Release Notes for Cisco ASDM, Version 6.2(x)

January 2010

This document contains release information for the following Cisco ASDM versions for the Cisco ASA 5500 series:

- 6.2(5)
- 6.2(3)
- 6.2(1)

This document includes the following sections:

Important Notes

- For Smart Call Home Version 3.0(1), full support for the adaptive security appliance on the backend server is not yet available. The following features are *not* available, and will only be available in Cisco Smart Call Home Version 3.1 (not yet released):
  a. Web portal reports related to Threat, Telemetry, and Snapshot messages.
  b. Configuration message parsing to generate a feature list on the web portal.

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

c. Diagnostic messages that trigger any action, such as to open an SR case.

- AIP SSC Setup Screen in ASDM—AIP (IPS) users will be unable to use ASDM to set up SSC if you mistype a password in the SSC-setup screen.
- ASDM Launcher Upgrade Failure—Upgrading from an older version of ASDM, such as ASDM 6.1.5.51, which includes ASDM Launcher 1.5.30, sometimes fails in the following two ways on Windows XP or Vista:
  - CSCsy7572—When using the ASDM Launcher to upgrade, the installer fails, and the following message appears: "The system cannot open the device or file specified." Clicking Retry does not succeed.
  - CSCsz35267—When using a web browser, clicking the "Install ASDM Launcher and Run ASDM" button downloads the dm-launcher.msi installer. Running dm-launcher.msi may produce an error 1307 or 1316 dialog giving the full pathname of the file that either cannot be found or for which a network error occurred.

  Workaround : To recover from such events, use the Add or Remove Programs control panel to remove the Cisco ASDM Launcher or Cisco ASDM-IDM Launcher. (Any of the ASDM on *IP address* programs do not need to be removed.) Afterwards, launch a web browser; access ASDM with a URL such as https://*IP_Address* /admin; and install the new ASDM-IDM Launcher using the Install ASDM Launcher and Run ASDM button.

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 Explore	Firefox	Safari	
Microsoft Windows (English and Japanese): • 7 • Vista • 2003 Server • XP • 2000 (Service Pack 4 or higher)	6.0 or above	1.5 or above	No support.	• 5.0 (1.5.0) • 6.0
Apple Macintosh OS X: • 10.6 • 10.5 • 10.4	No support.	1.5 or above	2.0 or above	• 5.0 (1.5.0) • 6.0
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • WS	N/A	1.5 or above	N/A	• 5.0 (1.5.0) • 6.0

1. Obtain Sun Java from java.sun.com.

Note ASDM supports up to a maximum of a 512 KB configuration. If you exceed this amount, you may experience performance issues.

Supported Platforms

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 and SSM version.

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

Note Although ASDM 6.2 supports many ASA versions, the ASDM 6.2 documentation and online help only include features for ASA 8.2. For older ASA versions, you might find that using the ASDM 6.2 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 6.2(5)/ASA 8.2(2)

Released: January 11, 2010

Table 2 lists the new features for ASA Version 8.2(2)/ASDM Version 6.2(5).

Table 2 New Features for ASA Version 8.2(2)/ASDM Version 6.2(5)

Feature	Description
Remote Access Features	
Scalable Solutions for Waiting-to-Resume VPN Sessions	An administrator can now keep track of the number of users in the active state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in. The following screen was modified: Monitoring > VPN > VPN Statistics > Sessions. *Also available in Version 8.0(5).*

Table 2 New Features for ASA Version 8.2(2)/ASDM Version 6.2(5) (continued)

Feature	Description
Application Inspection Features	
Inspection for IP Options	You can now control which IP packets with specific IP options should be allowed through the adaptive security appliance. You can also clear IP options from an IP packet, and then allow it through the adaptive security appliance. Previously, all IP options were denied by default, except for some special cases. **Note** This inspection is enabled by default. Therefore, the adaptive security appliance allows RSVP traffic that contains packets with the Router Alert option (option 20) when the adaptive security appliance is in routed mode. The following screens were introduced: Configuration > Firewall > Objects > Inspect Maps > IP-Options Configuration > Firewall > Service Policy > Add/Edit Service Policy Rule > Rule Actions > Protocol Inspection
Enabling Call Set up Between H.323 Endpoints	You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The adaptive security appliance includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint IP address is unknown and the adaptive security appliance opens a pinhole through source IP address/port 0/0. By default, this option is disabled. The following screen was modified: Configuration > Firewall > Objects > Inspect Maps > H.323 > Details > State Checking. *Also available in Version 8.0(5).*
Unified Communication Features	
Mobility Proxy application no longer requires Unified Communications Proxy license	The Mobility Proxy no longer requires the UC Proxy license.
Interface Features	
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresess are also now persistent accross reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2. The following screen was modified: Configuration > Context Management > Security Contexts. *Also available in Version 8.0(5).*
Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces	You can now enable pause (XOFF) frames for flow control. The following screens were modified: (Single Mode) Configuration > Device Setup > Interfaces > Add/Edit Interface > General (Multiple Mode, System) Configuration > Interfaces > Add/Edit Interface
Firewall Features	

Table 2 New Features for ASA Version 8.2(2)/ASDM Version 6.2(5) (continued)

