Release Notes for Cisco ASDM, Version 6.3(x)

April 2011

This document contains release information for Cisco ASDM Version 6.3(1) through 6.3(5) on Cisco ASA 5500 series adaptive security appliances.

This document includes the following sections:

Note Before you upgrade to ASA Version 8.3, be sure to see the *Cisco ASA 5500 Migration Guide for Version 8.3*. The following major changes require configuration migration:

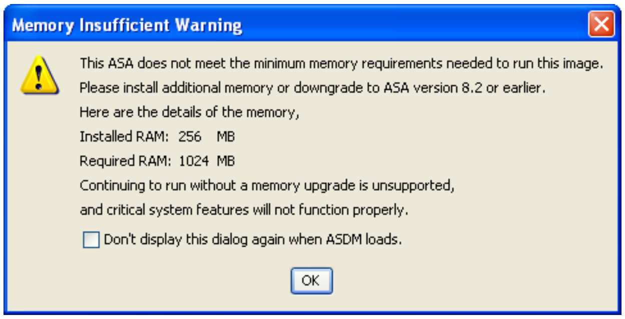
- NAT redesign.
- Real IP addresses in access rules instead of mapped addresses.
- Named network objects and service objects.

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

Important Notes

- If your system runs ASDM Version 6.3.1 or higher and you want to use ASDM to upgrade either the ASA or ASDM image using the Tools > Check for ASA/ASDM Updates menu option, then ASDM might prompt twice for your Cisco.com credentials.
- Maximum configuration size—ASDM supports up to a maximum of a 512 KB configuration. If you exceed this amount, you may experience performance issues.
- Memory requirements—To run Version 8.3 in a production environment, you 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 install a memory upgrade, you receive the following message upon logging in:

.



Memory Insufficient Warning

This ASA does not meet the minimum memory requirements needed to run this image.
Please install additional memory or downgrade to ASA version 8.2 or earlier.
Here are the details of the memory,
Installed RAM: 256 MB
Required RAM: 1024 MB
Continuing to run without a memory upgrade is unsupported,
and critical system features will not function properly.

☐ Don't display this dialog again when ASDM loads.

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 • 2003 Server • XP	6.0 or later	1.5 or later	No support	• 5.0 (1.5.0) • 6.0
Apple Macintosh OS X: • 10.6 • 10.5 • 10.4	No support	1.5 or later	2.0 or later	• 5.0 (1.5.0) • 6.0
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • Desktop with Workstation	N/A	1.5 or later	N/A	• 5.0 (1.5.0) • 6.0

1. Obtain Sun Java from http://www.java.com/en/download/manual.jsp.
2. ASDM requires an SSL connection from the browser to the adaptive security appliance. By default, Firefox does not support base encryption (DES) for SSL and therefore requires the adaptive security appliance to have a strong encryption (3DES/AES) license. As a workaround, you can enable the security.ssl3.dhe_dss_des_sha setting in Firefox. See http://kb.mozillazine.org/About:config to learn how to change hidden configuration preferences.

Supported Platforms

See *Cisco ASA 5500 Series Hardware and Software Compatibility* for the minimum supported version of ASDM for each ASA and SSM version.

Note ASDM 6.2(1) and later is not supported on the PIX platforms. The last ASDM version supported on the PIX is 6.1(5).

Although ASDM 6.3 supports many ASA versions, the ASDM 6.3 documentation and online help only include features for ASA 8.3. For older ASA versions, you might find that using the ASDM 6.3 documentation is inaccurate for your older feature set. Instead, refer to the ASDM guide in which support for your platform version was added (to see when support was added, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility* for the minimum supported version of ASDM for each ASA version; this version is the one where support was added). Although the specific information about the ASDM GUI might be inaccurate in that guide, the platform feature set is documented correctly.

New Features

This section includes the following topics:

New Features in ASDM 6.3(5)/8.2(4.4)

Released: March 4, 2011

Table 2 lists the new features for ASA Version 8.2(4.4)/ASDM Version 6.3(5).

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. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Table 2 New Features for ASA Version 8.2(4.4)/ASDM Version 6.3(5)

Feature	Description
Hardware Features	
Support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X	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.
Remote Access Features	
Clientless SSL VPN support for Outlook Web Access 2010	By default, Clientless SSL VPN now provides content transformation (rewriting) support for Outlook Web Access (OWA) 2010 traffic. We did not modify any screens.

New Features in ASDM 6.3(5)/8.2(4.1)

Released: January 18, 2011

Table 3 lists the new features for ASA Version 8.2(4.1)/ASDM Version 6.3(5).

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. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Table 3 New Features for ASA Version 8.2(4.1)/ASDM Version 6.3(5)

Feature	Description
Remote Access Features	
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.

New Features in ASDM 6.3(4)/ASA 8.2(3.9)

Released: November 2, 2010

Table 4 lists the new features for ASA interim Version 8.2(3.9)/ASDM Version 6.3(4).

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. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Table 4 New Features for ASA Version 8.2(3.9)/ASDM Version 6.3(4)

Feature	Description
Remote Access Features	
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.

New Features in ASDM 6.3(3) and 6.3(4)/ASA 8.2(3)

Released: August 9, 2010

Table 5Table 5 lists the new features for ASA Version 8.2(3)/ASDM Version 6.3(3)/6.3(4).

Note ASDM 6.3(4) does not include any new features; it includes a caveat fix required for support of the ASA 5585-X.

