Release Notes for Cisco ASDM, Version 6.4(x)

Released: January 31, 2011
Updated: August 13, 2012

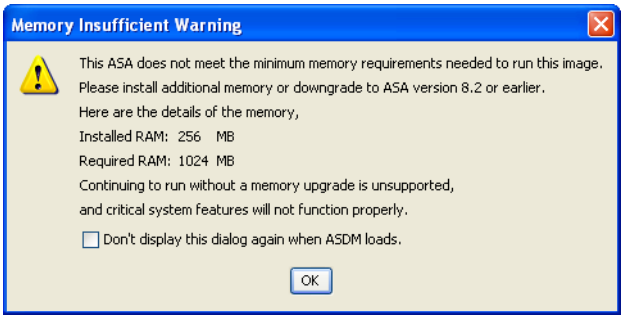
This document contains release information for Cisco ASDM Versions 6.4(1) through 6.4(9.103) for the Cisco ASA 5500 series. This document includes the following sections:

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

Important Notes

Memory Requirements

To run Version 8.3 or later in a production environment, you may need to upgrade the memory on the Cisco ASA 5505, 5510, 5520, or 5540. See the ASA release notes for more information. If you do not have enough memory, you receive the following message upon logging in:



Maximum Configuration Size

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 (Windows only), and then modify the ASDM-IDM Launcher shortcut by performing the following steps:

Step 1 Right-click the shortcut for the ASDM-IDM Launcher, and choose **Properties**.

Step 2 Click the **Shortcut** tab.

Step 3 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. For more information about this parameter, see the Oracle document in the following location: http://docs.oracle.com/javase/1.5.0/docs/tooldocs/windows/java.html

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			Sun Java SE Plug-in[1]
	Internet Explorer	Firefox[2]	Safari	
Microsoft Windows (English and Japanese): • 7 • Vista • 2008 Server • XP	6.0 or later[2]	1.5 or later	No support	6.0
Apple Macintosh OS X: • 10.7[3] • 10.6 • 10.5 • 10.4	No support	1.5 or later	2.0 or later	6.0
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • Desktop with Workstation	N/A	1.5 or later	N/A	6.0

1. Support for Java 5.0 was removed in ASDM 6.4. Obtain Sun Java updates from java.sun.com.
2. ASDM requires an SSL connection from the browser to the ASA. By default, Internet Explorer on Windows Vista and later and Firefox on all operating systems do not support base encryption (DES) for SSL, and therefore require the ASA to have a strong encryption (3DES/AES) license. 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.
3. 6.4(7) and later. 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.

ASDM Compatibility

Table 2 lists information about ASDM, module, and VPN compatibility with the ASA 5500 series.

Table 2 ASDM, SSM, SSC, and VPN Compatibility

Application	Description
ASDM	ASA Version 8.4(1) requires ASDM Version 6.4(1) or later. ASA Version 8.4.1(11) requires ASDM Version 6.4(2) or later. ASA Version 8.2(5) requires ASDM Version 6.4(3) or later. ASA Version 8.4(2) requires ASDM Version 6.4(5) or later. ASA Version 8.4(3) requires ASDM Version 6.4(7) or later. ASA Version 8.4(4.1) requires ASDM Version 6.4(9). For information about ASDM requirements for other releases, see *Cisco ASA Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html
VPN	For the latest OS and browser test results, see the *Supported VPN Platforms, Cisco ASA 5500 Series*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html
Module applications	For information about module application requirements, 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*.

New Features

This section includes the following topics:

Note New, changed, and deprecated syslog messages are listed in *Cisco ASA 5500 Series System Log Messages*.

New Features in ASA 8.4(4.5)/ASDM 6.4(9.103)

Released: August 13, 2012

Table 11 lists the new features for ASA interim Version 8.4(4.5)/ASDM Version 6.4(9.103).

Note Version 8.4(4.3) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.5) or later.

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release.

Table 3 New Features for ASA Version 8.4(4.5)/ASDM Version 6.4(9.103)

Feature	Description
Firewall Features	
ARP cache additions for non-connected subnets	The ASA ARP cache only contains entries from directly-connected subnets by default. You can now enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries. You may want to use this feature if you use: • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. We modified the following screen: Configuration > Device Management > Advanced > ARP > ARP Static Table. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*

Table 3 New Features for ASA Version 8.4(4.5)/ASDM Version 6.4(9.103) (continued)

Feature	Description
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. *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 ASA 8.4(41)/ASDM 6.4(9)

Released: June 18, 2012

Table 4 lists the new features for ASA Version 8.4(4.1)/ASDM Version 6.4(9).

Note Version 8.4(4) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.1) or later.

Table 4 New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9)

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 5500 series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, and ASA 5585-X. 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. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
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 *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(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 using Base64 key up to 2048 bits. We introduced the following screen: Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Table 4 New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9) (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. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(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. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
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. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Image verification	Support for SHA-512 image integrity checking was added. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Table 4 New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9) (continued)

Feature	Description
Improved pseudo-random number generation	Hardware-based noise for additional entropy was added to the software-based random number generation process. This change makes pseudo-random number generation (PRNG) more random and more difficult for attackers to get a repeatable pattern or guess the next random number to be used for encryption and decryption operations. Two changes were made to improve PRNG: • Use the current hardware-based RNG for random data to use as one of the parameters for software-based RNG. • If the hardware-based RNG is not available, use additional hardware noise sources for software-based RNG. Depending on your model, the following hardware sensors are used: – ASA 5505—Voltage sensors. – ASA 5510 and 5550—Fan speed sensors. – ASA 5520, 5540, and 5580—Temperature sensors. – ASA 5585-X—Fan speed sensors. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Remote Access Features	
Clientless SSL VPN: Enhanced quality for rewriter engines	The clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN users. We did not add or modify any ASDM screens for this feature. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Failover Features	
Configure the connection replication rate during a bulk sync	You can now configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASA is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synced. *This feature is not available in 8.6(1) or 8.7(1). This feature is also in 8.5(1.7).*
Application Inspection Features	
SunRPC change from dynamic ACL to pin-hole mechanism	Previously, Sun RPC inspection does not support outbound access lists because the inspection engine uses dynamic access lists instead of secondary connections. In this release, when you configure dynamic access lists on the ASA, they are supported on the ingress direction only and the ASA drops egress traffic destined to dynamic ports. Therefore, Sun RPC inspection implements a pinhole mechanism to support egress traffic. Sun RPC inspection uses this pinhole mechanism to support outbound dynamic access lists. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*

Table 4 New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9) (continued)

Feature	Description
Inspection reset action change	Previously, when the ASA dropped a packet due to an inspection engine rule, the ASA sent only one RST to the source device of the dropped packet. This behavior could cause resource issues. In this release, when you configure an inspection engine to use a reset action and a packet triggers a reset, the ASA sends a TCP reset under the following conditions: • The ASA sends a TCP reset to the inside host when the **service resetoutbound** command is enabled. (The **service resetoutbound** command is disabled by default.) • The ASA sends a TCP reset to the outside host when the **service resetinbound** command is enabled. (The **service resetinbound** command is disabled by default.) For more information, see the **service** command in the ASA *Cisco Security Appliance Command Reference*. This behavior ensures that a reset action will reset the connections on the ASA and on inside servers; therefore countering denial of service attacks. For outside hosts, the ASA does not send a reset by default and information is not revealed through a TCP reset. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Module Features	
ASA 5585-X support for the ASA CX SSP-10 and -20	The ASA CX module lets you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees. We introduced the following screens: Home > ASA CX Status Wizards > Startup Wizard > ASA CX Basic Configuration Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA CX Inspection
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 *This feature is not available in 9.0(1), 9.0(2), or 9.1(1).*

New Features in ASA 8.4(3)/ASDM 6.4(7)

Released: January 9, 2012

Table 5 lists the new features for ASA Version 8.4(3)/ASDM Version 6.4(7).

Table 5 New Features for ASA Version 8.4(3)/ASDM Version 6.4(7)

Feature	Description
NAT Features	
Round robin PAT pool allocation uses the same IP address for existing hosts	When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. We did not modify any screens. *This feature is not available in 8.5(1).*
Flat range of PAT ports for a PAT pool	If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool. If you have a lot of traffic that uses the lower port ranges, when using a PAT pool, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535. We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object Configuration > Firewall > NAT Rules > Add/Edit NAT Rule *This feature is not available in 8.5(1).*
Extended PAT for a PAT pool	Each PAT IP address allows up to 65535 ports. If 65535 ports do not provide enough translations, you can now enable extended PAT for a PAT pool. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object Configuration > Firewall > NAT Rules > Add/Edit NAT Rule *This feature is not available in 8.5(1).*
Configurable timeout for PAT xlate	When a PAT xlate times out (by default after 30 seconds), and the ASA reuses the port for a new translation, some upstream routers might reject the new connection because the previous connection might still be open on the upstream device. The PAT xlate timeout is now configurable, to a value between 30 seconds and 5 minutes. We modified the following screen: Configuration > Firewall > Advanced > Global Timeouts. *This feature is not available in 8.5(1).*

Table 5 New Features for ASA Version 8.4(3)/ASDM Version 6.4(7) (continued)

Feature	Description
Automatic NAT rules to translate a VPN peer's local IP address back to the peer's real IP address	In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address. You can enable this feature on one interface per tunnel group. Object NAT rules are dynamically added and deleted when the VPN session is established or disconnected. You can view the rules using the **show nat** command. **Note** Because of routing issues, we do not recommend using this feature unless you know you need this feature; contact Cisco TAC to confirm feature compatibility with your network. See the following limitations: • Only supports Cisco IPsec and AnyConnect Client. • Return traffic to the public IP addresses must be routed back to the ASA so the NAT policy and VPN policy can be applied. • Does not support load-balancing (because of routing issues). • Does not support roaming (public IP changing). ASDM does not support this command; enter the command using the Command Line Tool.
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4.
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConnect Client > SSL Compression.
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout. We introduced the following screens: Remote Access VPN > Configuration > Clientless SSL VPN Access > Portal > Customizations > Add/Edit > Timeout Alerts Remote Access VPN > Configuration > Clientless SSL VPN Access > Group Policies > Add/Edit General
AAA Features	

Table 5 New Features for ASA Version 8.4(3)/ASDM Version 6.4(7) (continued)

Feature	Description
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this command in aaa-server host configuration mode). ASDM does not support this command; enter the command using the Command Line Tool.
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.
Key vendor-specific attributes (VSAs) sent in RADIUS access request and accounting request packets from the ASA	Four New VSAs—Tunnel Group Name (146) and Client Type (150) are sent in RADIUS access request packets from the ASA. Session Type (151) and Session Subtype (152) are sent in RADIUS accounting request packets from the ASA. All four attributes are sent for all accounting request packet types: Start, Interim-Update, and Stop. The RADIUS server (for example, ACS and ISE) can then enforce authorization and policy attributes or use them for accounting and billing purposes.
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*. ASDM does not support this command; enter the command using the Command Line Tool.

New Features in ASDM 6.4(5.206)

Released: October 24, 2011

There are no new features in Version 6.4(5.206).

New Features in ASDM 6.4(5.205)

Released: October 18, 2011

Due to caveat CSCtt45397, "ASDM Launcher version 1.5(53) fails to connect to ASA," this release has been removed from Cisco.com. Please upgrade to Version 6.4(5.206) or later.

