Cisco ASDM Release Notes Version 5.2(4)

April 2008

This document contains release information for Cisco ASDM Version 5.2(4) on Cisco ASA 5500 and PIX 500 Adaptive Series Security Appliances. It includes the following sections:

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

Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco ASA 5500 series adaptive security appliances and Cisco PIX security appliances through an intuitive, easy-to-use, web-based management interface. Bundled with supported security appliances, the device manager accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by the security appliance. Its secure, web-based design enables anytime, anywhere access to the security appliance.

New Features

Table 1 lists the new features for ASDM Version 5.2(4). All features apply only to ASA or PIX Version 7.2(4), unless otherwise noted.

Table 1 New Features for ASDM Version 5.2(4)/ASA Version 7.2(4') (Unless Otherwise Noted)

Feature	Description
Remote Access Features	
Application Profile Customization Framework	You can now use an Application Profile Customization Framework (APCF) script to modify the HTTP version in the HTTP header for clientless SSL VPN sessions. You might need to do so to view websites that work only if HTTP/1.1 is disabled in the browser, an impractical task to perform manually in large installations with multiple clients. An APCF is an XML-based rule set for Clientless SSL VPN. It lets the security appliance handle non-standard applications and web resources so they display correctly over a Clientless SSL VPN connection. You can store APCF profiles on the security appliance flash memory, or on an HTTP, HTTPS, or TFTP server. Use either ASDM or the **apcf** command in webvpn mode to identify and locate an APCF profile that you want to load on the security appliance. **Note** We recommend that you configure an APCF profile only with the assistance of Cisco personnel.
Routing Features	

Table 1 New Features for ASDM Version 5.2(4)/ASA Version 7.2(4') (Unless Otherwise Noted) (continued)

Feature	Description
IPv6 Multicast Listener Discovery Protocol v2 Support	The security appliance now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to discover the presence of multicast address listeners on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. The security appliance becomes a multicast address listener, or a host, but not a a multicast router, and responds to Multicast Listener Queries and sends Multicast Listener Reports only. The following commands support this feature: • **clear ipv6 mld traffic** The **clear ipv6 mld traffic** command allows you to reset all the Multicast Listener Discovery traffic counters. • **show ipv6 mld traffic** The **show ipv6 mld** command allows you to display all the Multicast Listener Discovery traffic counters. • **debug ipv6 mld** The enhancement to the **debug ipv6** command allows the user to display the debug messages for MLD, to see whether the MLD protocol activities are working properly. • **show debug ipv6 mld** The enhancement to the **show debug ipv6** command allows the user to display whether **debug ipv6 mld** is enabled or disabled.
Platform Features	
Native VLAN Support on ASA 5505 Trunk Ports	You can now allow native VLANs on a trunk port (see the **switchport trunk native vlan** command). In ASDM, see Configuration > Device Setup > Interfaces > Switch Ports > Edit dialog. *Also available in Version 8.0(4).*
Connection Features	
clear conn Command	The **clear conn** command was added to remove connections.
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 feature 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. *Also available in Version 8.0(4).*
Firewall Features	

Table 1 New Features for ASDM Version 5.2(4)/ASA Version 7.2(4') (Unless Otherwise Noted) (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 the Configuration > Global Objects > TCP Maps pane. *Also available in Version 8.0(4).*
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the **timeout sip-provisional-media** command. In ASDM, see the Configuration > Properties > Timeouts pane. *Also available in Version 8.0(4).*
Troubleshooting and Monitoring Features	
TCP Urgent Flag Syslog	When the TCP urgent flag of a TCP packet is cleared and debugging is enabled, a syslog is generated: ASA-7-419003.
capture command Enhancement	The **capture asp type asp-drop all** command captures all packets that the security appliance drops, including those dropped due to security checks.
MIB Enhancement	The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely.
show asp drop Command Enhancement	The **show asp drop** command now displays the **capture asp-drop type** keywords. This enhancement displays the particular capture type as part of the output of the **show asp drop** command. A timestamp was also added indicating when the last time the asp drop counters were cleared.
show asp table classify hits Command Enhancement	The **hits** option was added to the **show asp table classify** command, showing the timestamp indicating the last time the asp table counters were cleared. It also shows rules with hits values not equal to zero. This permits users to quickly see what rules are being hit, especially since a simple configuration may end up with hundreds of entries in the **show asp table classify** command.
ASDM Features	