Table 5 New Features for ASA Version 8.2(3)/ASDM Version 6.3(3) and 6.3(4)

Feature	Description
Hardware Features	
Support for the Cisco ASA 5585-X with SSP-20 and SSP-60	Support for the ASA 5585-X with Security Services Processor (SSP)-20 and -60 was introduced. **Note** The ASA 5585-X is not supported in Version 8.3(x). The ASA 5585-X requires ASDM 6.3(4).
Remote Access Features	
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware. **Note** For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment. **Note** The ASA 5580/5585-X platforms already integrate this capability; therefore, crypto engine commands are not applicable on these platforms. The following commands were introduced or modified: **crypto engine large-mod-accel**, **clear configure crypto engine**, **show running-config crypto engine**, and **show running-config crypto**. In ASDM, use the Command Line Interface tool to enter the **crypto engine large-mod-accel** command. *Also available in Version 8.3(2).*
Microsoft Internet Explorer proxy lockdown control	Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged; the default setting for the tab can be shown or hidden, depending on the user registry settings. The following command was introduced: **msie-proxy lockdown**. In ASDM, use the Command Line Interface tool to enter this command.
Trusted Network Detection Pause and Resume	This feature enables the AnyConnect client to retain its session information and cookie so that it can seamlessly restore connectivity after the user leaves the office, as long as the session does not exceed the idle timer setting. This feature requires an AnyConnect release that supports TND pause and resume.

New Features in ASDM 6.3(2)/ASA 8.3(2)

Released: August 2, 2010

Table 6 lists the new features for ASA Version 8.3(2)/ASDM Version 6.3(2).

Table 6 New Features for ASA Version 8.3(2)/ASDM Version 6.3(2)

Feature	Description
Monitoring Features	
Enhanced logging and connection blocking	When you configure a syslog server to use TCP, and the syslog server is unavailable, the adaptive security appliance blocks new connections that generate syslog messages until the server becomes available again (for example, VPN, firewall, and cut-through-proxy connections). This feature has been enhanced to also block new connections when the logging queue on the adaptive security appliance is full; connections resume when the logging queue is cleared. This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommend allowing new connections when syslog messages cannot be sent. To allow new connections, configure the syslog server to use UDP or check the **Allow user traffic to pass when TCP syslog server is down** check box on the Configuration > Device Management > Logging > Syslog Servers pane. The following syslog messages were introduced: 414005, 414006, 414007, and 414008 No ASDM screens were modified.
Syslog message filtering and sorting	Support has been added for the following: • Syslog message filtering based on multiple text strings that correspond to various columns • Creation of custom filters • Column sorting of messages. For detailed information, see the Cisco Security Appliance Configuration Guide using ASDM. The following screens were modified: Monitoring > Logging > Real-Time Log Viewer > View Monitoring > Logging > Log Buffer Viewer > View *This feature interoperates with all ASA versions.*
Clearing syslog messages for the CSC SSM	Support for clearing syslog messages has been added in the Latest CSC Security Events pane. The following screen was modified: Home > Content Security. *This feature interoperates with all ASA versions.*
Remote Access Features	

Table 6 New Features for ASA Version 8.3(2)/ASDM Version 6.3(2) (continued)

Feature	Description
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware. **Note** For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment. The following commands were introduced or modified: **crypto engine large-mod-accel**, **clear configure crypto engine**, **show running-config crypto engine**, and **show running-config crypto**. In ASDM, use the Command Line Interface tool to enter the **crypto engine large-mod-accel** command. *Also available in Version 8.2(3).*
Microsoft Internet Explorer proxy lockdown control	Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged; the default setting for the tab can be shown or hidden, depending on the user registry settings. The following command was introduced: **msie-proxy lockdown**. In ASDM, use the Command Line Interface tool to enter this command. *Also available in Version 8.2(3).*
Secondary password enhancement	You can now configure SSL VPN support for a common secondary password for all authentications or use the primary password as the secondary password. The following screen was modified: Configuration > Remote Access VPN > Clientless SSL Access > Connection Profiles > Add/Edit Clientless SSL VPN Connection Profile > Advanced > Secondary Authentication.

Table 6 New Features for ASA Version 8.3(2)/ASDM Version 6.3(2) (continued)

Feature	Description
General Features	

No Payload Encryption image for export	For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. For version 8.3(2), you can now install a No Payload Encryption image (asa832-npe-k8.bin) on the following models:
	• ASA 5505
	• ASA 5510
	• ASA 5520
	• ASA 5540
	• ASA 5550
	Features that are disabled in the No Payload Encryption image include:
	• Unified Communications.
	• Strong encryption for VPN (DES encryption is still available for VPN).
	• VPN load balancing (note that the GUI is still present; the feature will not function, however).
	• Downloading of the dynamic database for the Botnet Traffic Filer (Static black and whitelists are still supported. Note that the GUI is still present; the feature will not function, however.).
	• Management protocols requiring strong encryption, including SSL, SSHv2, and SNMPv3. You can, however, use SSL or SNMPv3 using base encryption (DES). Also, SSHv1 and SNMPv1 and v2 are still available.
	If you attempt to install a Strong Encryption (3DES/AES) license, you see the following warning:
	`WARNING: Strong encryption types have been disabled in this image; the`
	`VPN-3DES-AES license option has been ignored.`

New Features in ASDM 6.3(1)/ASA 8.3(1)

Released: March 8, 2010

Table 7 lists the new features for ASA Version 8.3(1)/ASDM Version 6.3(1).

