Release Notes for Cisco ASDM, Version 7.1(x)

Released: December 3, 2012
Updated: January 27, 2014

This document contains release information for Cisco ASDM Version 7.1(1) through 7.1(5.100) for the Cisco ASA series. This document includes the following sections:

Important Notes

- ASDM login issue in 9.1(3) and later—You can no longer log into ASDM with no username and the enable password. You must configure ASDM AAA authentication (Configuration > Device Management > Users/AAA > AAA Access > Authentication and associated username configuration) and/or ASDM certificate authentication (Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH). Before you upgrade to 9.1(3), be sure to configure one of these authentication methods. (CSCuj50862)
- ASA 9.1(3) features for the ASA CX require ASA CX Version 9.2(1).
- Upgrading to 9.1(2.8) or 9.1(3) or later—See the "Upgrade Path and Migrations" section on page 21.

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

System Requirements

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): • 8[1] • 7 • Vista • 2008 Server • XP	6.0 or later	1.5 or later	No support	18.0 or later	6.0 or later
Apple Macintosh OS X: • 10.8 • 10.7 • 10.6 • 10.5 • 10.4	No support	1.5 or later	2.0 or later	18.0 or later	6.0 or later
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • Desktop with Workstation	N/A	1.5 or later	N/A	18.0 or later	6.0 or later

1. ASDM Version 7.1(3) and later.

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 • Java Web Start requires newer ASDM version *or* workaround	To continue using the Launcher, either install a trusted certificate (from a known CA; a self-signed certificate will not work) on the ASA or downgrade Java to 7 update 45 or earlier. You can alternatively use Java Web Start. To use Java Web Start, do one of the following: • Upgrade ASDM to Version 7.1(5.100) or later. This ASDM version includes the Permissions attribute in the JAR manifest, which is required as of Java 7 Update 51. • To use ASDM 7.1(5) or earlier, add a security exception in the Java Control Panel for each ASA you want to manage with ASDM. See the "Workaround" section at: http://java.com/en/download/help/java_blocked.xml If you already upgraded Java, and can no longer launch ASDM in order to upgrade it to Version 7.1(5.100) or later, then you can either use the CLI to upgrade ASDM, or you can use the above security exception workaround to launch the older ASDM, after which you can upgrade to a newer version.
7 update 45	ASDM shows a yellow warning about the missing Permissions attribute	Java 7 update 45 shows a warning when an application does not have the Permissions attribute in the JAR manifest. **It is safe to ignore this warning**. To prevent this warning from appearing, upgrade to ASDM 7.1(5.100) or later; this ASDM version includes the Permissions attribute, which will be required as of Java 7 Update 51. **Note** Due to a bug in Java, even if you upgrade to ASDM 7.1(5.100) or later, if you also do not have a trusted certificate installed on the ASA, you continue to see the yellow warning about the missing 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** checkbox.

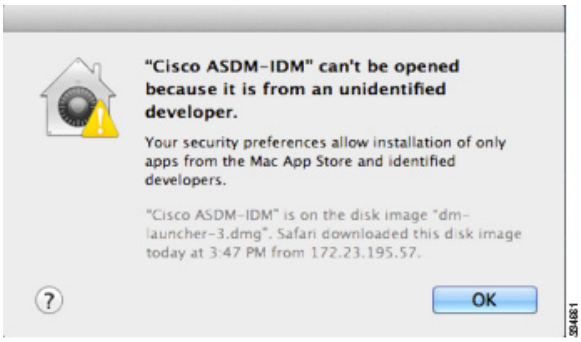
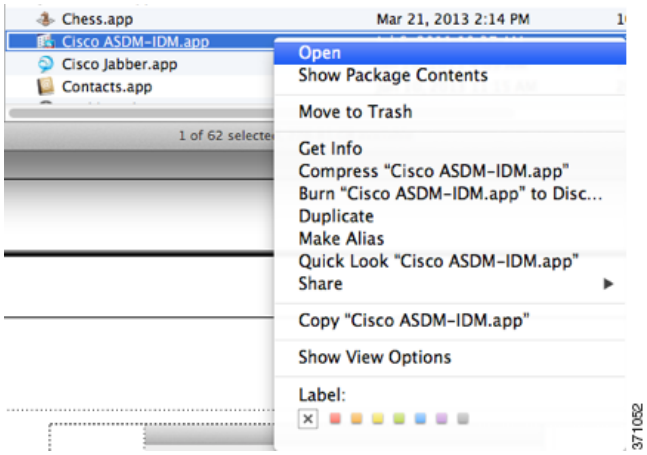
Table 2 Caveats for ASDM Compatibility

Java Version	Conditions	Notes
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).
	• ASDM 7.1(3) and earlier • MacOS	You may see the following error message when opening the ASDM Launcher: `Cannot launch Cisco ASDM-IDM. No compatible version of Java 1.5+ is available.` In this case, Java 7 is the currently-preferred Java version. Either upgrade ASDM to 7.1(4) or later, or you need to set Java 6 as the preferred Java version: Open the **Java Preferences** application (under Applications > Utilities), select the preferred Java version, and drag it up to be the first line in the 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 *or* 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: • 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	• Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari	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.
	• SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 *or* disable SSL false start in Chrome. • Chrome	If you change the SSL encryption on the ASA to exclude both RC4-MD5 and RC4-SHA1 algorithms (these algorithms are enabled by default), then Chrome cannot launch ASDM due to the Chrome "SSL false start" feature. We suggest re-enabling one of these algorithms (see the Configuration > Device Management > Advanced > SSL Settings pane); or you can disable SSL false start in Chrome using the **--disable-ssl-false-start** flag according to http://www.chromium.org/developers/how-tos/run-chromium-with-flags .
	IE9 for servers	For Internet Explorer 9.0 for servers, the "Do not save encrypted pages to disk" option is enabled by default (See Tools > Internet Options > Advanced). This option causes the initial ASDM download to fail. Be sure to disable this option to allow ASDM to download.
	MacOS	On MacOS, 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.

Table 2 Caveats for ASDM Compatibility

Java Version	Conditions	Notes
All	MacOS 10.8 and later	You need to allow ASDM to run because it is not signed with an Apple Developer ID. If you do not change your security preferences, you see an error screen.  1. To allow ASDM to run, right-click (or Ctrl-Click) the **Cisco ASDM-IDM Launcher** icon, and choose **Open**.  2. You see a similar error screen; however, you can open ASDM from this screen. Click **Open**. The ASDM-IDM Launcher opens. 

ASA and ASDM Compatibility

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

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

Note ASDM supports many ASA versions. The ASDM documentation and online help includes all of the latest features supported by the ASA. If you are running an older version of ASA software, the documentation might include features that are not supported in your version. Similarly, if a feature was added into a maintenance release for an older major or minor version, then the ASDM documentation includes the new feature even though that feature might not be available in all later ASA releases. Please refer to the new features tables to determine when features were added. For the minimum supported version of ASDM for each ASA version, see *Cisco ASA Compatibility*.

VPN Compatibility

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

http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

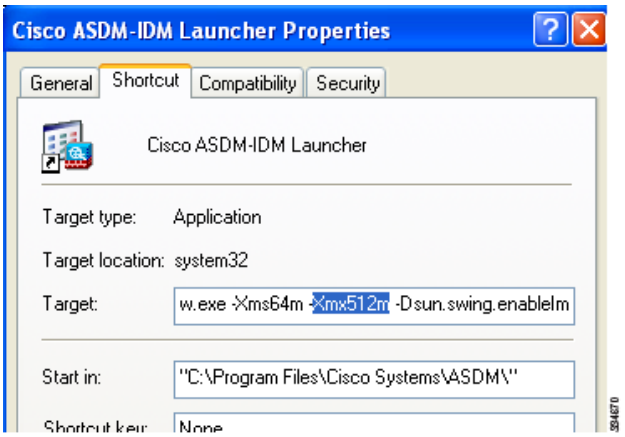
Maximum Configuration Size in ASDM

- 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:

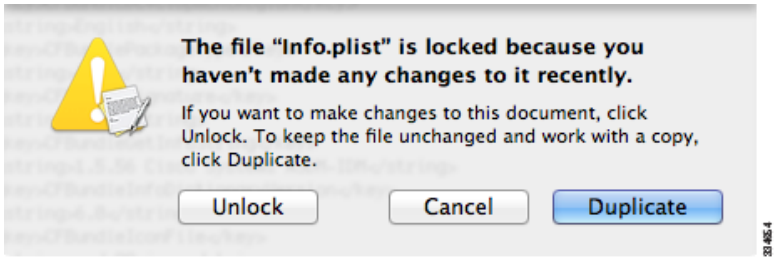
a. Right-click the **Cisco ASDM-IDM** icon, and choose **Show Package Contents**.

