Cisco ASDM Release Notes Version 6.1(5)

October 2008

This document contains release information for Cisco ASDM Version 6.1(5) on Cisco ASA 5500 series and Cisco PIX 500 series security appliances. It includes the following sections:

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	Version	Browser	Other Requirements
Microsoft Windows	Windows Vista Windows 2003 Server Windows XP Windows 2000 (Service Pack 4)	Internet Explorer 6.0 or 7.0 with Sun Java SE[1] Plug-in 1.4.2, 5.0 (1.5.0), or 6.0 Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Note ASDM supports both the English and Japanese versions of Windows.		**Note** **HTTP 1.1**—Settings for **Internet Options > Advanced > HTTP 1.1** should use HTTP 1.1 for both proxy and non-proxy connections.	

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

Table 1 Operating System and Browser Requirements (continued)

Operating System	Version	Browser	Other Requirements
Apple Macintosh	Apple Macintosh OS X	Firefox 1.5 or 2.0 or Safari 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0[2]	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 4 running GNOME or KDE	Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	

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

[2] With Apple Macintosh, only 32-bit Java SE will be supported. Currently, this also excludes Java 6. The 32-bit Java can run on a 64-bit Mac OS.

Note After upgrading ASDM, in order to restore normal memory usage on a Mac, existing ASDM desktop applications must be deleted and a new ASDM desktop application installed in its place. The following instructions avoid CSCsu31299.

On the Mac, go to **Applications** > **Utilities** > **Java** > **Java Preferences**. From the **Java Preferences** dialog select **View**. The Java Cache Viewer dialog appears. Select **Applications** from the **Show** pull-down menu. Select the ASDM on *ip_addr* row in the table that you want to delete, and select the '**X**' to remove the selected item, and click **OK**.
Next, from the **Java Preferences** dialog select **Settings**. Then select **Delete Files**. Choose all options from this pop-up dialog and click on **Delete**. On the **Temporary Files Setting** dialog, click **OK**.
Go to the **Java Preference**s menu and select **Quit Java Preferences**. If the deleted desktop IP address application still appears on the desktop, drag and drop the application into the trash. Launch ASDM from a web browser, either Safari or Firefox, and, if desired, install a new ASDM desktop application when prompted.

Caution If you launch ASDM version 5.0 or later using Java 6 Update 10 or later, the message "ASDM cannot be loaded. Click OK to exit ASDM. Unconnected sockets not implemented" appears.

To get ASDM to load correctly with Java 6 Update 10, update ASDM to ASDM 6.1(5)51. For more information about this issue (CSCsv12681) and obtaining the software, see the Release Notes at: http://download-sj.cisco.com/cisco/crypto/3DES/ciscosecure/asa/interim/asdm-61551-release_notes.html.
Two other issues (CSCsu00498 and CSCsu79785) are also resolved by this build.

Table 2 lists the supported and recommended client operating systems and Java for ASDM.

Table 2 Operating System and Browser Requirements

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

[1] Support for Java 5.0 was removed in ASDM 6.4. Obtain Sun Java updates from java.sun.com.

[2] ASDM requires an SSL connection from the browser to the security appliance. By default, Firefox does not support base encryption (DES) for SSL and therefore requires the 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.

ASDM Compatibility

Table 3 lists information about ASDM, module, and VPN compatibility with the ASA 5500 series.

Table 3 ASDM, SSM, SSC, and VPN Compatibility

Application	Description
ASDM	ASA 5580 Version 8.1(2) requires ASDM Version 6.1(5) or later. For information about ASDM requirements for other releases, see *Cisco ASA Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html
VPN	For the latest OS and browser test results, see the *Supported VPN Platforms, Cisco ASA 5500 Series*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html
Module applications	For information about module application requirements, see *Cisco ASA Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

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

New Features

Released: October 10, 2008

Table 4 lists the new features for ASA Version 8.1(2)/ASDM Version 6.1(5). This ASA software version is only supported on the ASA 5580.