Table 7 New Features for ASA Version 8.3(1)/ASDM Version 6.3(1)

Feature	Description
Remote Access Features	
Smart Tunnel Enhancements	Logoff enhancement—Smart tunnel can now be logged off when all browser windows have been closed (parent affinity), or you can right click the notification icon in the system tray and confirm log out. Tunnel Policy—An administrator can dictate which connections go through the VPN gateway and which do not. An end user can browse the Internet directly while accessing company internal resources with smart tunnel if the administrator chooses. Simplified configuration of which applications to tunnel—When a smart tunnel is required, a user no longer needs to configure a list of processes that can access smart tunnel and in turn access certain web pages. An “enable smart tunnel” check box for either a bookmark or standalone application allows for an easier configuration process. Group policy home page—Using a check box in ASDM, administrators can now specify their home page in group policy in order to connect via smart tunnel. The following screen was modified: Configuration > Remote Access VPN > AAA/Local Users > Local Users > Edit > VPN Policy > Clientless SSL VPN.
Newly Supported Platforms for Browser-based VPN	Release 8.3(1) provides browser-based (clientless) VPN access from the following newly supported platforms: • Windows 7 x86 (32-bit) and x64 (64-bit) via Internet Explorer 8.x and Firefox 3.x • Windows Vista x64 via Internet Explorer 7.x/8.x, or Firefox 3.x. • Windows XP x64 via Internet Explorer 6.x/7.x/8.x and Firefox 3.x • Mac OS 10.6.x 32- and 64-bit via Safari 4.x and Firefox 3.x. Firefox 2.x is likely to work, although we no longer test it. Release 8.3(1) introduces browser-based support for 64-bit applications on Mac OS 10.5. Release 8.3(1) now supports smart tunnel access on all 32-bit and 64-bit Windows OSs supported for browser-based VPN access, Mac OS 10.5 running on an Intel processor only, and Mac OS 10.6.x. The adaptive security appliance does not support port forwarding on 64-bit OSs. Browser-based VPN access does not support Web Folders on Windows 7, Vista, and Internet Explorer 8. An ActiveX version of the RDP plug-in is not available for 64-bit browsers. **Note** Windows 2000 and Mac OS X 10.4 are no longer supported for browser-based access.

Table 7 New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)

Feature	Description
IPv6 support for IKEv1 LAN-to-LAN VPN connections	For LAN-to-LAN connections using mixed IPv4 and IPv6 addressing, or all IPv6 addressing, the adaptive security appliance supports VPN tunnels if both peers are Cisco ASA 5500 series adaptive security appliances, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6). Specifically, the following topologies are supported when both peers are Cisco ASA 5500 series adaptive security appliances: • The adaptive security appliances have IPv4 inside networks and the outside network is IPv6 (IPv4 addresses on the inside interfaces and IPv6 addresses on the outside interfaces). • The adaptive security appliances have IPv6 inside networks and the outside network is IPv4 (IPv6 addresses on the inside interface and IPv4 addresses on the outside interfaces). • The adaptive security appliances have IPv6 inside networks and the outside network is IPv6 (IPv6 addresses on the inside and outside interfaces). **Note** The defect CSCtd38078 currently prevents the Cisco ASA 5500 series from connecting to a Cisco IOS device as the peer device of a LAN-to-LAN connection. The following screens were modified or introduced: Wizards > IPsec VPN Wizard, Configuration > Site-to-Site VPN > Connection Profiles Configuration > Site-to-Site VPN > Connection Profiles > Basic > Add IPsec Site-to-Site Connection Profile Configuration > Site-to-Site VPN > Group Policies Configuration > Site-to-Site VPN > Group Policies > Edit Internal Group Policy Configuration > Site-to-Site VPN > Advanced > Crypto Maps Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Add > Create IPsec Rule Configuration > Site-to-Site VPN > Advanced > ACL Manager
Plug-in for AnyConnect Profile Editor	The AnyConnect Profile Editor is a convenient GUI-based configuration tool you can use to configure the AnyConnect 2.5 or later client profile, an XML file containing settings that control client features. Previously, you could only change profile settings manually by editing the XML tags in the profile file. The AnyConnect Profile Editor is a plug-in binary file named anyconnectprof.sgz packaged with the ASDM image and installed in the root directory of disk0:/ in the flash memory on the adaptive security appliance. This design allows you to update the editor to be compatible with new AnyConnect features available in new client releases.
SSL VPN Portal Customization Editor	You can rebrand and customize the screens presented to clientless SSL VPN users using the new Edit Customization Object window in ASDM. You can customize the logon, portal and logout screens, including corporate logos, text messages, and the general layout. Previously, the customization feature was embedded in the adaptive security appliance software image. Moving it to ASDM provides greater usability for this feature and future enhancements. The following screen was modified: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization.

Table 7 New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)

Feature	Description
Usability Improvements for Remote Access VPN	ASDM provides a step-by-step guide to configuring Clientless SSL VPN, AnyConnect SSL VPN Remote Access, or IPsec Remote Access using the ASDM Assistant. The ASDM Assistant is more comprehensive than the VPN wizards, which are designed only to get you up and running. The following screen was modified: Configuration > Remote Access VPN > Introduction > ASDM Assistant.
Firewall Features	
Interface-Independent Access Policies	You can now configure access rules that are applied globally, as well as access rules that are applied to an interface. If the configuration specifies both a global access policy and interface-specific access policies, the interface-specific policies are evaluated before the global policy. The following screen was modified: Configuration > Firewall > Access Rules.
Network and Service Objects	You can now create named network objects that you can use in place of a host, a subnet, or a range of IP addresses in your configuration and named service objects that you can use in place of a protocol and port in your configuration. You can then change the object definition in one place, without having to change any other part of your configuration. This release introduces support for network and service objects in the following features: • NAT • Access rules • Network object groups **Note** ASDM used network objects internally in previous releases; this feature introduces platform support for network objects. The following screens were modified or introduced: Configuration > Firewall > Objects > Network Objects/Groups, Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > NAT Rules, Configuration > Firewall > Access Rules
Object-group Expansion Rule Reduction	Significantly reduces the network object-group expansion while maintaining a satisfactory level of packet classification performance. The following screen was modified: Configuration > Firewall > Access Rules > Advanced.
NAT Simplification	The NAT configuration was completely redesigned to allow greater flexibility and ease of use. You can now configure NAT using auto NAT, where you configure NAT as part of the attributes of a network object, and manual NAT, where you can configure more advanced NAT options. The following screens were modified or introduced: Configuration > Firewall > Objects > Network Objects/Group Configuration > Firewall > NAT Rules

