



# Cisco ASDM Release Notes Version 5.0(7)

---

## July 2007

This document contains release information for Cisco ASDM Version 5.0(7), which runs with Cisco PIX 500 series (except for Cisco PIX 501, 506/506E, and 520, which are not supported) and Cisco ASA 5500 series adaptive security appliance software Version 7.0. This document includes the following sections:

- [Introduction, page 1](#)
- [Important Notes, page 2](#)
- [New Device Manager Features, page 2](#)
- [System Requirements, page 2](#)
- [Upgrading ASDM, page 4](#)
- [Getting Started with ASDM, page 6](#)
- [Unsupported Commands, page 12](#)
- [Caveats, page 14](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 17](#)

## Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco PIX 500 series (except for Cisco PIX 501, 506/506E, and 520, which are not supported) and ASA 5500 series adaptive security appliances through an intuitive, easy-to-use 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 software Version 7.0. Its secure design enables anytime, anywhere access to security appliances.



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

## Supported Platforms

- Windows Vista, Windows XP, Windows 2000 (Service Pack 4 or higher), Windows 2003 Server (English or Japanese version)
  - Firefox 1.5 or 2.0 -or- Internet Explorer 6.0 or 7.0
  - Java SE 1.4.2, 5.0, or 6
- Red Hat Desktop, Red Hat Enterprise Linux WS version 4
  - Firefox 1.5 or 2.0
  - Java SE 1.4.2, 5.0, or 6



---

**Note** Solaris and Macintosh are not supported in Version 5.0(7).

---

## Important Notes

The security appliance does not support both an ASDM session and a WebVPN session on the same interface. To use ASDM and WebVPN at the same time, configure them on different interfaces.

## New Device Manager Features

Security appliance software Version 7.0 includes significant enhancements to firewall and inspection capabilities, VPN services, network integration, high availability, and management/monitoring features. These software features are supported in ASDM 5.0.

This document contains release information about ASDM only. See the [Cisco ASA 5500 Series Release Notes](#) or the [Cisco PIX Security Appliance Release Notes](#) for a list of platform features supported in the CLI software.

## DNS Guard

This command is provided for backward compatibility. When configured, DNS guard is enabled on all interfaces by default, even if DNS inspection is not configured. DNS inspection configuration on individual interface overrides the default DNS guard behavior. The DNS Guard field is in the Client DNS Panel.

## System Requirements

This section includes the following topics:

- [Hardware Requirements, page 3](#)
- [Client PC Operating System and Browser Requirements, page 3](#)

## Hardware Requirements

ASDM Version 5.0(7) software runs on the following platforms:

- Cisco ASA 5510 adaptive security appliance
- Cisco ASA 5520 adaptive security appliance
- Cisco ASA 5540 adaptive security appliance
- Cisco PIX 515/515E security appliance
- Cisco PIX 525 security appliance
- Cisco PIX 535 security appliance
- Cisco ASA Advanced Inspection and Prevention Security Services Module (supported on the ASA 5500 series only)

**Note**

---

ASDM 5.0 is not supported on PIX 501, PIX 506/506E, or PIX 520 hardware.

---

For more information on minimum hardware requirements, see:

<http://www.cisco.com/en/US/docs/security/asa/asa71/asdm51/webhelp/sysreq.html>

Certain features, such as load balancing and QoS, require particular hardware platforms. Other features require licensing.

For more information on feature support for each platform license, see:

[http://www.cisco.com/en/US/docs/security/asa/asa71/asdm51/webhelp/gen\\_info\\_licenses.html](http://www.cisco.com/en/US/docs/security/asa/asa71/asdm51/webhelp/gen_info_licenses.html)

## Client PC Operating System and Browser Requirements

**Table 1** lists the supported and recommended PC operating systems and browsers for Version 5.0(7). While ASDM might work on other browsers and browser versions, these are the only officially supported browsers. Note that unlike earlier PDM releases, you must have the Java Plug-in or J2SE installed. The native JVM on Windows is no longer supported and does not work.