Feature	Description
Botnet Traffic Filter Enhancements	The Botnet Traffic Filter now supports automatic blocking of blacklisted traffic based on the threat level. You can also view the category and threat level of malware sites in statistics and reports. Reporting was enhanced to show infected hosts. The 1 hour timeout for reports for top hosts was removed; there is now no timeout. The following screens were introduced or modified: Configuration > Firewall > Botnet Traffic Filter > Traffic Settings Monitoring > Botnet Traffic Filter > Infected Hosts
Connection timeouts for all protocols	The idle timeout was changed to apply to all protocols, not just TCP. The following screen was modified: Configuration > Firewall > Service Policies > Rule Actions > Connection Settings.
Routing Features	
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	This enhancement introduces adaptive security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each DHCP server configured for VPN clients, you can now configure the adaptive security appliance to send the Subnet Selection option or the Link Selection option. The following screen was modified: Remote Access VPN > Network Access > IPsec connection profiles > Add/Edit. *Also available in Version 8.0(5).*
High Availablility Features	
IPv6 Support in Failover Configurations	IPv6 is now supported in failover configurations. You can assign active and standby IPv6 addresses to interfaces and use IPv6 addresses for the failover and Stateful Failover interfaces. The following screens were modified: Configuration > Device Management > High Availability > Failover > Setup Configuration > Device Management > High Availability > Failover > Interfaces Configuration > Device Management > High Availability > HA/Scalability Wizard
No notifications when interfaces are brought up or brought down during a switchover event	To distinguish between link up/down transitions during normal operation from link up/down transitions during failover, no link up/link down traps are sent during a failover. Also, no syslog messages about link up/down transitions during failover are sent. *Also available in Version 8.0(5).*
AAA Features	
100 AAA Server Groups	You can now configure up to 100 AAA server groups; the previous limit was 15 server groups. The following screen was modified: Configuration > Device Management > Users/AAA > AAA Server Groups.
Monitoring Features	
Smart Call Home	Smart Call Home offers proactive diagnostics and real-time alerts on the adaptive security appliance and provides higher network availability and increased operational efficiency. Customers and TAC engineers get what they need to resolve problems quickly when an issue is detected. **Note** Smart Call Home server Version 3.0(1) has limited support for the adaptive security appliance. See the "Important Notes" for more information. The following screen was introduced: Configuration> Device Management> Smart Call Home.

New Features in ASDM 6.2(3)/ASA 8.0(5)

Released: November 3, 2009

Table 3 lists the new features for ASA Version 8.0(5)/ASDM Version 6.2(3).

Note Version 8.0(5) is not supported on the PIX security appliance.

Table 3 New Features for ASA Version 8.0(5)/ASDM Version 6.2(3)

Feature	Description
Remote Access Features	
Scalable Solutions for Waiting-to-Resume VPN Sessions	An administrator can now keep track of the number of users in the active state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in The following ASDM screen was modified: Monitoring > VPN > VPN Statistics > Sessions. *Also available in Version 8.2(2).*
Application Inspection Features	
Enabling Call Set up Between H.323 Endpoints	You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The adaptive security appliance includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the security appliance opens a pinhole through source IP address/port 0/0. By default, this option is disabled. The following ASDM screen was modified: Configuration > Firewall > Objects > Inspect Maps > H.323 > Details > State Checking. *Also available in Version 8.2(2).*
Interface Features	
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresess are also now persistent accross reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2. The following ASDM screen was modified: Configuration > Context Management > Security Contexts. *Also available in Version 8.2(2).*
High Availablility Features	
No notifications when interfaces are brought up or brought down during a switchover event	To distinguish between link up/down transitions during normal operation from link up/down transitions during failover, no link up/link down traps are sent during a failover. Also, no syslog messages about link up/down transitions during failover are sent. *Also available in Version 8.2(2).*
Routing Features	

Table 3 New Features for ASA Version 8.0(5)/ASDM Version 6.2(3) (continued)

Feature	Description
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	This enhancement introduces adaptive security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). The following ASDM screen was modified: Remote Access VPN > Network Access > IPsec connection profiles > Add/Edit. *Also available in Version 8.2(2).*
SSM Features	
CSC 6.3 Support in ASDM	ASDM displays Web Reputation, User Group Policies, and User ID Settings in the Plus License listing on the main home page. CSC 6.3 security event enhancements are included, such as the new Web Reputation events and user and group identifications.

New Features in ASDM 6.2(1)/ASA 8.2(1)

Released: May 6, 2009

Table 4 lists the new features for ASA Version 8.2(1)/ASDM Version 6.2(1).

Table 4 New Features for ASA Version 8.2(1)/ASDM Version 6.2(1)

Feature	Description
Remote Access Features	
One Time Password Support for ASDM Authentication	ASDM now supports administrator authentication using one time passwords (OTPs) supported by RSA SecurID (SDI). This feature addresses security concerns about administrators authenticating with static passwords. New session controls for ASDM users include the ability to limit the session time and the idle time. When the password used by the ASDM administrator times out, ASDM prompts the administrator to re-authenticate. In ASDM, see Configuration > Device Management > Management Access > ASDM/HTTPD/Telnet/SSH.
Customizing Secure Desktop	You can use ASDM to customize the Secure Desktop windows displayed to remote users, including the Secure Desktop background (the lock icon) and its text color, and the dialog banners for the Desktop, Cache Cleaner, Keystroke Logger, and Close Secure Desktop windows. In ASDM, see Configuration > CSD Manager > Secure Desktop Manager.
Pre-fill Username from Certificate	The pre-fill username feature enables the use of a username extracted from a certificate for username/password authentication. With this feature enabled, the username is “pre-filled” on the login screen, with the user being prompted only for the password. The double-authentication feature is compatible with the pre-fill username feature, as the pre-fill username feature can support extracting a primary username and a secondary username from the certificate to serve as the usernames for double authentication when two usernames are required. In ASDM, see Configuration> Remote Access VPN > Network (Client) Access > AnyConnect or Clienltess SSL VPN Connection Profiles > Advanced. Settings are in the Authentication, Secondary Authentication, and Authorization panes.