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>Java</key>
<dict>
        <key>WorkingDirectory</key>
        <string>$APP_PACKAGE/Contents/Resources/Java</string>
        <key>VMOptions</key>
        <string>-Xms64mm -Xmx512mm</string>
        <key>MainClass</key>
        <string>com.cisco.launcher.Launcher</string>
        <key>JVMVersion</key>
        <string>1.5+</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 7.1(5.100)

Released: January 14, 2014

There are no new features in Version 7.1(5.100).

New Features in Version 7.1(5)

Released: December 9, 2013

Table 3 lists the new features for ASA Version 9.1(4)/ASDM Version 7.1(5).

Table 3 New Features for ASA Version 9.1(4)/ASDM Version 7.1(5)

Feature	Description
Remote Access Features	
HTML5 WebSocket proxying	HTML5 WebSockets provide persistent connections between clients and servers. During the establishment of the clientless SSL VPN connection, the handshake appears to the server as an HTTP Upgrade request. The ASA will now proxy this request to the backend and provide a relay after the handshake is complete. Gateway mode is not currently supported. We did not modify any ASDM screens.
Inner IPv6 for IKEv2	IPv6 traffic can now be tunneled through IPsec/IKEv2 tunnels. This makes the ASA to AnyConnect VPN connections fully IPv6 compliant. GRE is used when both IPv4 and IPv6 traffic are being tunneled, and when both the client and headend support GRE. For a single traffic type, or when GRE is not supported by the client or the headend, we use straight IPsec. **Note** This feature requires AnyConnect Client Version 3.1.05 or later. We did not modify any ASDM screens.
Mobile Devices running Citrix Server Mobile have additional connection options	Support for mobile devices connecting to Citrix server through the ASA now includes selection of a tunnel-group, and RSA Securid for authorization. Allowing mobile users to select different tunnel-groups allows the administrator to use different authentication methods. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access.

Table 3 New Features for ASA Version 9.1(4)/ASDM Version 7.1(5) (continued)

Feature	Description
Split-tunneling supports exclude ACLs	Split-tunneling of VPN traffic has been enhanced to support both exclude and include ACLs. Exclude ACLs were previously ignored. **Note** This feature requires AnyConnect Client Version 3.1.03103 or later. We did not modify any ASDM screens.
High Availability and Scalability Features	
ASA 5500-X support for clustering	The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now support 2-unit clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 5512-X, you need the Security Plus license. We did not modify any ASDM screens.
Improved VSS and vPC support for health check monitoring	If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, you can now increase stability with health check monitoring. For some switches, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable the VSS/vPC health check feature, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them. We modified the following screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster
Support for cluster members at different geographical locations (inter-site); Individual Interface mode only	You can now place cluster members at different geographical locations when using individual interface mode. See the configuration guide for inter-site guidelines. We did not modify any ASDM screens.
Basic Operation Features	
DHCP rebind function	During the DHCP rebind phase, the client now attempts to rebind to other DHCP servers in the tunnel group list. Prior to this release, the client did not rebind to an alternate server, when the DHCP lease fails to renew. We introduced the following screen: Monitoring > Interfaces > DHCP> DHCP Lease Information.
Troubleshooting Features	
Crashinfo dumps include AK47 framework information	Application Kernel Layer 4 to 7 (AK47) framework-related information is now available in crashinfo dumps. A new option, **ak47**, has been added to the **debug menu** command to help in debugging AK47 framework issues. The framework-related information in the crashinfo dump includes the following: • Creating an AK47 instance. • Destroying an AK47 instance. • Generating an crashinfo with a memory manager frame. • Generating a crashinfo after fiber stack overflow. • Generating a crashinfo after a local variable overflow. • Generating a crashinfo after an exception has occurred.

New Features in Version 7.1(4)

Released: September 18, 2013

Table 7 lists the new features for ASA Version 9.1(3)/ASDM Version 7.1(4).

Table 4 New Features for ASA Version 9.1(3)/ASDM Version 7.1(4)

Feature	Description
Module Features	
Support for the ASA CX module in multiple context mode	You can now configure ASA CX service policies per context on the ASA. **Note** Although you can configure per context ASA service policies, the ASA CX module itself (configured in PRSM) is a single context mode device; the context-specific traffic coming from the ASA is checked against the common ASA CX policy. Requires ASA CX 9.2(1) or later. We did not modify any ASDM screens.
ASA 5585-X with SSP-40 and -60 support for the ASA CX SSP-40 and -60	ASA CX SSP-40 and -60 modules can be used with the matching level ASA 5585-X with SSP-40 and -60. Requires ASA CX 9.2(1) or later. We did not modify any screens.
Filtering packets captured on the ASA CX backplane	You can now filter packets that have been captured on the ASA CX backplane using the **match** or **access-list** keyword with the **capture interface asa_dataplane** command. Control traffic specific to the ASA CX module is not affected by the access-list or match filtering; the ASA captures all control traffic. In multiple context mode, configure the packet capture per context. Note that all control traffic in multiple context mode goes only to the system execution space. Because only control traffic cannot be filtered using an access list or match, these options are not available in the system execution space. Requires ASA CX 9.2(1) or later. A new option, Use backplane channel, was added to the Ingress Traffic Selector screen and the Egress Selector screen, in the Packet Capture Wizard to enable filtering of packets that have been captured on the ASA CX backplane.
Monitoring Features	

Table 4 New Features for ASA Version 9.1(3)/ASDM Version 7.1(4) (continued)

Feature	Description
Smart Call Home	We added a new type of Smart Call Home message to support ASA clustering. A Smart Call Home clustering message is sent for only the following three events: • When a unit joins the cluster • When a unit leaves the cluster • When a cluster unit becomes the cluster master Each message that is sent includes the following information: • The active cluster member count • The output of the **show cluster info** command and the **show cluster history** command on the cluster master We did not modify any ASDM screens. *Also available in 9.0(3).*
Remote Access Features	
user-storage value command password is now encrypted in **show** commands	The password in the **user-storage value** command is now encrypted when you enter **show running-config**. We modified the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > More Options > Session Settings**. *Also available in 8.4(6).*

New Features in Version 7.1(3)

ASDM 7.1(3) for ASA 9.0(3)

Released: July 22, 2013

Table 8 lists the new features for ASA Version 9.0(3)/ASDM Version 7.1(3).

Note Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(3) unless they were listed in the 9.0(1) feature table.

Table 5 New Features for ASA Version 9.0(3)/ASDM Version 7.1(3)

Feature	Description
Monitoring Features	
Smart Call Home	We added a new type of Smart Call Home message to support ASA clustering. A Smart Call Home clustering message is sent for only the following three events: • When a unit joins the cluster • When a unit leaves the cluster • When a cluster unit becomes the cluster master Each message that is sent includes the following information: • The active cluster member count • The output of the **show cluster info** command and the **show cluster history** command on the cluster master

ASDM 7.1(3) for ASA 9.1(2)

Released: May 14, 2013

Table 6 lists the new features for ASA Version 9.1(2)/ASDM Version 7.1(3).

Note Features added in 8.4(6) are not included in 9.1(2) unless they are explicitly listed in this table.

Table 6 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3)

Feature	Description
Certification Features	
FIPS and Common Criteria certifications	The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 FIPS 140-2 validation for the Cisco ASA series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X, and the ASA Services Module. The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which provides the basis for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform solutions.
Encryption Features	
Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications	Instead of using the proprietary encryption for the failover key, you can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption. **Note** Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license. We modified the following screen: Configuration > Device Management > High Availability > Failover > Setup.