There are no new features in Version 6.4(5.205).

New Features in ASDM 6.4(5.204)

Released: October 11, 2011

Due to caveat CSCtt42234, "Unlicensed IPS warning incorrectly displayed when allocating traffic," this release has been removed from Cisco.com. Please upgrade to Version 6.4(5.205) or later.

There are no new features in Version 6.4(5.204).

New Features in ASDM 6.4(5.106)

ASDM Version 6.4(5.106) supports new features in the following ASA interim versions:

New Features in ASA 8.2(5.13)

Released: September 18, 2011

Table 8 lists the new features for ASA interim Version 8.2(5.13)/ASDM Version 6.4(5.106).

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Table 6 New Features for ASA Interim Version 8.2(5.13)/ASDM Version 6.4(5.106)

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. *Also available in Version 8.3(2.25) and 8.4.2(8).*

Table 6 New Features for ASA Interim Version 8.2(5.13)/ASDM Version 6.4(5.106) (continued)

Feature	Description
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConnect Client > SSL Compression. *Also available in Version 8.3(2.25) and Version 8.4.2(8).*
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*. ASDM does not support this command; enter the command using the Command Line Tool. *Also available in Version 8.3(2.25) and Version 8.4.2(8).*

New Features in ASA 8.3(2.25)

Released: August 31, 2011

Table 8 lists the new features for ASA interim Version 8.3(2.25)/ASDM Version 6.4(5.106).

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Table 7 New Features for ASA Interim Version 8.3(2.25)/ASDM Version 6.4(5.106)

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. *Also available in Version 8.2(5.13) and 8.4.2(8).*
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConnect Client > SSL Compression. *Also available in Version 8.2(5.13) and 8.4.2(8).*
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*. ASDM does not support this command; enter the command using the Command Line Tool. *Also available in Version 8.2(5.13) and 8.4.2(8).*

New Features in ASA 8.4(2.8)

Released: August 31, 2011

Table 8 lists the new features for ASA interim Version 8.4(2.8)/ASDM Version 6.4(5.106).

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release.

Table 8 New Features for ASA Interim Version 8.4(2.8)/ASDM Version 6.4(5.106)

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. *Also available in Version 8.2(5.13) and 8.3.2(25).*
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConnect Client > SSL Compression. *Also available in Version 8.2(5.13) and 8.3.2(25).*
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout. We introduced the following screens: Remote Access VPN > Configuration > Clientless SSL VPN Access > Portal > Customizations > Add/Edit > Timeout Alerts Remote Access VPN > Configuration > Clientless SSL VPN Access > Group Policies > Add/Edit General
AAA Features	
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this command in aaa-server host configuration mode). ASDM does not support this command; enter the command using the Command Line Tool.
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.

Table 8 New Features for ASA Interim Version 8.4(2.8)/ASDM Version 6.4(5.106) (continued)

Feature	Description
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*. ASDM does not support this command; enter the command using the Command Line Tool. *Also available in Version 8.2(5.13) and 8.3.2(25).*

New Features in ASA 8.4(2)/ASDM 6.4(5)

Released: June 20, 2011

Table 9 lists the new features for ASA Version 8.4(2)/ASDM Version 6.4(5).

Table 9 New Features for ASA Version 8.4(2)/ASDM Version 6.4(5)

Feature	Description
Firewall Features	
Identity Firewall	Typically, a firewall is not aware of the user identities and, therefore, cannot apply security policies based on identity. The Identity Firewall in the ASA provides more granular access control based on users' identities. You can configure access rules and security policies based on usernames and user groups name rather than through source IP addresses. The ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped usernames instead of network IP addresses. The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping. The ASA uses Windows Active Directory as the source to retrieve the current user identity information for specific IP addresses. In an enterprise, some users log onto the network by using other authentication mechanisms, such as authenticating with a web portal (cut-through proxy) or by using a VPN. You can configure the Identity Firewall to allow these types of authentication in connection with identity-based access policies. We introduced the following screens: Configuration > Firewall > Identity Options. Configuration > Firewall > Objects > Local User Groups Monitoring > Properties > Identity We modified the following screen: Configuration > Device Management > Users/AAA > AAA Server Groups > Add/Edit Server Group.

Table 9 New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)

Feature	Description
Identity NAT configurable proxy ARP and route lookup	In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was always used to determine the egress interface. You could not configure these settings. In 8.4(2) and later, the default behavior for identity NAT was changed to match the behavior of other static NAT configurations: proxy ARP is enabled, and the NAT configuration determines the egress interface (if specified) by default. You can leave these settings as is, or you can enable or disable them discretely. Note that you can now also disable proxy ARP for regular static NAT. For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: **no-proxy-arp** and **route-lookup**. The **unidirectional** keyword that was used for migrating to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. The **unidirectional** keyword is removed. We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object > Advanced NAT Settings Configuration > Firewall > NAT Rules > Add/Edit NAT Rule
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy. **Note** Currently in 8.4(2), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634). We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object Configuration > Firewall > NAT Rules > Add/Edit NAT Rule
IPv6 Inspection	You can configure IPv6 inspection by configuring a service policy to selectively block IPv6 traffic based on the extension header. IPv6 packets are subjected to an early security check. The ASA always passes hop-by-hop and destination option types of extension headers while blocking router header and no next header. You can enable default IPv6 inspection or customize IPv6 inspection. By defining a policy map for IPv6 inspection you can configure the ASA to selectively drop IPv6 packets based on following types of extension headers found anywhere in the IPv6 packet: • Hop-by-Hop Options • Routing (Type 0) • Fragment • Destination Options • Authentication • Encapsulating Security Payload We introduced the following screen: Configuration > Firewall > Objects > Inspect Maps > IPv6.

Table 9 New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)

Feature	Description
Remote Access Features	
Portal Access Rules	This enhancement allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in the HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Portal Access Rules. *Also available in Version 8.2(5).*
Clientless support for Microsoft Outlook Web App 2010	The ASA 8.4(2) clientless SSL VPN core rewriter now supports Microsoft Outlook Web App 2010.
Secure Hash Algorithm SHA-2 Support for IPsec IKEv2 Integrity and PRF	This release supports the Secure Hash Algorithm SHA-2 for increased cryptographic hashing security for IPsec/IKEv2 AnyConnect Secure Mobility Client connections to the ASA. SHA-2 includes hash functions with digests of 256, 384, or 512 bits, to meet U.S. government requirements. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies > Add/Edit IKEv2 Policy (Proposal).
Secure Hash Algorithm SHA-2 Support for Digital Signature over IPsec IKEv2	This release supports the use of SHA-2 compliant signature algorithms to authenticate IPsec IKEv2 VPN connections that use digital certificates, with the hash sizes SHA-256, SHA-384, and SHA-512. SHA-2 digital signature for IPsec IKEv2 connections is supported with the AnyConnect Secure Mobility Client, Version 3.0.1 or later.
Split Tunnel DNS policy for AnyConnect	This release includes a new policy pushed down to the AnyConnect Secure Mobility Client for resolving DNS addresses over split tunnels. This policy applies to VPN connections using the SSL or IPsec/IKEv2 protocol and instructs the AnyConnect client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyConnect client does not try to resolve the address through public DNS servers. By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy: tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Group Policy > Advanced > Split Tunneling (see the Send All DNS Lookups Through Tunnel check box). *Also available in Version 8.2(5).*

Table 9 New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)

Feature	Description
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	You can now configure the ASA to permit or deny VPN connections to mobile devices, enable or disable mobile device access on a per group bases, and gather information about connected mobile devices based on a mobile device's posture data. The following mobile platforms support this capability: AnyConnect for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Android Version 2.4.x. **Licensing Requirements** Enforcing remote access controls and gathering posture data from mobile devices requires an AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to be installed on the ASA. You receive the following functionality based on the license you install: • **AnyConnect Premium License Functionality** Enterprises that install the AnyConnect Premium license will be able to enforce DAP policies, on supported mobile devices, based on these DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device. • **AnyConnect Essentials License Functionality** Enterprises that install the AnyConnect Essentials license will be able to do the following: – Enable or disable mobile device access on a per group basis and to configure that feature using ASDM. – Display information about connected mobile devices via CLI or ASDM without having the ability to enforce DAP policies or deny or allow remote access to those mobile devices. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add/Edit Endpoint Attributes > Endpoint Attribute Type:AnyConnect. *Also available in Version 8.2(5).*
SSL SHA-2 digital signature	You can now use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5(1) or later (2.5(2) or later recommended). This release does not support SHA-2 for other uses or products. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. We did not modify any screens. *Also available in Version 8.2(5).*
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	ASA supports SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients when using the L2TP/IPsec protocol. We did not modify any screens. *Also available in Version 8.2(5).*

Table 9 New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)

Feature	Description
Enable/disable certificate mapping to override the group-url attribute	This feature changes the preference of a connection profile during the connection profile selection process. By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This optional feature changes the preference to a connection profile that specifies the group URL requested by the endpoint. The new option lets administrators rely on the group URL preference used by many older ASA software releases. We modified the following screens: Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profiles Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles *Also available in Version 8.2(5).*
ASA 5585-X Features	
Support for Dual SSPs for SSP-40 and SSP-60	For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). Each SSP acts as an independent device, with separate configurations and management. You can use the two SSPs as a failover pair if desired. **Note** When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled. We did not modify any screens.
Support for the IPS SSP-10, -20, -40, and -60	We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10. *Also available in Version 8.2(5).*
CSC SSM Features	
CSC SSM Support	For the CSC SSM, support for the following features has been added: • HTTPS traffic redirection: URL filtering and WRS queries for incoming HTTPS connections. • Configuring global approved whitelists for incoming and outgoing SMTP and POP3 e-mail. • E-mail notification for product license renewals. We modified the following screens: Configuration > Trend Micro Content Security > Mail > SMTP Configuration > Trend Micro Content Security > Mail > POP3 Configuration > Trend Micro Content Security > Host/Notification Settings Configuration > Trend Micro Content Security > CSC Setup > Host Configuration
Monitoring Features	
Smart Call-Home Anonymous Reporting	Customers can now help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device. We modified the following screen: Configuration > Device Monitoring > Smart Call-Home. *Also available in Version 8.2(5).*

Table 9 New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)

Feature	Description
IF-MIB ifAlias OID support	The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will be set to the value that has been set for the interface description. *Also available in Version 8.2(5).*
Interface Features	
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interfaces; support was previously added for 10-Gigabit Ethernet interfaces in 8.2(2). We modified the following screens: (Single Mode) Configuration > Device Setup > Interfaces > Add/Edit Interface > General (Multiple Mode, System) Configuration > Interfaces > Add/Edit Interface *Also available in Version 8.2(5).*
Management Features	
Increased SSH security; the SSH default username is no longer supported	Starting in 8.4(2), you can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or Configuration > Device Management > Users/AAA > AAA Access > Authentication (ASDM); then define a local user by entering the **username** command (CLI) or choosing Configuration > Device Management > Users/AAA > User Accounts (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.
Unified Communications Features	
ASA-Tandberg Interoperability with H.323 Inspection	H.323 Inspection now supports uni-directional signaling for two-way video sessions. This enhancement allows H.323 Inspection of one-way video conferences supported by Tandberg video phones. Supporting uni-directional signaling allows Tandberg phones to switch video modes (close their side of an H.263 video session and reopen the session using H.264, the compression standard for high-definition video). We did not modify any screens. *Also available in Version 8.2(5).*
Routing Features	
Timeout for connections using a backup static route	When multiple static routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value. We modified the following screen: Configuration > Firewall > Advanced > Global Timeouts. *Also available in Version 8.2(5).*

Table 9 New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)

Feature	Description
ASDM Features	
Migrate Network Object Group Members	If you migrate to 8.3 or later, the ASA creates named network objects to replace inline IP addresses in some features. In addition to named objects, ASDM automatically creates non-named objects for any IP addresses used in the configuration. These auto-created objects are identified by the IP address only, do not have a name, and are not present as named objects in the platform configuration. When the ASA creates named objects as part of the migration, the matching non-named ASDM-only objects are replaced with the named objects. The only exception are non-named objects in a network object group. When the ASA creates named objects for IP addresses that are inside a network object group, ASDM retains the non-named objects as well, creating duplicate objects in ASDM. To merge these objects, choose **Tools > Migrate Network Object Group Members**. We introduced the following screen: Tools > Migrate Network Object Group Members. See *Cisco ASA 5500 Migration to Version 8.3 and Later* for more information.