Table 4 New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)

Feature	Description
Double Authentication	The double authentication feature implements two-factor authentication for remote access to the network, in accordance with the Payment Card Industry Standards Council Data Security Standard. This feature requires that the user enter two separate sets of login credentials at the login page. For example, the primary authentication might be a one-time password, and the secondary authentication might be a domain (Active Directory) credential. If either authentication fails, the connection is denied. Both the AnyConnect VPN client and Clientless SSL VPN support double authentication. The AnyConnect client supports double authentication on Windows computers (including supported Windows Mobile devices and Start Before Logon), Mac computers, and Linux computers. The IPsec VPN client, SVC client, cut-through-proxy authentication, hardware client authentication, and management authentication do not support double authentication. **Note** The RSA/SDI authentication server type cannot be used as the secondary username/password credential. It can only be used for primary authentication. In ASDM, see Configuration > Remote Access VPN > Network (Client) Access or Clientless SSL VPN > AnyConnect Connection Profiles > Add/Edit > Advanced > Secondary Authentication.
AnyConnect Essentials	AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the adaptive security appliance, that provides the full AnyConnect capability, with the following exceptions: • No CSD (including HostScan/Vault/Cache Cleaner) • No clientless SSL VPN • Optional Windows Mobile Support The AnyConnect Essentials client provides remote end users running Microsoft Windows Vista, Windows Mobile, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client. **Note** This license cannot be used at the same time as the shared SSL VPN premium license. In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials License. The AnyConnect Essentials license must be installed for ASDM to show this pane.
Disabling Cisco Secure Desktop per Connection Profile	When enabled, Cisco Secure Desktop automatically runs on all computers that make SSL VPN connections to the adaptive security appliance. This new feature lets you exempt certain users from running Cisco Secure Desktop on a per connection profile basis. It prevents the detection of endpoint attributes for these sessions, so you might need to adjust the Dynamic Access Policy (DAP) configuration. In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Add or Edit > Advanced, Clientless SSL VPN Configuration. or Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add or Edit > Advanced > SSL VPN.

Table 4 New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)

Feature	Description
Certificate Authentication Per Connection Profile	Previous versions supported certificate authentication for each adaptive security appliance interface, so users received certificate prompts even if they did not need a certificate. With this new feature, users receive a certificate prompt only if the connection profile configuration requires a certificate. This feature is automatic. In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Basic. or Configuraiton > Remote Access VPN > Clientless SSL VPN > Connection Profiles > Add/Edit>Basic.
EKU Extensions for Certificate Mapping	This feature adds the ability to create certificate maps that look at the Extended Key Usage extension of a client certificate and use these values in determining what connection profile the client should use. If the client does not match that profile, it uses the default group. The outcome of the connection then depends on whether or not the certificate is valid and the authentication settings of the connection profile. In ASDM, use the IPSec Certificate to Connection Maps > Rules pane, or Certificate to SSL VPN Connections Profile Maps pane.
SSL VPN SharePoint Support for Win 2007 Server	Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.
Shared license for SSL VPN sessions	You can purchase a shared license with a large number of SSL VPN sessions and share the sessions as needed among a group of adaptive security appliances by configuring one of the adaptive security appliances as a shared license server, and the rest as clients. **Note** This license cannot be used at the same time as the AnyConnect Essentials license. In ASDM, see Configuration > Device Management > Licensing > Shared SSL VPN Licenses. Also see, Monitoring > VPN > Clientless SSL VPN > Shared Licenses.
Updated VPN Wizard	The VPN Wizard (accessible by choosing Wizards > IPSec VPN Wizard) was updated. The step to select IPsec Encryption and Authentication (formerly Step 9 of 11) was removed because the Wizard now generates default values for these settings. In addition, the step to select IPsec Settings (Optional) now includes new fields to enable perfect forwarding secrecy (PFS) and set the Diffie-Hellman Group.
Firewall Features	
TCP state bypass	If you have asymmetric routing configured on upstream routers, and traffic alternates between two adaptive security appliances, then you can configure TCP state bypass for specific traffic. In ASDM, see Configuration > Firewall > Service Policy Rules > Rule Actions > Connection Settings.
Per-Interface IP Addresses for the Media-Termination Instance Used by the Phone Proxy	In Version 8.0(4), you configured a global media-termination address (MTA) on the adaptive security appliance. In Version 8.2, you can now configure MTAs for individual interfaces (with a minimum of two MTAs). As a result of this enhancement, the old CLI has been deprecated. You can continue to use the old configuration if desired. However, if you need to change the configuration at all, only the new configuration method is accepted; you cannot later restore the old configuration. In ASDM, see Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Media Termination Address.

