



Cisco ASDM Release Notes Version 5.1(2)

March 2006

This document contains release information for Cisco ASDM Version 5.1(2), which runs with Cisco PIX 500 series and Cisco ASA 5500 series adaptive security appliance software Version 7.1(2). This document includes the following sections:

- [Introduction, page 1](#)
- [Important Notes, page 2](#)
- [System Requirements, page 2](#)
- [Platform Feature Licenses, page 3](#)
- [Upgrading ASDM, page 7](#)
- [Getting Started with ASDM, page 9](#)
- [Unsupported Commands, page 15](#)
- [Caveats, page 17](#)
- [Related Documentation, page 19](#)
- [Obtaining Documentation, page 19](#)
- [Documentation Feedback, page 20](#)
- [Obtaining Technical Assistance, page 21](#)
- [Obtaining Additional Publications and Information, page 23](#)

Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco PIX 500 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 Cisco PIX 500 and ASA 5500 series adaptive security appliance software Version 7.1(2). 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

© 2005 Cisco Systems, Inc. All rights reserved.

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.
- ASDM does not support any non-English characters or any other special characters. If you enter non-English characters in any text entry field, they become unrecognizable when you submit the entry, and you cannot delete or edit them.

If you are using a non-English keyboard or usually type in language other than English, be careful not to enter non-English characters accidentally.

For a workaround, see caveat CSCeh39437.

System Requirements

This section includes the following topics:

- [Hardware Requirements, page 2](#)
- [Client PC Operating System and Browser Requirements, page 3](#)

Hardware Requirements

ASDM software runs on the following platforms:

- Cisco ASA 5510 security appliance
- Cisco ASA 5520 security appliance
- Cisco ASA 5540 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 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 1](#) lists the supported and recommended PC operating systems and browsers for Version 5.1(2). 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

	Operating System	Browser with Java Applet	ASDM Launcher	Other Requirements
Windows ¹	Windows 2000 (Service Pack 4) or Windows XP operating systems	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 Windows NT4.

2. Download the latest Java Plug-in or J2SE from <http://java.sun.com/>.

Platform Feature Licenses

[Table 2](#) lists the feature support for the ASA 5500 series adaptive security appliances.

[Table 3](#) lists the feature support for the PIX 500 series security appliances.



Note

Items that are in italics are separate, optional licenses that you can replace the base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 WebVPN license plus the GTP/GPRS license; or all four licenses together.

Table 2 ASA 5500 Series Adaptive Security Appliance License Features

Platforms and Features	Licenses	
ASA 5510	Base License	Security Plus
Security Contexts	No support	
VPN Sessions ¹	250 combined IPSec and WebVPN	
Max. IPSec Sessions	250	
Max. WebVPN Sessions	2	<i>Optional Licenses:</i>
		<i>10 25 50 100 250</i>
VPN Load Balancing	No support	
Failover	None	
GTP/GPRS	No support	
Max. VLANs	10	
Concurrent Firewall Connections ²	50 K	
Max. Physical Interfaces	3 at 10/100 plus the Management interface for management traffic only (to-the-security-appliance)	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Min. RAM	256 MB	
ASA 5520	Base License	
Security Contexts	2	<i>Optional Licenses:</i>
		<i>5 10 20</i>
VPN Sessions ¹	750 combined IPSec and WebVPN	
Max. IPSec Sessions	750	
Max. WebVPN Sessions	2	<i>Optional Licenses:</i>
		<i>10 25 50 100 250 500 750</i>
VPN Load Balancing	Supported	
Failover	Active/Standby Active/Active	
GTP/GPRS	None	<i>Optional license: Enabled</i>
Max. VLANs	100	
Concurrent Firewall Connections ²	280 K	
Max. Physical Interfaces	Unlimited	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Min. RAM	512 MB	

Table 2 ASA 5500 Series Adaptive Security Appliance License Features (continued)

Platforms and Features	Licenses									
ASA 5540	Base License									
Security Contexts	2	<i>Optional licenses:</i>								
		5	10	20	50					
VPN Sessions ¹	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2	<i>Optional Licenses:</i>								
		10	25	50	100	250	500	750	1000	2500
VPN Load Balancing	Supported									
Failover	Active/Standby									
	Active/Active									
GTP/GPRS	None	<i>Optional license: Enabled</i>								
Max. VLANs	200									
Concurrent Firewall Connections ²	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>								
Min. RAM	1024 MB									

- Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
- The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Table 3 PIX 500 Series Security Appliance License Features