New Features in ASA 8.2(5)/ASDM 6.4(3)

Released: May 23, 2011

Table 10 lists the new features for ASA Version 8.2(5)/ASDM Version 6.4(3).

Table 10 New Features for ASA Version 8.2(5)/ASDM Version 6.4(3)

Feature	Description
Monitoring Features	
Smart Call-Home Anonymous Reporting	Customers can now help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device. We modified the following screen: Configuration > Device Monitoring > Smart Call-Home. *Also available in Version 8.4(2).*
IF-MIB ifAlias OID support	The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will be set to the value that has been set for the interface description. *Also available in Version 8.4(2).*
Remote Access Features	
Portal Access Rules	This enhancement allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in the HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Portal Access Rules. *Also available in Version 8.4(2).*

Table 10 New Features for ASA Version 8.2(5)/ASDM Version 6.4(3) (continued)

Feature	Description
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	You can now configure the ASA to permit or deny VPN connections to mobile devices, enable or disable mobile device access on a per-group basis, and gather information about connected mobile devices based on the mobile device posture data. The following mobile platforms support this capability: AnyConnect for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Android Version 2.4.x. You do not need to enable CSD to configure these attributes in ASDM. **Licensing Requirements** Enforcing remote access controls and gathering posture data from mobile devices requires an AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to be installed on the ASA. You receive the following functionality based on the license you install: • **AnyConnect Premium License Functionality** Enterprises that install the AnyConnect Premium license will be able to enforce DAP policies, on supported mobile devices, based on these DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device. • **AnyConnect Essentials License Functionality** Enterprises that install the AnyConnect Essentials license will be able to do the following: – Enable or disable mobile device access on a per-group basis and to configure that feature using ASDM. – Display information about connected mobile devices via CLI or ASDM without having the ability to enforce DAP policies or deny or allow remote access to those mobile devices. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add/Edit Endpoint Attributes > Endpoint Attribute Type:AnyConnect. *Also available in Version 8.4(2).*
Split Tunnel DNS policy for AnyConnect	This release includes a new policy pushed down to the AnyConnect Secure Mobility Client for resolving DNS addresses over split tunnels. This policy applies to VPN connections using the SSL or IPsec/IKEv2 protocol and instructs the AnyConnect client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyConnect client does not try to resolve the address through public DNS servers. By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy—tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Group Policy > Advanced > Split Tunneling (see the Send All DNS Lookups Through Tunnel check box). *Also available in Version 8.4(2).*

Table 10 New Features for ASA Version 8.2(5)/ASDM Version 6.4(3) (continued)

Feature	Description
SSL SHA-2 digital signature	You can now use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5(1) or later (2.5(2) or later recommended). This release does not support SHA-2 for other uses or products. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. We did not modify any screens. *Also available in Version 8.4(2).*
L2TP/IPsec support for Android	We now support VPN connections between Android mobile devices and ASA 5500 series devices, when using the L2TP/IPsec protocol and the native Android VPN client. Mobile devices must be using the Android 2.1 or later operating system. We did not modify any screens. *Also available in Version 8.4(1).*
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	ASA supports SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients when using the L2TP/IPsec protocol. We did not modify any screens. *Also available in Version 8.4(2).*
Enable/disable certificate mapping to override the group-url attribute	This feature changes the preference of a connection profile during the connection profile selection process. By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This optional feature changes the preference to a connection profile that specifies the group URL requested by the endpoint. The new option lets administrators rely on the group URL preference used by many older ASA software releases. We modified the following screens: Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profiles Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles *Also available in Version 8.4(2).*
Interface Features	
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interfaces; support was previously added for 10-Gigabit Ethernet interfaces in 8.2(2). We modified the following screens: (Single Mode) Configuration > Device Setup > Interfaces > Add/Edit Interface > General (Multiple Mode, System) Configuration > Interfaces > Add/Edit Interface *Also available in Version 8.4(2).*
Unified Communications Features	

Table 10 New Features for ASA Version 8.2(5)/ASDM Version 6.4(3) (continued)

Feature	Description
ASA-Tandberg Interoperability with H.323 Inspection	H.323 Inspection now supports uni-directional signaling for two-way video sessions. This enhancement allows H.323 Inspection of one-way video conferences supported by Tandberg video phones. Supporting uni-directional signaling allows Tandberg phones to switch video modes (close their side of an H.263 video session and reopen the session using H.264, the compression standard for high-definition video). We did not modify any screens. *Also available in Version 8.4(2).*
Routing Features	
Timeout for connections using a backup static route	When multiple static routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value. We modified the following screen: Configuration > Firewall > Advanced > Global Timeouts. *Also available in Version 8.4(2).*

New Features in ASA 8.4(1.11)/ASDM 6.4(2)

Released: May 20, 2011

Table 11 lists the new features for ASA interim Version 8.4(1.11)/ASDM Version 6.4(2).

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release.

Table 11 New Features for ASA Version 8.4(1.11)/ASDM Version 6.4(2)

Feature	Description
Firewall Features	
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy. **Note** Currently in 8.4(1.11), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634). We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object Configuration > Firewall > NAT Rules > Add/Edit NAT Rule

New Features in ASA 8.4(1)/ASDM 6.4(1)

Released: January 31, 2011

Table 12 lists the new features for ASA Version 8.4(1)/ASDM Version 6.4(1).

Table 12 New Features for ASA Version 8.4(1)/ASDM Version 6.4(1)

Feature	Description
Hardware Features	
Support for the ASA 5585-X	We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10, -20, -40, and -60. **Note** Support was previously added in 8.2(3) and 8.2(4); the ASA 5585-X is not supported in 8.3(x).
No Payload Encryption hardware for export	You can purchase the ASA 5585-X with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. The ASA software senses a No Payload Encryption model, and disables the following features: • Unified Communications • VPN You can still install the Strong Encryption (3DES/AES) license for use with management connections. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL).
Remote Access Features	
L2TP/IPsec Support on Android Platforms	We now support VPN connections between Android mobile devices and ASA 5500 series devices, when using the L2TP/IPsec protocol and the native Android VPN client. Mobile devices must be using the Android 2.1, or later, operating system. *Also available in Version 8.2(5).*

Table 12 New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)

Feature	Description
UTF-8 Character Support for AnyConnect Passwords	AnyConnect 3.0 used with ASA 8.4(1), supports UTF-8 characters in passwords sent using RADIUS/MSCHAP and LDAP protocols.
IPsec VPN Connections with IKEv2	Internet Key Exchange Version 2 (IKEv2) is the latest key exchange protocol used to establish and control Internet Protocol Security (IPsec) tunnels. The ASA now supports IPsec with IKEv2 for the AnyConnect Secure Mobility Client, Version 3.0(1), for all client operating systems. On the ASA, you enable IPsec connections for users in the group policy. For the AnyConnect client, you specify the primary protocol (IPsec or SSL) for each ASA in the server list of the client profile. IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses. Site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). The Other VPN license is included in the Base license. We modified the following screens: Configure > Site-to-Site VPN > Connection Profiles Configure > Remote Access > Network (Client) Access > AnyConnect Connection Profiles Network (Client) Access > Advanced > IPsec > IKE Parameters > IKE Policies Network (Client) Access > Advanced > IPsec > IKE Parameters > IKE Parameters Network (Client) Access > Advanced > IPsec > IKE Parameters > IKE Proposals
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommended). This release does not support SHA-2 for other uses or products. This feature does not involve configuration changes. **Caution**: To support failover of SHA-2 connections, the standby ASA must be running the same image. To support this feature, we added the Signature Algorithm field to the **show crypto ca certificate command** to identify the digest algorithm used when generating the signature.
SCEP Proxy	SCEP Proxy provides the AnyConnect Secure Mobility Client with support for automated third-party certificate enrollment. Use this feature to support AnyConnect with zero-touch, secure deployment of device certificates to authorize endpoint connections, enforce policies that prevent access by non-corporate assets, and track corporate assets. This feature requires an AnyConnect Premium license and will not work with an Essentials license.
Host Scan Package Support	This feature provides the necessary support for the ASA to install or upgrade a Host Scan package and enable or disable Host Scan. This package may either be a standalone Host Scan package or one that ASA extracts from an AnyConnect Next Generation package. In previous releases of AnyConnect, an endpoint's posture was determined by Cisco Secure Desktop (CSD). Host Scan was one of many features bundled in CSD. Unbundling Host Scan from CSD gives AnyConnect administrators greater freedom to update and install Host Scan separately from the other features of CSD.