**Table 1**      **Operating System, Browser, and Java Requirements**

	<b>Operating System</b>	<b>Browser with Java Applet</b>	<b>ASDM Launcher</b>	<b>Other Requirements</b>
Windows <sup>1</sup>	Windows 2000 (Service Pack 4) or Windows XP operating system	Internet Explorer 6.0 with Java Plug-in <sup>2</sup> 1.4.2 or 5.0 (1.5)  <b>Note</b> <b>HTTP 1.1</b> —Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections.  Netscape 7.1/7.2 with Java Plug-in <sup>2</sup> 1.4.2 or 5.0 (1.5)	J2SE 1.4.2 or 5.0 (1.5)	<b>SSL Encryption Settings</b> —All available encryption options are enabled for SSL in the browser preferences.
Linux	Red Hat Linux 9.0 or Red Hat Linux WS, Version 3 running GNOME or KDE	Mozilla 1.7.3 with Java Plug-in <sup>2</sup> 1.4.2	Not available.	

1. ASDM is not supported on Windows 3.1, 95, 98, ME, or NT 4.
2. Download the latest Java Plug-in or J2SE from <http://java.sun.com/>.

## Upgrading ASDM

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

<http://www.cisco.com/public/sw-center/index.shtml>

This section includes the following topics:

- [Upgrading from PDM, page 4](#)
- [Upgrading to a New ASDM Release, page 5](#)

## Upgrading from PDM

Before you upgrade the device manager, upgrade the platform software to Version 7.0. See the [Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0](#) for more information.

To upgrade to ASDM, perform the following steps:

- 
- Step 1**    Copy the ASDM binary file to a TFTP or FTP server on your network.
  - Step 2**    Log in to the security appliance and enter privileged EXEC mode:  
  

```
hostname> enable
password:
hostname#
```
  - Step 3**    Ensure that you have connectivity from the security appliance to the TFTP/FTP server.
  - Step 4**    Delete the old version of PDM by entering the following command:  
  

```
hostname# delete flash:/pdm
```

**Step 5** Copy the ASDM binary to the security appliance using the appropriate command:

- TFTP

```
hostname# copy tftp://server_ip/pathtofile flash:/asdm_filename
```

- FTP

```
hostname# copy ftp://server_ip/pathtofile flash:/asdm_filename
```

For more information on the **copy** command and its options, see the [Cisco Security Appliance Command Reference](#).

**Step 6** Identify the path to the ASDM image by entering the following command:

```
hostname# configure terminal
hostname(config)# asdm image flash:/asdm_filename
```

This command lets you identify the image to load if you have multiple ASDM images in Flash memory.



**Note**

After you enter this command, the ASA security appliance changes the path to **asdm image disk0**.

**Step 7** To enable the HTTPS server (if it is not already enabled), enter the following command:

```
hostname(config)# http server enable
```

**Step 8** To identify the IP addresses that are allowed to access ASDM, enter the following command:

```
hostname(config)# http ip_address mask interface
```

Enter **0** for the *ip\_address* and *mask* to allow all IP addresses.

**Step 9** Save your configuration by entering the following command:

```
hostname(config)# write memory
```

## Deleting Your Old Cache

In early beta releases of ASDM and in previous releases of PDM (Versions 4.1 and earlier), the device manager stored its cache in <userdir>\pdmcache. For example, D:\Documents and Settings\jones\pdmcache.

Now, the cache directory for ASDM is in <user dir>\.asdm\cache.

The File > Clear ASDM Cache option in ASDM clears this new cache directory. It does not clear the old one. To free up space on your system, if you are no longer using your older versions of PDM or ASDM, delete the contents of the \pdmcache directory manually.

## Upgrading to a New ASDM Release

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.
- Step 2** Launch ASDM.
- Step 3** From the Tools menu, click **Upload Image from Local PC**.
- Step 4** With the ASDM Image option button selected, click the **Browse Local** button 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 the **Browse Flash** button.
- 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, you see the following message:  
 “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 in the **Configuration > Features > Device Administration > Boot System/Configuration** pane.
- Step 8** To run the new ASDM image, you must quit out of ASDM and reconnect.
- Step 9** Download the new platform image using the **Tools > Upload Image from Local PC** tool.  
 To reload the new image, reload the security appliance using the **Tools > System Reload** tool.
- 

## 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, page 7](#)
- [Downloading the ASDM Launcher, page 7](#)
- [Starting ASDM from the ASDM Launcher, page 8](#)
- [Starting ASDM from a Web Browser, page 8](#)
- [Using the Startup Wizard, page 8](#)
- [Using the VPN Wizard, page 9](#)
- [Configuring Stateful Failover, page 9](#)
- [Printing from ASDM, page 12](#)

## 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. 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** command at the security appliance CLI.