Table 4 New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)

Feature	Description
H.239 Message Support in H.323 Application Inspection	In this release, the adaptive security appliance supports the H.239 standard as part of H.323 application inspection. H.239 is a standard that provides the ability for H.300 series endpoints to open an additional video channel in a single call. In a call, an endpoint (such as a video phone), sends a channel for video and a channel for data presentation. The H.239 negotiation occurs on the H.245 channel. The adaptive security appliance opens a pinhole for the additional media channel. The endpoints use open logical channel message (OLC) to signal a new channel creation. The message extension is part of H.245 version 13. The decoding and encoding of the telepresentation session is enabled by default. H.239 encoding and decoding is preformed by ASN.1 coder. In ASDM, see Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard > Rule Actions > Protocol Inspection > H.323 H.225. Click **Configure** and then choose the H.323 Inspect Map.
Processing H.323 Endpoints When the Endpoints Do Not Send OLCAck	H.323 application inspection has been enhanced to process common H.323 endpoints. The enhancement affects endpoints using the extendedVideoCapability OLC with the H.239 protocol identifier. Even when an H.323 endpoint does not send OLCAck after receiving an OLC message from a peer, the adaptive security appliance propagates OLC media proposal information into the media array and opens a pinhole for the media channel (extendedVideoCapability). In ASDM, see Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard > Rule Actions > Protocol Inspection > H.323 H.225.
IPv6 in transparent firewall mode	Transparent firewall mode now participates in IPv6 routing. Prior to this release, the adaptive security appliance could not pass IPv6 traffic in transparent mode. You can now configure an IPv6 management address in transparent mode, create IPv6 access lists, and configure other IPv6 features; the adaptive security appliance recognizes and passes IPv6 packets. All IPv6 functionality is supported unless specifically noted. In ASDM, see Configuration > Device Management > Management Access > Management IP Address.
Botnet Traffic Filter	Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity. You can also supplement the dynamic database with a static database by entering IP addresses or domain names in a local “blacklist” or “whitelist.” **Note** This feature requires the Botnet Traffic Filter license. See the following licensing document for more information: http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html In ASDM, see Configuration > Firewall > Botnet Traffic Filter.
AIP SSC card for the ASA 5505	The AIP SSC offers IPS for the ASA 5505 adaptive security appliance. Note that the AIP SSM does not support virtual sensors. In ASDM, see Configuration > Device Setup > SSC Setup and Configuration > IPS.
IPv6 support for IPS	You can now send IPv6 traffic to the AIP SSM or SSC when your traffic class uses the **match any** command, and the policy map specifies the **ips** command. In ASDM, see Configuration > Firewall > Service Policy Rules.
Management Features	

Table 4 New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)

Feature	Description
SNMP version 3 and encryption	This release provides DES, 3DES, or AES encryption and support for SNMP Version 3, the most secure form of the supported security models. This version allows you to configure authentication characteristics by using the User-based Security Model (USM). In ASDM, see Configuration > Device Management > Management Access > SNMP.
NetFlow	This feature was introduced in Version 8.1(1) for the ASA 5580; this version introduces the feature to the other platforms. The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. In ASDM, see Configuration > Device Management > Logging > Netflow.
Routing Features	
Multicast NAT	The adaptive security appliance now offers Multicast NAT support for group addresses.
Troubleshooting Features	
Coredump functionality	A coredump is a snapshot of the running program when the program has terminated abnormally. Coredumps are used to diagnose or debug errors and save a crash for later or off-site analysis. Cisco TAC may request that users enable the coredump feature to troubleshoot application or system crashes on the adaptive security appliance. To enable coredump, use the **coredump enable** command.
ASDM Features	
ASDM Support for IPv6	All IPv6 functionality is supported unless specifically noted.
Support for Public Server configuration	You can use ASDM to configure a public server. This allows to you define servers and services that you want to expose to an outside interface. In ASDM, see Configuration > Firewall > Public Servers.

Upgrading the Adaptive Security Appliance

This section describes how to upgrade the adaptive security appliance to a new ASDM release. If you have a Cisco.com login, you can obtain ASDM from one of the following websites:

http://www.cisco.com/cgi-bin/tablebuild.pl/asa

or

http://www.cisco.com/cgi-bin/tablebuild.pl/pix

Note If you are upgrading from PIX Version 6.3, first upgrade to Version 7.0 according to *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*. Then upgrade PDM to ASDM according to the ASDM 5.0 release notes.

If you have a previous release of ASDM on your adaptive security appliance and want to upgrade to the latest release, you can do so from within ASDM. We recommend that you upgrade the ASDM image before the platform image. ASDM is backward compatible, so you can upgrade the platform image using the new ASDM; you cannot use an old ASDM with a new platform image.

Note If the ASA or PIX is running a version earlier than 8.0, then ASA and ASDM must be upgraded at the same time as the ASA or PIX operating system using the existing version of ASDM. This should be compatible with the existing operating system.
But, if ASA or PIX is running version 8.0 or later, then ASDM 6.2 is backward compatible and may be upgraded before the ASA or PIX operating system.

To upgrade ASDM, perform the following steps:

Step 1 Download the new ASDM image to your PC.

Optionally, you can download a new platform image to your PC if the installed image is earlier than 8.0.