Table 6 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
Additional ephemeral Diffie-Hellman ciphers for SSL encryption	The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher suites: • DHE-AES128-SHA1 • DHE-AES256-SHA1 These cipher suites are specified in RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS*). When supported by the client, DHE is the preferred cipher because it provides Perfect Forward Secrecy. See the following limitations: • DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS 1.0 for the SSL server. • Some popular applications do not support DHE, so include at least one other SSL encryption method to ensure that a cipher suite common to both the SSL client and server can be used. • Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Secure Desktop, and Internet Explorer 9.0. We modified the following screen: Configuration > Device Management > Advanced > SSL Settings. *Also available in 8.4(4.1).*
Management Features	
Support for administrator password policy when using the local database	When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters. We introduced the following screen: Configuration > Device Management > Users/AAA > Password Policy. *Also available in 8.4(4.1).*
Support for SSH public key authentication	You can now enable public key authentication for SSH connections to the ASA on a per-user basis. You can specify a public key file (PKF) formatted key or a Base64 key. The PKF key can be up to 4096 bits. Use PKF format for keys that are too large to for the ASA support of the Base64 format (up to 2048 bits). We introduced the following screens: Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Using PKF *Also available in 8.4(4.1); PKF key format support is only in 9.1(2).*
AES-CTR encryption for SSH	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
Improved SSH rekey interval	An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic.

Table 6 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported. We modified the following screen: Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH. *Also available in 8.4(4.1).*
Support for a maximum number of management sessions	You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions. We introduced the following screen: Configuration > Device Management > Management Access > Management Session Quota. *Also available in 8.4(4.1).*
Support for a pre-login banner in ASDM	Administrator can define a message that appears before a user logs into ASDM for management access. This customizable content is called a pre-login banner, and can notify users of special requirements or important information.
The default Telnet password was removed	To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication. Formerly, when you cleared the password, the ASA restored the default of "cisco." Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASA SM (see the **session** command). For initial ASA SM access, you must use the **service-module session** command, until you set a login password. We did not modify any ASDM screens. *Also available in 9.0(2).*
Platform Features	
Support for Power-On Self-Test (POST)	The ASA runs its power-on self-test at boot time even if it is not running in FIPS 140-2-compliant mode. Additional tests have been added to the POST to address the changes in the AES-GCM/GMAC algorithms, ECDSA algorithms, PRNG, and Deterministic Random Bit Generator Validation System (DRBGVS).
Improved pseudo-random number generation (PRNG)	The X9.31 implementation has been upgraded to use AES-256 encryption instead of 3DES encryption to comply with the Network Device Protection Profile (NDPP) in single-core ASAs.
Support for image verification	Support for SHA-512 image integrity checking was added. We did not modify any ASDM screens. *Also available in 8.4(4.1).*
Support for private VLANs on the ASA Services Module	You can use private VLANs with the ASA SM. Assign the primary VLAN to the ASA SM; the ASA SM automatically handles secondary VLAN traffic. There is no configuration required on the ASA SM for this feature; see the switch configuration guide for more information.

Table 6 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
CPU profile enhancements	The **cpu profile activate** command now supports the following: • Delayed start of the profiler until triggered (global or specific thread CPU%) • Sampling of a single thread We did not modify any ASDM screens. *Also available in 8.4(6).*
DHCP Features	
DHCP relay servers per interface (IPv4 only)	You can now configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. IPv6 is not supported for per-interface DHCP relay. We modified the following screen: Configuration > Device Management > DHCP > DHCP Relay.
DHCP trusted interfaces	You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface. We modified the following screen: Configuration > Device Management > DHCP > DHCP Relay.
Module Features	
ASA 5585-X support for network modules	The ASA 5585-X now supports additional interfaces on network modules in slot 1. You can install one or two of the following optional network modules: • ASA 4-port 10G Network Module • ASA 8-port 10G Network Module • ASA 20-port 1G Network Module *Also available in 8.4(4.1).*
ASA 5585-X DC power supply support	Support was added for the ASA 5585-X DC power supply. *Also available in 8.4(5).*
Support for ASA CX monitor-only mode for demonstration purposes	For demonstration purposes only, you can enable monitor-only mode for the service policy, which forwards a copy of traffic to the ASA CX module, while the original traffic remains unaffected. Another option for demonstration purposes is to configure a traffic-forwarding interface instead of a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic directly to the ASA CX module, bypassing the ASA. We modified the following screen: Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA CX Inspection. The traffic-forwarding feature is supported by CLI only.
Support for the ASA CX module and NAT 64	You can now use NAT 64 in conjunction with the ASA CX module. We did not modify any ASDM screens.

Table 6 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
NetFlow Features	
Support for NetFlow flow-update events and an expanded set of NetFlow templates	In addition to adding the flow-update events, there are now NetFlow templates that allow you to track flows that experience a change to their IP version with NAT, as well as IPv6 flows that remain IPv6 after NAT. Two new fields were added for IPv6 translation support. Several NetFlow field IDs were changed to their IPFIX equivalents. For more information, see the *Cisco ASA Implementation Note for NetFlow Collectors*.
Firewall Features	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL. We modified the following screen: Configuration > Device Management > Management Access > EtherType Rules. *Also available in 8.4(5).*
Decreased the half-closed timeout minimum value to 30 seconds	The half-closed timeout minimum value for both the global timeout and connection timeout was lowered from 5 minutes to 30 seconds to provide better DoS protection. We modified the following screens: Configuration > Firewall > Service Policy Rules > Connection Settings Configuration > Firewall > Advanced > Global Timeouts.
Remote Access Features	
IKE security and performance improvements	The number of IPsec-IKE security associations (SAs) can be limited for IKE v1 now, as well as IKE v2. We modified the following screen: Configuration > Site-to-Site VPN > Advanced > IKE Parameters.
	The IKE v2 Nonce size has been increased to 64 bytes. There are no ASDM screen or CLI changes.
	For IKE v2 on Site-to-Site, a new algorithm ensures that the encryption algorithm used by child IPsec SAs is not higher strength than the parent IKE. Higher strength algorithms will be downgraded to the IKE level. This new algorithm is enabled by default. We recommend that you do not disable this feature. We did not modify any ASDM screens.
	For Site-to-Site, IPsec data-based rekeying can be disabled. We modified the following screen: Configuration > Site-to-Site > IKE Parameters.
Improved Host Scan and ASA Interoperability	Host Scan and the ASA use an improved process to transfer posture attributes from the client to the ASA. This gives the ASA more time to establish a VPN connection with the client and apply a dynamic access policy. *Also available in 8.4(5).*

Table 6 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems. We support the following browsers on Windows 8: • Internet Explorer 10 (desktop only) • Firefox (all supported Windows 8 versions) • Chrome (all supported Windows 8 versions) See the following limitations: • Internet Explorer 10: – The Modern (AKA Metro) browser is not supported. – If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone. – If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported. • A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported. *Also available in 9.0(2).*
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check. See the following limitations: • Secure Desktop (Vault) is not supported with Windows 8. *Also available in 9.0(2).*
Dynamic Access Policies: Windows 8 Support	ASDM was updated to enable selection of Windows 8 in the DAP Operating System attribute. *Also available in 9.0(2).*
Monitoring Features	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the **show xlate count** command. We did not modify any ASDM screens. *Also available in 8.4(5).*
NSEL	Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent. We modified the following screens: Configuration > Device Management > Logging > NetFlow. Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard - Rule Actions > NetFlow > Add Flow Event *Also available in 8.4(5).*

New Features in Version 7.1(2.102)

Released: April 29, 2013

Table 7 lists the new features for ASA Version 8.4(6)/ASDM Version 7.1(2.102).

Table 7 New Features for ASA Version 8.4(6)/ASDM Version 7.1(2.102)

Feature	Description
Monitoring Features	
Ability to view top 10 memory users	You can now view the top bin sizes allocated and the top 10 PCs for each allocated bin size. Previously, you had to enter multiple commands to see this information (the **show memory detail** command and the **show memory binsize** command); the new command provides for quicker analysis of memory issues. No ASDM changes were made. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
CPU profile enhancements	The **cpu profile activate** command now supports the following: • Delayed start of the profiler until triggered (global or specific thread CPU %) • Sampling of a single thread No ASDM changes were made. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
Remote Access Features	
user-storage value command password is now encrypted in **show** commands	The password in the **user-storage value** command is now encrypted when you enter **show running-config**. We modified the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > More Options > Session Settings**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*

New Features in Version 7.1(2)

Released: February 25, 2013

Table 8 lists the new features for ASA Version 9.0(2)/ASDM Version 7.1(2).