Table 4 New Features for ASA Version 8.1(2)/ASDM Version 6.1(5)

Feature	Description
Remote Access Features	
Auto Sign-On with Smart Tunnels for IE	This feature lets you enable the replacement of logon credentials for WININET connections. Most Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does not, so it is not supported by this feature. It also supports HTTP-based authentication, therefore form-based authentication does not work with this feature. Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. Also, because of the association with destinations hosts, providing support for an auto sign-on enabled host may not be desirable if you want to deny access to some of the services on that host. To configure a group auto sign-on for smart tunnels, you create a global list of auto sign-on sites, then assign the list to group policies or user names. This feature is not supported with Dynamic Access Policy. In ASDM, see Configuration > Firewall > Advanced > ACL Manager.
Entrust Certificate Provisioning	ASDM 6.1.3 (which lets you manage security appliances running Versions 8.0x and 8.1x) includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA. In ASDM, see Configuration > Remote Access VPN > Certificate Management > Identity Certificates > Enroll ASA SSL VPN head-end with Entrust.
Extended Time for User Reauthentication on IKE Rekey	You can configure the security appliance to give remote users more time to enter their credentials on a Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunnels and a phase 1 rekey occurred, the security appliance prompted the user to authenticate and only gave the user approximately 2 minutes to enter their credentials. If the user did not enter their credentials in that 2 minute window, the tunnel would be terminated. With this new feature enabled, users now have more time to enter credentials before the tunnel drops. The total amount of time is the difference between the new Phase 1 SA being established, when the rekey actually takes place, and the old Phase 1 SA expiring. With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the rekey interval. In ASDM, see Configuration > Device Management > Certificate Management > Identity Certificates.

Table 4 New Features for ASA Version 8.1(2)/ASDM Version 6.1(5) (continued)

Feature	Description
Persistent IPsec Tunneled Flows	With the persistent IPsec tunneled flows feature enabled, the security appliance preserves and resumes stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dropped when the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP flows allows some older or sensitive applications to keep working through a short-lived tunnel drop. This feature supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a hardware client. It does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the **sysopt connection preserve-vpn-flows** command. This option is disabled by default. In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options. Check the **Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM)** checkbox to enable persistent IPsec tunneled flows.
Show Active Directory Groups	The CLI command **show ad-groups** was added to list the active directory groups. ASDM Dynamic Access Policy uses this command to present the administrator with a list of MS AD groups that can be used to define the VPN policy. In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit DAP > Add/Edit AAA Attribute.
Smart Tunnel over Mac OS	Smart tunnels now support Mac OS. In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels.
Firewall Features	
NetFlow Filtering	You can filter NetFlow events based on traffic and event-type, and then send records to different collectors. For example, you can log all flow-create events to one collector, but log flow-denied events to a different collector. See the **flow-export event-type** command. In ASDM, see Configuration > Firewall > Security Policy > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > NetFlow.
NetFlow Delay Flow Creation Event	For short-lived flows, NetFlow collecting devices benefit from processing a single event as opposed to seeing two events: flow creation and teardown. You can now configure a delay before sending the flow creation event. If the flow is torn down before the timer expires, only the flow teardown event will be sent. See the **flow-export delay flow-create** command. **Note** The teardown event includes all information regarding the flow; there is no loss of information. In ASDM, see Configuration > Device Management > Logging > NetFlow.
QoS Traffic Shaping	If you have a device that transmits packets at a high speed, such as the security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the **shape** command. See also the **crypto ipsec security-association replay** command, which lets you configure the IPSec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPSec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms. In ASDM, see Configuration > Firewall > Security Policy > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.