Step 2 Launch ASDM.

Step 3 From the Tools menu:

a. In ASDM 5.0 and 5.1, choose **Tools > Upload Image from Local PC**.

b. In ASDM 5.2, choose **Tools > Upgrade Software**.

c. In ASDM 6.0 or later, choose **Tools > Upload Software from Local Computer**.

Step 4 With ASDM selected, click **Browse Local** to select the new ASDM image.

Step 5 To specify the location in Flash memory where you want to install the new image, enter the directory path in the field or click **Browse Flash**.

If your adaptive security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifying the same destination filename. You can rename the image after it was uploaded using the **Tools > File Management** tool.

If you have enough memory for both versions, you can specify a different name for the new version. If you need to revert to the old version, it is still in your Flash memory.

Step 6 Click **Upload Image**.

When ASDM is finished uploading, the following message appears:

"ASDM Image is Uploaded to Flash Successfully."

Step 7 **For Version 5.x only**: If the new ASDM image has a different name than the old image, then you must configure the adaptive security appliance to load the new image. Use the **Configuration > Properties > Device Administration > Boot System/Configuration** pane.

Step 8 If installing a new platform image, download the new platform image using the **Tools > Upgrade Software** tool with ASA or PIX selected.

If your adaptive security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifying the same destination filename. You can rename the image after it was uploaded using the **Tools > File Management** tool.

Step 9 If installing a new image, select ASA as the new image, and reload the security appliance using the **Tools > System Reload** tool.

Make sure to choose "Save the running configuration at time of reload".

Step 10 To run the new ASDM image, exit ASDM and reconnect.

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

Table 5 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 5 List of Unsupported Commands

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used.
capture	Ignored.
coredump	Ignored. This can be configured only using the CLI.
eject	Unsupported.
established	Ignored.
failover timeout	Ignored.
ipv6 nd prefix	Unsupported.
match-metric	Ignored. This is a subcommand of route-map.
match-interface	Ignored. This is a subcommand of route-map.
match route-type	Ignored. This is a subcommand of route-map.
pager	Ignored.
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`

Table 5 List of Unsupported Commands **(continued)**

Unsupported Commands	ASDM Behavior
set metric	Ignored.
sysopt nodnsalias	Ignored.
sysopt uauth allow-http-cache	Ignored.
terminal	Ignored.
tunnel-group name general-attributes dhcp-server	The **dhcp-server** subcommand is unsupported. ASDM only allows one setting for all DHCP servers.

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**.
- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.

  Monitor-only mode allows access to the following functions:

  – The Monitoring area

  – The CLI tool (Tools > Command Line Interface), which lets you use the CLI commands

  To exit Monitor-only mode, use the CLI tool or access the adaptive security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.

Note You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to three by your system administrator, which allows Monitor-only mode. For more information, choose **Configuration > Device Masagement > Users/AAA > User Accounts** and **Configuration > Device Management > Users/AAA > AAA Access**.

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. From the ASDM Tools menu, click **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 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 6.2(3), then you need to add the caveats in this section to the resolved caveats from 6.2(3)and above 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 6 Open Caveats

Caveat ID	Description
CSCsx17471	Public Server: ASDM should pop up error message for Network Address
CSCsx20290	Deleting 'default' res class won't create default class with default val
CSCsx74139	Multiple session ASDM/IDM do not get change notification
CSCsy07567	Navigating to help cause exception: no such entry help/mappingfiles/CSDM
CSCsy41640	Deleting certificate cannot be cancelled if done from a Manage dialog
CSCsy46539	PIM multicast boundary config - Hit Cancel still deletes a rule

Table 6 Open Caveats (continued)

Caveat ID	Description
CSCsy47247	After deletion of subint from system context, blank screen is displayed
CSCsy47315	IPv6: Unable to edit more than one IPv6 address in Startup Wizard
CSCsy47893	Reboot message not displayed for tls-proxy max sessions in trans modes
CSCsy48841	ASDM should exclude intfs in contexts from redundant intf member list
CSCsy49878	Event classes listed in ASDM and ASA in various modes don't match.
CSCsy55390	ASDM should allow users to correct connection parameters - password
CSCsy60282	ASDM 6.2: Warning is displayed while navigating away from PP screen
CSCsy60567	SNMPv3 users is able to be deleted when trap host is configured.
CSCsy66490	PS: Changing public server entry might affect other entries.
CSCsz31684	ASDM-DAP uses wrong logic when evaluating cmd endpoint "Does Not Exist"
CSCsz37172	Device setup panel was not updating when switching from 5520 to 5505
CSCsz53036	CCO upgrade tool needs to select image by platform
CSCsz67338	CSD: Prelogin Screen is jumpy & difficult to configure
CSCsz83538	ASDM unable to connect to SSC when max password attempts are set
CSCta28735	Usability - ASDM not capable of configuring "no client-types" CLI
CSCtc38749	ACL name with ISO-8859-1 char set not shown properly in ASDM
CSCtc41192	auto-signon password variable/macros should be shown, and not dots
CSCtc41594	Files Blocked in CSC Threat Summary display incorrect value
CSCtc53304	With a large config, ASDM takes a long time to change config windows
CSCtc55212	Files Blocked value in threats monitoring is incorrect
CSCtc55238	URL Blocked value in threats monitoring is incorrect
CSCtc83526	ASDM Config Guide AAA section needs corrections/updates
CSCtc95629	FO happens again after 4 minutes of initial FO.
CSCtd64607	"HA and scalability Wizard" show wrong Switch port in page 3/6
CSCtd64820	ASDM IPS throws an error when attempting to configure signature def
CSCte01163	ASA will not copy a zero size file to flash:
CSCte05092	ASDM throws error when copying small size file to flash: and copy fails
CSCte07747	Wrong URL Used for Dowloading Other Context Captures Through Admin
CSCte15451	ASDM: Implement AnyConnect proxy settings to be configuarable
CSCte35751	ASDM does not read 30 word auth-prompt banner from config