Note Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(2) unless they were listed in the 9.0(1) feature table.

Table 8 New Features for ASA Version 9.0(2)/ASDM Version 7.1(2)

Feature	Description
Remote Access Features	
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems. We support the following browsers on Windows 8: • Internet Explorer 10 (desktop only) • Firefox (all supported Windows 8 versions) • Chrome (all supported Windows 8 versions) See the following limitations: • Internet Explorer 10: – The Modern (AKA Metro) browser is not supported. – If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone. – If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported. • A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported.
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check. See the following limitations: • Secure Desktop (Vault) is not supported with Windows 8.
Dynamic Access Policies: Windows 8 Support	ASDM was updated to enable selection of Windows 8 in the DAP Operating System attribute.
Management Features	
The default Telnet password was removed	To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication. Formerly, when you cleared the password, the ASA restored the default of "cisco." Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASA SM (see the **session** command). For initial ASA SM access, you must use the **service-module session** command, until you set a login password. We did not modify any ASDM screens.

New Features in Version 7.1(1)

Released: December 3, 2012

Table 9 lists the new features for ASA Version 9.1(1)/ASDM Version 7.1(1).

Note Features added in 8.4(4.x), 8.4(5), 8.4(6), and 9.0(2) are not included in 9.1(1) unless they were listed in the 9.0(1) feature table.

Table 9 New Features for ASA Version 9.1(1)/ASDM Version 7.1(1)

Feature	Description
Module Features	
Support for the ASA CX SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA CX SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. The ASA CX software module requires a Cisco solid state drive (SSD) on the ASA. For more information about the SSD, see the ASA 5500-X hardware guide. We did not modify any screens.

Upgrading the Software

This section describes how to upgrade to the latest version and includes the following topics:

Note For CLI procedures, see the ASA documentation.

Upgrade Path and Migrations

- If you are upgrading from a pre-8.3 release:
  - See the *Cisco ASA 5500 Migration Guide to Version 8.3 and Later* for important information about migrating your configuration.
  - You cannot upgrade directly to 9.0 or later. You must first upgrade to Version 8.3 or 8.4 for a successful migration.
- If you are upgrading from a pre-9.0 release, because of ACL migration, you cannot later perform a downgrade; be sure to back up your configuration file in case you want to downgrade. See the ACL migration section in the 9.0 release notes for more information.
- If you are upgrading from one of the following versions, you can successfully upgrade to 9.1(2.8) and 9.1(3) or later:
  - 8.4(5) or later
  - 9.0(2) or later

– 9.1(2)

However, if you are running any earlier versions, you cannot upgrade directly to 9.1(2.8) or 9.1(3) or later without *first* upgrading to one of the above versions. For example:

ASA Version	First Upgrade to:	Then Upgrade to:
8.2(1)	8.4(6)	9.1(2.8) or 9.1(3) or later
8.4(4)	8.4(6)	9.1(2.8) or 9.1(3) or later
9.0(1)	9.0(3)	9.1(2.8) or 9.1(3) or later
9.1(1)	9.1(2)	9.1(2.8) or 9.1(3) or later

- Software Version Requirements for Zero Downtime Upgrading:

  The units in a failover configuration or ASA cluster should have the same major (first number) and minor (second number) software version. However, you do not need to maintain version parity on the units during the upgrade process; you can have different versions on the software running on each unit and still maintain failover support. To ensure long-term compatibility and stability, we recommend upgrading all units to the same version as soon as possible.

  Table 1-10 shows the supported scenarios for performing zero-downtime upgrades.

Table 1-10 Zero-Downtime Upgrade Support

Type of Upgrade	Support
Maintenance Release	You can upgrade from any maintenance release to any other maintenance release within a minor release. For example, you can upgrade from 8.4(1) to 8.4(6) without first installing the maintenance releases in between.

Table 1-10 Zero-Downtime Upgrade Support (continued)

Type of Upgrade	Support
Minor Release	You can upgrade from a minor release to the next minor release. You cannot skip a minor release. For example, you can upgrade from 8.2 to 8.3. Upgrading from 8.2 directly to 8.4 is not supported for zero-downtime upgrades; you must first upgrade to 8.3. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.2 to 8.4 (the model is not supported on 8.3). **Note** Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.2 to 8.3.
Major Release	You can upgrade from the last minor release of the previous version to the next major release. For example, you can upgrade from 8.6 to 9.0, assuming that 8.6 is the last minor version in the 8.x release series for your model. Upgrading from 8.6 directly to 9.1 is not supported for zero-downtime upgrades; you must first upgrade to 9.0. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.4 to 9.0 (the model is not supported on 8.5 or 8.6). **Note** Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.4 to 9.0.

Viewing Your Current Version

The software version appears on the ASDM home page; view the home page to verify the software version of your ASA.

Downloading the Software from Cisco.com

If you are using the ASDM Upgrade Wizard, you do not have to pre-download the software. If you are manually upgrading, for example for a failover upgrade, download the images to your local computer.

If you have a Cisco.com login, you can obtain the OS and ASDM images from the following website:

http://www.cisco.com/go/asa-software

Upgrading a Standalone Unit

This section describes how to install the ASDM and operating system (OS) images.

- Upgrading from Your Local Computer, page 24
- Upgrading Using the Cisco.com Wizard, page 25

Upgrading from Your Local Computer

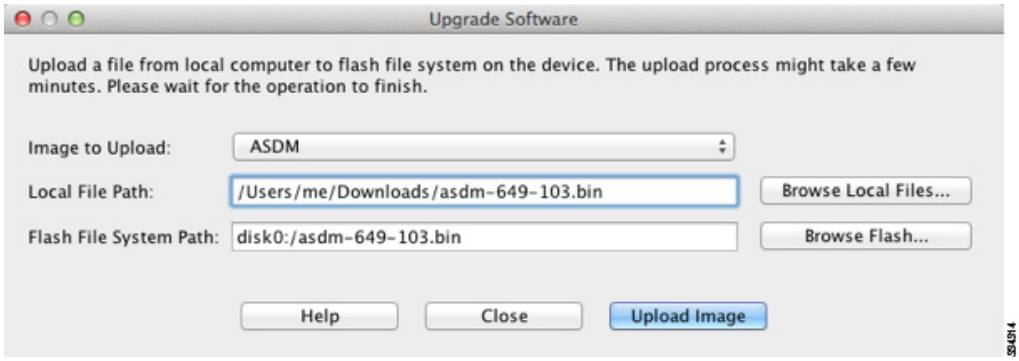
The Upgrade Software from Local Computer tool lets you upload an image file from your computer to the flash file system to upgrade the ASA.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software dialog box appears.



Step 3 From the Image to Upload drop-down list, choose **ASDM**.

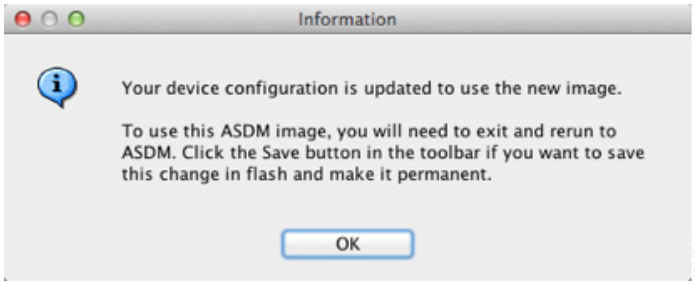
Step 4 In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

Step 7 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 8 You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.



Step 9 Repeat Step 2 through Step 8, choosing **ASA** from the Image to Upload drop-down list. You can also use this procedure to upload other file types.

Step 10 Choose **Tools > System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload.

a. Click the **Save the running configuration at the time of reload** radio button (the default).

b. Choose a time to reload (for example, **Now**, the default).

c. Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 11 After the ASA reloads, restart ASDM.

Upgrading Using the Cisco.com Wizard

The Upgrade Software from Cisco.com Wizard lets you automatically upgrade the ASDM and ASA to more current versions.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.