Table 7 New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)

Feature	Description
Use of Real IP addresses in access lists instead of translated addresses	When using NAT, mapped addresses are no longer required in an access list for many features. You should always use the real, untranslated addresses when configuring these features. Using the real address means that if the NAT configuration changes, you do not need to change the access lists. The following features that use access lists now use real IP addresses. These features are automatically migrated to use real IP addresses when you upgrade to 8.3, unless otherwise noted. • Access rules • Service policy rules • Botnet Traffic Filter • AAA rules • WCCP redirect. **Note** WCCP is not automatically migrated when you upgrade to 8.3.
Threat Detection Enhancements	You can now customize the number of rate intervals for which advanced statistics are collected. The default number of rates was changed from 3 to 1. For basic statistics, advanced statistics, and scanning threat detection, the memory usage was improved. The following screen was modified: Configuration > Firewall > Threat Detection.
Unified Communication Features	
SCCP v19 support	The IP phone support in the Cisco Phone Proxy feature was enhanced to include support for version 19 of the SCCP protocol on the list of supported IP phones.
Cisco Intercompany Media Engine Proxy	Cisco Intercompany Media Engine (UC-IME) enables companies to interconnect on-demand, over the Internet with advanced features made available by VoIP technologies. Cisco Intercompany Media Engine allows for business-to-business federation between Cisco Unified Communications Manager clusters in different enterprises by utilizing peer-to-peer, security, and SIP protocols to create dynamic SIP trunks between businesses. A collection of enterprises work together to end up looking like one large business with inter-cluster trunks between them. The following screens were modified or introduced: Wizards > Unified Communications Wizard > Cisco Intercompany Media Engine Proxy Configuration > Firewall > Unified Communications, and then click UC-IME Proxy Configuration > Firewall > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > Select SIP Inspection Map
SIP Inspection Support for IME	SIP inspection has been enhance to support the new Cisco Intercompany Media Engine (UC-IME) Proxy. The following screen was modified: Configuration > Firewall > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > Select SIP Inspection Map.

Table 7 New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)

Feature	Description
Unified Communication Wizard	The Unified Communications wizard guides you through the complete configuration and automatically configures required aspects for the following proxies: Cisco Mobility Advantage Proxy, Cisco Presence Federation Proxy, Cisco Intercompany Media Engine proxy. Additionally, the Unified Communications wizard automatically configures other required aspects of the proxies. The following screens were modified: Wizards > Unified Communications Wizard Configuration > Firewall > Unified Communications
Enhanced Navigation for Unified Communication Features	The Unified Communications proxy features, such as the Phone Proxy, TLS Proxy, CTL File, and CTL Provider pages, are moved from under the Objects category in the left Navigation panel. to the new Unified Communications category. In addition, this new category contains pages for the new Unified Communications wizard and the UC-IME Proxy page. *This feature interoperates with all ASA versions.*
Routing Features	
Route map support	ASDM has added enhanced support for static and dynamic routes. The following screen was modified: Configuration > Device Setup > Routing > Route Maps. *This feature interoperates with all ASA versions.*
Monitoring Features	
Time Stamps for Access List Hit Counts	Displays the timestamp, along with the hash value and hit count, for a specified access list. The following screen was modified: Configuration > Firewall > Access Rules. (The timestamp appears when you hover the mouse over a cell in the Hits column.)
High Performance Monitoring for ASDM	You can now enable high performance monitoring for ASDM to show the top 200 hosts connected through the adaptive security appliance. Each entry of a host contains the IP address of the host and the number of connections initiated by the host, and is updated every 120 seconds. The following screen was introduced: Home > Firewall Dashboard > Top 200 Hosts.
Licensing Features	
Non-identical failover licenses	Failover licenses no longer need to be identical on each unit. The license used for both units is the combined license from the primary and secondary units. **Note** For the ASA 5505 and 5510 adaptive security appliances, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license. The following screen was modified: Configuration > Device Management > Licensing > Activation Key.

Table 7 New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)

Feature	Description
Stackable time-based licenses	Time-based licenses are now stackable. In many cases, you might need to renew your time-based license and have a seamless transition from the old license to the new one. For features that are only available with a time-based license, it is especially important that the license not expire before you can apply the new license. The adaptive security appliance allows you to *stack* time-based licenses so you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early. For licenses with numerical tiers, stacking is only supported for licenses with the same capacity, for example, two 1000-session SSL VPN licenses. You can view the state of the licenses at Configuration > Device Management > Licensing > Activation Key.
Intercompany Media Engine License	The IME license was introduced.
Multiple time-based licenses active at the same time	You can now install multiple time-based licenses, and have one license per feature active at a time. The following screen was modified: Configuration > Device Management > Licensing > Activation Key.
Discrete activation and deactivation of time-based licenses.	You can now activate or deactivate time-based licenses using a command. The following command was modified: **activation-key** [**activate** | **deactivate**]. The following screen was modified: Configuration > Device Management > Licensing > Activation Key.
General Features	
Master Passphrase	The master passphrase feature allows you to securely store plain text passwords in encrypted format. It provides a master key that is used to universally encrypt or mask all passwords, without changing any functionality. The Backup/Restore feature supports the master passphrase. The following screens were introduced: Configuration > Device Management > Advanced > Master Passphrase Configuration > Device Management > Device Administration > Master Passphrase
ASDM Features	
Upgrade Software from Cisco.com Wizard	The Upgrade Software from Cisco.com wizard has changed to allow you to automatically upgrade ASDM and the adaptive security appliance to more current versions. Note that this feature is only available in single mode and, in multiple context mode, in the System execution space. It is not available in a context. The following screen was modified: Tools > Check for ASA/ASDM Updates. *This feature interoperates with all ASA versions.*
Backup/Restore Enhancements	The Backup Configurations pane was re-ordered and re-grouped so you can choose the files you want to backup more easily. A Backup Progress pane was added allowing you to visually measure the progress of the backup. And you will see significant performance improvement when using backup or restore. The following screen was modified: Tools > Backup Configurations or Tools > Restore Configurations. *This feature interoperates with all ASA versions.*