Resolved Caveats

This section includes the following topics:

Resolved Caveats for Software Version 6.2(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 7 Resolved Caveats in Version 6.2(5)

Caveat ID	Description
CSCse13901	spaces in empty banner messages should be retained by ASDM
CSCsm81302	Delete key should work
CSCso05236	Pasting of address bar fails in some applications
CSCsy11676	Config in IPS>Launch Startup Wizard does not sync with IPS>Setup screen
CSCsy15320	TCP Map: incorrect defaults are used by ASDM
CSCsy21876	MTA: CLI error if configure interface address from the wrong subnet
CSCsy24230	Global MTA throws error if configured to a named network object
CSCsy25029	ASDM should not allow deleting a TLS proxy that is used by phone proxy
CSCsy46207	PIM multicast boundary config edit show blank screen
CSCsy48032	When switching from single to multiple mode, get activation key error
CSCsy58982	ASDM Traffic Allocation help link Page cannot be found for SSC
CSCsy60576	ASDM errors when initially connecting to the IPS
CSCsy61040	Link to monitoring track in search results lead to no page found
CSCsz35987	PIM multicast boundary filter not applied to interface
CSCsz42408	CSC Email Reputation Service typo
CSCta09416	Phone Proxy: do not enforce TFTP servers
CSCta35861	challenge/response (CRACK) needs to be removed from site-to-site wizard
CSCtb15564	Missing support for SSL encryption algorithm null-sha1
CSCtb25499	ASDM fails to show IPsec connections page
CSCtb39103	Logging > E-mail Setup: Adding an entry for Warning causes a CLI warning
CSCtb83506	Not showing the URL to get crypto access when upgrading ASA/ASDM
CSCtc10255	ASDM PDF Botnet Traffic Filter Top Reports axis need names + no .5 conn
CSCtc17246	ASDM Home, VPN Sessions panel has SSL counts discrepancy
CSCtc23480	ASDM still uses aaa.cisco.class attribute with 8.0.4.x
CSCtc33135	ASDM: Ping and Traceroute buttons are not visible for priv 5 users
CSCtc36640	Language translation table edit doesn't work properly
CSCtc41316	ASDM: Needs to alphabetize domain names in localization
CSCtc54761	ASDM: SSL VPN Client Profile - need the ability to re-submit the command
CSCtc59297	ASDM: Update text in clientless bookmarks for password macro caveats

Table 7 Resolved Caveats in Version 6.2(5) (continued)

Caveat ID	Description
CSCtc62500	ASDM: Edit Context Interface list not populated
CSCtc68152	Need an ERROR msg when overlap IPv6 address assigned to an intf.
CSCtc68258	No ERROR msg when multicast IPv6 assigned in failover
CSCtc68845	Losing Web links in Trend Micro Content Security
CSCtc76298	NAT: Error message on Global pool configuration in Transparent mode
CSCtc80421	ASDM parser for "wr mem" does not parse Error output properly
CSCtc81893	ASDM will not allow interface as source or destination on ACL line
CSCtc83664	ASDM: Last Updated time on screens does not account for time zone
CSCtc85528	Packet Capture Wizard missing buttons
CSCtc87863	ldap aaa-server using SASL Kerberos-show Kerberos servers drop down
CSCtc88140	IPv6 access rule will not allow interface as source or destination
CSCtc95845	"HA and scalability Wizard" doesn't show IPv6 address in page 5/6
CSCtd05080	IPv6 link-local standby address configuration not supported
CSCtd15820	ASDM:object-group:User should not be allowed to select object "any"
CSCtd19950	IllegalArgumentException when adjust the range for CPU Alert Threshold
CSCtd32204	MTA: selecting interface without IP causes an exception
CSCtd32616	cannot add HTTP subscribers with port
CSCtd37791	HA and Scalability Wizard stops at step 2/6 in 5505 transparent mode
CSCtd38449	No license information showed in Multimode
CSCtd44359	Error in sending command when setting IP for primary in HAS wizard
CSCtd52186	Cisco Certificate for signed java classes in JAR has expired 11/13/09
CSCtd81549	Values of few fields are not showing in Security Context page
CSCtd94449	ASDM (JNLP) does not have a digital signature.

Resolved Caveats for Software Version 6.2(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 8 Resolved Caveats in Version 6.2(3)

Caveat ID	Description
CSCsk42250	ASDM does not support 1000 mbit/s ports on ASA5510
CSCso60199	Packet Tracer Tool not available with ASDM Read-Only profile.
CSCsq10143	Edit Static NAT Rule dialog is overlapping other text.
CSCsw78887	ASDM does not build Protocol 50 based reverse access-lists.
CSCsy13589	Remove http idle-timeout check box.