  Note ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 9.1(4), the download might be 9.1(4.2). This behavior is expected, so you may proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, restart the ASA to save the configuration and complete the upgrade.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 Choose **Tools > Check for ASA/ASDM Updates**.

In multiple context mode, access this menu from the System.

The Cisco.com Authentication dialog box appears.

Step 3 Enter your assigned Cisco.com username and the Cisco.com password, and then click **Login**.

The Cisco.com Upgrade Wizard appears.

Note If there is no upgrade available, a dialog box appears. Click **OK** to exit the wizard.

Step 4 Click **Next** to display the Select Software screen.

The current ASA version and ASDM version appear.

Step 5 To upgrade the ASA version and ASDM version, perform the following steps:

a. In the ASA area, check the **Upgrade to** check box, and then choose an ASA version to which you want to upgrade from the drop-down list.

b. In the ASDM area, check the **Upgrade to** check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.

Step 6 Click **Next** to display the Review Changes screen.

Step 7 Verify the following items:

- The ASA image file and/or ASDM image file that you have downloaded are the correct ones.
- The ASA image file and/or ASDM image file that you want to upload are the correct ones.
- The correct ASA boot image has been selected.

Step 8 Click **Next** to start the upgrade installation.

You can then view the status of the upgrade installation as it progresses.

The Results screen appears, which provides additional details, such as the upgrade installation status (success or failure).

Step 9 If the upgrade installation succeeded, for the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA, and restart ASDM.

Step 10 Click **Finish** to exit the wizard and save the configuration changes that you have made.

Note To upgrade to the next higher version, if any, you must restart the wizard.

Upgrading a Failover Pair or ASA Cluster

Upgrading an Active/Standby Failover Pair

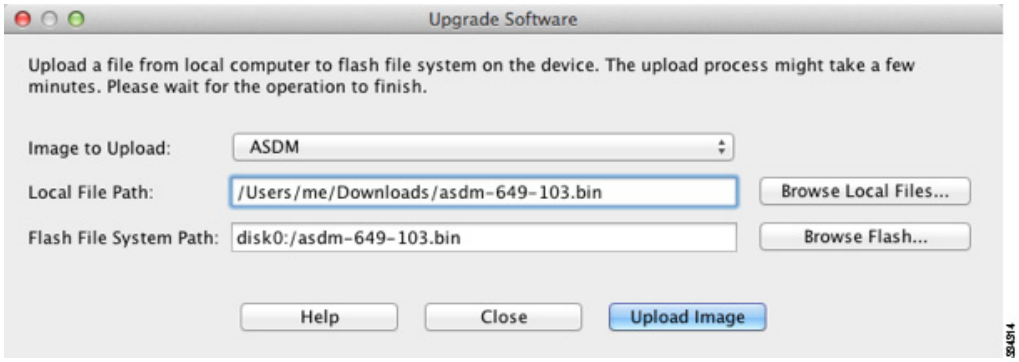
To upgrade the Active/Standby failover pair, perform the following steps.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 On the active unit, in the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software dialog box appears.



Step 3 From the Image to Upload drop-down list, choose **ASDM**.

Step 4 In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

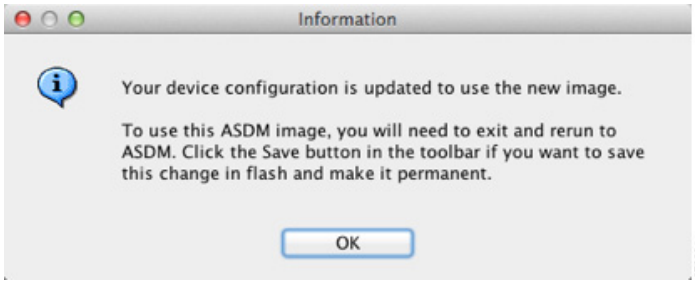
Step 5 In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

Step 7 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 8 You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 9 Repeat Step 2 through Step 8, choosing **ASA** from the Image to Upload drop-down list.



Step 10 Click the **Save** icon on the toolbar to save your configuration changes.

Step 11 Connect ASDM to the *standby* unit, and upload the ASA and ASDM software according to Step 2 through Step 9, using the same file locations you used on the active unit.

Step 12 Choose **Tools > System Reload** to reload the standby ASA.

A new window appears that asks you to verify the details of the reload.

a. Click the **Save the running configuration at the time of reload** radio button (the default).

b. Choose a time to reload (for example, **Now**, the default).

c. Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 13 After the standby ASA reloads, restart ASDM and connect to the standby unit to make sure it is running.

Step 14 Connect ASDM to the *active* unit again.

Step 15 Force the active unit to fail over to the standby unit by choosing **Monitoring > Properties > Failover > Status**, and clicking **Make Standby**.

Step 16 Choose **Tools > System Reload** to reload the (formerly) active ASA.

A new window appears that asks you to verify the details of the reload.

a. Click the **Save the running configuration at the time of reload** radio button (the default).

b. Choose a time to reload (for example, **Now**, the default).

c. Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

After the ASA comes up, it will now be the standby unit.

Upgrading an Active/Active Failover Pair

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Requirements

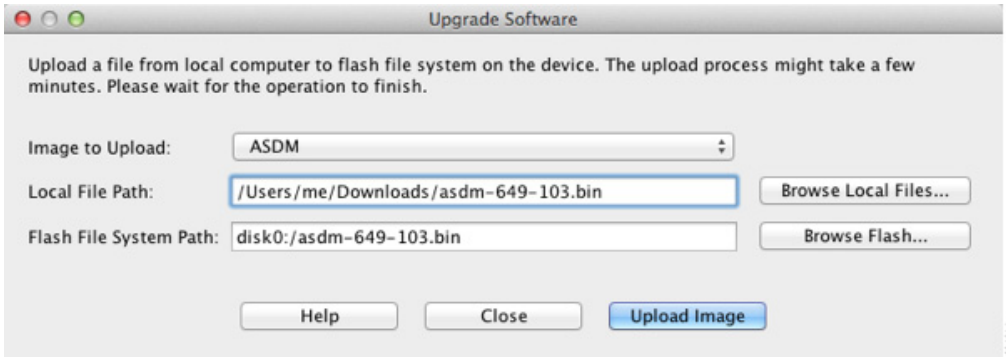
Perform these steps in the system execution space.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 On the primary unit, in the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software dialog box appears.



Step 3 From the Image to Upload drop-down list, choose **ASDM**.

Step 4 In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

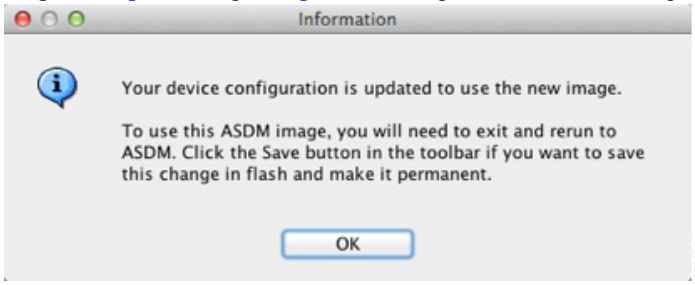
Step 5 In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

Step 7 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 8 You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 9 Repeat Step 2 through Step 8, choosing **ASA** from the Image to Upload drop-down list.



Step 10 Click the **Save** icon on the toolbar to save your configuration changes.

Step 11 Make both failover groups active on the primary unit by choosing **Monitoring > Failover > Failover Group #**, where **#** is the number of the failover group you want to move to the primary unit, and clicking **Make Active**.

Step 12 Connect ASDM to the *secondary* unit, and upload the ASA and ASDM software according to Step 2 through Step 9, using the same file locations you used on the active unit.

Step 13 Choose **Tools > System Reload** to reload the secondary ASA.

A new window appears that asks you to verify the details of the reload.

a. Click the **Save the running configuration at the time of reload** radio button (the default).

b. Choose a time to reload (for example, **Now**, the default).

c. Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 14 Connect ASDM to the *primary* unit, and check when the secondary unit reloads by choosing **Monitoring > Failover > System**.

Step 15 After the secondary unit comes up, force the primary unit to fail over to the secondary unit by choosing **Monitoring > Properties > Failover > System**, and clicking **Make Standby**.