Table 4 New Features for ASA Version 8.1(2)/ASDM Version 6.1(5) (continued)

Feature	Description
TCP Normalization Enhancements	You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets. • TCP invalid ACK check (the **invalid-ack** command) • TCP packet sequence past window check (the **seq-past-window** command) • TCP SYN-ACK with data check (the **synack-data** command) You can also set the TCP out-of-order packet buffer timeout (the **queue** command **timeout** keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value. The default action for packets that exceed MSS has changed from drop to allow (the **exceed-mss** command). The following non-configurable actions have changed from drop to clear for these packet types: • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option In ASDM, see Configuration > Firewall > Objects > TCP Maps.
TCP Intercept statistics	You can enable collection for TCP Intercept statistics using the **threat-detection statistics tcp-intercept** command, and view them using the **show threat-detection statistics** command. In ASDM, see Configuration > Firewall > Threat Detection.
Threat detection shun timeout	You can now configure the shun timeout for threat detection using the **threat-detection scanning-threat shun duration** command. In ASDM, see Configuration > Firewall > Threat Detection.
Threat detection host statistics fine tuning	You can now reduce the amount of host statistics collected, thus reducing the system impact of this feature, by using the **threat-detection statistics host number-of-rate** command. In ASDM, see Configuration > Firewall > Threat Detection.
Platform Features	
Increased VLANs	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.
SNMP support for unnamed interfaces	Formerly, SNMP only provided information about interfaces that were configured using the **nameif** command. For example, SNMP only sent traps and performed walks on the IF MIB and IP MIB for interfaces that were named. SNMP was enhanced to show information about all physical interfaces and logical interfaces; a **nameif** command is no longer required to display the interfaces using SNMP.

Upgrading the Security Appliance

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

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

Note If you are upgrading from PIX Version 6.3, first upgrade to Version 7.0 according to the *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 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.

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, 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 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 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 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 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 8
- Effects of Unsupported Commands, page 9
- Discontinuous Subnet Masks Not Supported, page 10
- Interactive User Commands Not Supported by the ASDM CLI Tool, page 10

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
dns-guard	Ignored
eject	Unsupported
established	Ignored.
failover timeout	Ignored
icmp-unreachable rate-limit	Ignored
ipv6, any IPv6 addresses	Ignored
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
route-map	Ignored

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`

switchport trunk native vlan	Ignored

Table 5 List of Unsupported Commands (continued)

Unsupported Commands	ASDM Behavior
sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	Ignored
terminal	Ignored