Table 8 Resolved Caveats in Version 6.2(3) (continued)

Caveat ID	Description
CSCsy41336	ASDM: Ascertain parity with warning messages for ACE / CSD.
CSCsy43548	IPv6: ASDM Static Route Panel support not allow hop count to be less than 255.
CSCsy48416	NAT: ASDM displays overlap error message for valid static NAT entry.
CSCsy55679	ASDM sometimes deletes the wrong Global Pool entry.
CSCsy62866	SSLVPN: Can't edit DAP record name that contains spaces.
CSCsy70075	Restore Configs use backward slash on Mac OS X.
CSCsy73695	IPv6: Edit IPv6 address in object group fails when group had IPv4 address.
CSCsy73787	IPv6: cut / paste fails on ACL Manager.
CSCsy80386	ASDM: Disabling 1 L2L ipsec connection profile may also disable others.
CSCsy81499	High Availability Wizard doesn't send join-failover-group.
CSCsy90560	ASDM windows sometimes lack access to some options.
CSCsy93539	Can't edit a language translation table.
CSCsy98518	ASDM: RDPv2 needs to be added as an import option.
CSCsz09478	IPv6 standby error in HAS wizard.
CSCsz24613	AnyConnect Conn Profile shouldn't list Portal Page Customization option.
CSCsz32744	Display incorrect default value from "Enable TTL evasion protection".
CSCsz35267	Unable to upgrade ASDM Launcher. Upgrading the ASDM demo also fails..
CSCsz35773	Apply button inactive for DNS added static NAT.
CSCsz37223	ASDM: New proposal for translation domain presentation and text.
CSCsz50664	TNXXXX Plugins should not be shown in ASDM until we officially support.
CSCsz53047	"Clear content" on ASDM Syslog messages window doesn't work.
CSCsz57819	ASDM displaying message of unsupported characters when adding bookmarks.
CSCsz61110	ASDM login failure with a trailing space in password.
CSCsz66274	Unable to add aaa-server from ASDM.
CSCsz66527	Editing AAA rules to include multiple services throws exception.
CSCsz68231	ASDM warns before shutting down a subinterface incorrectly.
CSCsz74906	ASDM: Support for the new username & password for auto-signon.
CSCsz83205	ASDM: Unable to logoff VPN users without command authorization.
CSCta05224	ASDM always removing track and sla along with tracked static route.
CSCta09436	In ASDM 6.2 unable to set Radius-SDI-Xauth under Tunnel-Group.
CSCta14142	Strip-Realm for SSL VPN Connection Profiles needs to be added to ASDM.
CSCta42388	Source and Destination not correct in Real-Time Log Viewer.
CSCta43123	VPN loadbalancing cluster load page stuck at 72%.
CSCta49499	DAP: ldap memberof attribute match should not be case sensitive.
CSCta54516	ACL and NAT diagram hides config choices at bottom of screen.
CSCta59407	Launcher v. 1.5(43) doesn't work with ASA 8.2/ASDM 6.2.

Table 8 Resolved Caveats in Version 6.2(3) (continued)

Caveat ID	Description
CSCta73805	Space character not allowed in DAP not for older ASA images.
CSCta94242	Cut/paste of ACL with object-group does not work.
CSCtb17517	ASDM:Filter not working in 'Crypto Map > Find'.
CSCtb53837	Phone Proxy: CLI error because of incorrect http-proxy config.
CSCtb73849	ASDM does not work with MAC OS 10.6 (Snow Leopard).
CSCtb81523	ASDM RA-VPN wizard will not complete configuration.
CSCtc49841	Cannot perform ASDM backup with some CSD configs.
CSCtc53541	JideSplitButton text clipped in toolbars with JIDE 2.7.3.
CSCtc54002	Java console logs on Packet-tracer.
CSCtc55401	Configuration > Firewall has unexpected panel behavior.
CSCtc57536	Adding and immediately deleting an access rule causes null pointer exception.
CSCtc58631	Exception thrown while taking the backup.
CSCtc59963	Filter fields in Services and Addresses panes have translucent backgrounds.
CSCtc60020	ASDM:CSD panels missing from 6.3.0.88 and above, and 6.2.2.51.
CSCtc62500	ASDM: Edit Context Interface list not populated.
CSCtc65947	Addresses panel reappears when switching between Firewall tree nodes

Resolved Caveats for Software Version 6.2(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 9 Resolved Caveats in Version 6.2(1)

Caveat ID	Description
CSCse00007	VPN session monitoring: data is not loaded when filter is changed.
CSCsf19215	ASDM hard timeout for device i/o causes disconnect with large ACL.
CSCso63191	ASDM users with Privilege Level 0,1 Shouldn't Gain ASDM Access.
CSCsr29312	Unable to bring up Spyware Blocked Graph in Monitoring Module.
CSCsr56857	Click on configuration>content security hangs ASDM.
CSCsr59735	ASDM: SSL Server/Client Settings.
CSCsu00498	ASDM fails to add ACLs when access rules are filtered.
CSCsu22860	Time-range object for periodic/recurring time always displays Sunday.
CSCsu36051	The panel for File Transfer between Remote Server and Flash is hidden.
CSCsu43237	Global VPN parameters being set from tunnel-group screen.
CSCsu74661	ASDM monitoring stats are being cached between devices.
CSCsu78452	Can't enter domain name with multiple DNS server groups option.