Step 16 Choose **Tools > System Reload** to reload the (formerly) active ASA.

A new window appears that asks you to verify the details of the reload.

a. Click the **Save the running configuration at the time of reload** radio button (the default).

b. Choose a time to reload (for example, **Now**, the default).

c. Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the **Monitoring > Failover > Failover Group #** pane.

Upgrading an ASA Cluster

To upgrade all units in an ASA cluster, perform the following steps on the master unit. For multiple context mode, perform these steps in the system execution space.

Detailed Steps

Step 1 Launch ASDM on the master unit.

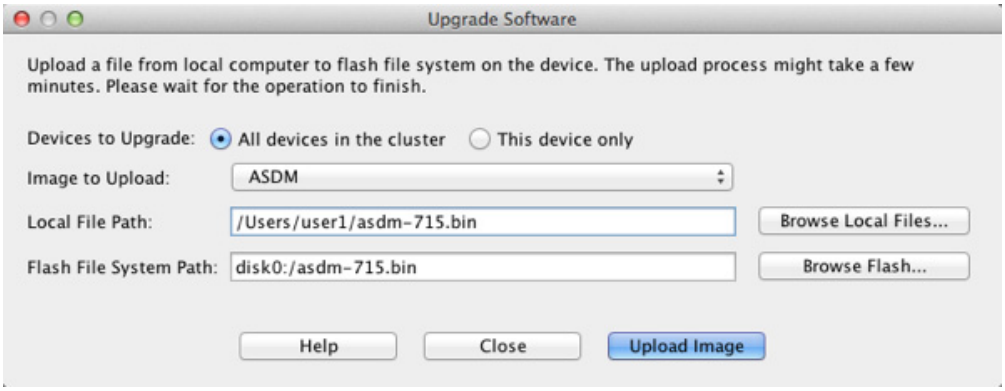
Step 2 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 3 In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software from Local Computer dialog box appears.

Step 4 Click the **All devices in the cluster** radio button.

The Upgrade Software dialog box appears.



Step 5 From the Image to Upload drop-down list, choose **ASDM**.

Step 6 In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

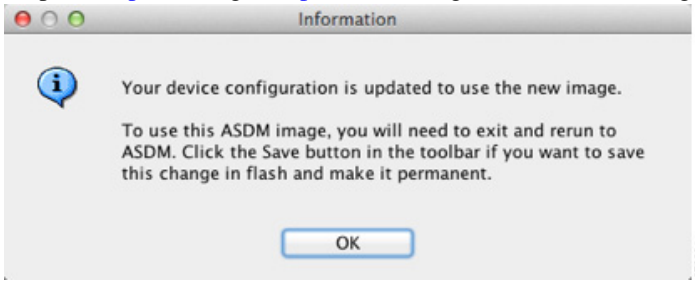
Step 7 In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 8 Click **Upload Image**. The uploading process might take a few minutes.

Step 9 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 10 You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 11 Repeat Step 3 through Step 10, choosing **ASA** from the Image to Upload drop-down list.

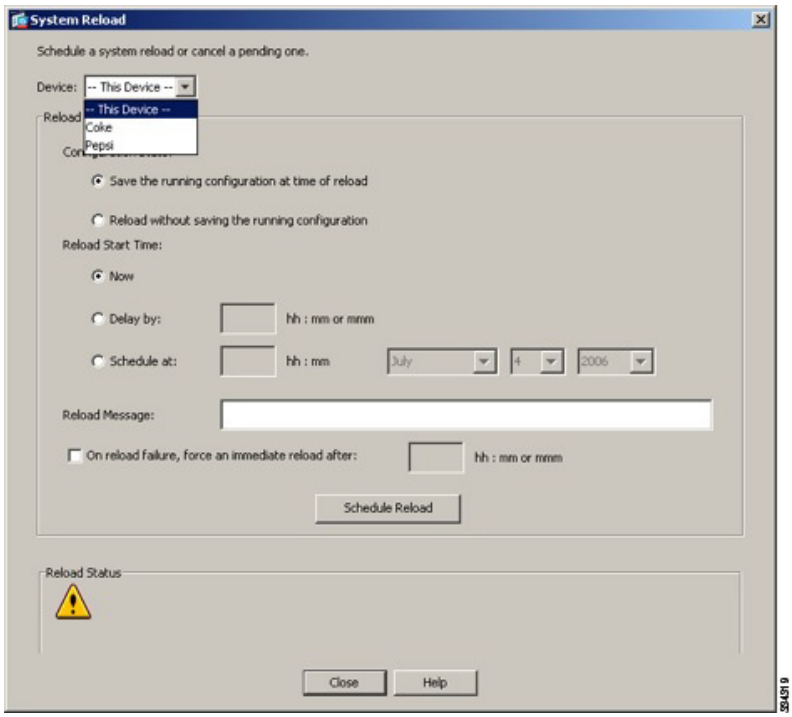


Step 12 Click the **Save** icon on the toolbar to save your configuration changes.

Step 13 Choose **Tools > System Reload**.

The System Reload dialog box appears.

Step 14 Reload each slave unit one at a time by choosing a slave unit name from the Device drop-down list, and then clicking **Schedule Reload** to reload the unit now.



To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up (approximately 5 minutes) before reloading the next unit. To view when a unit rejoins the cluster, see the Monitoring > ASA Cluster > Cluster Summary pane.

Step 15 After all slave units have reloaded, disable clustering on the master unit by choosing **Configuration > Device Management > High Availability and Scalability > ASA Cluster**, uncheck the **Participate in ASA cluster** check box, and click **Apply**.

Wait for 5 minutes for a new master to be selected and traffic to stabilize. When the former master unit rejoins the cluster, it will be a slave.

Do not save the configuration; when the master unit reloads, you want clustering to be enabled on it.

Step 16 Choose **Tools > System Reload** and reload the master unit from the System Reload dialog box by choosing **--This Device--** from the Device drop-down list.

Step 17 Quit and restart ASDM; you will reconnect to the new master unit.

Unsupported Commands

ASDM supports almost all commands available for the adaptive ASA, but ASDM ignores some commands in an existing configuration. Most of these commands can remain in your configuration; see Tools > Show Commands Ignored by ASDM on Device for more information.

This section includes the following topics:

Ignored and View-Only Commands

Table 11 lists commands that ASDM supports in the configuration when added through the CLI, but that cannot be added or edited in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If the command is view-only, then it appears in the GUI, but you cannot edit it.

Table 11 List of Unsupported Commands

Unsupported Commands	ASDM Behavior
capture	Ignored.
coredump	Ignored. This can be configured only using the CLI.
crypto engine large-mod-accel	Ignored.
dhcp-server (tunnel-group name general-attributes)	ASDM only allows one setting for all DHCP servers.
eject	Unsupported.
established	Ignored.
failover timeout	Ignored.
fips	Ignored.
nat-assigned-to-public-ip	Ignored.
pager	Ignored.
pim accept-register route-map	Ignored. You can configure only the **list** option using ASDM.

service-policy global	Ignored if it uses a **match access-list** class. For example:
	`access-list myacl extended permit ip any any`
	`class-map mycm`
	`  match access-list myacl`
	`policy-map mypm`
	`  class mycm`
	`  inspect ftp`
	`service-policy mypm global`

set metric	Ignored.
sysopt nodnsalias	Ignored.
sysopt uauth allow-http-cache	Ignored.
terminal	Ignored.
threat-detection rate	Ignored.

Effects of Unsupported Commands

If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, choose **Tools > Show Commands Ignored by ASDM on Device**.

Discontinuous Subnet Masks Not Supported

ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, you cannot use the following:

```
ip address inside 192.168.2.1 255.255.0.255
```

Interactive User Commands Not Supported by the ASDM CLI Tool

The ASDM CLI tool does not support interactive user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter "[yes/no]" but does not recognize your input. ASDM then times out waiting for your response.

For example:

1. Choose **Tools > Command Line Interface**.
2. Enter the **crypto key generate rsa** command.

   ASDM generates the default 1024-bit RSA key.
3. Enter the **crypto key generate rsa** command again.