Platforms and Features	Licenses									
PIX 515/515E	R (Restricted)		UR (Unrestricted)		FO (Failover) ¹		FO-AA (Failover Active/Active) ¹			
Security Contexts	No support		2	<i>Optional license: 5</i>	2	<i>Optional license: 5</i>	2	<i>Optional license: 5</i>		
IPSec Sessions	2000		2000		2000		2000			
WebVPN Sessions	No support		No support		No support		No support			
VPN Load Balancing	No support		No support		No support		No support			
Failover	No support		Active/Standby Active/Active		Active/Standby		Active/Standby Active/Active			
GTP/GPRS	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>		
Max. VLANs	10		25		25		25			
Concurrent Firewall Connections ²	48 K		130 K		130 K		130 K			

Table 3 PIX 500 Series Security Appliance License Features (continued)

Platforms and Features	Licenses											
Max. Physical Interfaces	3		6				6		6			
Encryption	None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>	
		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>
Min. RAM	64 MB		128 MB				128 MB		128 MB			
PIX 525	R (Restricted)		UR (Unrestricted)				FO (Failover)¹		FO-AA (Failover Active/Active)¹			
Security Contexts	No support		2	<i>Optional licenses:</i>		2	<i>Optional licenses:</i>		2	<i>Optional licenses:</i>		
				5	10		20	50		5	10	20
IPSec Sessions	2000		2000				2000		2000			
WebVPN Sessions	No support		No support				No support		No support			
VPN Load Balancing	No support		No support				No support		No support			
Failover	No support		Active/Standby Active/Active				Active/Standby		Active/Standby Active/Active			
GTP/GPRS	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>		None	<i>Optional license: Enabled</i>		None	<i>Optional license: Enabled</i>		
Max. VLANs	25		100				100		100			
Concurrent Firewall Connections ²	140 K		280 K				280 K		280 K			
Max. Physical Interfaces	6		10				10		10			
Encryption	None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>	
		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>
Min. RAM	128 MB		256 MB				256 MB		256 MB			
PIX 535	R (Restricted)		UR (Unrestricted)				FO (Failover)¹		FO-AA (Failover Active/Active)¹			
Security Contexts	No support		2	<i>Optional licenses:</i>		2	<i>Optional licenses:</i>		2	<i>Optional licenses:</i>		
				5	10		20	50		5	10	20
IPSec Sessions	2000		2000				2000		2000			
WebVPN Sessions	No support		No support				No support		No support			
VPN Load Balancing	No support		No support				No support		No support			

Table 3 PIX 500 Series Security Appliance License Features (continued)

Platforms and Features	Licenses											
Failover	No support		Active/Standby Active/Active		Active/Standby		Active/Standby Active/Active					
GTP/GPRS	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>	None	<i>Optional license: Enabled</i>		
Max. VLANs	50		150		150		150					
Concurrent Firewall Connections ²	250 K		500 K		500 K		500 K					
Max. Physical Interfaces	8		14		14		14					
Encryption	None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>	
		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>
Min. RAM	512 MB		1024 MB		1024 MB		1024 MB					

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

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 7](#)
- [Upgrading to a New ASDM Release, page 8](#)

Upgrading from PDM

Before you upgrade your device manager, upgrade your 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.

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 your 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 ASDM Image selected, choose **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 choose **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 **Tools > File Management**.
- 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** Choose **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 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 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 10](#)
- [Downloading the ASDM Launcher, page 10](#)
- [Starting ASDM from the ASDM Launcher, page 11](#)
- [Starting ASDM from a Web Browser, page 11](#)
- [Using the Startup Wizard, page 11](#)
- [Using the VPN Wizard, page 12](#)
- [Configuring Failover, page 12](#)
- [Printing from ASDM, page 15](#)

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 PIX default configuration includes an inside interface, but the ASA 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**.

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 Choose **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 Choose **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 choose **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** Choose **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** Choose **Run ASDM as a Java Applet**
- Step 4** Choose **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.

Use the Startup Wizard to configure the basic set-up 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. Choose **Configuration > Wizards > Startup**.
 - b. Choose **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** panel.
 - b. Be sure to allocate interfaces to the context.
 - c. When you apply the changes, ASDM prompts you to use the Startup Wizard.
 - d. Choose the **Context** icon on the upper header bar and select the context name from the Context menu on the lower header bar.
 - e. Choose **Context > Configuration > Wizards > Startup**.
 - f. Choose **Launch Startup Wizard**.
 - Step 2** Choose **Next** as you proceed through the Startup Wizard panels, filling in the appropriate information in each panel, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.
 - Step 3** Choose **Finish** on the last panel 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** panels.
-

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.

- Step 1** Choose **Configuration > Wizards > VPN**.
 - Step 2** Choose **Launch VPN Wizard**.
 - Step 3** Supply information on each wizard panel. Choose **Next** to move through the VPN Wizard panels. You may use the default IPSec and IKE policies. Choose **Help** for more information on each field.
 - Step 4** After you complete entering the VPN Wizard information, choose **Finish** on the last panel to transmit your configuration to the security appliance.
-

Configuring Failover

This section describes how to implement failover on security appliances connected via a LAN.