Upgrading the Software

Note Before you upgrade, be sure to see the *Cisco ASA 5500 Migration Guide for Version 8.3*. The following major changes require configuration migration:

- NAT redesign.
- Real IP addresses in access rules instead of mapped addresses.
- Named network objects and service objects.

The *Cisco ASA 5500 Migration Guide for Version 8.3* also describes how to downgrade.

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

- Viewing Your Current Version, page 17
- Upgrading the Operating System and ASDM Images, page 17

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 adaptive security appliance.

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 adaptive security appliance 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 adaptive security appliance 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 6.2 or Earlier, page 18
- Upgrading Using ASDM 6.3 or Later, page 18

Upgrading Using ASDM 6.2 or Earlier

Detailed Steps

Step 1 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.

Note If you are running ASDM Version 5.2 or lower, then the Upgrade Software from Cisco.com Wizard is not available. You can download the software from the following URL:

http://www.cisco.com/cisco/software/navigator.html

Then use **Tools > Upgrade Software**.

Step 2 Click **Next**.

The Authentication screen appears.

Step 3 Enter your Cisco.com username and password, and click **Next**.

The Image Selection screen appears.

Step 4 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 5 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 6 Click **Yes**.

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

Step 7 Click **Finish** to exit the wizard when the upgrade is finished.

Upgrading Using ASDM 6.3 or Later

Detailed Steps

Step 1 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 2 Enter your assigned Cisco.com username and the Cisco.com password, and then click **Login**.

The Cisco.com Upgrade Wizard appears.

Step 3 Complete the upgrade wizard.

Step 4 For the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the adaptive security appliance and restart ASDM.

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

Unsupported Commands

ASDM supports almost all commands available for the adaptive adaptive security appliance, 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, page 19
- Effects of Unsupported Commands, page 20
- Discontinuous Subnet Masks Not Supported, page 20
- Interactive User Commands Not Supported by the ASDM CLI Tool, page 20

Ignored and View-Only Commands

Table 8 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 8 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[1]	Ignored.
dhcp-server (tunnel-group name general-attributes)	ASDM only allows one setting for all DHCP servers.
eject	Unsupported.
established	Ignored.
failover timeout	Ignored.
ipv6 nd prefix	Unsupported.
pager	Ignored.

Table 8 List of Unsupported Commands **(continued)**

Unsupported Commands	ASDM Behavior
pim accept-register route-map	Ignored. You can configure only the **list** option using ASDM.
prefix-list	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 line 1 extended permit ip any any`
	`class-map mycm`
	`match access-list mycl`
	`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.

[1] ASA 8.3(2) and above.

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
ke00000000000000$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 in Version 6.3

This section contains open caveats in the latest maintenance release.

If you are running an older release, and you need to determine the open caveats for your release, then add the caveats in this section to the resolved caveats from later releases. For example, if you are running Release 6.3(1), then you need to add the caveats in this section to the resolved caveats from 6.3(2)and later to determine the complete list of open caveats.

If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 9 Open Caveats in Version 6.3

Caveat ID	Description
CSCtb07337	Preview window shows wild characters under logon page/language
CSCtb19950	Route-map deletion: Requires a pop-up window when route-map is attached
CSCtd05274	Standby unit console will show all the object XML file when editing obj
CSCte28894	ASDM: WebVPN Help Customization needs to have templates for export
CSCte51943	Cannot expand some dialog boxes in Linux
CSCte72290	ASDM: Navigation Panel being removed causes confusion
CSCte72582	ASDM Prompts for Certificate Authorization and Fails to Contact ASA
CSCte75929	ASDM: Upgrade from CCO wizard experiences ghosting on a Macintosh
CSCte91390	Public Server should support "--Any--" for Public Interface
CSCte95652	ASDM OLH: Smart Tunnels is a broken link
CSCtf08847	Timeout issues when using IPS Setup Wizard
CSCtf12814	Nothing happens when no protocol specified with protocol type specified
CSCtf13860	Need a confirmation dialog when downgrading

Table 9 Open Caveats in Version 6.3 (continued)