Table 12 New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)

Feature	Description
Kerberos Constrained Delegation (KCD)	This release implements the KCD protocol transition and constrained delegation extensions on the ASA. KCD provides Clientless SSL VPN (also known as WebVPN) users with SSO access to any web services protected by Kerberos. Examples of such services or applications include Outlook Web Access (OWA), Sharepoint, and Internet Information Server (IIS). Implementing protocol transition allows the ASA to obtain Kerberos service tickets on behalf of remote access users without requiring them to authenticate to the KDC (through Kerberos). Instead, a user authenticates to ASA using any of the supported authentication mechanisms, including digital certificates and Smartcards, for Clientless SSL VPN (also known as WebVPN). When user authentication is complete, the ASA requests and obtains an impersonate ticket, which is a service ticket for ASA on behalf of the user. The ASA may then use the impersonate ticket to obtain other service tickets for the remote access user. Constrained delegation provides a way for domain administrators to limit the network resources that a service trusted for delegation (for example, the ASA) can access. This task is accomplished by configuring the account under which the service is running to be trusted for delegation to a specific instance of a service running on a specific computer. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Microsoft KCD Server.
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Apple Safari 5.
Clientless VPN Auto Sign-on Enhancement	Smart tunnel now supports HTTP-based auto sign-on on Firefox as well as Internet Explorer. Similar to when Internet Explorer is used, the administrator decides to which hosts a Firefox browser will automatically send credentials. For some authentication methods, if may be necessary for the administrator to specify a realm string on the ASA to match that on the web application (in the Add Smart Tunnel Auto Sign-on Server window). You can now use bookmarks with macro substitutions for auto sign-on with Smart tunnel as well. The POST plug-in is now obsolete. The former POST plug-in was created so that administrators could specify a bookmark with sign-on macros and receive a kick-off page to load prior to posting the the POST request. The POST plug-in approach allows requests that required the presence of cookies, and other header items, fetched ahead of time to go through. The administrator can now specify pre-load pages when creating bookmarks to achieve the same functionality. Same as the POST plug-in, the administrator specifies the pre-load page URL and the URL to send the POST request to. You can now replace the default preconfigured SSL VPN portal with your own portal. The administrators do this by specifying a URL as an External Portal. Unlike the group-policy home page, the External Portal supports POST requests with macro substitution (for auto sign-on) as well as pre-load pages. We introduced or modified the following screens: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization. Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Edit > Edit Bookmark

Table 12 New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)

Feature	Description
Expanded Smart Tunnel application support	Smart Tunnel adds support for the following applications: • Microsoft Outlook Exchange Server 2010 (native support). Users can now use Smart Tunnel to connect Microsoft Office Outlook to a Microsoft Exchange Server. • Microsoft Sharepoint/Office 2010. Users can now perform remote file editing using Microsoft Office 2010 Applications and Microsoft Sharepoint by using Smart Tunnel.
Interface Features	
EtherChannel support (ASA 5510 and higher)	You can configure up to 48 802.3ad EtherChannels of eight active interfaces each. **Note** You cannot use interfaces on the 4GE SSM, including the integrated 4GE SSM in slot 1 on the ASA 5550, as part of an EtherChannel. We introduced or modified the following screens: Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface Configuration > Device Setup > Interfaces > Add/Edit Interface Configuration > Device Setup > EtherChannel
Bridge groups for transparent mode	If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups. You can configure up to 8 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group. **Note** Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group. We modified or introduced the following screens: Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface
Scalability Features	
Increased contexts for the ASA 5550, 5580, and 5585-X	For the ASA 5550 and ASA 5585-X with SSP-10, the maximum contexts was increased from 50 to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was increased from 50 to 250.
Increased VLANs for the ASA 5580 and 5585-X	For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.
Additional platform support	Google Chrome has been added as a supported platform for ASA Version 8.4. Both 32-bit and 64-bit platforms are supported on Windows XP, Vista, and 7 and Mac OS X Version 6.0.

Table 12 New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)

Feature	Description
Increased connections for the ASA 5580 and 5585-X	We increased the firewall connection limits: • ASA 5580-20—1,000,000 to 2,000,000. • ASA 5580-40—2,000,000 to 4,000,000. • ASA 5585-X with SSP-10: 750,000 to 1,000,000. • ASA 5585-X with SSP-20: 1,000,000 to 2,000,000. • ASA 5585-X with SSP-40: 2,000,000 to 4,000,000. • ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.
Increased AnyConnect VPN sessions for the ASA 5580	The AnyConnect VPN session limit was increased from 5,000 to 10,000.
Increased Other VPN sessions for the ASA 5580	The other VPN session limit was increased from 5,000 to 10,000.
High Availability Features	
Stateful Failover with Dynamic Routing Protocols	Routes that are learned through dynamic routing protocols (such as OSPF and EIGRP) on the active unit are now maintained in a Routing Information Base (RIB) table on the standby unit. Upon a failover event, traffic on the secondary active unit now passes with minimal disruption because routes are known. Routes are synchronized only for link-up or link-down events on an active unit. If the link goes up or down on the standby unit, dynamic routes sent from the active unit may be lost. This is normal, expected behavior. We did not modify any screens.
Unified Communication Features	
Phone Proxy addition to Unified Communication Wizard	The Unified Communications wizard guides you through the complete configuration and automatically configures required aspects for the Phone Proxy. The wizard automatically creates the necessary TLS proxy, then guides you through creating the Phone Proxy instance, importing and installing the required certificates, and finally enables the SIP and SCCP inspection for the Phone Proxy traffic automatically. We modified the following screens: Wizards > Unified Communications Wizard. Configuration > Firewall > Unified Communications.
UC Protocol Inspection Enhancements	SIP Inspection and SCCP Inspection are enhanced to support new features in the Unified Communications Solutions; such as, SCCP v2.0 support, support for GETPORT messages in SCCP Inspection, SDP field support in INVITE messages with SIP Inspection, and QSIG tunneling over SIP. Additionally, the Cisco Intercompany Media Engine supports Cisco RT Lite phones and third-party video endpoints (such as, Tandberg). We did not modify any screens.
Inspection Features	
DCERPC Enhancement	DCERPC Inspection was enhanced to support inspection of RemoteCreateInstance RPC messages. We did not modify any screens.
Troubleshooting and Monitoring Features	

Table 12 New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)

Feature	Description
SNMP traps and MIBs	Supports the following additional keywords: **connection-limit-reached**, **entity cpu-temperature**, **cpu threshold rising**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. The entPhysicalTable reports entries for sensors, fans, power supplies, and related components. Supports the following additional MIBs: ENTITY-SENSOR-MIB, CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, NAT-MIB, EVENT-MIB, EXPRESSION-MIB Supports the following additional traps: warmstart, cpmCPURisingThreshold, mteTriggerFired, cirResourceLimitReached, natPacketDiscard, ciscoEntSensorExtThresholdNotification. We modified the following screen: Configuration > Device Management > Management Access > SNMP.
TCP Ping Enhancement	TCP ping allows users whose ICMP echo requests are blocked to check connectivity over TCP. With the TCP ping enhancement you can specify a source IP address and a port and source interface to send pings to a hostname or an IPv4 address. We modified the following screen: Tools > Ping.
Show Top CPU Processes	You can now monitor the processes that run on the CPU to obtain information related to the percentage of the CPU used by any given process. You can also see information about the load on the CPU, broken down per process, at 5 minutes, 1 minute, and 5 seconds prior to the log time. Information is updated automatically every 5 seconds to provide real-time statistics, and a refresh button in the pane allows a manual data refresh at any time. We introduced the following screen: Monitoring > Properties > CPU - Per Process.
General Features	
Password Encryption Visibility	You can show password encryption in a security context. We did not modify any screens.
ASDM Features	
ASDM Upgrade Enhancement	When ASDM loads on a device that has an incompatible ASA software version, a dialog box notifies users that they can select from the following options: • Upgrade the image version from Cisco.com. • Upgrade the image version from their local drive. • Continue with the incompatible ASDM/ASA pair (new choice). We did not modify any screens. This feature interoperates with all ASA versions.

Table 12 New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)

Feature	Description
Implementing IKEv2 in Wizards	IKEv2 support has been implemented into the AnyConnect VPN Wizard (formerly SSL VPN wizard), the Clientless SSL VPN Wizard, and the Site-to-Site IPsec VPN Wizard (formerly IPSec VPN Wizard) to comply with IPsec remote access requirements defined in federal and public sector mandates. Along with the enhanced security, the new support offers the same end user experience independent of the tunneling protocol used by the AnyConnect client session. IKEv2 also allows other vendors' VPN clients to connect to the ASAs. We modified the following wizards: Site-to-Site IPsec VPN Wizard, AnyConnect VPN Wizard, and Clientless SSL VPN Wizard.
IPS Startup Wizard enhancements	For the IPS SSP in the ASA 5585-X, the IPS Basic Configuration screen was added to the startup wizard. Signature updates for the IPS SSP were also added to the Auto Update screen. The Time Zone and Clock Configuration screen was added to ensure the clock is set on the ASA; the IPS SSP gets its clock from the ASA. We introduced or modified the following screens: Wizards > Startup Wizard > IPS Basic Configuration Wizards > Startup Wizard > Auto Update Wizards > Startup Wizard > Time Zone and Clock Configuration

Upgrading the Software

Note You can upgrade from any previous release (if available for your model) directly to the latest release. If you are upgrading from a pre-8.3 release to a post-8.3 release, see the *Cisco ASA 5500 Migration Guide to Version 8.3 and Later* for important information about migrating your configuration to Version 8.3 or later.

Upgrading from some releases may have consequences for downgrading; be sure to back up your configuration file in case you want to downgrade.

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

Note For CLI procedures, see the ASA release notes.

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.

Upgrading the Operating System and ASDM Images

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

We recommend that you upgrade the ASDM image before the OS image. ASDM is backward compatible, so you can upgrade the OS using the new ASDM; however, you cannot use an old ASDM image with a new OS.

Note If the ASA is running Version 8.0 or later, then you can upgrade to the latest version of ASDM (and disconnect and reconnect to start running it) before upgrading the OS.

If the ASA is running a version earlier than 8.0, then use the already installed version of ASDM to upgrade both the OS and ASDM to the latest versions, and then reload.

This section includes the following topics:

Upgrading Using ASDM 6.3 or Later

Detailed Steps

Step 1 Back up your existing configuration. For example, choose **File > Show Running Configuration in New Window** to open the configuration as an HTML page. You can also use one of the File > Save Running Configuration options.

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.

Step 4 Complete the upgrade wizard.

Step 5 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 6 Click **Finish** to exit the wizard and save the configuration changes that you made.

Upgrading Using ASDM 6.0 Through ASDM 6.2

Detailed Steps

Step 1 Back up your existing configuration. For example, choose **File > Show Running Configuration in New Window** to open the configuration as an HTML page. You can also use one of the File > Save Running Configuration options.

Step 2 From the Tools menu, choose **Tools > Upgrade Software from Cisco.com**.

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

The Upgrade Software from Cisco.com Wizard appears.

Step 3 Click **Next**.

The Authentication screen appears.

Step 4 Enter your Cisco.com username and password, and click **Next**.

The Image Selection screen appears.

Step 5 Check the **Upgrade the ASA version** check box and the **Upgrade the ASDM version** check box to specify the most current images to which you want to upgrade, and click **Next**.

The Selected Images screen appears.

Step 6 Verify that the image file you have selected is the correct one, and then click **Next** to start the upgrade.

The wizard indicates that the upgrade will take a few minutes. You can then view the status of the upgrade as it progresses.

The Results screen appears. This screen provides additional details, such as whether the upgrade failed or whether you want to save the configuration and reload the ASA.

If you upgraded the ASA version and the upgrade succeeded, an option to save the configuration and reload the ASA appears.

Step 7 Click **Yes**.

For the upgrade versions to take effect, you must save the configuration, reload the ASA, and restart ASDM.

Step 8 Click **Finish** to exit the wizard when the upgrade is finished.

Step 9 After the ASA reloads, restart ASDM.

Upgrading Using ASDM 5.2 or Earlier

Detailed Steps

Step 1 You can obtain the OS and ASDM images from the following website:

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

Download the images to your local computer.

Step 2 In ASDM, back up your existing configuration. For example, choose **File > Show Running Configuration in New Window** to open the configuration as an HTML page. You can also use one of the File > Save Running Configuration options.

Step 3 Choose **Tools > Upgrade Software**.

Step 4 From the Image to Upload drop-down list, choose **ASDM**.

Step 5 Click **Browse Local Files**, and browse to the ASDM image you downloaded from Cisco.com.

Step 6 Click **Browse Flash** to determine where to install the new ASDM image.

The Browse Flash dialog box appears. Choose the new location, and click **OK**. If you do not have room for both the current image and the new image, you can install over the current image.

Step 7 Click **Upload Image**.

Wait for the image to upload. An information window appears that indicates a successful upload.