If you are connecting two ASA security appliances for failover, you must connect them via a LAN. If you are connecting two PIX security appliances, you can connect them using either a LAN or a serial cable.



Tip If your PIX 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 LAN and state 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 failover on your security appliance, perform the following steps:

-
- Step 1** Configure the secondary device for HTTPS IP connectivity. See the “[Before You Begin](#)” section on [page 10](#), 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 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 10](#).)
 - Step 4** Perform one of the following steps, depending on your context mode:
 - a. If your device is in multiple context mode, choose **Context**. Choose the **admin** context from the **Context** drop-down menu, and choose **Configuration > Features > Properties > Failover**.
 - b. If your device is in single mode, choose **Configuration > Features > Properties > Failover**. Choose the **Interfaces** tab.
 - Step 5** Perform one of the following steps, depending on your firewall mode:
 - a. If your device is in routed mode, configure standby addresses for all routed mode interfaces.
 - b. 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:
 - a. If your device is in multiple security context mode: choose **System > Configuration > Features > Failover**.
 - b. If your device is in single mode: choose **Configuration > Features > Properties > Failover**.
 - Step 7** On the **Setup** tab of the **Failover** panel under **LAN Failover**, select the interface that is cabled for LAN 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 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** Choose **Apply**, read the warning dialog that appears, and choose **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** Choose **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 reenables failover. When failover is reenables, the failover communication is encrypted with the 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.
 - Choose **Apply**. (Choose **OK** if CLI preview is enabled.)
- Step 3** Enter the failover key in the **Shared Key** field.
- Step 4** Reenable failover.
- Select the **Enable failover** check box.
 - Choose **Apply**. (Choose **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** Choose **OK**. (Choose **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 15](#)
- [Ignored and View-Only Commands, page 16](#)
- [ASDM Limitations, page 17](#)
- [Other CLI Limitations, page 17](#)

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 3 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

The following table 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.

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used, except for use in VPN group policy screens
capture	Ignored
established	Ignored
failover timeout	Ignored
ipv6 , any IPv6 addresses	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 (choose **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 panels. 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.

Caveats

This section describes caveats for the 5.1.2 version, and includes the following topics:

- [Open Caveats, page 18](#)
- [Resolved Caveats, page 18](#)

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 might 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

Table 4 **Open Caveats**

ID Number	Caveat Title
CSCsd06006	Syslog: Create Rule feature may not pre-assign the correct direction

Resolved Caveats

Table 5 **Resolved Caveats**

ID Number	Caveat Title
CSCsc10806	ASDM: VPN wizard should not create crypto ACL for remote access
CSCsc81417	clear xlate preference not saved in launcher or browser
CSCsc99305	Removal of static command swaps global IP for real IP on interface ACL
CSCsd00651	Preview CLI does not take effect when changed from another ASDM instance
CSCsd16847	Make JBuilder build compatible with release build variable
CSCsd22635	IDS tree occupies the whole space when IDS button is clicked
CSCsd22676	ASDM does not allow ACL rule with same src and dst interface
CSCsd29372	ASDM should not read version from monitoring handler data
CSCsd29568	CSC Home page latest update reporting Anti-Spam engine update all times
CSCsd33096	PDM stuck at 47% during loading due to access list configurations
CSCsd38435	ASDM stuck at 47% during loading due to access list configurations
CSCsd42941	LDAP test-ASDM doesn't accept username with space even enclosed with
CSCsd51425	Home page syslog window is not expanding when ASDM window maximized
CSCsd56172	Demo install fails on Japanese OS
CSCsd58987	Proxy Bypass allowable ports are wrong
CSCsd60332	ASDM does not implement cache-static-content for WebVPN cache
CSCsd60339	LMFactor range needs to be updated for webVPN Cache
CSCsd61183	Without SubInterface range - alias name fails if it ends with Digit
CSCsd61313	ASDM does not implement WebVPN java-trustpoint <name>
CSCsd61359	ASDM:Group-policy hic-fail-deny msg should be limited to 491 chars
CSCsd61734	Context>Config>Intf edit intf descr field doesn't read descr completely
CSCsd64356	'http redirect' fails with ASDM sessions..OK for WebVPN sessions

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*
- *Release Notes for Cisco Intrusion Prevention System 5.1*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

<http://www.cisco.com>

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/en/US/docs/general/illus_process/PDI/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support 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 (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

Submitting a Service Request

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 TAC engineer. The TAC Service Request Tool is located at this URL:

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

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 TAC 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/en/US/support/index.html>

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)—Your 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 operation 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 your network is impaired, but 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.

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

<http://www.cisco.com/cgi-bin/marketplace/welcome.pl>

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

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

- *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 Cisco Systems technical user magazine for maximizing Internet and networking investments. 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 access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *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>
- 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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

© 2006 Cisco Systems, Inc.
All rights reserved