Caveat ID	Description
CSCtf15050	The PREVIEW Window doesn't show preview customized GUI
CSCtf19237	Object NAT: Edit NAT rule is not enabling service in Advance tab
CSCtf19793	Custom Panes Help incorrectly redirects to Device Management
CSCtf22576	Unable to delete nested object groups (nested to the maximum level)
CSCtf23225	HAS Wizard stops after changing peer to multi mode for A/A failover
CSCtf25281	exporting ID cert as PEM sends wrong CLI and shouldn't require password
CSCtf26239	Custom Panes Help button pop up wrong online help information
CSCtf26413	ASDM sends useless cmds with master passphrase if empty red intf exists
CSCtf26476	Route Map -> Edit -> help leads to page not found
CSCtf33370	ASDM control for cert export are inaccurate + need info popup
CSCtf33394	ASDM backup does not save ldap-login-password to startup-config
CSCtf49339	Support upgrade from internal development images to CCO release images
CSCtf52510	When Adding A New Client Profile, The Group Policy Dropdown Is Invisible
CSCtf61639	asdm_launcher.sh does not run. Unable to launch ASDM demo.
CSCtf75441	ASDM sending wrong CLI to enable ASDM cert auth
CSCtf79571	Sending incorrect WEBVPN customization commands to ASA
CSCtf81226	AC Profile Editor: Disable Cert Selection option is not clear
CSCtf87384	ASDM presenting blank Auth dialog after apparent idle timeout + exceptio
CSCtg39274	ASDM: revert webcontent is treated as config mode command
CSCtg50910	Client Software Update panel: Cells are squished together
CSCtg61562	Create subinterface of a Redundant interface
CSCtg74308	ASDM 6.3 adds additional information to exported certificate
CSCtg79827	ASDM Help should provide more details on anyconnect firewall
CSCtg90925	LDAP Attribute Map configuration commands rejected
CSCth29238	Files in File Manager dialog are not sorted
CSCth33868	Secondary auth panel behavior change due to CSCte84210..Help change
CSCth36518	ASDM 6.3.1 failing to backup SSL Certificates
CSCth40911	Upgrade from Cisco.com wizard does not list interim releases
CSCth46155	Syslog filter is wiped out after all messages are shown
CSCth46318	Syslog filter: filtering by time reverses the order of syslogs
CSCth55569	ASDM 6.3 : Smart tunnel all application needs option for Mac platform
CSCth60280	ASDM:Management Access-Certificate intf only shows inside and outside
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
CSCti03490	Update ASDM splash screen and startup page for Spyker

Table 9 Open Caveats in Version 6.3 (continued)

Caveat ID	Description
CSCti04733	ASDM 6.3: No error while adding Crypto CA server DB users with '+' in SN
CSCti06336	Preview windows shows more plugins on ASDM 6.3.1 for webvpn
CSCti09087	ASDM: ASDM running on Spyker fails to connect on IPS links
CSCti16853	Upgrade popup hidden

Resolved Caveats

This section includes the following topics:

Resolved Caveats for Software Version 6.3(5)

The caveats listed in Table 10 were resolved in software Version 6.3(5). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 10 Resolved Caveats in Version 6.3(5)

Caveat ID	Description
CSCtg99616	Network Object Lookup by IP Address Does Not Work.
CSCth39120	Memory insufficient warning appearing on ASA 8.2.
CSCti44774	Missing rdp2-hlp.inc in help customization CSCti58620 ASDM: Restricting LOCAL user IDs from connecting via SSH/Telnet/ASDM.
CSCti58646	ASDM: LOCAL user ID edit screen mentions the command syntax incorrectly.
CSCti65286	ASDM failing to load locked up at 77% with 6.3.3 CSCti71030 ASDM 6.3(3) and 6.3(3.50) not able to configure NetFlow.
CSCti73603	Unable to import .vbs scripts through the ASDM.
CSCti74532	Hitcount not shown with optimization on.
CSCti74889	Environmental output has left and right reversed for Power Supply slots.
CSCti82411	Object NAT parsed as ip address.
CSCti84093	Unable to select AnyConnect module if package does not have DART module.
CSCti95692	Can't filter by port string in Edit window of Destination Port.
CSCti96426	More Option isn't displayed with Edit Internal Group Policy in ASDM.
CSCtj07636	ASDM filter sslvpn sessions by IP address hangs the GUI.

Table 10 Resolved Caveats in Version 6.3(5) (continued)

Caveat ID	Description
CSCtj28588	Can't switch to another device due to an exception.
CSCtj54779	Parse error exception in java console.
CSCtj56897	Jumbo frame reservation checkbox is not shown in the Interfaces panel.
CSCtj84217	Existing Filter Rules are invisible while editing - RIP->Filter Rules.

Resolved Caveats for Software Version 6.3(4)

The caveats listed in Table 11 were resolved in software Version 6.3(4). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 11 Resolved Caveats in Version 6.3(4)

Caveat ID	Description
CSCti63196	ASDM did not get a response from the ASA

Resolved Caveats for Software Version 6.3(3)

The caveats listed in Table 12 were resolved in software Version 6.3(3). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 12 Resolved Caveats in Version 6.3(3)

Caveat ID	Description
CSCsy43876	IPv6 : Display v6 prefix-length on Edit Network object
CSCtc11885	ASDM-Nat : Unable to add the service groups in the nat cfg
CSCtc53304	With a large config, ASDM takes a long time to change config windows
CSCtd90414	NAT diagram messy display with long names
CSCtd91840	UDP port range is shown incorrectly while add/edit service policy rules
CSCte95392	NAT: ASDM should generate error message on EDIT object used in NAT
CSCtf03898	Unable to add network object through NAT config window
CSCtf07819	ASDM:NAT:Egress traffic, address not correctly captured in diagram
CSCtf65657	Config->FW->NatRules RIght Side Object Mgt "Where Used" not working.
CSCtf98735	Remove button not enabled - Edit regular expression class map
CSCtg47907	Home Page: environment status is UNKNOWN for all ASA-5585 models
CSCtg50875	ASDM launcher fails to switch between ASAs
CSCth08396	ASDM Defined User Roles Setup gets error in multi-context mode
CSCth12953	Unable to edit site-to-site vpn connection profile with network object.