Table 1 New Features for ASDM Version 5.2(4)/ASA Version 7.2(4') (Unless Otherwise Noted) (continued)

Feature	Description
Network Objects	You can now add true network objects that you can use in firewall rules. Objects can be named, and when you edit an object, the change is inherited wherever the object is used. Also, when you create a rule, the networks that you specify in the rule are automatically added to the network object list so you can reuse them elsewhere. You can name and edit these automatic entries as well. See Configuration > Objects > Network Objects/Groups.
Enhanced ASDM Rule Table	The ASDM rule tables have been redesigned to streamline policy creation.

ASDM Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for ASDM Version 5.2(4).

Table 2 Operating System and Browser Requirements

Operating System	Version	Browser
Microsoft Windows	Windows Vista Windows 2003 Server Windows XP Windows 2000 (Service Pack 4 or higher)	Internet Explorer 6.0 or higher with Sun Java (JRE)[1] 1.4.2, 5.0 (1.5), or 6.0 Firefox 1.5 or higher with Sun Java (JRE) 1.4.2, 5.0 (1.5), or 6.0
Linux	Red Hat Linux, Red Hat Enterprise Linux WS version 4 running GNOME or KDE	Firefox 1.5 or higher with Sun Java (JRE) 1.4.2, 5.0 (1.5), or 6.0

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

For information on supported platforms and feature licenses, see:

http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/specs.html

Upgrading ASDM and ASA or PIX

This section describes how to upgrade ASDM and ASA 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.

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 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.

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, click **Tools > Upload Image from Local PC**.

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

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** panel.

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 ASA 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 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.

Getting Started with ASDM

This section describes how to connect to ASDM and start your configuration. If you are using the security appliance for the first time, your security appliance might include a default configuration. You can connect to a default IP address with ASDM so that you can immediately start to configure the security appliance from ASDM. If your platform does not support a default configuration, you can log in to the CLI and run the **setup** command to establish connectivity. See Before You Begin for more detailed information about networking.

This section includes the following topics:

Before You Begin

If your security appliance includes a factory default configuration, you can connect to the default management address of 192.168.1.1 with ASDM. On the ASA 5500 series Adaptive Security Appliance, the interface to which you connect with ASDM is Management 0/0. On the PIX 500 series Adaptive Security Appliance, the default interface to which you connect with ASDM is Ethernet1. The PIX535 Adaptive Security Appliance has no default interface. For the PIX 500 series security appliance, the interface to which you connect with ASDM is Ethernet 1. To restore the default configuration, enter the **configure factory-default** CLI. The CLI can be entered through the serial console or through a Telnet or SSH session.

It is also recommended that you install the recommended version of Java before you begin the installation.

Make sure the PC is on the same network as the security appliance. You can use DHCP on the client to obtain an IP address from the security appliance, or you can set the IP address to a 192.168.1.0/24 network address.

If your platform does not support the factory default configuration, or you want to add to an existing configuration to make it accessible for ASDM, access the security appliance CLI according to the *Cisco Security Appliance Command Line Configuration Guide*, and enter the **setup** command.

Note If your platform does not support the factory default configuration, running the **setup** command may remove any existing configuration.

You must have an inside interface already configured to use the **setup** command. Before using the **setup** command, enter the **interface gigabitethernet** *slot*/*port* command, and then the **nameif inside** command. The *slot* for interfaces that are built in to the chassis is **0**. For example, enter **interface gigabitethernet 0/1.**

The ASA 5510 Adaptive Security Appliance has an Ethernet-type interface. When using the using the **setup** command, remember that the interface ID is dependent upon the platform. For example, on PIX 500 series, enter the **ethernet** *port*. On ASA, enter **interface gigabitethernet** *slot*/*port* command.

Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher is an improvement over running ASDM in a browser. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches faster, and caches previously-entered IP addresses and usernames.

To download the ASDM Launcher, perform the following steps:

Step 1 From a supported web browser on the security appliance network, enter the following URL:

https://*interface_ip_address/admin*

In transparent firewall mode, enter the management IP address.

Note Be sure to enter **https**, not **http**.

Step 2 Click **OK** or **Yes** to all prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**
- **Run the ASDM applet in a browser**

Step 3 Click **Download ASDM Launcher and Start ASDM**.

The installer downloads to your PC.

Step 4 Run the installer to install the ASDM Launcher.

Starting ASDM from the ASDM Launcher

The ASDM Launcher is for Windows only.

To start ASDM from the ASDM Launcher, perform the following steps:

Step 1 Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or start it from the **Start** menu.

Step 2 Enter the security appliance IP address or hostname, your username, and your password, and then click **OK**.

If there is a new version of ASDM on the security appliance, the ASDM Launcher automatically downloads it before starting ASDM.

Using ASDM in Demo Mode

ASDM Demo Mode is available as a separately installed application running under Windows. It makes use of the ASDM Launcher and pre-packaged configuration files to let you run ASDM without having a live device available. ASDM Demo Mode lets you:

- Demonstrate ASDM or security appliance features using the ASDM interface.
- Perform configuration and select monitoring tasks via ASDM as though you were interacting with a real device.

ASDM Demo Mode provides simulated monitoring data, including real-time system log messages. The data shown is randomly generated, but the experience is identical to what you would see when connecting to a real device.

ASDM Demo Mode has the following limitations:

- Changes made to the configuration will appear in the GUI but are not applied to the configuration file. That is, when you click the **Refresh** button, it will revert back to the original configuration. The changes are never saved to the configuration file.
- File/Disk operations are not supported.
- Monitoring and logging data are simulated. Historical monitoring data is not available.
- You can only log in as an admin user; you cannot log in as a monitor-only or read-only user.
- Demo Mode does not support the following features:
  - File menu:

    Reset Device to the Factory Default Configuration

    Save Running Configuration to Flash

    Save Running Configuration to TFTP Server

    Save Running Configuration to Standby Unit

    Save Internal Log Buffer to Flash

    Clear Internal Log Buffer
  - Tools menu:

    Command Line Interface

    Ping

Traceroute

File Management

Upgrade Software

Upload Assistant Guide

System Reload

- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Failover—Configuring a standby device

- These operations cause a reread of the configuration and therefore will revert the configuration back to the original settings.
  - Switching contexts
  - Making changes in the Interface panel
  - NAT panel changes
  - Clock panel changes

To run ASDM in Demo Mode, perform the following steps:

Step 1 If you have not yet installed the Demo Mode application, perform the following steps:

a. Download the ASDM Demo Mode installer 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.

The filename is asdm-demo-524.msi.

b. Double-click the installer to install the software.

Step 2 Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or start it from the **Start** menu.

Step 3 Check **Run in Demo Mode**.

Step 4 To set the platform, context and firewall modes, and ASDM Version, click **Demo** and make your selections from the Demo Mode area.

Step 5 To use new ASDM images as they come out, you can either download the latest installer, or you can download the normal ASDM images and install them for Demo Mode:

a. Download the image from the download page (see Step 1).

The filename is asdm-*version*.bin.

b. In the Demo Mode area, click **Install ASDM Image**.

A file browser appears. Find the ASDM image file in the browser.

Step 6 Click **OK** to launch ASDM Demo Mode.

You see a Demo Mode label in the title bar of the window.

Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

Step 1 From a supported web browser on the security appliance network, enter the following URL:

https://*interface_ip_address/admin*

In transparent firewall mode, enter the management IP address.

Note Be sure to enter **https**, not **http**.

Step 2 Click **OK** or **Yes** to all browser prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Install ASDM Launcher and Run ASDM (only with Windows)**
- **Run ASDM Applet**
- **Run Startup Wizard Applet**

Step 3 Click **the appropriate selection for your machine.**.