   Instead of regenerating the RSA keys by overwriting the previous one, ASDM displays the following error:

```
Do you really want to replace them? [yes/no]:WARNING: You already have RSA
ke0000000000000$A key
Input line must be less than 16 characters in length.

%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

Workaround:

- You can configure most commands that require user interaction by means of the ASDM panes.
- For CLI commands that have a **noconfirm** option, use this option when entering the CLI command. For example:

```
crypto key generate rsa noconfirm
```

Open Caveats

Open Caveats in 7.1(5) and 7.1(5.100)

Table 12 contains open caveats in ASDM software Version 7.1(5) and 7.1(5.100).

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 12 Open Caveats in ASDM Version 7.1(5) and 7.1(5.100)

Caveat	Description
CSCuj71540	ASDM: Not able to apply edit dead interval time for interface in ospfv2
CSCuj74855	Can't bring up ASDM from the Launcher with IPv6 address without brackets
CSCuj75028	SSL VPN bookmark's form parameter has unclear value
CSCuj88707	ASDM did not get a response from the ASA in the last 60 seconds
CSCuj95685	Can't add EC with mode set to On (cluster control link requirement)
CSCuj98126	In spanned EC mode (Cluster), can't set any EC member interface params
CSCul07863	'Pre-login Page URL' is not saved within ASDM
CSCul11018	Cluster wizard fails ungracefully with CCL issues
CSCul15841	Security warning after Java is upgraded to Java 7.45
CSCul22607	ASDM: Botnet Infected Host "Last Connection" Column Sorts by Day
CSCul28030	ASDM: External portal page config-Portal URL for XenDesktop is malformed
CSCul32541	ERROR com.cisco.dmcommon.util.DMCommonEnv-CLIMetricsParser
CSCul37206	Objects of AnyConnect-customization cannot be replicated to standby unit
CSCul38916	ASDM:Not able to configure "Shun Duration" for threat-detection
CSCul38948	ASDM: ASDM hangs when an object group is modified
CSCul53360	IPv6 filed added to AnyConnect profile by wizard is invalid
CSCum57517	ASDM launcher is not working with Java 7u51

Open Caveats in 7.1(4)

Table 13 contains open caveats in ASDM software Version 7.1(4).

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 13 Open Caveats in ASDM Version 7.1(4)

Caveat	Description
CSCuh24961	Need to add new Desktop ACIDEX attributes to DAP AnyConnect EndPoint IDs
CSCuh28694	ASDM on Mac: System font issues (font too large)
CSCui24893	ASDM Launcher is not working with java7u25
CSCui39567	ASDM 7.x certificate maps mapped to IPsec and SSL only show under IPSec

Table 13 Open Caveats in ASDM Version 7.1(4) (continued)

Caveat	Description
CSCui85113	ASDM 7.1 Unable to delete object nat when object conflicts with name
CSCui91127	ASDM Error: Number of IP address in the pool exceeds the limit 65536.
CSCui97678	VDI Server proxy applied to DfltGrpPolicy instead of Tunnel GroupPoliy
CSCuj02930	No Change dialog pop up after VDI Server proxy was changed
CSCuj06653	ASDM:Credentials displayed in clear text when using Cisco.com wizard

Open Caveats in 7.1(3)

Table 14 contains open caveats in ASDM software Version 7.1(3).

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 14 Open Caveats in ASDM Version 7.1(3)

Caveat	Description
CSCuf91463	ASDM resending the same passcode during OTP authentication - failing it

Open Caveats in 7.1(2.102)

Table 15 contains open caveats in ASDM software Version 7.1(2.102).

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 15 Open Caveats in ASDM Version 7.1(2.102)

Caveat	Description
CSCue46483	ASDM shows incomplete ASA connection table entries
CSCue48827	ASA Local CA server add user-db in ASDM fails if blank line Subject (DN)
CSCue63828	Unable to config failover via ASDM due to Firmware version check failure
CSCue73337	Clicking Refresh after Make Standby in ASDM would cause switchover again
CSCuf16865	Bug CSCtl22199 needs added clarity
CSCuf47673	ASA-SM/ASDM: non-admin context may require auth multiple times
CSCuf60336	ASDM: Unable to handle names in DNS servers
CSCuf66300	ASDM 7.1 config bookmarks causes confusion for KCD and SharePoint use
CSCuf66309	ASDM: inside interface does not exist error during TFTP copy
CSCuf91463	ASDM resending the same passcode during OTP authentication - failing it
CSCuf93527	ASDM: HA/Scalability Wizard cannot be prompted by clicking "Launch"

Table 15 Open Caveats in ASDM Version 7.1(2.102) (continued)

Caveat	Description
CSCug00061	Multiple naming-attributes not yet supported ASDM indicates otherwise
CSCug28975	network objects not available for VPN RA wizzard

Open Caveats in 7.1(2)

Table 16 contains open caveats in ASDM software Version 7.1(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 16 Open Caveats in ASDM Version 7.1(2)

Caveat	Description
CSCud40686	Entering Incorrect Credentials Makes the ASDM Hang
CSCud68382	Java Web Start may not work on MacOS
CSCud75192	client profile not properly bound to group policy
CSCud80033	ASDM: Cannot specify "anyconnect profiles none" in webvpn group-policy
CSCud96465	HTTP authen: username greater than 50 characters failed
CSCue17774	ASDM Loses Connectivity after 24 hrs when Monitoring some Traffic's.
CSCue31262	ASDM: cannot configure BIOS check in DAP
CSCue48827	ASA Local CA server add user-db in ASDM fails if blank line Subject (DN)

Open Caveats in 7.1(1)

Table 17 contains open caveats in ASDM software Version 7.1(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 17 Open Caveats in ASDM Version 7.1(1)

Caveat	Description
CSCud03239	ASDM 7.1.1: Host Scan Image section - Instructions incorrect
CSCud07583	ASDM 7.0 ASA 9.0 multi context L2L needs more explicit warning/error.
CSCud10835	ASDM "run demo" opens a new box with unreadable characters.
CSCud24825	Need to add prompt "cluster-unit" option
CSCud35180	Access Rule Lookup in Real-Time Log Viewer Does Not Support Global ACL
CSCud67542	ASDM does not detect IPS module in ASA 5512-X and 5515-X
CSCud72575	Unable to add a sub-interface

Resolved Caveats

Resolved Caveats in 7.1(5.100)

Table 18 contains the resolved caveats in ASDM software Version 7.1(5.100).

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 18 Resolved Caveats in ASDM Version 7.1(5.100)

Caveat	Description
CSCum46193	ASDM is being blocked by Java after an upgrade to Java 7.51

Resolved Caveats in 7.1(5)

Table 19 contains the resolved caveats in ASDM software Version 7.1(5).

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 19 Resolved Caveats in ASDM Version 7.1(5)

Caveat	Description
CSCui39567	ASDM 7.x certificate maps mapped to IPsec and SSL only show under IPSec
CSCui91127	ASDM Error: Number of IP address in the pool exceeds the limit 65536.
CSCuj06653	ASDM:Credentials displayed in clear text when using Cisco.com wizard
CSCuj21794	ASDM: ID FW Monitor user-group defined with 'Space' char. not reflected
CSCuj29282	ASDM session does not timeout after idle-timeout expires
CSCuj37962	Group Policies are not bound to AnyConnect Profiles
CSCuj40436	ASDM Local CA Server Certificate Expiration Reminder update issue
CSCuj67380	Cluster wizard asking for MTU to join cluster but no place to enter
CSCuj67511	Cluster wizard: cannot edit an interface

Table 19 Resolved Caveats in ASDM Version 7.1(5) (continued)

Caveat	Description
CSCuj70997	ASDM is sending wrong cli when copy,paste group policy which has + sign.
CSCuj72318	Enable IPv6 checkbox is unchecked when editing interface
CSCuj72362	ASDM: Does not allow to configure EIGRP key using Special Characters
CSCuj75131	WebVPN configs not synced with standby - ASDM symptom

Resolved Caveats in 7.1(4)

Table 20 contains the resolved caveats in ASDM software Version 7.1(4).

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 20 Resolved Caveats in ASDM Version 7.1(4)

Caveat	Description
CSCsm55710	WebVPN Customization: easier way to configure font needed
CSCto34582	Sorting ASDM connections table by sent/received sorts lexicographically