Step 8 Repeat Step 3 through Step 7, choosing **ASA** from the Image to Upload drop-down list.

Step 9 Click **Close** to exit the Upgrade Software dialog box.

Step 10 If you saved the new images to a different location from the old ones, you need to configure the ASA to use the new image locations.

a. Choose **Configuration > Properties > Device Administration > Boot Image/Configuration**.

b. In the Boot Configuration table, click **Add** to add the new image (if you have fewer than four images listed); or you can choose an existing image and click **Edit** to change it to the new one.

If you do not specify an image, the ASA searches the internal flash memory for the first valid image to boot; we recommend booting from a specific image.

c. Click **Browse Flash**, choose the OS image, and click **OK**.

d. Click **OK** to return to the Boot Image/Configuration pane.

e. Make sure the new image is the first image in the table by using the **Move Up** button as needed.

f. In the ASDM Image Configuration area, click **Browse Flash**, choose the ASDM image, and click **OK**.

g. Click **Apply**.

Step 11 Choose **File > Save Running Configuration to Flash** to save your configuration changes.

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

A new window appears that asks you to verify the details of the reload. Select Save the running configuration at the time of reload and then choose a time to reload. Choose the option as desired.

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 ASA reloads, restart ASDM.

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 13 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 13 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.
prefix-list (supported in 6.4(7) and later)	Ignored if not used in an OSPF area.

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

This section contains open caveats in ASDM software Versions 6.4 and includes the following topics:

Open Caveats in Version 6.4(9)

Table 14 contains open caveats in ASDM software Version 6.4(9).

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

http://tools.cisco.com/Support/BugToolkit/

Table 14 Open Caveats in ASDM Version 6.4(9)

Caveat	Description
CSCtx48965	ASDM gets stuck parsing ASA config (77%) - reserved XML filename issue
CSCtz81226	ASDM is not working after upgrading from 8.0.5 to 8.2.5.x
CSCtz89870	ASDM: Cannot apply access-list as a VPN filter with a user defined

Open Caveats in Version 6.4(7)

Table 15 contains open caveats in ASDM software Version 6.4(7).

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

http://tools.cisco.com/Support/BugToolkit/

Table 15 Open Caveats in ASDM Version 6.4(7)

Caveat	Description
CSCtq69054	Management Inteface panel should not be listed on ASA NPE -K7 models
CSCtq76917	IPS Home window freezes after trying to get to Details in Sensor Health
CSCtq78816	ASDM IPSec IKEv1 Wizard fails with split-tunnel option
CSCtq84939	Remove redundant Unified Communication panels
CSCtq87726	IDFW: Cannot easily remove primary AD Agent from server group
CSCtq88352	Translation table files are created under disk0 after restore with ASDM
CSCtq95042	FQDN: Cannot configure "expire-entry-timer" and "poll-timer" on ASDM
CSCtr00700	Implement Scripting in AC for CP detection.
CSCtr29271	ASDM doc:VPN monitoring option to easily identify user
CSCtr37439	Newly Created n/w objects and objectgroups not listed in n/w to shun win
CSCtr49362	AC profile saved to flash before config is saved and completed in ASDM
CSCtr54025	Interface flow control CLI is not generated for non-10GE interfaces
CSCtr62524	ASDM forces user to apply changes when switching between sections
CSCtr68540	ASDM-ClientlessVPN-Customization-Applications-All plugins shown to edit
CSCtr80669	Inapplicable fields are shown for EC interfaces
CSCts13394	Startup wizard generates incorrect clock set CLI
CSCts24145	ASDM Group Policies have duplicate options caused user confusion
CSCts24777	OWA 2010&2007 fail auto sign on using template bookmark

Table 15 Open Caveats in ASDM Version 6.4(7) (continued)

Caveat	Description
CSCts31190	ASDM does not backup SNMP Community string in startup-config
CSCts79696	No SCEP forwarding URL none
CSCts86675	ASDM Startup Wizard does not cleanly exit when resetting config
CSCts96100	ASDM downgrade error: can't delete external portal page post parameters
CSCtt15676	Navigation to IDM panel can lock up ASDM
CSCtt19636	ASDM on missing the warning for multiple crypto peer
CSCtt24721	False Error when Manually Enabling Anonymous Reporting the First Time
CSCtt45459	HostScan config is not restored by ASDM.
CSCtu53621	ASDM DAP Symantec needs to add both SymantecAV and NortonAV
CSCtw47962	ASDM online help index is incomplete
CSCtw47975	ASDM online help contains duplicate/multiple entries
CSCtw58877	ASDM crypto map view is not showing peer with its name
CSCtw60293	Apply button is not enabled in Filter Rules & Default Information screen
CSCtw73611	Manage CA server on TLS proxy
CSCtz78974	Cannot connect to ASDM via launcher on OSX

Open Caveats in Version 6.4(5)

Table 16 contains open caveats in ASDM software Version 6.4(5).

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

http://tools.cisco.com/Support/BugToolkit/

Table 16 Open Caveats in ASDM Version 6.4(5)

Caveat	Description
CSCtn09908	Error handling missing for some CLIs
CSCtn20274	BG: Could not create redundant interface as a bridge group member
CSCtn26913	enabling ikev2 start snmp trap sends multiple commands
CSCtn42409	ASDM : Deleting interface results in error in TFW single mode
CSCtn43398	Configuring EtherChannel interface on TenGig interfaces causes cli error
CSCtn53020	ASDM: interface specific address pools does not support IPv6 pools.
CSCtn66959	ASDM: Adding entry for hosts to connect to ASA using SSH/Telnet
CSCtn68101	ASDM : Removing MAC address and configuring ether channel interface fail
CSCto87891	Garbage character of translation table after restoring configuration
CSCto89322	ASDM unable to launch ASDM-IDM or read Device Manager version
CSCtq15322	Exception when switching from non-admin context to another device
CSCtq19131	Clientless WebVPN-Delete bookmark which in use-error msg not consistent

Table 16 Open Caveats in ASDM Version 6.4(5) (continued)

Caveat	Description
CSCtq36479	asdm launcher doesn't authentocate when using OTP
CSCtq47107	ClientlesVPN-bookmark links-Advanced options not valid for few protocols
CSCtq58218	UC Wizard: Phone proxy failed to create new keypair and gives cli errors
CSCtq63193	IDFW: User name and group name validation should match ASA
CSCtq65475	ASDM does not read access-list with object-groups named with parenthesis
CSCtq76917	IPS Home window freezes after trying to get to Details in Sensor Health
CSCtq83519	Error message while launching ASDM by user with less privilege
CSCtq84939	Remove redundant Unified Communication panels
CSCtq87344	IDFW: Users only filtered by Prefix match
CSCtq87726	Cannot easily remove primary AD Agent from AD Agent AAA server group
CSCtq88352	Translation table files are created under disk0 after restore with ASDM
CSCtq93121	IDFW: "java.lang.NullPointerException" Upon configuring AD Server Group
CSCtq95042	FQDN: Cannot configure "expire-entry-timer" and "poll-timer" on ASDM
CSCtz78974	Cannot connect to ASDM via launcher on OSX

Open Caveats in Version 6.4(3)

Table 17 contains open caveats in ASDM software Version 6.4(3).

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

http://tools.cisco.com/Support/BugToolkit/

Table 17 Open Caveats in ASDM Version 6.4(3)

Caveat	Description
CSCtn09307	Plugins and plugin protocols are not shown in ASDM
CSCtn09908	Error handling missing for some CLIs
CSCtn18649	ASDM associates incorrect port with 'ssl certificate-authentication .."
CSCtn20274	BG: Could not create redundant interface as a bridge group member
CSCtn21285	NAT: ASA error when translating dynamic source from 'any' to 'original'
CSCtn24255	The length limit for Renewal Notification Input Box less than 1024
CSCtn24450	Traffic Selection for Scanning Window - Access lists not cleared up
CSCtn30763	ASDM:Packet-Tracer fails as destination field is incorrectly auto-filled
CSCtn42409	ASDM : Deleting interface results in error in TFW single mode
CSCtn42484	CSC: Web Reputation always shows Enabled
CSCtn43398	Configuring EtherChannel interface on TenGig interfaces causes cli error
CSCtn50192	ASDM: IKEv2eEnable client services
CSCtn53020	ASDM: interface specific address pools does not support IPv6 pools.

Table 17 Open Caveats in ASDM Version 6.4(3) (continued)

Caveat	Description
CSCtn66959	ASDM: Adding entry for hosts to connect to ASA using SSH/Telnet
CSCtn68101	ASDM : Removing MAC address and configuring ether channel interface fail
CSCtn71535	Show all connections in VPN Monitoring panel--easily identity a user
CSCtn72924	Sorting of Threat Summary results based on fields Last 7 days & 30 days
CSCtn75665	ASDM counts "Bytes Tx/Bytes Rx" for only one ipsec sa session.
CSCtn77676	Can't generate CSR for idntity cert after installation of CA cert
CSCtn87124	Image and configuration management tools available for read-only users
CSCto16199	IPSec VPN Wizard is failed to push modified configurations to ASA
CSCto34624	Refreshing ASDM connection table causes Monitoring tab to freeze
CSCto35519	Cannot configure advanced syslog settings
CSCto41793	wrong subnet mask generated when new network object added
CSCto87891	Garbage character of translation table after restoring configuration
CSCto89322	ASDM unable to launch ASDM-IDM or read Device Manager version
CSCtq07699	RDP option in the dropdown menu for Web type ACLs in DAP missing
CSCtq08544	Java Exception for Connections monitoring
CSCtq12849	Changing DHCP Client Address assignment changes Group policy settings
CSCtq15322	Exception when switching from non-admin context to another device
CSCtq15969	only configured languages should be visible under customization
CSCtq33036	ASDM: ASA interface list cannot be sorted by IP address
CSCte75929	ASDM: Upgrade from Cisco.com wizard experiences ghosting on a Macintosh
CSCti73585	Monitoring > Connections: Filtering returns an error
CSCtj58183	Exception when parsing BLOCK statistics
CSCtk32357	When jumbo-frame is enabled, warn users about increasing MTU and reboot
CSCtk80263	Asdm vpn session field in the home/general tab reports AC sess as IPSec
CSCtk81802	snmpv3 host cannot be added
CSCtk94322	UC wizard, phone proxy: cannot update CAPF certificate
CSCtl03766	ASDM:"flowcontrol send on" should not be allowed on Te0/8 for HA
CSCtl03880	"ip address dhcp setroute" should not be allowed on shared interface
CSCtl05195	UC Wizard:multiple errors when changing server type on step2 phone proxy
CSCtl08189	IPv6 :ASDM allows MTU 150 on interface configured for IPv6 address
CSCtl08327	ASDM: limit resource mac-address throws error in Multiple routed mode
CSCtl08354	ASDM:Bridge group interface should not be available in Routed mode
CSCtl18481	Deleting ACL then renaming network object causes CLI errors
CSCtl50711	Configuring traffic shaping on 5580 and 5585 models causes CLI errors
CSCtl83348	Firewall > Threat Detection: not clear TCP intercept related to statisti

Open Caveats in Version 6.4(2)

Table 18 contains open caveats in ASDM software Version 6.4(2).