Step 4 Click **OK** or **Yes** to all Java prompts, including the name and password prompt. By default, leave the name and password blank.

Using the Startup Wizard

The Startup Wizard helps you easily configure a single mode security appliance or a context in multiple context mode.

To use the Startup Wizard to configure the basic setup of the security appliance, perform the following steps:

Step 1 Launch the wizard according to the steps for the correct security context mode.

- In single context mode, click **Wizards > Startup Wizard**.
- In multiple context mode, for each new context, perform the following steps:
  a. Create a new context using the **System > Configuration > Security Context** pane.
  b. Be sure to allocate interfaces to the context.
  c. When you apply the changes, ASDM prompts you to use the Startup Wizard.
  d. Click the **System/Contexts** icon on the toolbar, and choose the context name.
  e. Click **Wizards > Startup Wizard**.

Step 2 Click **Next** as you proceed through the Startup Wizard screens, filling in the appropriate information in each screen, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.

Step 3 Click **Finish** on the last pane to transmit the configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of the connection changes.

Step 4 Enter other configuration details on the **Configuration** panes.

Using the IPsec VPN Wizard

The IPsec VPN Wizard configures basic VPN access for LAN-to-LAN or remote client access. The VPN Wizard is available only for security appliances running in single context mode and routed (not transparent) firewall mode.

To use the VPN Wizard to configure VPN, perform the following steps:

Step 1 Click **Wizards > VPN Wizard**.

Step 2 Supply information on each wizard pane. Click **Next** to move through the VPN Wizard panes. You may use the default IPSec and IKE policies. Click **Help** for more information about each field.

Step 3 After you complete the VPN Wizard information, click **Finish** on the last pane to transmit the configuration to the security appliance.

Printing from ASDM

Note Printing is supported only for Microsoft Windows 2000 or XP in this release.

ASDM supports printing for the following features:

- The **Configuration > Interfaces** table
- All **Configuration > Security Policy** tables
- All **Configuration > NAT** tables
- The **Configuration > VPN > IPSec > IPSec Rules** table
- **Monitoring > Connection Graphs** and its related table

ASDM Limitations

This section describes ASDM limitations, and includes the following topics:

Unsupported Commands

ASDM does not support the complete command set of the CLI. For any CLI configuration that ASDM does not support, the commands remain unchanged in the configuration.

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**.

Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when you add them through the CLI, but that you cannot add or edit 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.

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used, except for use in VPN group policy screens.
alias	Use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.
established	Ignored
failover timeout	Ignored
ignore-ipsec-keyusage	Ignored; under the "crypto ca trustpoint <tp-name>" mode.
ignore-ssl-keyusage	Ignored; under the "crypto ca trustpoint <tp-name>" mode
ipv6, any IPv6 addresses	Ignored
pager	Ignored
pim accept-register route-map	Ignored. You can only configure the **list** option using ASDM.
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored

Unsupported Commands	ASDM Behavior

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	Ignoredin Ethernet interface mode.
sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	Ignored
system internal and all subcommands	Ignored
terminal	Ignored

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 in 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 command: **`crypto key generate rsa`**

   ASDM generates the default 1024-bit RSA key.
3. Enter the command again: **`crypto key generate rsa`**