CSCty62963	ASDM base license vlan restriction error message ambigious for ASA5505
CSCuc63501	Assist NAT exemption to site-to-site VPN configuration
CSCue53976	ASA webtype ACL may block traffic (such as Citrix) with 'permit any'
CSCuf91463	ASDM resending the same passcode during OTP authentication - failing it
CSCug37391	Already existing bookmark title cannot be edited in ASDM
CSCuh16890	Unable to edit network object in ASDM
CSCuh17598	ASDM:Password policy feature not working when configured via ASDM
CSCuh31395	ASDM: Asdm sending username command against password-policy feature
CSCuh37948	ASDM - unable to configure one-to-one translation for NAT46
CSCuh43772	IPv6 standby address is not configurable to BVI
CSCuh51335	Making service-object failed if port number field and name field is same
CSCuh51989	ASDM Anyconnect Client Profile editor file path broken
CSCuh52001	Anyconnect Profile could not be deleted if the file deleted from flash
CSCuh65051	ACL remarks applied in ASDM 6.5.1.101 cause remarks to shift
CSCuh84199	ASDM-IDM Launcher will not open on Mac OS X due to missing signature.
CSCui16956	ASDM:Real-time loging does'nt show logs after clearing invalid ip filter
CSCui20063	ASDM not displaying threat-detection information from ASA
CSCui42011	Unable to edit network object in ASDM, getting Stackoverflow error
CSCui60045	Unable to browse the IPS module from ASDM-IDM
CSCui66400	ASDM should allow all icmp/icmp6 any/any4/any6 combinations
CSCui75720	ASDM launcher: AnyConnect profiles not loading on Windows;OK with Java

Resolved Caveats in 7.1(3)

Table 21 contains the resolved caveats in ASDM software Version 7.1(3).

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 21 Resolved Caveats in ASDM Version 7.1(3)

Caveat	Description
CSCuc07375	ASDM Add User Account attribute stuck in loop
CSCud51020	ASDM not clearing xlates when making NAT changes
CSCud80033	ASDM: Cannot specify "anyconnect profiles none" in webvpn group-policy
CSCue31262	ASDM: cannot configure BIOS check in DAP
CSCue46483	ASDM shows incomplete ASA connection table entries
CSCue48763	AnyConnect Connection Profiles doesn't show group-policy in ASDM
CSCue48827	ASA Local CA server add user-db in ASDM fails if blank line Subject (DN)
CSCue63828	Unable to config failover via ASDM due to Firmware version check failure
CSCue73337	Clicking Refresh after Make Standby in ASDM would cause switchover again
CSCue97613	Unable to adjust SNMP CPU Utilization and Monitoring Interval in ASDM
CSCuf16865	Bug CSCtl22199 needs added clarity
CSCuf47673	ASA-SM/ASDM: non-admin context may require auth multiple times
CSCuf60336	ASDM: Unable to handle names in DNS servers
CSCuf66300	ASDM 7.1 config bookmarks causes confusion for KCD and SharePoint use
CSCuf66309	ASDM: inside interface does not exist error during TFTP copy
CSCuf66741	ASDM: Crypto trustpool import fails with error
CSCuf93527	ASDM: HA/Scalability Wizard cannot be prompted by clicking "Launch"
CSCug00061	Multiple naming-attributes not yet supported ASDM indicates otherwise
CSCug28975	network objects not available for VPN RA wizzard

Resolved Caveats in 7.1(2.102)

We did not resolve any caveats in this release.

Resolved Caveats in 7.1(2)

Table 22 contains the resolved caveats in ASDM software Version 7.1(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 22 Resolved Caveats in ASDM Version 7.1(2)

Caveat	Description
CSCub14386	Upgrade image to whole cluster: sometime fail to copy images
CSCud07583	ASDM 7.0 ASA 9.0 multi context L2L needs more explicit warning/error.
CSCud35180	Access Rule Lookup in Real-Time Log Viewer Does Not Support Global ACL
CSCud45909	asdm empty Vendor field when setting dap policy for anti-spyware
CSCud46446	Checkbox text too long to cause usability problem
CSCud46473	ASDM 7 doesn't save logical operation value for DAP entries
CSCud48451	ASDM: Enabling Route Tracking defaults route metric 128
CSCud55732	Unexpected configuration tag 'timeout-alert' appears when booting ASA
CSCud77692	User Accounts has two Identity tree nodes
CSCud83155	PPPOE interface shows up as static and not available for VPN connection
CSCud89093	NAT64: Need to error message for incorrect manual nat64
CSCud96486	A status popup should be dismissed after adding cluster member
CSCue05073	Display warning when admin selectis SSLv3 options
CSCue06198	Adding a unit through the wizard changes master's cluster config
CSCue06218	Cannot re-add unit to cluster via High Availability & Scalability wizard
CSCue46483	ASDM shows incomplete ASA connection table entries
CSCue53719	ASA Cluster node is missing under System in multi mode

Resolved Caveats in 7.1(1)

Table 23 contains the resolved caveats in ASDM software Version 7.1(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 23 Resolved Caveats in ASDM Version 7.1(1)

Caveat	Description
CSCsw98659	IPv6: Restore the default value of "DAD Attempts", "Reachable Time".
CSCsz56544	ASDM: Implement the ability to better sort ACL's
CSCtk48070	Make the IPv4/IPv6 view options for ACLs sticky
CSCtq19131	Clientless WebVPN-Delete bookmark which in use-error msg not consistent
CSCtt24721	False Error when Manually Enabling Anonymous Reporting the First Time
CSCtw48086	IPv4 to be made as default for Access Rules/ACL Manager
CSCtx17400	ENH:space availability in flash should be checked before transfer starts
CSCty23077	Deferred update - ASDM

Table 23 Resolved Caveats in ASDM Version 7.1(1) (continued)

Caveat	Description
CSCtz88888	ASDM Falcon: Make the IP address in the ASA CX/PRSM URL configurable
CSCtz91753	UI mis-alignment in ASDM w/ Win 2008 R2 and Java 1.7
CSCua79518	Horizontal scroll bar is needed for Interface panel of HA cluster wizard
CSCub14334	ASA-CX startup wizard panel does not display mask and gateway
CSCub22142	ASACX - Display ASA CX dashboard with deivce info and interface status
CSCub32255	Java Error in VPN Load Balance
CSCub43701	Need online help on Torino
CSCub52216	ASA fails to select DAP record when checking for device type Endpoint ID
CSCuc09172	Cluster Dashboard: allow the user to resize the table vertically
CSCuc37658	ASDM Services panel fails to locate Service Object with Where Used btn
CSCuc59446	IPv6/IPv4 option missing when configuring network object
CSCuc61363	Improper column sizing for File Management Panel
CSCuc63797	Static policy nat is not working in ASDM 6.49-103
CSCuc68351	ASDM truncates regular expression in username-from-certificate script
CSCuc77445	Design change on ASDM when cluster is configured without cluster license
CSCuc81697	ASDM changes AES to DES in IKEv1 policy
CSCuc93858	Add deprecation message to Secure Desktop setup panel
CSCuc97140	Torino: service policy for CX redirect, destination fields don't match
CSCuc97192	Torino: ASDM ignored commands shown for valid ASA commands
CSCud02591	Dynamic NAT using names may not be displayed properly
CSCud03838	ASDM 7.0 warning "uploaded file is not a valid ASA-SM image" on 9.0.1
CSCud05948	New iPads device type needs to be added to DAP
CSCud06933	AnyConnect Connection Profiles with external group-policy in ASDM
CSCud09472	ASDM 7.0.2 doesn't recognize "trustpoint" keyword in View/Clear CRL
CSCud10605	ASDM: restrict aes-gmac IPSec encryption for AnyConnect IPSec Proposals
CSCud16594	ASDM 7.0 Edit Bookmark Window empty
CSCud20548	ASDM 7.0 does not display unidirectional NAT rules with service.
CSCud25139	Config >RA VPN>Clientless SSL VPN Access>Portal>Bookmarks assign issue
CSCud30081	ASDM Torino: Change release notes link
CSCud32116	ASDM Torinio: Service Policy Rules help link is not correct
CSCud32117	Postpone ASDM Enhancement to VDI

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/asadocs

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* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. 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.

©2012-2014 Cisco Systems, Inc. All rights reserved.