Release Notes for Cisco ASDM Version 5.2(5)

May 2010

This document contains release information for Cisco ASDM Version 5.2(5) on the Cisco ASA 5500. It includes the following sections:

- New Features, page 1
- System Requirements, page 1
- Upgrading ASDM, page 3
- Getting Started with ASDM, page 4
- ASDM Limitations, page 9
- Open Caveats, page 12
- Resolved Caveats, page 13
- End-User License Agreement, page 13
- Related Documentation, page 13
- Obtaining Documentation and Submitting a Service Request, page 14

New Features

There were no new features in ASA 7.2(5)/ASDM 5.2(5)

System Requirements

This section includes the following topics:

- ASDM Client PC Operating System and Browser Requirements, page 2
- ASDM, SSM, and VPN Compatibility, page 2
- Supported Models, page 2

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

ASDM Client PC Operating System and Browser Requirements

Table 1 lists the supported and recommended PC operating systems and browsers for ASDM Version 5.2(5).

Table 1 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.

ASDM, SSM, and VPN Compatibility

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

Table 2 ASDM, SSM, and VPN Compatibility

Application	Description
ASDM	ASA 5500 Version 7.2 requires ASDM Version 5.2. For information about ASDM requirements for other releases, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software 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
SSM applications	For information about SSM application requirements, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

Supported Models

This software version supports the following models:

- ASA 5505
- ASA 5510
- ASA 5520

- ASA 5540
- ASA 5550

Note The Cisco PIX security appliance is not supported on ASDM 5.2(5)/ASA 7.2(5).

Upgrading ASDM

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

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 ASA image.

To upgrade ASDM, perform the following steps:

Step 1 Download the new ASDM image to your PC.

Optionally, you can download a new ASA 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**.

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 ASA image, download the new ASA image using the **Tools > Upgrade Software** tool with ASA selected.

If your adaptive 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. This section includes the following topics:

- Before You Begin, page 4
- Downloading the ASDM Launcher, page 5
- Starting ASDM from the ASDM Launcher, page 6
- Using ASDM in Demo Mode, page 6
- Starting ASDM from a Web Browser, page 7
- Using the Startup Wizard, page 8
- Using the IPsec VPN Wizard, page 9
- Printing from ASDM, page 9

Before You Begin

If you are using the adaptive security appliance for the first time, your adaptive security appliance might include a factory default configuration. You can connect to a default IP address with ASDM so that you can immediately start to configure the adaptive security appliance from ASDM. You can alternatively log in to the CLI from the console port and enter the **setup** command to establish ASDM connectivity. You must have an inside interface already configured to use the **setup** command.

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 5505, connect to Ethernet 0/1 through 0/7. For other models, connect to the Management 0/0 interface. To restore the factory default configuration, enter the **configure factory-default** command. The CLI can be entered through the serial console or through a Telnet or SSH session.

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

For more information about adding to an existing configuration to make it accessible for ASDM, see the *Cisco Security Appliance Command Line Configuration Guide*.

We also recommend that you install the recommended version of Java to your PC before you begin the installation.

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 adaptive 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 appears 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 adaptive 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 adaptive 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 do the following:

- Demonstrate ASDM or adaptive 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 **Refresh**, 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

- The following 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 pane
  - NAT pane changes
  - Clock pane 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

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 the **Run in Demo Mode** check box.

Step 4 To set the model, 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 adaptive 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.

Click one of the following options:

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

Step 3 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 adaptive security appliance or a context in multiple context mode.

To use the Startup Wizard to configure the basic setup of the adaptive 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, choose **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. Choose **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 adaptive security appliance. Reconnect to ASDM using the new IP address, if the IP address of the connection changes.

Step 4 Enter other configuration details in 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 adaptive 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 Choose **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 adaptive 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:

- Configuration > Interfaces table
- Configuration > Security Policy tables
- Configuration > NAT tables
- 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, page 10
- Interactive User Commands Not Supported in ASDM CLI Tool, page 11

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 mode.
ignore-ssl-keyusage	Ignored; under the crypto ca trustpoint 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	Ignored in 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, choose **Command Line Interface**.
2. Enter the following 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

Open Caveats

Table 3 lists the open caveats for Version 5.2(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 3 Open Caveats in Version 5.2(5)

Caveat ID	Description
CSCse23663	Status window and command preview window pop up at same time on Linux
CSCse53604	ASDM is not detecting FTP inspection not enabled scenario
CSCse54801	ASDM hardcodes some colors instead of using system defaults
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	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 addr
CSCsj96262	Startup Wiz:When switch from static IP to PPPoE, sends ip addr also
CSCso45620	HAS wizard cannot configure A/A failover with A/S failover configured
CSCso58958	ASDM SNMP error in configuring SNMP listen port
CSCso60526	Page not found error on searching for inspect maps in ASDM Assistant

Resolved Caveats

Table 4 lists the resolved caveats for Version 5.2(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 4 Resolved Caveats in Version 5.2(5)

Caveat ID	Description
CSCsf19215	ASDM hard timeout for device I/O causes disconnect with large ACLs
CSCsk42250	ASDM does not support 1000 mbit/s ports on ASA5510
CSCsk90235	ASDM shows subinterfaces without IP address and down/down
CSCsm85594	NTP: Add server without interface, then edit, shows first interface
CSCsm95257	ASDM: ACL with trailing remark causes ASDM to add bogus remarks to ACL
CSCsq07318	ASDM - Modifying NAT rules may clear all xlates for the interface
CSCsq10143	Edit Static NAT Rule dialog is overlapping other text.
CSCsq34600	Unable to Manage AIP-SSM Running 6.1(1) from ASDM 5.2
CSCsq71857	ASDM will may freeze for 3 to 4 minutes after an ACL is edited
CSCsq85965	ASDM "where used" on network objects shows duplicated results
CSCsq94285	ASDM not defining inline service groups properly
CSCsv12681	Error while loading ASDM: "Unconnected sockets not implemented"
CSCsv16675	"Error in getting/parsing the monitoring data." - Empty route table
CSCsv66700	ASDM: "only originate-only" error when configuring multi VPN peers
CSCsy20611	ASDM does not parse access-list line remarks correctly
CSCsz12875	HA Wizard throws null pointer exception isValid
CSCtb37678	ASDM for ASA should not use "nfs" keywork for ACL entries
CSCtf61705	Certificate expired in ASDM 5.2(4)

End-User License Agreement

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

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

Related Documentation

For additional information on the Cisco ASA 5500 series adaptive security appliances, see the following URL on Cisco.com:

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.