Table 9 Resolved Caveats in Version 6.2(1) (continued)

Caveat ID	Description
CSCsu78499	Deleting group-policy Stop msg still used by Connection Profile
CSCsu79785	ASDM did not stop user to config vlan over system limit.
CSCsv02654	Number-of-rate option has wrong default for threat-detection config.
CSCsv12681	Error while loading ASDM: "Unconnected sockets not implemented".
CSCsv21391	ASDM Privacy Protection panel...Secure Desktop (Vault) clarification.
CSCsv21411	ClassNotFoundException on switching between devices.
CSCsv22348	CSC: CPU and memory graphs not displayed correctly.
CSCsv31292	ASDM:Group Policies panel description mods & link to LDAPAttribute Map.
CSCsv31821	ASDM panels need to state where parameter can be enforced.
CSCsv34865	Help > Release Notes is pointing to the wrong Release Notes.
CSCsv40389	ASDM :Privacy Protection in endpoint attributes "None".
CSCsv46652	ASDM: Include a link in Webtype ACL's to group policy and user.
CSCsv48386	ASDM handling of group-policies with special chars.
CSCsv48531	Logging : event classes listed in ASDM and ASA don't match.
CSCsv52632	User preferences: log color chooser dialog not modal.
CSCsv58991	ASDM: Description field in "Add Network Object" depends on Name field.
CSCsv60678	ASDM with CSC blank panels and left navigation only.
CSCsv65908	Unable to enroll user using local CA on with ASDM 6.1.5.
CSCsv66686	Add information text when enabling Smart Tunnel on a Bookmark.
CSCsv66700	ASDM: "only originate-only" error when configuring multi VPN peers.
CSCsv66778	Add a Bookmark Entry, Enable Smart Tunnel option modify Help.
CSCsv80695	ASDM is not able to configure webvpn http-proxy.
CSCsv83883	Network object group changes are not reflected in the GUI.
CSCsv90515	Addresses window moves back to the top when opening a nw object group.
CSCsv90530	The left or right-hand ASDM pane is reduced in width.
CSCsw15502	DAP screen text changes for better usability.
CSCsw18031	ASDM:Present drop-down-list of URL variables/macros in Bookmarks panels.
CSCsw35562	ASDM: POST options need to be grayed in bookmark if ST is enabled.
CSCsw36338	DAP: DfltAccessPolicy mispelled as DflAccessPolicy on a couple of places.
CSCsw37361	ASDM: Usability for wildcarding with Webtype ACL's.
CSCsw37812	ASDM: Apply button is not always available upon deleting a smart tunnel window.
CSCsw41993	Clientless group-alias & group-url config needs Edit capability.
CSCsw43601	DAP DfltAccessPolicy Info bubble message corrections.
CSCsw43603	ASDM not recognizing pre-shared keys with "(" or ")".
CSCsw44286	Clicking refresh results in "saving the configuration to flash" message.

Table 9 Resolved Caveats in Version 6.2(1) (continued)

Caveat ID	Description
CSCsw45755	ASDM: Usability Improvement for Auto Signon with Smart Tunnels.
CSCsw49253	ASDM: Informative icon for fnmatch with ASO Smart Tunnels host name.
CSCsw63632	Group Filter field only lists the extended access-lists.
CSCsw67961	Support ASA CLI: merge-dacl.
CSCsw69606	SSL wizard: selecting "Group Alias/URL" clears the selected Certificate.
CSCsw75528	Can't apply change to LDAP server scope.
CSCsw76614	ASDM:VPN graphs WebVPN/SVC Active Sessions - Terminology change needed.
CSCsw77282	Connection Profile - address pool appears as blank line in advanced view.
CSCsw81248	ASDM:webvpn auto-signon shows CIFS incorrectly as auth type with FTP.
CSCsw85477	ASDM: Smart Tunnels auto signon informative ballon is cut off by window.
CSCsx03483	ASDM should not set a number-of-rate value for TD host statistics.
CSCsx04911	ASDM: "group-url" can't be disabled from ASDM.
CSCsx07674	ASDM - network object group changes with filter causes errored entries.
CSCsx24433	ASDM fails to start with java.lang.StringIndexOutOfBoundsException error.
CSCsx27956	ASDM should use 'user-alert cancel' instead of 'no user-alert'.
CSCsx42814	Remove ASDM restriction in order to support ISO-8859-1.
CSCsx48813	ASDM Support for DAP record name with spaces.
CSCsx50131	CSC graphs show wrong time for timezones other than UTC.
CSCsx59463	ASDM: DHCP server panel help missing Allow VPN over-ride option.
CSCsx97142	TCP Map: creating a map on ASA 8.0 fails.
CSCsy27439	ASDM: Check for L2TP/IPSec PPP auth and AAA server combos.
CSCsy58573	ASDM: Disabling 1 connection profile entry may also disable others.
CSCsy60266	Botnet monitoring not available for read-only/ monitor-only user.

End-User License Agreement

For information on the end-user license agreement, go to:
http://www.cisco.com/univercd/cc/td/doc/es_inpck/eu1jen__.pdf

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

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.