Table 12 Resolved Caveats in Version 6.3(3) (continued)

Caveat ID	Description
CSCth24721	HAS wizard displays clear text failover key in commands preview window
CSCth24734	HAS wizard can close compatibility checking wait window and proceed
CSCth26129	Unexpected "Unapplied Change" window pop-up when clicking Refresh icon
CSCth34271	Upgrade from CCO wizard forces to upgrade the ASA image
CSCth38473	CCO Upgrade: after checking for upgrades can't switch to another device
CSCth39253	Deleting any access rule always deletes the first one
CSCth49102	Packet Tracer: when errors are shown, the tracer window disappears
CSCth53088	Implement NPE changes in ASDM
CSCth53605	ASDM HA Wizard checks for identical license under ASA 8.3 code
CSCth57526	ASDM 6.3: Migration from 8.0 to 8.3 names CLI conversion showing names
CSCth62064	ASDM ACL error "duplicate element found" while editing static policy nat
CSCth70502	Port syslog filter changes from asdm_6_3_2 to asdm_6_3
CSCth75473	File transfer not working on ASDM with MAC OS X
CSCth87660	ASDM takes very long time to show network object table
CSCti03151	ASA reporting of PSTEMP and PSFAN changed to show both slots

Resolved Caveats for Software Version 6.3(2)

The caveats listed in Table 13 were resolved in software Version 6.3(2). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 13 Resolved Caveats in Version 6.3(2)

Caveat ID	Description
CSCtb08697	Refactor ICME references in the code to IME
CSCtd64607	"HA and scalability Wizard" show wrong Switch port in page 3/6
CSCtd72956	UC TLS Proxy: Exception when click on Edit or Delete
CSCtd79324	IME Wiz:updating acl,c-map,p-map,uc conf not requird if public prt chang
CSCte58118	For policy NAT mapped address, options are incorrect
CSCte83924	ASDM: Include the filename extension in the script name (i.e .bat)
CSCte84210	ASDM: Support to config the secondary password CLI
CSCte87383	Connection Profile Customization should be named Login and Logout Page
CSCtf03652	Smart Call Home should be allowed to configure mail server priority
CSCtf11495	ASDM AC Profile Editor: Indefinite XML validation when adding a profile
CSCtf11521	ASDM AC Profile Editor: Group Policy drop down arrow missing
CSCtf11667	ASDM AC Profile Editor: New profiles can be added with same name
CSCtf11752	ASDM AC Profile Editor: Inconsistent import profile behavior

Table 13 Resolved Caveats in Version 6.3(2) (continued)

Caveat ID	Description
CSCtf11811	ASDM AC Profile Editor: Incorrect device path can be displayed in export
CSCtf11944	ASDM AC Profile Editor: Unable to remove group policy
CSCtf20578	ASDM 6.3: Invalid values accepted for RTP min-max port with global MTA
CSCtf20814	ASDM HAS wizard waiting time is too short for A/A failover configuration
CSCtf23277	WebVPN http-proxy PAC configuration does not display
CSCtf25968	ASDM CUMA generate wrong outside nat command
CSCtf26441	ASDM: AC Profile Editor - Infinite refresh duration when in prof. editor
CSCtf28333	CUMA wizard should allow outside NAT to map clients to inside IP address
CSCtf29954	Warning window pops up when we try to backup configuration
CSCtf32083	Object NAT: Displaying blank if static translated addr as interface.
CSCtf35115	Public Server: ASA Rejects CLI on "Edit Public Server"
CSCtf48627	UC Wizard, CUP/CUMA: Changing FQDN is not reflected in CSR
CSCtf49621	Webcontents do not show up in ASDM
CSCtf62623	ASDM java exception when loading config with svc routing-filtering-ignor
CSCtf65929	UC Wizard, UC-IME:remote-side cert exchange diagrams are wrong
CSCtf69505	Load balancing node doesn't show up on the 5510
CSCtf71056	"Name" disappears when modify Network Object Netmask in ASDM
CSCtf75958	Non-existing "How do I?" topic shows up in the ASDM Assistant search
CSCtf77014	ASDM can not apply service-object with "destination", prior to ASA8.3
CSCtf78470	ASDM sending dhcp-server tunnel-group CLI even when not changed
CSCtf80760	ASA and ASDM is not showing the proper version of loaded ASDM image.
CSCtf81076	AnyConnect profile editor - cannot edit profile - schema errors
CSCtf87386	ASDM: Portal customization shows CLI commands in the field
CSCtf96607	Error thrown after visiting Portal page of DfltGrpPolicy for clientless
CSCtf97774	AC Profile Client can not handle spaces in group name
CSCtf98888	group-policy setting not being saved - Client Profile to Download
CSCtg29415	JPN: Better to come up an error message right after DBCS users are added
CSCtg39652	n/a on all interface line, link and kbps
CSCtg42135	ASDM displays Botnet Filter is not configured after screen is refreshed
CSCtg48351	UC Wizard, Mobility/Federation: add warning to install cert on server
CSCtg48463	UC Wizard: "inside" is hardcoded for pnone proxy
CSCtg56494	ASDM 6.3.1 - editing access-list object groups can cause UI to lock up
CSCtg66779	VPN-session-monitoring, 1st session loses 2nd data line after Refresh
CSCtg75448	ASDM public server names lost in upgrade from 8.x to 8.3
CSCtg76211	ASDM restore hanging at 98% - doesn't allow user to close dialog
CSCtg97262	Exception in Home Panel Resources

Table 13 Resolved Caveats in Version 6.3(2) (continued)

