Release Notes for Cisco ASDM, Version 7.1(x)

Released: December 3, 2012
Updated: March 3, 2015

This document contains release information for Cisco ASDM Version 7.1(1) through 7.1(7) 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 "Upgrading the Software" section on page 23.

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

	Browser				
Operating System	**Internet Explorer**	**Firefox**	**Safari**	**Chrome**	**Java SE Plug-in**
Microsoft Windows (English and Japanese): • 8[1] • 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 Macintosh 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): • Desktop • Desktop with Workstation	N/A	1.5 or later	N/A	18 or later	6 or later

1. ASDM Version 7.1(3) and 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 • Java Web Start requires newer ASDM version *or* workaround	To continue using the Launcher, do one of the following: • 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. 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 work-around 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.

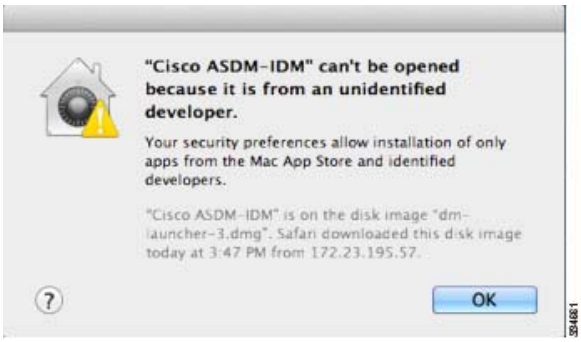
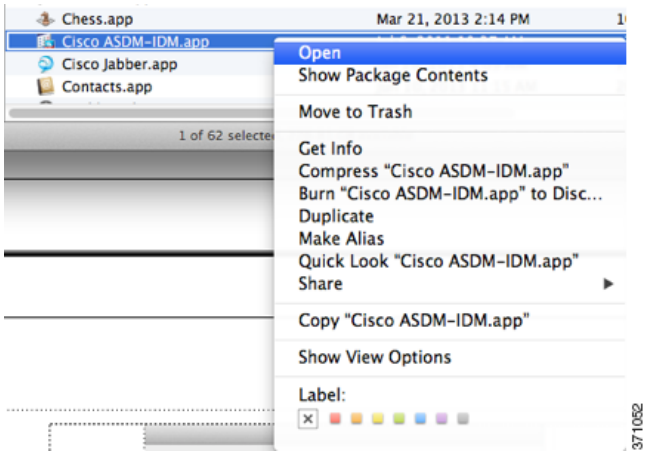
Table 2 Caveats for ASDM Compatibility

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. 

Installing an Identity Certificate for ASDM

When using Java 7 update 51 and later, the ASDM Launcher requires a trusted certificate. An easy approach to fulfill the certificate requirements is to install a self-signed identity certificate. You can use Java Web Start to launch ASDM until you install a certificate.

See 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/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

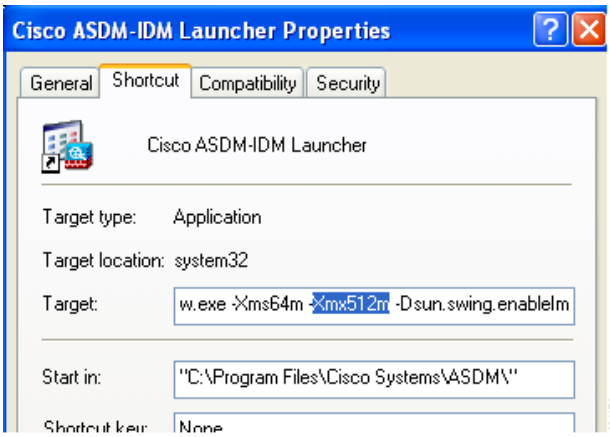
Maximum Configuration Size in ASDM

- 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**.

