missing in ASDM
CSCuo89106	ASDM does not show empty object group in object-group section
CSCuo97033	ASDM nat- ASDM changes interface to object if obj. with such name exists
CSCup01753	ASDM doesnt populate the value when username from script is configrd
CSCup01970	Editing username from cer script throws unable to parse error
CSCup26608	ASDM logs out vpn sessions when trying to cancel operation
CSCup27452	ASDM persistently polling ASA with CX installed
CSCup33692	Unable to add PUBLIC SERVER through ASDM
CSCup35489	No "Run ASDM" button in IE 11

Open Caveats in Version 7.2(1)

Table 6 contains open caveats in ASDM software Version 7.2(1).

Registered Cisco.com users can view more information about each caveat by using Bug Search at the following website:

<https://tools.cisco.com/bugsearch>

Table 6 *Open Caveats in ASDM Version 7.2(1)*

Caveat	Description
CSCuh28694	ASDM on Mac: System font issues (font too large)
CSCu11018	Cluster wizard fails ungracefully when CCL interface is disconnected
CSCum00219	Cannot create an IPv6 network
CSCum10167	Unable to apply regex in web type acl via ASDM
CSCum89863	ASDM is not clearing the default user group for SNMP v3
CSCun78199	ASDM unable to add subinterfaces

Table 6 Open Caveats in ASDM Version 7.2(1) (continued)

Caveat	Description
CSCun87045	ASDM - When IPv6 configured, startup wizard hangs on Interface Setting
CSCuo10523	ASDM 7.1 - Trustsec support is not enabled for ASA-SM in ASDM
CSCuo41545	ASDM messages displays incorrect information regarding ASAv licensing

Resolved Caveats

- [Resolved Caveats in 7.2\(2\), page 16](#)
- [Resolved Caveats in 7.2\(1\), page 16](#)

Resolved Caveats in 7.2(2)

There were no resolved caveats in Version 7.2(2).

Resolved Caveats in 7.2(1)

[Table 7](#) contains the resolved caveats in ASDM software Version 7.2(1).

Registered Cisco.com users can view more information about each caveat by using Bug Search at the following website:

<https://tools.cisco.com/bugsearch>

Table 7 Resolved Caveats in ASDM Version 7.2(1)

Caveat	Description
CSCuj75028	SSL VPN bookmark's form parameter has unclear value
CSCum08151	ASDM: Clicking whitespace after chkbox text should not change its state.
CSCum09750	ASDM Top 10 Protected Servers graph shows large Others value for cluster
CSCum39889	ASDM does not show upgrade options for few OS versions:
CSCum46193	ASDM is being blocked by Java after an upgrade to Java 7u51
CSCum62475	ASDM sending wrong encrypted password
CSCum98114	ASDM not responding properly when group url doesn't contain http/https
CSCun64783	ASDM treats "not used" object with auto-NAT as not in use.
CSCun69981	ASDM: Object group not displayed in Threat detection exclude shun list
CSCuo25494	ASDM 7.1.6 not recognizing SSH commands

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*:
<http://www.cisco.com/go/asadoocs>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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. 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. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2014 Cisco Systems, Inc. All rights reserved.