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. The **setup** command prompts you for a minimal configuration to connect to the security appliance using ASDM.



### Note

You must have an inside interface already configured to use the **setup** command. The Cisco PIX security appliance default configuration includes an inside interface, but the Cisco ASA adaptive security appliance default configuration does not. 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 Cisco PIX 500 series and the ASA 5510 adaptive security appliance have an Ethernet-type interface.

## Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher is an improvement over running ASDM in a Java Applet. 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
```

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 as a Java Applet**

**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**

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:

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

- Step 3** Click **Run ASDM as a Java Applet**.

- 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 your security appliance:

- 
- Step 1** Launch the wizard according to the steps for your security context mode.
- In single context mode, perform the following steps:
    - a. Click **Configuration > Wizards > Startup**.
    - b. Click **Launch Startup Wizard**.
  - In multiple context mode, for each new context, perform the following steps:
    - a. Create a new context using the **System > Configuration > Features > 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 **Context** icon on the upper header bar and select the context name from the Context menu on the lower header bar.
    - e. Click **Context > Configuration > Wizards > Startup**.
    - f. Click **Launch 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 your configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of your connection changes.
- Step 4** You can now enter other configuration details on the **Configuration > Features** panes.
- 

## Using the VPN Wizard

The 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:

- 
- Step 1** Click **Configuration > Wizards > VPN**.
- Step 2** Click **Launch VPN Wizard**.
- Step 3** 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 the **Help** button for more information on each field.
- Step 4** After you complete the VPN Wizard information, click **Finish** on the last pane to transmit your configuration to the security appliance.
- 

## Configuring Stateful Failover

This section describes how to implement Stateful Failover on security appliances connected via a LAN. If you are connecting two security appliances for failover, you must connect them via a LAN. If you are connecting two security appliances, you can connect them using either a LAN or a serial cable.



**Tip** If your security appliances are located near each other, you might prefer connecting them with a serial cable to connecting them via the LAN. Although the serial cable is slower than a LAN connection, using a cable prevents having to use an interface or having the LAN and Stateful Failover share an interface, which could affect performance. Also, using a cable enables the detection of power failure on the peer device.

As specified in the *Cisco Security Appliance Command Line Configuration Guide*, both devices must have appropriate licenses and have the same hardware configuration.

Before you begin, decide on active and standby IP addresses for the interfaces ASDM connects through on the primary and secondary devices. These IP addresses must be assigned to device interfaces with HTTPS access.

To configure LAN Stateful Failover on your security appliance, perform the following steps:

- 
- Step 1** Configure the secondary device for HTTPS IP connectivity. See the [Before You Begin, page 7](#), and use a different IP address on the same network as the primary device.
- Step 2** Connect the pair of devices together and to their networks in their Stateful Failover LAN cable configuration.
- Step 3** Start ASDM from the primary device through a supported web browser. (See the section [Downloading the ASDM Launcher, page 7](#).)
- Step 4** Perform one of the following steps, depending on your context mode:
- If your device is in multiple context mode, click **Context**. Choose the **admin** context from the **Context** drop-down menu, and click **Configuration > Features > Properties > Failover**.
  - If your device is in single mode, click **Configuration > Features > Properties > Failover**. Click the **Interfaces** tab.
- Step 5** Perform one of the following steps, depending on your firewall mode:
- If your device is in routed mode, configure standby addresses for all routed mode interfaces.
  - If your device is in transparent mode, configure a standby management IP address.
- 
- Note** Interfaces used for failover connectivity should not have names (in single mode) or be allocated to security contexts (in multiple security context mode). In multiple context mode, other security contexts may also have standby IP addresses configured.
- 
- Step 6** Perform one of the following steps, depending on your security context mode:
- If your device is in multiple security context mode: click **System > Configuration > Features > Failover**.
  - If your device is in single mode: click **Configuration > Features > Properties > Failover**.
- Step 7** On the **Setup** tab of the **Failover** pane under **LAN Failover**, select the interface that is cabled for LAN Stateful Failover.
- Step 8** Configure the remaining **LAN Failover** fields.