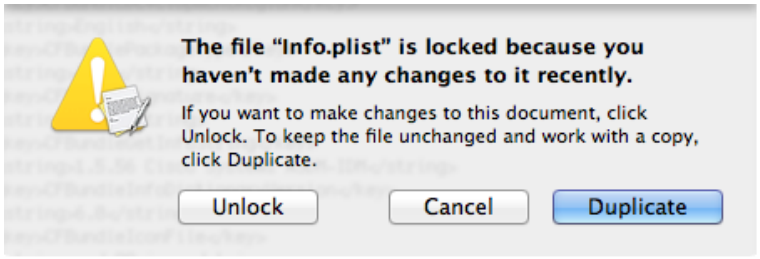
b. In the Contents folder, double-click the Info.plist file. If you have Developer tools installed, it opens in the Property List Editor. Otherwise, it opens in TextEdit.

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>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

Note Versions prior to 7.1(6) are no longer available to download. Please upgrade to a later version.

New Features in Version 7.1(7)

Released: March 3, 2015

There are no new features in this version.

New Features in Version 7.1(6)

Released: March 31, 2014

Table 3 lists the new features for ASA Version 9.1(5)/ASDM Version 7.1(6).

Table 3 New Features for ASA Version 9.1(5)/ASDM Version 7.1(6)

Feature	Description
Administrative Features	
Secure Copy client	The ASA now supports the Secure Copy (SCP) client to transfer files to and from a SCP server. We modified the following screens: Tools > File Management > File Transfer > Between Remote Server and Flash Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server
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.
Firewall Features	

Table 3 New Features for ASA Version 9.1(5)/ASDM Version 7.1(6) (continued)

Feature	Description
Transactional Commit Model on rule engine for access groups	When enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. We introduced the following screen: Configuration > Device Management > Advanced > Rule Engine.
Monitoring Features	
SNMP hosts, host groups, and user lists	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. We modified the following screen: Configuration > Device Management > Management Access > SNMP.
Remote Access Features	
AnyConnect DTLS Single session Performance Improvement	UDP traffic, such as streaming media, was being affected by a high number of dropped packets when sent over an AnyConnect DTLS connection. For example, this could result in streaming video playing poorly or cease streaming completely. The reason for this was the relatively small size of the flow control queue. We increased the DTLS flow-control queue size and offset this by reducing the admin crypto queue size. For TLS sessions, the priority of the crypto command was increased to high to compensated for this change. For both DTLS and TLS sessions, the session will now persist even if packets are dropped. This will prevent media streams from closing and ensure that the number of dropped packets is comparable with other connection methods. We did not modify any ASDM screens.
Webtype ACL enhancements	We introduced URL normalization. URL normalization is an additional security feature that includes path normalization, case normalization and scheme normalization. URLs specified in an ACE and portal address bar are normalized before comparison; for making decisions on webvpn traffic filtering. We did not modify any ASDM screens.

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

Table 4 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 > Clientliess SSL VPN Access > VDI Access.
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, such as the Nexus 5000, 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

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

Feature	Description
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.
Support for clustering with the Cisco Nexus 5000 and Cisco Catalyst 3750-X	The ASA supports clustering when connected to the Cisco Nexus 5000 and Cisco Catalyst 3750-X. We modified the following screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster
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 5 lists the new features for ASA Version 9.1(3)/ASDM Version 7.1(4).

Table 5 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	
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).*

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

Feature	Description
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 6 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 6 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 7 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 7 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.
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	

Table 7 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
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.
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.

Table 7 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
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 ASASM (see the **session** command). For initial ASASM 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 ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information.
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.

Table 7 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
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.
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	

Table 7 New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)

Feature	Description
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 7 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 8 lists the new features for ASA Version 8.4(6)/ASDM Version 7.1(2.102).

Table 8 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 9 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 9 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.
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 ASASM (see the **session** command). For initial ASASM 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 10 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 10 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

See http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/upgrade/upgrade91.html.

Open Caveats

Open Caveats in 7.1(7)

Table 11 contains open caveats in ASDM software Version 7.1(7).