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

http://tools.cisco.com/Support/BugToolkit/

Table 18 Open Caveats in ASDM Version 6.4(2)

Caveat	Description
CSCtn09307	Plugins and plugin protocols are not shown in ASDM
CSCtn09908	Error handling missing for some CLIs
CSCtn18649	ASDM associates incorrect port with 'ssl certificate-authentication .."
CSCtn20274	BG: Could not create redundant interface as a bridge group member
CSCtn21285	NAT: ASA error when translating dynamic source from 'any' to 'original'
CSCtn24255	The length limit for Renewal Notification Input Box less than 1024
CSCtn24450	Traffic Selection for Scanning Window - Access lists not cleared up
CSCtn30763	ASDM:Packet-Tracer fails as destination field is incorrectly auto-filled
CSCtn42409	ASDM : Deleting interface results in error in TFW single mode
CSCtn42484	CSC: Web Reputation always shows Enabled
CSCtn43398	Configuring EtherChannel interface on TenGig interfaces causes cli error
CSCtn50192	ASDM: IKEv2eEnable client services
CSCtn53020	ASDM: interface specific address pools does not support IPv6 pools.
CSCtn66959	ASDM: Adding entry for hosts to connect to ASA using SSH/Telnet
CSCtn68101	ASDM : Removing MAC address and configuring ether channel interface fail
CSCtn71535	Show all connections in VPN Monitoring panel--easily identity a user
CSCtn72924	Sorting of Threat Summary results based on fields Last 7 days & 30 days
CSCtn75665	ASDM counts "Bytes Tx/Bytes Rx" for only one ipsec sa session.
CSCtn77676	Can't generate CSR for idntity cert after installation of CA cert
CSCtn87124	Image and configuration management tools available for read-only users
CSCto16199	IPSec VPN Wizard is failed to push modified configurations to ASA
CSCto34624	Refreshing ASDM connection table causes Monitoring tab to freeze
CSCto35519	Cannot configure advanced syslog settings
CSCto41793	wrong subnet mask generated when new network object added
CSCto87891	Garbage character of translation table after restoring configuration
CSCto89322	ASDM unable to launch ASDM-IDM or read Device Manager version
CSCtq07699	RDP option in the dropdown menu for Web type ACLs in DAP missing
CSCtq08544	Java Exception for Connections monitoring
CSCtq12849	Changing DHCP Client Address assignment changes Group policy settings
CSCtq15322	Exception when switching from non-admin context to another device

Table 18 Open Caveats in ASDM Version 6.4(2) (continued)

Caveat	Description
CSCtq15969	only configured languages should be visible under customization
CSCtq27456	Cluster Loads Monitoring fails with error
CSCtq33036	ASDM: ASA interface list cannot be sorted by IP address

Open Caveats in Version 6.4(1)

Table 19 contains the open caveats in ASDM software Version 6.4(1).

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

http://tools.cisco.com/Support/BugToolkit/

Table 19 Open Caveats for ASDM Version 6.4.1

Caveat	Description
CSCtb19950	Route-map deletion: Requires a pop-up window when route-map is attached
CSCte51943	Cannot expand some dialog boxes in Linux
CSCte75929	ASDM: Upgrade from Cisco.com wizard experiences ghosting on a Macintosh
CSCtf33370	ASDM control for cert export are inaccurate + need info popup
CSCtf61639	Unable to launch ASDM demo on Linux
CSCtg90925	LDAP Attribute Map configuration commands rejected
CSCth60280	ASDM:Management Access-Certificate intf only shows inside and outside
CSCth99206	ASDM MFM: Config refresh warning not triggered by CLI changes
CSCti04733	ASDM 6.3: No error while adding Crypto CA server DB users with '+' in SN
CSCti73585	Monitoring > Connections: Filtering returns an error
CSCti98675	ASDM:Help for LDAP attribute Maps section needs updating
CSCtj54385	ASA 55x5 NPE:ASDM DAP rework support only Cut-Thru-Proxy functionality
CSCtj78026	ASDM 6.3 may display garbage in webvpn plugin menu on older ASA versions
CSCtk00668	ASDM:reconcile Backup and Restore panels terminology
CSCtk32357	When jumbo-frame is enabled, warn users about increasing MTU and reboot
CSCtk36790	UC Wizard: Validation for hostname is incomplete
CSCtk68793	UC wizard, phone proxy: failed CAPF certificate breaks PP configuration
CSCtk68913	Error when changing network object IP version
CSCtk80263	Asdm vpn session field in the home/general tab reports AC sess as IPSec
CSCtk81802	snmpv3 host cannot be added
CSCtk84308	UC wizard, phone proxy: ntwk objects get recreated each time fqdn change
CSCtk94322	UC wizard, phone proxy: cannot update CAPF certificate
CSCtk97385	UC Wizard: Phone Proxy, redundant Objects in Config after edit/delete
CSCtk97991	UC Wizard: Deleting TFTP server from UC panel does not reflect corectly

Table 19 Open Caveats for ASDM Version 6.4.1 (continued)

Caveat	Description
CSCtl03766	ASDM:"flowcontrol send on" should not be allowed on Te0/8 for HA
CSCtl03818	ASDM EC :Remove "configure hardware properties" on PC Sub interface
CSCtl03880	"ip address dhcp setroute" should not be allowed on shared interface
CSCtl05195	UC Wizard:multiple errors when changing server type on step2 phone proxy
CSCtl05396	ASDM EC :ASDM should send min-bundle & Max-bundle commands in order
CSCtl05441	ASDM : Java logs on click ok button in "Hardware Properties" pop up
CSCtl08189	IPv6 :ASDM allows MTU 150 on interface configured for IPv6 address
CSCtl08354	ASDM:Bridge group interface should not be available in Routed mode
CSCtl09170	MTA ports are not parsed if one of them is set to default
CSCtl09434	Exception when ASDM unable to determine the version of IPS
CSCtl18316	UC Wizard: Adding TFTP with same as UCM causes CLI error & redundant nat
CSCtl18481	Deleting ACL then renaming network object causes CLI errors
CSCtl33185	java exception when importing customization if language left blank
CSCtl37989	Etherchannel: Adding interface with no members throws error from ASA
CSCtl42678	ASDM Hangs When Creating Ipsec Connection Profile Using Connection Name.
CSCtl42804	Max number of IKEv2 SA allowed config setting not implemented properly
CSCtl47507	Uninstall hostscan button deletes the data.xml file
CSCtl50711	Configuring traffic shaping on 5580 and 5585 models causes CLI errors
CSCtl53144	Changes to use-script option (via ASDM) corrupts username_from_cert.xml
CSCtl79487	Anyconnect 3.0: profile editor doesn't work on ASDM 6.3.x or earlier
CSCtl83348	Firewall > Threat Detection: not clear TCP intercept related to statisti
CSCtl83348	Firewall > Threat Detection: not clear TCP intercept related to statisti
CSCtl83928	Disabling Easy VPN Remote fails with ASDM 6.3.5
CSCtl84837	ASDM freezes when Read only user (Privilege Level 5) runs ASDM query
CSCtl88549	ASDM error dialog contains no error codes
CSCtl96001	Compression Stats..SVC should be AnyConnect Client
CSCtl96038	Can't display VPN Encryption Stats for a specific Conn Profile..All OK
CSCtl96054	Can't display specific Conn Profile VPN-Protocol Stats ..only All
CSCtl96897	ASDM: TFW - Adding port-channel/Redundant interface throws error
CSCtl97431	5585-K7 NPE:Identity Certificates panel-remove VPN from Entrust button

Resolved Caveats

This section contains the following topics:

Note Due to caveats CSCtt42234 and CSCtt45397, Versions 6.4(5.204) and 6.4(5.205) have been removed from Cisco.com. Please upgrade to Version 6.4(5.206) or later.

Resolved Caveats in Version 6.4(9.103)

Table 20 contains the resolved caveats in ASDM software Version 6.4(9.103).

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

http://tools.cisco.com/Support/BugToolkit/

Table 20 Resolved Caveats in ASDM Version 6.4(9.103)

Caveat	Description
CSCtf33394	ASDM: Backup/restore of startup-config breaks hidden passwords and keys
CSCtz81226	ASDM is not working after upgrading from 8.0.5 to 8.2.5.x
CSCtz99283	ASDM should support backup of AnyConnect customization content
CSCua29374	Read-only user logged into ASDM-Unauthorized command msg keeps pop up
CSCua29422	Read-only user logged into ASDM-Unauthorized change-password msg appears
CSCua31679	ASDM issues when adding an IPv6 filter to a user or group policy
CSCua37476	ASDM: java.lang.NullPointerException when adding vlan to trunk
CSCua45309	Unable to modify ACEs in ASDM after adding remarks
CSCua53773	ASDM ACL Changes managed from User Policies Apply button remains Grey
CSCua58014	ASDM support new show module return value for CX 9.0.2
CSCua71251	ASDM 6.4.9 inserting ACL while modifing Group Policy
CSCua74341	Read-only user logged into ASDM-Clientless portal fields are not visible
CSCua79250	ASDM arp permit-nonconnected should be in system context multiple mode

Resolved Caveats in Version 6.4(9)

Table 21 contains the resolved caveats in ASDM software Version 6.4(9).

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

http://tools.cisco.com/Support/BugToolkit/

Table 21 Resolved Caveats in ASDM Version 6.4(9)

Caveat	Description
CSCtd68876	User can type in selected source field in Browse source dialog
CSCte75929	ASDM: Upgrade from Cisco.com wizard experiences ghosting on a Macintosh
CSCtf07846	ASDM: Help section for Edit Static NAT rule is not appropriate
CSCtf33394	ASDM: Backup/restore of startup-config breaks hidden passwords and keys
CSCtl22199	ASDM split DNS should warn that AnyConnect supports ten (10) entries
CSCtn88072	Access rule description replication issue
CSCtq78816	ASDM IPSec IKEv1 Wizard fails with split-tunnel option
CSCtq83519	IDFW: Error message while launching ASDM by user with fewer privileges
CSCtq88135	Unable to enumerate disk contents in GUI if filename contains "error" kw
CSCtr49362	AC profile saved to flash before config is saved and completed in ASDM
CSCts24145	ASDM Group Policies have duplicate options caused user confusion
CSCtt19636	ASDM on missing the warning for multiple crypto peer
CSCtu13680	Falcon startup wizard CLI is not generated
CSCtv21773	ASDM fails to send/parse commands with whitespace in group-policy name
CSCtw56901	Falcon dashboard and gadgets should be renamed on ASDM
CSCtw57441	ASDM doesn't include Slot 1 in flash size calculation for dev. dashboard
CSCtw58877	ASDM crypto map view is not showing peer with its name
CSCtw87442	NAT: Translated Packet Source address is showing DM_INLINE_NETWORK
CSCtw95930	Manual NAT not displaying the PP options
CSCtx01016	ASDM: Home screen graphs may show ghost images on Windows and Macintosh
CSCtx10581	ASDM real time logs do not refresh automatically after clearing filter
CSCtx12851	ASDM CRL check in trustpoint does not reflect CLI configuration
CSCtx29805	User specific info for user specific VPN connection
CSCtx32641	Falcon port latest code from asdm branch to asdm_6_4_9
CSCtx48940	ASDM:Capability to Backup/Restore WEBVPN bookmarks doesn't work
CSCtx58035	Error message does not contain the Field name
CSCtx68663	Russia, Belarus and Egypt no longer observe Daylight Saving Time
CSCtx70202	ASDM not sending right command for deleting DHCP server from the list
CSCtx79284	"TCP timeout" should be modified "Timeout" on ASDM
CSCtx84041	ASDM: Manual NAT configuration may conflict with ip local pool
CSCty00927	ASDM fails to send/parse commands with whitespace in group-policy name
CSCty03459	ASDM not showing ICMP rules under the "Both" Filter option
CSCty04464	IDFW VPN Filter ACL - ASDM issue
CSCty08134	ASDM landing page is not consistent across all browser-OS platforms
CSCty12281	Configured description is ignored when adding Access Rule via ASDM

Table 21 Resolved Caveats in ASDM Version 6.4(9)

Caveat	Description
CSCty22611	ASDM: shared license server configuration page missing
CSCty49739	Local CA Certificate servers CA Certs lifetime value dependency
CSCty74203	DAP GUI should not show unsupported Anyconnect endpoint attributes
CSCtz21253	SSL protocol selection link is missing btw group policy and conn profile
CSCtz28590	Support failover replication rate
CSCtz35662	Manage User Database - Add should allow empty subject
CSCtz38604	ASDM removes crypto map instead of disabling IKEv1
CSCtz97084	ASDM Upgrade Assistant shows incorrect version 8.6(0) available

Resolved Caveats in Version 6.4(7)

Table 22 contains the resolved caveats in ASDM software Version 6.4(7).