Caveat ID	Description
CSCth00579	IPv6 : ASA rejects "Enforce EUI-64 Null" command
CSCth03470	Implement sorting for the ASDM syslog viewers.
CSCth09715	Log viewer display incorrect if interface name contains a ':'
CSCth20780	ASDM does not show custom portals under group policy
CSCth26928	Jumbo frame feature is not available in single mode
CSCth32160	Update CCO Update wizard to recognize ASA 8.3.2/ASDM 6.3.2 releases
CSCth34271	Upgrade from CCO wizard forces to upgrade the ASA image
CSCth39253	Deleting any access rule always deletes the first one
CSCth46136	Syslog filtering: can't filter by a port string, only by port number
CSCth46203	Syslog filter: can't clear the filter dialog
CSCth53605	ASDM HA Wizard checks for identical license under ASA 8.3 code
CSCth63669	Syslog filter: not clear how to exclude IP address/range
CSCth68233	Syslog filter: add info icons for each field to show expected format
CSCth75698	ASDM syslogs:Clear Filter button doesn't clear the filter rules
CSCti03471	Update ASDM splash screen for 6.3.2

Resolved Caveats for Software Version 6.3(1)

The caveats listed in Table 14 were resolved in software Version 6.3(1). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 14 Resolved Caveats in Version 6.3(1)

Caveat ID	Description
CSCsu90066	Capability to Backup/Restore config/start-up configs
CSCsy47949	ASDM backup config - does not properly back up pre-shared key for TG
CSCsy60117	Unable to configure shun hosts in scanning threat detection
CSCsz34305	ASDM backup does not save ldap-login-password when exporting config
CSCta60218	ASDM: rewrite panel doesn't update screen after adding a rule
CSCta83701	VPN Peers licensing information is not shown on the Home page
CSCta83741	Tunnel Group authent CLI for Hide username from end user rejected by ASA
CSCtb11934	security scroll bar in DCERPC inspect maps not function properly
CSCtb12190	options in FTP Match Criterion does not match CLI
CSCtb53472	system resource usage: memory status bar chart does not work correctly
CSCtb70513	ASDM doesn't send cert chain Connection Profile change for IPv6 profile
CSCtb70615	VPN ASDM Assistant needs rework--better order flow and description
CSCtb89486	Smart tunnel list edit gives wrong CLI when inherit is select

Table 14 Resolved Caveats in Version 6.3(1) (continued)

Caveat ID	Description
CSCtb89646	DAP: Remove the error for 128 characters with combined URL lists
CSCtb98266	Site-to-site VPN: Cannot Add local/remote network to conn profile.
CSCtc01651	Class-map type inspect rtsp command is recognized by ASDM
CSCtc03470	DAP: Port-Forward Unchanged setting needs to gray out Add button
CSCtc13448	Redundant intf not deleted properly
CSCtc20263	Site-to-Site Wizard: entering invalid IP address creates bad tunn group.
CSCtc20331	Edit conn profile for L2L: Switch between v4 and v6 should clear nets
CSCtc20462	ASDM should not allow configuring no authorization + author required
CSCtc20820	L2L conn profile: the wrong ACL command sent when switch btw v4/v6.
CSCtc25081	Monitoring > VPN Sessions > Detail: Missing IPv6 ACL Tab.
CSCtc25382	IPsec Wizard - step 5: Local/remote nets do not correlate with net type.
CSCtc28937	IPsec Rules: bidirectional conn types should allow IPv4/IPv6 mixed peers
CSCtc53143	Erroneous warning when adding interface in System mode
CSCtc55353	Clicking cancel on Intrusion Prevention tab causes exception
CSCtc68210	Java exception when editing an originate only/ans only crypto map.
CSCtd01568	Site-to-site conn profile: Toggling network types only works once.
CSCtd35353	Failover status panel on homepage not working properly for A/A failover
CSCtd47400	ASDM: ACL Priority not saved in DAP
CSCtd64345	Unable to add more than one network object in an object group at a time.
CSCtd79439	Editing smart tunnel application failed
CSCtd82905	Long pre-shared key is truncated in the summary page of IPsec Wizard
CSCtd88278	Mac users unable to edit or view some fields in local CA Server options
CSCtd90392	IPv6 access rule will not allow ICMP6 service
CSCtd92261	Switching to another device throws an exception
CSCte04433	ASDM: Needs to gray out use LOCAL auth if Cert auth is being used
CSCte17617	Apply button causes exception when changing signature's configuration
CSCte36135	ASDM: SSHv2 plugin should be removed as an option
CSCte55748	ASDM: Incorrectly shows SVC compression as being enabled
CSCte58123	SVC Image Order modification not refreshed in ASDM
CSCte62006	ASDM ignores crypto maps with ipv6-local-address
CSCte70327	Failed to assign clientless sslvpn bookmark list with smart tunnel
CSCte83654	ASDM: AnyConnect Customization scripts facility
CSCte83873	ASDM: OnDisconnect script import fails for AnyConnect
CSCtf20814	ASDM HAS wizard waiting time is too short for A/A failover configuration
CSCtf21045	With Java 6, Update 18, IDM does not load due to heap size check

End-User License Agreement

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

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

Related Documentation

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

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

Note Although ASDM 6.3 supports many ASA versions, the ASDM 6.3 documentation and online help only include features for ASA 8.3. For older ASA versions, you might find that using the ASDM 6.3 documentation is inaccurate for your older feature set. Instead, refer to the ASDM guide in which support for your platform version was added (to see when support was added, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility* for the minimum supported version of ASDM for each ASA version; this version is the one where support was added). Although the specific information about the ASDM GUI might be inaccurate in that guide, the platform feature set is documented correctly.

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:

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.

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