- Step 9** (Optional) Provide information for other fields in all of the failover tabs. If you are configuring Active/Active failover, you must configure failover groups in multiple security context mode. If more than one failover pair of devices coexist on a LAN in Active/Active Stateful Failover, provide failover-group MAC addresses for any interfaces on shared LAN networks.

- Step 10** On the **Setup** tab, check the **Enable Failover** check box. If you are using the PIX 500 series security appliance, check the **Enable LAN rather than serial cable failover** check box.
- Step 11** Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.
- Step 12** Enter the IP address of the secondary device, which you configured as the standby IP address of the ASDM interface. Wait about 60 seconds. The standby peer still could become temporarily inaccessible.
- Step 13** Click **OK**. Wait for configuration to be synchronized to the standby device over the failover LAN connection.

The secondary device should now enter standby failover state using the standby IP addresses. Any further configuration of the active device or an active context is replicated to the standby device or the corresponding standby context.

## Securing the Failover Key

To prevent the failover key from being replicated to the peer unit in clear text for an existing failover configuration, disable failover on the active unit (or in the system execution space on the unit that has failover group 1 in the active state), enter the failover key on both units, and then reenabling failover. When Stateful Failover is reenabled, the failover communication is encrypted with the key.

To secure the failover key, follow this procedure on the active device:

- Step 1** Perform one of the following steps, depending on your security context mode:
- If your device is in single mode, navigate to **Configuration > Features > Properties > Failover > Setup**.
  - If your device is in multiple mode, navigate to **System > Configuration > Features > Failover > Setup**.
- Step 2** Turn off failover. (The standby should switch to pseudo-standby mode.)
- Uncheck the **Enable failover** check box.
  - Click **Apply**. (Click **OK** if CLI preview is enabled.)
- Step 3** Enter the failover key in the **Shared Key** box.
- Step 4** Reenable failover.
- Check the **Enable failover** check box.
  - Click **Apply**. (Click **OK** if CLI preview is enabled.) A dialog box about configuring the peer appears.
- Step 5** Enter the IP address of the peer. Wait about 60 seconds. Even though the standby peer does not have the shared failover key, the standby peer still could become inaccessible.
- Step 6** Click **OK**. (Click **OK** if CLI preview is enabled.) Wait for configuration to be synchronized to the standby device over the encrypted failover LAN connection.

## Printing from ASDM



### Note

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

If you want to print from within ASDM, start ASDM in application mode. Printing is not supported in applet mode in this release.

ASDM supports printing for the following features:

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

## Unsupported Commands

ASDM does not support the complete command set of the CLI. In most cases, ASDM ignores unsupported commands, and they can remain in your configuration. In the case of the **alias** command, ASDM enters into Monitor-only mode until you remove the command from your configuration.

See the following sections for more information:

- [Effects of Unsupported Commands, page 12](#)
- [Ignored and View-Only Commands, page 13](#)
- [Other CLI Limitations, page 14](#)

## 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, see **Options > 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 Line Configuration Guide](#) 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, see Configuration > Device Administration > User Accounts and Configuration > Device Administration > AAA Access.

## Ignored and View-Only Commands

Table 2 lists commands that ASDM supports in the configuration when added by 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 it is view-only, then the command appears in the GUI, but you cannot edit it.

**Table 2** *Unsupported and View-Only Commands*

Unsupported Commands	ASDM Behavior
<b>access-list</b>	Ignored if not used, except for use in VPN group policy screens.
<b>asr-group</b>	Ignored
<b>capture</b>	Ignored
<b>established</b>	Ignored
<b>failover timeout</b>	Ignored
<b>ipv6</b> , any IPv6 addresses	Ignored
<b>logging</b> (in system in multiple context mode)	Ignored
<b>object-group icmp-type</b>	View-only
<b>object-group network</b>	Nested group is view-only
<b>object-group protocol</b>	View-only
<b>object-group service</b>	Nested group cannot be added
<b>pager</b>	Ignored
<b>pim accept-register route-map</b>	Ignored. Only the <b>list</b> option can be configured using ASDM.
<b>prefix-list</b>	Ignored if not used in an OSPF area
<b>route-map</b>	Ignored
<b>service-policy global</b>	Ignored if it uses a <b>match access-list</b> class. For example:  <pre>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</pre>
<b>service resetinbound interface &lt;intf&gt;</b>	Ignored
<b>sysopt nodnsalias</b>	Ignored

**Table 2**      **Unsupported and View-Only Commands (continued)**

Unsupported Commands	ASDM Behavior
<b>sysopt uauth allow-http-cache</b>	Ignored
<b>terminal</b>	Ignored
<b>virtual</b>	Ignored
<b>icmp unreachable</b>	Ignored in ASDM in configure mode

## Other CLI Limitations

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
```