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 11 Open Caveats in ASDM Version 7.1(7)

Caveat	Description
CSCuj75028	SSL VPN bookmark's form parameter has unclear value
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
CSCul11018	Cluster wizard fails ungracefully with CCL issues

Table 11 Open Caveats in ASDM Version 7.1(7) (continued)

Caveat	Description
CSCul38916	ASDM:Not able to configure "Shun Duration" for threat-detection
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:
CSCum57517	ASDM launcher is not working with Java 7u51
CSCum62475	ASDM sending wrong encrypted password
CSCum67073	ASDM : No warning while activating AC essentials license
CSCum98114	ASDM not responding properly when group url doesn't contain http/https
CSCun64783	ASDM "not used" treats object with auto-NAT as not in use.

Open Caveats in 7.1(6)

Table 12 contains open caveats in ASDM software Version 7.1(6).

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(6)

Caveat	Description
CSCuj75028	SSL VPN bookmark's form parameter has unclear value
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
CSCul11018	Cluster wizard fails ungracefully with CCL issues
CSCul38916	ASDM:Not able to configure "Shun Duration" for threat-detection
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:
CSCum57517	ASDM launcher is not working with Java 7u51
CSCum62475	ASDM sending wrong encrypted password
CSCum67073	ASDM : No warning while activating AC essentials license
CSCum98114	ASDM not responding properly when group url doesn't contain http/https
CSCun64783	ASDM "not used" treats object with auto-NAT as not in use.

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

Table 13 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 13 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
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
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 14 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 14 Open Caveats in ASDM Version 7.1(4)

Caveat	Description
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
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

Table 14 Open Caveats in ASDM Version 7.1(4) (continued)

Caveat	Description
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 15 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 15 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 16 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 16 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"
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 17 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 17 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 18 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 18 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(7)

There are no resolved caveats in this version.

Resolved Caveats in 7.1(6)

Table 19 contains the resolved caveats in ASDM software Version 7.1(6).

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(6)

Caveat	Description
CSCuh28694	ASDM on Mac: System font issues (font too large)
CSCuj88707	ASDM did not get a response from the ASA in the last 60 seconds
CSCul07863	'Pre-login Page URL' is not saved within ASDM
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
CSCul53360	IPv6 filed added to AnyConnect profile by wizard is invalid
CSCum16945	ASDM cannot be properly filtered by "Access Rules"
CSCum62475	ASDM sending wrong encrypted password
CSCum65694	ASDM Unable to add user in system context

Resolved Caveats in 7.1(5.100)

Table 20 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 20 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 21 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 21 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
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 22 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 22 Resolved Caveats in ASDM Version 7.1(4)

Caveat	Description
CSCto34582	Sorting ASDM connections table by sent/received sorts lexicographically
CSCuf91463	ASDM resending the same passcode during OTP authentication - failing it

Table 22 Resolved Caveats in ASDM Version 7.1(4) (continued)

Caveat	Description
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
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 23 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 23 Resolved Caveats in ASDM Version 7.1(3)

Caveat	Description
CSCuc07375	ASDM Add User Account attribute stuck in loop
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
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

Table 23 Resolved Caveats in ASDM Version 7.1(3) (continued)

Caveat	Description
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 24 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 24 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
CSCud48451	ASDM: Enabling Route Tracking defaults route metric 128
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

Resolved Caveats in 7.1(1)

Table 25 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 25 Resolved Caveats in ASDM Version 7.1(1)

Caveat	Description
CSCtq19131	Clientless WebVPN-Delete bookmark which in use-error msg not consistent
CSCtt24721	False Error when Manually Enabling Anonymous Reporting the First Time
CSCty23077	Deferred update - ASDM
CSCub32255	Java Error in VPN Load Balance
CSCuc59446	IPv6/IPv4 option missing when configuring network object
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
CSCuc97192	Torino: ASDM ignored commands shown for valid ASA commands
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/c/en/us/td/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 delivers 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.