Effects of Unsupported Commands

- If ASDM loads an existing running configuration and finds IPv6-related commands, ASDM displays a dialog box informing you that it does not support IPv6. You cannot configure any IPv6 commands in ASDM, but all other configuration is available.
- 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 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 Management > 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
   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
  ```

Caveats

The following sections describe the open and resolved caveats for Version 6.1(5).

- Open Caveats—Version 6.1(5), page 11
- Resolved Caveats—Version 6.1(5), page 12

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

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

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats—Version 6.1(5)

Table 6 lists the open caveats for Version 6.1(5).

Table 6 Open Caveats

ID Number	Software Version 6.1(5)	
	Corrected	Caveat Title
CSCsl50642	No	Add/Del Interface through CLI not shown in ASDM home page.
CSCsm85034	No	ASDM refresh errors after failover - no response for 60 secs warning.
CSCsm91240	No	Boot image config empty after switch from multiple to single context mode.
CSCso05236	No	Pasting of address bar fails in some applications.
CSCso46258	No	Cannot view DAP for Read-only admins.
CSCsu00498	No	ASDM fails to add ACLs when access rules are filtered.
CSCsu22860	No	Time-range object for periodic/recurring time always displays Sunday.
CSCsu43237	No	Global vpn parameters being set from tunnel-group screen.
CSCsu49256	No	Restoring a certificate via ASDM makes running config change for CA TP.
CSCsu55134	No	Timeout popup displayed on device switch from 8.1 to 8.0 or back.
CSCsu74661	No	ASDM monitoring stats are being cached between devices.
CSCsu77794	No	IPsec cert rules sends incorrect CLI (DN Group Matching).
CSCsu78055	No	ASDM no reponse warning with multiple devices open.
CSCsu78452	No	Can't enter domain name with multiple DNS server groups option.
CSCsu79785	No	ASDM did not stop user to config vlan over system limit.
CSCsu80896	No	Warning for delete CA certificate when being used on ssl interface.
CSCsu83711	No	Rule Tables preference have fields in the wrong place.
CSCsu89521	No	AnyConnect Profile validation should report xml schema errors.
CSCsu95791	No	Preference to limit log file retention not working.
CSCsv12681	No	Error while loading ASDM: "Unconnected sockets not implemented.

Resolved Caveats—Version 6.1(5)

Table 7 lists the resolved caveats for Version 6.1(5).

Table 7 Resolved Caveats

ID Number	Software Version 6.1(5)	
	Corrected	Caveat Title
CSCsr14948	Yes	Can't Launch Network Sniffer Application from ASDM in Non-Admin Contexts
CSCsr41717	Yes	ASDM: sends a [no] upon modifying a ST auto signon list.
CSCsr58575	Yes	Read-only user denied access to config screens in non-admin context.
CSCsr65521	Yes	ASDM: User link in Smart Tunnels is broken.
CSCsr71032	Yes	ASDM is unable to modify an address pool without removing it first.
CSCsr74830	Yes	ASDM generated cert request contains invalid character.
CSCsr87090	Yes	ASDM: Wizard for SSL Client taking me to download SVC Client.

Table 7 Resolved Caveats (continued)

ID Number	Software Version 6.1(5)	
	Corrected	Caveat Title
CSCsr89144	Yes	ASDM: java.lang.NumberFormatException: For input string: "1 year 0".
CSCsr91800	Yes	ASDM: SSL VPN home page value needs to remove http https restrictions.
CSCsr93881	Yes	ASDM: Top ACLs may display 'n/a - config out of sync'.
CSCsu00875	Yes	ASDM incorrectly displays 0 for ACL 'Hits' total in Access Rules config.
CSCsu08960	Yes	Firewall dashboard top ACL rule # is one less than the real ACL rule number.
CSCsu11455	Yes	Get AD Groups button missing after rebranding ver ASA 8.0.3.39 to 8.0.4.
CSCsu24355	Yes	Remove offset by 100 in the version check.
CSCsu29428	Yes	ASDM: Domain Name should allow starting with a number.
CSCsu29446	Yes	Enable traffic shaping option will not appear when Back button is used.
CSCsu30281	Yes	UC feature screens should be removed from service policy screens.
CSCsu31299	Yes	ASDM 6.1.3 Memory leak in MAC/Apple OS X.
CSCsu36193	Yes	NetFlow-related NPE in service policy rules prior to 8.1.2.
CSCsu43696	Yes	ASDM Fails to Load when AIP-SSM Version Can't Be Read.
CSCsu61384	Yes	Mac OSX: popups generated from ASDM menu not fully displayed.
CSCsu64769	Yes	ASDM is allowing >,<,!=, operators for port-object of Object-group.
CSCsu65197	Yes	ASDM not functioning properly with JRE 1.4.
CSCsu65445	Yes	UC features in the TLS Proxy config should be removed for 8.1.2.
CSCsu67684	Yes	After device switch from 8.1.2 to 8.0.4 ASDM becomes useless.
CSCsu68580	Yes	Upgrade from local PC: file exists warning dialog is not modal.
CSCsu70424	Yes	PFS group 2 added in ASDM VPN Wizard - no option to remove.
CSCsu74962	Yes	ACL to syslog correlation broken for 106100 and 106023.
CSCsu77028	Yes	ASDM graphs not updated with real time data.
CSCsu81027	Yes	System config access for monitor-only user.

End-User License Agreement

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

http://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

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.