The ASDM CLI tool does not support interactive user commands. ASDM provides a CLI tool (click **Tools > Command Line Interface**) that lets you enter certain CLI commands from ASDM. The ASDM CLI tool does not support interactive user commands. You can configure most commands that require user interaction by means of the ASDM panes. 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, if you enter the **crypto key generate rsa** command, ASDM displays the following prompt and 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>
```

For commands that have a **noconfirm** option, use the **noconfirm** option when entering the CLI command. For example, enter the **crypto key generate rsa noconfirm** command.

- ASDM does not support the one-time password (OTP) authentication mechanism.

## Caveats

The following sections describe the caveats for Version 5.0(7).

For your convenience in locating caveats in Cisco’s Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

**Note**

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

[http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)

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(7)

Table 3 lists the open caveats for Version 5.0(7).

**Table 3**      **Open Caveats- Version 5.0(7)**

ID Number	Caveat Title
CSCeg14905	Applying service group change causes no ACL CLI to be generated
CSCeg69476	ASDM can not take any input from keyboard from SunOS 5.8 / Mozilla
CSCeh06459	ASDM can not create appropriate ACL for QoS on outbound interface
CSCeh20409	Startup Wizard allows not naming any interface
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
CSCsb92243	ASDM IPsec Rules display incorrectly when static policy NAT is used
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
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.
CSCsf14129	ASDM failover stateful link takes LAN link setting as default
CSCsj36806	ASDM 5.0 does not allow spaces in group-policy names
CSCsj37287	Clock: Timezones are not sent correctly for changes

## Resolved Caveats - Version 5.0(7)

Table 4 lists the resolved caveats for Version 5.0(7).

**Table 4**      **Resolved Caveats - Version 5.0(7)**

ID Number	Caveat Title
CSCeh39437	Non-English characters do not display properly in some screens
CSCsc60062	ASDM hangs and loops at 52% when processing ACLs with object-groups.
CSCsd37914	ASDM hangs at 47% with an ICMP port group configured in access-list
CSCse93262	ASDM - Indexation issues with ACL remarks
CSCsf33083	Adding an ACL is deleting the route.
CSCsg40549	Access rule is incomplete for network groups
CSCsg78595	Need to check certs presented by devices and drop conn if cert changes
CSCsg80786	ASDM duplicating object groups by appending 1 to the name
CSCsg98384	PDM sees some ACL rules as null when static is configured
CSCsh06083	ASDM Hangs at 47% loading config with DHCPD options in configuration
CSCsh07196	Reference meta groups are displayed in ASDM (but are not in PDM)
CSCsh17341	ASDM: ACL destination IP does not match CLI config
CSCsh67187	ASDM hangs at 47% for contexts in active/active failover configuration
CSCsi05228	ASDM Monitor mode displays failover interface in Interface Status
CSCsi25571	PDM: Access Policy shows as null
CSCsi94874	ASDM going in loop while loading configuration
CSCsj27834	Support dns-guard
CSCsj35609	ASDM freezes on navigating back after viewing Device administration
CSCsj36678	need no warning message for supported browser

## 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 Installation 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 Guide](#)

- *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*

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

© 2007 Cisco Systems, Inc.  
All rights reserved.