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

http://tools.cisco.com/Support/BugToolkit/

Table 22 Resolved Caveats in ASDM Version 6.4(7)

Caveat	Description
CSCtu51124	Unable to access ASDM using launcher due to Java out-of-heap exception
CSCtt42234	Unlicensed IPS warning incorrectly displayed when allocating traffic
CSCtt99884	ASDM 6.4.5.205 on Windows 7 is missing the option to pin
CSCtu39942	VPN Filter ACL not displayed in session detail
CSCtu33179	ASDM: AnyConnect DAP attributes for iPhone 4S need to be added
CSCtt26310	CSD warning msg shouldn't be seen when using logical Op. with ACIDx
CSCtr35540	ASDM: Cannot Assign Smart Tunnel Application list to Local User
CSCtw56513	ASDM IPSec Connection Profile help link broken
CSCtu01065	Network object browser panel shows Browse null title
CSCtu96599	ASDM error if using ip local pool as destination in NAT
CSCtu00952	Recent Object NAT changes not consistent with previous behavior
CSCts73119	ASDM incorrect handling of prefix-list on route-map
CSCtl08189	IPv6: ASDM allows MTU 150 on interface configured for IPv6 address
CSCtt37390	ASDM displays global ACL in Management Access Rules
CSCtq93121	IDFW: "java.lang.NullPointerException" Upon configuring AD Server Group
CSCtq63193	IDFW: User name and group name validation should match ASA
CSCtu45290	ASDM shows object-group names in static route entries
CSCtu33481	Add support for new **timeout xlate-pat** command
CSCtt68397	Add support for NAT options 'extended' and 'flat'

Table 22 Resolved Caveats in ASDM Version 6.4(7)

Caveat	Description
CSCtq65475	ASDM does not read access-list with object-groups named with parenthesis
CSCts67543	DOC: ASDM - top 10 users need documentation for this feature
CSCtw70401	Cosmetic changes on CA Server page
CSCtu33693	Issues on CA Server page
CSCtr69135	ASDM does not apply lifetime for CA certificate
CSCts58444	Add Doc Roadmap link to Help menu
CSCts40044	ACL remark - inconsistency between packet tracer and ASDM
CSCts09430	ASDM: Commands ignored by ASDM
CSCtu37722	Update Online Help for 6.4.7
CSCtw52336	Online help on ASDM for NAT CCB is not available
CSCtt92798	ASDM caches the clear text SNMPv3 PW for Authentication and Encryption
CSCtq88352	Translation table files are created under disk0 after restore with ASDM
CSCtt22534	Clientless SSL VPN Customization: Unable to change the logon fields order

Resolved Caveats in Version 6.4(5.206)

Table 23 contains the resolved caveats in ASDM software Version 6.4(5.206).

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

http://tools.cisco.com/Support/BugToolkit/

Table 23 Resolved Caveats in ASDM Version 6.4(5.206)

Caveat	Description
CSCsk99620	ENH: Enable the VPN session logoff button for read-only/monitor users
CSCtq27456	ASDM: Cluster Loads Monitoring fails with error
CSCtq33036	ASDM: ASA interface list cannot be sorted by IP address
CSCtq55259	ASDM sending crypto map commands when changing name
CSCtr38862	SNMP ignored commands
CSCtr38893	ASDM no longer has Top N statistics in the Firewall dashboard
CSCtr40909	ASDM shows Maximum number of VLANs allowed is 3 in non-admin context
CSCtr67989	ASDM support for new auto-logoff with Essentials License
CSCtr70171	ASDM fails to display NAT rules if interface name contains parentheses
CSCtr75039	Add RegEx to negate a specified character pops up the error window twice
CSCtr83228	Duplicate ACL shown in ASDM for SNMP protocol
CSCts01331	Need to show a warning message if IPS license is disabled
CSCts17526	ASDM Launcher does not work with JAVA version 7.
CSCts27101	ASDM-IDM Launcher upgrade facility broken on Mac OS X

Table 23 Resolved Caveats in ASDM Version 6.4(5.206)

Caveat	Description
CSCts39989	ASDM: packet tracer: link "show rule in access rules table" doesn't work
CSCts40202	Unable to access multiple ASA using ASDM 6.4.5 with ASA ver 8.4.2
CSCts56216	The "timeout floating-conn" command is ignored
CSCts58444	Add Doc Roadmap link to Help menu
CSCts69911	ASDM Cannot Copy then Paste Group Policy
CSCts74881	Unable to Configure Port Forward Name for Group Policy -RemoteAccessVPN
CSCts83402	Site-to-Site wizard: IKEv1 trustpoint cmd should start with 'ikev1'.

Resolved Caveats in Version 6.4(5.106)

Table 24 contains the resolved caveats in ASDM software Version 6.4(5.106).

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

http://tools.cisco.com/Support/BugToolkit/

Table 24 Resolved Caveats in ASDM Version 6.4(5.106)

Caveat	Description
CSCsv86119	ASDM 6.x: Remove "IKE Policy" step from IPsec VPN Wizard for RA VPN
CSCth23218	"Re-authentication on IKE Re-key" shows 'enable' in ASDM when disabled
CSCtj99030	Rename the AnyConnect Settings tab
CSCtk65552	Change text on KCD Server Page, remove the reference to SQL
CSCtk83575	ASDM Monitoring window to have Assigned and Public IP tab for AC
CSCtn24431	Browser Incompatability (On Mac)
CSCtn53020	ASDM: interface specific address pools does not support IPv6 pools.
CSCtn71535	Show all connections in VPN Monitoring panel--easily identity a user
CSCto08669	ASDM needs to add time-out option for logon page
CSCto87891	Garbage character of translation table after restoring configuration
CSCtq41521	Support new compression CLI for anyconnect
CSCtq64765	ASDM: Real time log viewer filter does not clear completely
CSCtr04719	CCO upgrade for ASDM is not working on ASA SMP platform
CSCtr18474	WebVPN Group Policy and Customization Timeout Alerts panels - text mods
CSCtr24392	Remove link navigation from Group,username,customization Timeout Alerts
CSCtr34351	ASDM- ACL hit count issue stayed 0 with ASA v8.4.2
CSCtr38165	Cannot edit EtherChannel interface settings in a security context
CSCtr41265	ASDM: Used Memory may show incorrect values in multiple mode
CSCtr44809	Changes made to group policy through Edit are not reflecting - RemoteAcc
CSCtr73011	Edit Network Object Group Panel shows redundant members

Resolved Caveats in Version 6.4(5)

Table 25 contains the resolved caveats in ASDM software Version 6.4(5).

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

http://tools.cisco.com/Support/BugToolkit/

Table 25 Resolved Caveats in ASDM Version 6.4(5)

Caveat	Description
CSCso83453	ASDM:DAP:Attributes should be case insensitive
CSCtb06515	ASDM ignores some special characters used in tunnel-group names
CSCti04733	ASDM 6.3: No error while adding Crypto CA server DB users with '+' in SN
CSCti38852	ASDM: Filter may not work in the ACL panel under IPV4 Network Object add
CSCtj78026	ASDM 6.3 may display garbage in webvpn plugin menu on older ASA versions
CSCtk00668	ASDM: reconcile Backup and Restore panels terminology
CSCtk46281	ASDM for FWSM: tcp-udp object-group can be removed even if applied
CSCtk68793	UC wizard, phone proxy: failed CAPF certificate breaks PP configuration
CSCtk84308	UC wizard, phone proxy: ntwk objects get recreated each time fqdn change
CSCtk97991	UC Wizard: Deleting TFTP server from UC panel does not reflect corectly
CSCtl03818	ASDM EC :Remove "configure hardware properties" on PC Sub interface
CSCtl05396	ASDM EC :ASDM should send min-bundle & Max-bundle commands in order
CSCtl05441	ASDM : Java logs on click ok button in "Hardware Properties" pop up
CSCtl09170	MTA ports are not parsed if one of them is set to default
CSCtl09434	Exception when ASDM unable to determine the version of IPS
CSCtl18316	UC Wizard: Adding TFTP with same as UCM causes redundant nat statements
CSCtl33185	java exception when importing customization if language left blank
CSCtl37989	Etherchannel: Adding interface with no members throws error from ASA
CSCtl42678	ASDM Hangs When Creating Ipsec Connection Profile Using Connection Name.
CSCtl42804	Max number of IKEv2 SA allowed config setting not implemented properly
CSCtl47507	Uninstall hostscan button deletes the data.xml file
CSCtl53144	Changes to use-script option (via ASDM) corrupts username_from_cert.xml
CSCtl72356	Install Certificate error in ASDM should be more specific
CSCtl74973	Ping tool: source interface not selectable for ICMP ping
CSCtl83928	Disabling Easy VPN Remote fails with ASDM 6.3.5
CSCtl84837	ASDM freezes when Read only user (Privilege Level 5) runs ASDM query
CSCtl96038	VPN Encryption Stats;remove Total Active /Cumulative Sessions fields
CSCtl96054	ID certificate:"Import Identity Certificate from a FIle" text change
CSCtl97431	5585-K7 NPE:Identity Certificates panel-remove VPN from Entrust button
CSCtn09307	Plugins and plugin protocols are not shown in ASDM

Table 25 Resolved Caveats in ASDM Version 6.4(5) (continued)

Caveat	Description
CSCtn21285	NAT: ASA error when translating dynamic source from 'any' to 'original'
CSCtn24255	The length limit for Renewal Notification Input Box less than 1024
CSCtn30763	ASDM:Packet-Tracer fails as destination field is incorrectly auto-filled
CSCtn42484	CSC: Web Reputation always shows Enabled
CSCtn50192	ASDM: IKEv2eEnable client services
CSCtn68795	Edit Access Rule throws NullPtrException
CSCtn72924	Sorting of Threat Summary results based on fields Last 7 days & 30 days
CSCtn75665	ASDM counts "Bytes Tx/Bytes Rx" for only one ipsec sa session
CSCtn77676	Can't generate CSR for idntity cert after installation of CA cert
CSCtn87124	Image and configuration management tools available for read-only users
CSCto16199	IPSec VPN Wizard is failed to push modified configurations to ASA
CSCto32221	Error in client package sorting on ASDM
CSCto34027	ASDM 6.3(5) CSD and AnyConnect packages not able to restore from backup
CSCto34624	Refreshing ASDM connection table causes Monitoring tab to freeze
CSCto35519	Cannot configure advanced syslog settings
CSCto41793	wrong subnet mask generated when new network object added
CSCto50431	Always enable AAA server Test button
CSCtq07699	RDP option in the dropdown menu for Web type ACLs in DAP missing
CSCtq08544	Java Exception for Connections monitoring

Resolved Caveats in Version 6.4(3)

Table 26 contains the resolved caveats in ASDM software Version 6.4(3).