   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
```

Caveats

The following sections describes the open and resolved caveats for Version 5.2(4).

- Open Caveats - Version 5.2(4), page 15
- Resolved Caveats - Version 5.2(4), page 16

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 5.2(4)

The following list shows caveats that are opened for Version 5.2(4):

Table 3 Open ASDM Caveats

	Software Version 5.2(4)	
ID Number	**Corrected**	**Caveat Title**
CSCse53604		ASDM is not detecting FTP inspection not enabled scenario.
CSCsf05395		Error in configuring aaa authentication include.
CSCsf18305		Wrong CLI generation in dynamic crypto map, IPSec rules panel.
CSCsi65804		CSC SSM failed to login through ASDM.
CSCsj55412		IPS Monitoring navigation is wrong.
CSCsj74335		ASDM: trustpoint fields become editable after clicking New.
CSCsj75290		Can't reconnect to SSM after executing IPS Password Reset using GUI.
CSCsj90833		PPPoE:When switch from Specify to Obtain address, ASDM sends the address.
CSCsj96262		Startup Wiz:When switch from static IP to PPPoE, sends ip addr also.

Table 3 Open ASDM Caveats (continued)

	Software Version 5.2(4)	
ID Number	**Corrected**	**Caveat Title**
CSCsk05752		ASDM does not detect changes on asa when filter rules clash.
CSCsm85594		ntp: add server without interface, then edit, shows first interface.
CSCso24981		ASDM is unable to contact ASA temporarily when opening Monitor page.
CSCso45620		HAS wizard cannot configure A/A failover with A/S failover configured.
CSCso52792		Privilege1 ASDM users can view ACLs.
CSCso58958		ASDM SNMP error in configuring SNMP listen port.

Resolved Caveats - Version 5.2(4)

The following list shows caveats that are resolved for Version 5.2(4):

Note The Resolved Caveats list does **NOT** include defects that were not known in Version 5.2(3).

Table 4 Resolved ASDM Caveats

	Software Version 5.2(4)	
ID Number	**Corrected**	**Caveat Title**
CSCeg54076		Failover enabled popup incorrect or misleading.
CSCsc63204		ASDM to honor New Zealand Daylight Savings time (NZDT).
CSCse43201		HTTP map advanced view inspection tab causes error.
CSCse74616		HAS Wizard, Load Balancing: Wrong error order.
CSCsg64625		ASA 5505 Startup Wizard PPPoE finish button enabled in error.
CSCsg68303		Boot system: ASDM allows more than 4 boot entries.
CSCsh39808		PFS group 2 added in ASDM VPN Wizard - no option to remove.
CSCsj40690		ASDM NAT-control Option Window Behavior.
CSCsj61309		Routing/Static: Editing metric value - one failure case.
CSCsj61586		Hit return in single line of Command Line Interface closes the window.
CSCsj68425		Confusing message when enabling HTTP replication.
CSCsj81132		Refresh function for "show wccp web hash" is not working.
CSCsj85297		Cannot set sla mon timeout to greater than 60000.
CSCsk08332		ASDM: Cannot sort on VPN statistics table using Linux.
CSCsk09308		Missing host/network concept in ASDM 5.2 and above.
CSCsk66888		Add support for "icmp unreachable rate-limit <rate> burst-size <size>".
CSCsk83257		ASDM doesn't report the user licenses in use.
CSCsk88808		SDM adds semicolon ";" to msie exception list end.

Table 4 Resolved ASDM Caveats (continued)

	Software Version 5.2(4)	
ID Number	**Corrected**	**Caveat Title**
CSCsl53550		Logging filters for specific event classes are wrong on the PIX.
CSCsl54594		ASDM 5.2(2): Unable to save Log buffer contents to file.
CSCsm53341		Enrollment: False FQDN warning shown (again).
CSCsm76473		Name entries in ASA not showing as Network Objects in ASDM.
CSCso33359		In the network object grp IP address column displays name.
CSCso40804		Exceed MSS from TCP-MAP default setting should be ALLOW.
CSCso45991		Changing address of network object removes it from the object group.
CSCso49954		Gives error "brs" when filtering for object-group.
CSCso53486		ASDM cannot delete failover group 1.

End-User License Agreement

For infromation 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 the ASDM online Help or the following documentation found on Cisco.com:

For additional information on ASDM or its platforms, see the ASDM online Help or the following documentation found on Cisco.com:

- *Cisco ASA 5500 Series Hardware Maintenance Guide*
- *Cisco ASA 5500 Series Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco PIX Security Appliance Release Notes*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Release Notes for Cisco Intrusion Prevention System 5.0*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.0*
- *Release Notes for Cisco Intrusion Prevention System 5.1*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*

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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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