



Cisco ASDM Release Notes Version 5.0(6)

August 2006

This document contains release information for Cisco ASDM Version 5.0(6), 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 3](#)
- [Upgrading ASDM, page 5](#)
- [Getting Started with ASDM, page 7](#)
- [Unsupported Commands, page 13](#)
- [Caveats, page 15](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation, page 17](#)
- [Documentation Feedback, page 18](#)
- [Cisco Product Security Overview, page 18](#)
- [Obtaining Additional Publications and Information, page 21](#)

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.



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

© 2006 Cisco Systems, Inc. All rights reserved.

Important Notes

- In ASA Version 7.0(5), the existing **service resetinbound** command was enhanced to take an additional interface option. There is no support for this in ASDM Version 5.0(5) or 5.0(6).
- 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.

Table 1 highlights the new device manager features in Version 5.0.

Table 1 **New ASDM Features, Version 5.0**

Feature	Benefits
Dynamic Dashboard (ASDM Home Page)	<ul style="list-style-type: none"> • Displays detailed device and licensing information for quick identification of system and resources available. • Displays real-time system and traffic profiling.
Real-time Log Viewer	<ul style="list-style-type: none"> • Displays real-time system log messages. • Advanced filtering capabilities make it easy to focus on key events.
Improved Java Web-Based Architecture	<ul style="list-style-type: none"> • Accelerates the loading of ASDM with optimized applet caching capability. • Provides anytime, anywhere access to all management and monitoring features.
Downloadable ASDM Launcher (on Microsoft Windows 2000 or XP operating systems only)	<ul style="list-style-type: none"> • Lets you download and run ASDM locally on your PC. • Multiple instances of ASDM Launcher provide administrative access to multiple security appliances simultaneously, from the same management workstation. • Automatically updates the software based on the installed version on the appliance, enabling consistent security management throughout the network. • Avoids double authentication and certificate dialog boxes. • Caches previously-entered IP addresses and usernames.
Comprehensive Cisco PIX and ASA Security Appliances Software Version 7.0 Feature Support	Provides support for more than 50 new features introduced in Cisco PIX 500 series and ASA 5500 adaptive security appliance software Version 7.0, such as transparent firewall, PIM sparse mode, QoS, and Active/Active failover, in addition to existing features such as OSPF and VLANs.

Table 1 **New ASDM Features, Version 5.0 (continued)**

Feature	Benefits
Advanced Application Protocol Inspection Configuration	Delivers robust management and monitoring capabilities for 30 specialized inspection engines that provide rich application control security services for numerous protocols, including HTTP, FTP, Extended Simple Mail Transfer Protocol (ESMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), ICMP, SQL*Net, Network File System (NFS), H.323 Versions 1-4, SIP, Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), GTP, Internet Locator Service (ILS), and SunRPC.
World-class Management of Virtualized Security Services	<ul style="list-style-type: none"> • Enables the rapid creation of multiple security contexts (virtual firewalls) within a single security appliance, with each context having its own set of security policies, logical interfaces, and administrative domain. • Lets you conveniently consolidate multiple firewalls into a single physical appliance or failover pair while retaining the ability to manage each of these virtual instances separately. • Allows service providers to deliver resilient multi-tenant firewall services with a pair of redundant appliances.
Robust Security Features	<ul style="list-style-type: none"> • Provides high-grade encryption through Secure Sockets Layer (SSL) protocol support in addition to support for DES and 3DES. • Provides 16 granular levels of user authorization.
Multiple Language Operating System Support	Supports both the English and Japanese versions of the Microsoft Windows operating systems listed in the next section, System Requirements .

System Requirements

This section includes the following topics:

- [Hardware Requirements, page 3](#)
- [Client PC Operating System and Browser Requirements, page 4](#)

Hardware Requirements

ASDM Version 5.0(6) 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/asa70/asdm50/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/asa70/asdm50/webhelp/gen_info_licenses.html.

Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for Version 5.0(6). 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 2 Operating System, Browser, and Java Requirements

	Operating System	Browser with Java Applet	ASDM Launcher	Other Requirements
Windows ¹	Windows 2000 (Service Pack 4) or Windows XP operating system	Internet Explorer 6.0 with Java Plug-in ² 1.4.2 or 5.0 (1.5) Note HTTP 1.1 —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 ² 1.4.2 or 5.0 (1.5)	J2SE 1.4.2 or 5.0 (1.5)	SSL Encryption Settings —All available encryption options are enabled for SSL in the browser preferences.
Sun Solaris	Sun Solaris 8 or 9 running CDE window manager	Mozilla 1.7.3 with Java Plug-in ² 1.4.2 or 5.0 (1.5)	Not available.	
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 ² 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 5](#)
- [Upgrading to a New ASDM Release, page 6](#)

Upgrading from PDM

Before you upgrade the device manager, upgrade the platform software to Version 7.0. See [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 8](#)
- [Starting ASDM from the ASDM Launcher, page 8](#)
- [Starting ASDM from a Web Browser, page 9](#)
- [Using the Startup Wizard, page 9](#)
- [Using the VPN Wizard, page 10](#)
- [Configuring Stateful Failover, page 10](#)
- [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 adaptive 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 8](#).)
- 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:
- a. If your device is in single mode, navigate to **Configuration > Features > Properties > Failover > Setup**.
 - b. 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.)
- a. Uncheck the **Enable failover** check box.
 - b. Click **Apply**. (Click **OK** if CLI preview is enabled.)
- Step 3** Enter the failover key in the **Shared Key** box.
- Step 4** Reenable failover.
- a. Check the **Enable failover** check box.
 - b. 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 13](#)
- [Ignored and View-Only Commands, page 13](#)
- [ASDM Limitations, page 14](#)
- [ASDM 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 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, see Configuration > Device Administration > User Accounts and Configuration > Device Administration > AAA Access.

Ignored and View-Only Commands

[Table 3](#) 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 3 *Unsupported and View-Only Commands*

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used, except for use in VPN group policy screens.
asr-group	Ignored
capture	Ignored
established	Ignored
failover timeout	Ignored
ipv6 , any IPv6 addresses	Ignored
logging (in system in multiple context mode)	Ignored
object-group icmp-type	View-only
object-group network	Nested group is view-only
object-group protocol	View-only
object-group service	Nested group cannot be added
pager	Ignored
pim accept-register route-map	Ignored. Only the list option can be configured 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: <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>
sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	Ignored
terminal	Ignored
virtual	Ignored

ASDM Limitations

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

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 the 5.0(6) release.

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/cgi-bin/Support/Bugtool/launch_bugtool.pl

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

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

Open Caveats - Release 5.0(6)

Table 4 *Open Caveats- Release 5.0(6)*

ID Number	Caveat Title
CSCeg14905	Applying service group change causes no ACL CLI to be generated.
CSCeg69476	ASDM can take any keyboard input from SunOS 5.8/Mozilla.
CSCeh06459	ASDM cannot create appropriate ACL for QoS on outbound interface.
CSCeh20409	Startup Wizard allows not naming any interface.
CSCeh24529	ASDM sometimes allows more than two traffic match criteria.
CSCeh39437	Non-English characters do not display properly in some screens.
CSCeh53158	Wrong cmds sent when objgp with PNAT is edited to add net-obj with NAT.
CSCsb61151	Disable/Enable of class in a service policy sends wrong commands.
CSCsb92243	PDM IPsec rules display incorrectly when static policy NAT is used.
CSCsc11004	CLI warning is not anticipated when creating a tunnel group.
CSCsc23386	Monitor > Routing > OSPF neighbors for P2P column display is shifted.
CSCsc60062	ASDM hangs and loops at 52% when processing ACLs with object-groups.
CSCsc99216	Unchecking default inspection traffic should clear rule actions.
CSCsd37914	ASDM hangs at 47% with an ICMP port group configured in access-list.
CSCsd89536	When PAT and static NAT configured, you cannot create ACE via ASDM.
CSCse02978	Filter rules: move up and move down are not working.
CSCse93262	ASDM - Indexing issues with ACL remarks.

Resolved Caveats - Release 5.0(6)

Table 5 *Resolved Caveats - Release 5.0(6)*

ID Number	Caveat Title
CSCse68161	ASDM will not show VPN statistics for tunnel groups with spaces in name.
CSCse68174	ASDM cannot set group lock for tunnel group with spaces in name.

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*
- *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

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security

Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. To register as a Cisco.com user, go to this URL:

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

Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



Note

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search

options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Tip**

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the magazine for Cisco networking professionals. Each quarter, *Packet* delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *Packet* magazine at this URL:

<http://www.cisco.com/packet>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

CCVP, the Cisco logo, and Welcome to the Human Network 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, 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, Networkers, Networking Academy, Network Registrar, 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. (0711R)