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

http://tools.cisco.com/Support/BugToolkit/

Table 26 Resolved Caveats in ASDM Software Version 6.4(3)

Caveat	Description
CSCtk34329	ASDM6.3(3) device-mgr- config restore gives errors for pre-shared-keys
CSCtl42903	ASDM does not send the right command for "dhcp-server subnet-selection"
CSCtl77943	Unable to save pcap file in multi-context mode
CSCtn54315	Restore of Certificate GUI has misleading error
CSCtn56002	Cannot set DOCTYPE in full customization with the Customization Editor
CSCtn90259	Cisco.com Upgrade wizard: forwarding service not fully implemented
CSCto03787	Add tunnel DNS to group policy
CSCto09119	Android Typo on DAP Endpoint Drop-down

Table 26 Resolved Caveats in ASDM Software Version 6.4(3)

Caveat	Description
CSCto36548	DAP Endpoint Attribute anyconnect platform device type add iPad 2 Verizon
CSCto74607	ASDM(6.4.1) shows error while backing up AnyConnect image and profile
CSCto88591	ASDM: DAP Privacy Protection fails to allow drop down parameters

Resolved Caveats in Version 6.4(2)

Table 27 contains the resolved caveats in ASDM software Version 6.4(2).

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

http://tools.cisco.com/Support/BugToolkit/

Table 27 Resolved Caveats in ASDM Version 6.4(2)

Caveat	Description
CSCtl77769	ASDM hangs at 96% with CSC 6.6
CSCtn90288	Update Cisco.com Upgrade wizard for ASDM 6.4.2 release
CSCtn68841	DAP: endpoint add dialog too small for AnyConnect condtion
CSCtn65930	AnyConnect endpoint condition should not depend on CSD
CSCtn75333	Remove iPhone 2G and iPod from AnyConnect endpoint condtion
CSCtn75422	Support tunnel-group-preference CLI
CSCtn80962	ASDM iPhone 3GS DAP record wrong string created by ASDM iphone CCB
CSCtj85485	Add the ability to convert migration issue on object group member
CSCtl05864	ASDM : Error message on Delete port-channel in Multiple route mode
CSCto00957	object nat with pat pool option "Advanced" tab not navigating
CSCtl53144	Changes to use-script option (via ASDM) corrupts username_from_cert.xml
CSCtn24339	Support NAT/PAT Pool and Round Robin in ASDM
CSCto03942	Issues with ASDM - object navigated twice in nat
CSCto03958	when interface option unselected object nat not showing in ASDM
CSCtl96897	ASDM: Single TFW - Adding port-channel/Redundant interface throws error
CSCtl99214	ASDM - Hit count not shown when using service object groups with no type
CSCtl43118	Need new parameters for SSL VPN bookmark to handle Microsoft OWA
CSCtl84837	ASDM freezes when Read only user (Privilege Level 5) runs ASDM query

Resolved Caveats in Version 6.4(1)

Table 28 contains the resolved caveats in ASDM software Version 6.4(1).

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

http://tools.cisco.com/Support/BugToolkit/

Table 28 Resolved Caveats in ASDM Version 6.4(1)

Caveat	Description
CSCsj74367	ASDM: export of pkcs12 should remove leading/trailing lines
CSCsy43885	IPv6 : Browse IP Address doesn't support Network Address in Route Panel
CSCsy46539	PIM multicast boundary config - Hit Cancel still deletes a rule
CSCsy48841	ASDM should exclude intfs in contexts from redundant intf member list
CSCsy60567	SNMPv3 users is able to be deleted when trap host is configured.
CSCtd95084	Error while changing from "routed" to "transparent" mode
CSCte39873	ASDM does not process acl cut and paste as expected
CSCte72290	ASDM: Navigation Panel being removed causes confusion
CSCte95392	NAT: ASDM should generate error message on EDIT object used in NAT
CSCtf13860	Need a confirmation dialog when downgrading
CSCtf17774	ASDM: Rename Smart Tunnels "Parent Affinity"
CSCtf25281	exporting ID cert as PEM sends wrong CLI and shouldn't require password
CSCtf31966	Unable to specify empty string for the value field in Bookmarks UI
CSCtf36957	Unable to add a redundant interface
CSCtf49621	Webcontents do not show up in ASDM
CSCtf58007	Enforce EUI-64" option gives an ERROR
CSCtg03361	Need to handle special characters in the Post pararmeters inBookmarks UI
CSCtg23401	Hide flow control from GUI if feature not available
CSCth21171	IPS gets stuck in infinite refresh mode
CSCth26973	WebVPN tabs show partial data in right pane when resizing ASDM
CSCth29238	Files in File Manager dialog are not sorted
CSCth37158	UC Wizard:CUMA configuration shows incorrect information message
CSCth38053	ASDM : Java logs on System Home page when sorting Interface Status tabl
CSCth38881	Enable fallback option errors even though hide username is checked
CSCth42791	WebVPN:Bookmark w/ preload url overwrite existing bookmark preload field
CSCth55731	Home panel horizontal scroll bar doesn't auto-adjust
CSCth62685	ASDM 6.3.1 gives error when used with ASA 8.2 or lower
CSCth70445	Firewall Mode display incorrect info
CSCth70451	Syslog filter: adding IP range freezes for a few seconds
CSCth72351	Delete button disabled even after adding a service policy

Table 28 Resolved Caveats in ASDM Version 6.4(1) (continued)

Caveat	Description
CSCth76292	ASDM: Not able to Enroll a certificate after authentication
CSCth79162	ASDM 6.4: Refresh Button does not work in Certificate management page
CSCth79165	ASDM 6.4: No option to enroll trustpoint that is already authenticated
CSCth84205	UC Wizard shouldn't be allowed to configure with single interface
CSCth87660	ASDM takes very long time to show network object table
CSCth91699	ASDM lost IPv4 info after click IPv6 radio button and back
CSCth96952	ASDM:"Config Hardware properties" should be available for physical Intf
CSCth97138	ASDM : ASA rejects CLI on redundant interface deletion
CSCth98836	UC Wizard: Presence federation, incorrect info message
CSCti09087	ASDM: ASDM running fails to connect on IPS links
CSCti16853	Upgrade from Cisco.com popup hidden
CSCti18222	Dont allow switching between ASDM for different platforms
CSCti26023	Java exception when exporting GUI/Text msg customization
CSCti27886	ASDM:Interface is not editable from system panel due to error:
CSCti28903	Can't delete object groups with no members
CSCti34709	ASDM allows user to config nameif in failover interface on startup wiz
CSCti43579	ASDM: Showing profile type of "unknown"
CSCti48238	WebVPN Customization Editor unable to customize some plugins via ASDM
CSCti53792	cannot add and delete crypto map peer at the same time
CSCti61628	Username Prompt for WebVPN logon page is not customizable on ASDM
CSCti63110	Environment status in 5580 should not be present for non-admin context
CSCti66912	Need to click twice to uncheck the 'Enable EIGRP Process' check box
CSCti67257	Records not visible in Edit Filter Rules window in RIP feature
CSCti67856	Can not enable AC essentials within ASDM
CSCti70504	ASDM: Unable to create AnyConnect Profiles on Disk1
CSCti82718	MTA Entry Dialog should not include DHCP interfaces
CSCti84712	ASDM shows wrong smart tunnel policy for group policy
CSCti86404	crypto ipsec lifetime cannot be changed using asdm
CSCtj00982	Syslog ID is not getting copied when selected through Copy button
CSCtj01031	Syslog message search is not scrolling to make the selection visible
CSCtj01094	ASDM : Could not create 3 interfaces on ASA 5505 with Security plus lic
CSCtj04841	ASDM can not delete acl with time-range set
CSCtj19061	ASDM not sending CLI to generate key pair during cert enrollment
CSCtj23279	ASDM : ASDM allows sub-interfaces to be shared across context
CSCtj25956	DAP editor: problem with adding bookmark.
CSCtj28497	Log Viewer : Validation Issues.

Table 28 Resolved Caveats in ASDM Version 6.4(1) (continued)

Caveat	Description
CSCtj28516	Backup/Restore not available in multi-context mode
CSCtj28923	When ASDM launches, device list should scroll to show the device
CSCtj29448	ASDM 6.4: Network Address is displayed while adding SMTP server address
CSCtj33780	Excptn when switching from ASA in transparent mode to ASA in routed mode
CSCtj44515	SSL Clientless wizard: error when adding new user and new group.
CSCtj54779	Parse error exception in java console
CSCtj55705	ASDM: Add button gets greyed out after adding 2 interfaces in add contex
CSCtj57843	NumberFormatException in Static Routes
CSCtj60665	Update Cisco.com Upgrade wizard for ASDM 6.3.5
CSCtj60967	Monitoring -> Logging -> Real-Time Log Viewer and Log Buffer issues
CSCtj62327	Upgrade from Cisco.com: ASDM freezes when there is not enough space
CSCtj66399	ASDM does not allow to set the max ssl vpn sessions to a number > 2
CSCtj67289	ASDM - Top 10 Access Rules shows blank interface and Internal Error
CSCtj77997	ASDM throws an error as new network object/w range option is added
CSCtj78215	ASDM startup wizard should create after-auto rule for outbound PAT
CSCtj78474	Environment Panel on an ASA 5580
CSCtj92482	Smart call maximum message size error
CSCtk01604	ASDM 6.3.x - packet trace button doesn't always work with large cfg
CSCtk08440	ASDM: When portal toolbar is removed, ASDM should point to WebACL config
CSCtk34916	Unable to create or edit username_from_cert.xml file
CSCtk46888	SNMP: Creating new host throws exception for empty username
CSCtk56258	Missing localization attributes in customization objects
CSCtk58319	Startup Wizard: Context interface address should not be editable
CSCtk63563	Incorrect OS Version attribute for iphone
CSCtk65914	Changing TLS proxy attached to phone proxy and policy rule causes error
CSCtk65937	Changing TLS proxy and MTA attached to the phone proxy causes an error
CSCtk75160	Cisco.com upgrade wizard prompts the user for credentials twice
CSCtk84067	ASDM Configuration restore hangs at 98% with nested web content folders
CSCtl04154	Cannot add a renamed network object to a new network object group
CSCtl45719	ASDM missing button due to resolution size

End-User License Agreement

For information about the end-user license agreement, go to:

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Related Documentation

For additional information about ASDM or its platforms, see *Navigating the Cisco ASA 5500 Series Documentation*:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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