Cisco ASDM Release Notes Version 5.0(9)

August 2009

This document contains release information for Cisco ASDM Version 5.0(9) on Cisco ASA 5500 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 PIX 500 series 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 Cisco ASA 5500 series adaptive security appliance software Version 7.0. Its secure, web-based design enables anytime, anywhere access to security appliances.

Note This release only supports the following Cisco ASA 5500 series adaptive security appliance platforms: 5510, 5520, 5540 - not 5505, 5550, or 5580.

New Features

No new features have been implemented since ASDM version 5.0(8).

ASDM Client PC Operating System and Browser Requirements

Table 1 lists the supported and recommended PC operating systems and browsers for ASDM Version 5.0(9).

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 Desktop 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 the Java website.

Supported Platforms and Feature Licenses

For information on supported platforms and feature licenses, see:

Cisco ASA 5500 Series Adaptive Security Appliance

http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html

Cisco PIX 500 Series Security Appliance

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_release_notes_list.html

Upgrading ASDM and ASA

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

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 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 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.

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. To restore the default configuration, enter the **configure factory-default** command at the security appliance CLI.

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 **interface ethernet** *slot*/*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 ASDM 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.

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**

Step 3 Click **Run ASDM**.

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**.
- 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.**

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
established	Ignored
failover timeout	Ignored
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

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`

sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	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
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

Miscellaneous Limitations

- Dynamic Access Policies, located in **Configuration > Remote Access VPN > Network (Client) Access and Configuration > Remote Access VPN > Clientless SSL VPN Access**, have limited support because it depends on Secure Desktop Manager which is not supported.

Caveats

The following sections describes the open caveats for Version 5.0(9).

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 5.0(9)

The following list shows caveats that are opened for Version 5.0(9):

Table 2 Open ASDM Caveats

	Software Version 5.0(9)	
ID Number	**Corrected**	**Caveat Title**
CSCeg14905		Applying service group change causes no ACL CLI to be generated.
CSCeh06459		ASDM cannot create appropriate ACL for QoS on outbound interface.
CSCeh20409		Startup Wizard allows not naming any interface.

Table 2 Open ASDM Caveats (continued)

	Software Version 5.0(9)	
ID Number	Corrected	Caveat Title
CSCeh24529		ASDM sometimes allows more than 2 traffic match criteria.
CSCeh53158		Wrong cmds sent when objgp w/ PNAT is edited to add net-obj with NAT.
CSCsb61151		Disable/Enable of class in a service policy sends wrong commands.
CSCsc11004		CLI warning is not anticipated when creating a tunnel group.
CSCsc11887		Refresh icon does not work properly sometimes.
CSCsc23386		Monitor > Routing > OSPF neighbors for P2P column display is shifted.
CSCsc99216		Unchecking default inspection traffic should clear rule actions.
CSCsd71927		Error msg given for correct behavior - Upload button stays enabled.
CSCsd89536		PAT and Static NAT configured you cannot create ACE via ASDM.
CSCse02978		Filter rules : move up and move down not working.
CSCsf12435		Editing URL Server config with existing URL-Block adds more config.
CSCsq38917		Java Null Pointer Exception - viewing detail of special keypair.
CSCsq41679		ASDM will show some static ARP entries as dynamic.
CSCsq41749		Monitoring tab always show ARP entry as noproxy ARP.
CSCsq43447		In Linux, Show All freezes Live Log after Filter by Text.
CSCsq43553		Clock: summertime settings configs sent are wrong.
CSCsq57808		"http/ASDM" option should not be available in AAA Access, Accounting tab.

Resolved Caveats - Version 5.0(9)

The following list shows caveats that are resolved for Version 5.0(9):

Table 3 Resolved ASDM Caveats

	Software Version 5.0(9)	
ID Number	Corrected	Caveat Title
CSCsj37287		Clock: Timezones are not sent correctly for changes.
CSCsv12681		Error while loading ASDM: "Unconnected sockets not implemented".
CSCtb04872		ASDM 5.0.x fails if running Java 6 Update 12 or above.

End-User License Agreement

For information on the end-user license agreement, go to:
https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Related Documentation

For additional information on ASDM or its platforms, see 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 5.1*
- *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.