



Cisco ASDM Release Notes Version 5.0(2)

July 2005

Contents

This document contains release information for Cisco ASDM Version 5.0(2) on Cisco PIX 500 series and Cisco ASA 5500 series security appliances 7.0(2). It includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 3](#)
- [Important Notes, page 4](#)
- [Caveats, page 14](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation, page 17](#)
- [Documentation Feedback, page 18](#)
- [Obtaining Technical Assistance, page 18](#)
- [Obtaining Additional Publications and Information, page 19](#)

Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco PIX 500 and ASA 5500 series security appliances through an intuitive, easy-to-use, web-based management interface. Bundled with supported security appliances, the device manager accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by Cisco PIX 500 and ASA 5500 series security appliance software Version 7.0(2). Its secure, web-based 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.

New Platform Features

The PIX 500 and ASA 5500 series security appliances 7.0(2) introduce significant enhancements to firewall and inspection capabilities, VPN services, network integration, high availability, and management/monitoring features. ASDM supports these new platform features.

This document contains release information about ASDM only.

New Device Manager Features

The following table highlights the new device manager features in this release.

| 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 syslog 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. |
| Comprehensive Cisco PIX and ASA Security Appliances Software Version 7.0(2) Feature Support | Provides support for more than 50 new features introduced in Cisco PIX 500 and ASA 5500 series security appliance software Version 7.0(2), such as transparent firewall, PIM sparse mode, QoS, and Active/Active failover, in addition to existing features such as OSPF and VLAN. |
| Advanced Application and 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. |

| Feature | Benefits |
|---|---|
| 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 under System Requirements . |

System Requirements

This section includes the following topics:

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

Hardware Requirements

ASDM software runs on the following platforms:

- Cisco ASA 5510 security appliance
- Cisco ASA 5520 security appliance
- Cisco ASA 5540 security appliance
- SSM-10
- SSM-20
- PIX 515/515E
- PIX 525
- PIX 535



Note

ASDM is not currently 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 5.0(2).

Table 1 Operating System and Browser Requirements

| | Operating System | Browser | Other Requirements |
|----------------------|---|---|--|
| Windows ¹ | Windows 2000 (Service Pack 4) or Windows XP operating systems | Internet Explorer 6.0 with Java Plug-in 1.4.2 or 1.5.0 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 1.4.2 or 1.5.0 | 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 1.4.2 or 1.5.0 | |
| 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 1.4.2 | |

1. ASDM is not supported on Windows 3.1, 95, 98, ME or Windows NT4.

Important Notes

This section includes the following topics:

- [Upgrading to a New Software Release](#)
- [Getting Started with ASDM](#)
- [Unsupported Characters](#)
- [ASDM CLI Does Not Support Interactive User Commands](#)
- [Printing from ASDM](#)
- [Unsupported Commands](#)
- [Securing the Failover Key](#)

Upgrading to a New Software Release

If you have a Cisco Connection Online (CCO) login, you can obtain software from the following website:

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

Refer to *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0* for more information.



Note

Before you upgrade your device manager, upgrade your platform software to Cisco PIX software Version 7.0.

To upgrade from PIX Device Manager to ASDM, perform the following steps:

-
- Step 1** Copy the ASDM binary file (asdm-501.bin) to a TFTP or FTP server on your network.
- Step 2** Log in to your security appliance using the console (or other appropriate method that you have configured).
- Step 3** Ensure that you have connectivity from your security appliance to your TFTP/FTP server.
- Step 4** If you have an existing copy of the PIX Device Manager, delete it:
- ```
delete flash:/pdm
```
- Step 5** Copy the ASDM binary onto your security appliance using the appropriate command:
- For TFTP: `copy tftp://your-server-IP/pathtofile flash:/asdm-501.bin`
  - For FTP: `copy ftp://your-server-IP/pathtofile flash:/asdm-501.bin`



### Note

For more information on the `copy` command and its options, see the *Cisco Security Appliance Command Reference*.

- 
- Step 6** If you have more than one ASDM image, enter the following command to configure the location of the ASDM image:
- ```
asdm image flash:/asdm501.bin
```
- Step 7** Enter the following command to enable the HTTPS server on the device:
- ```
http server enable
```
- Step 8** Identify the systems or networks that are allowed to access ASDM by specifying one or more hosts/networks, using the following command:
- ```
http 10.1.1.1 255.255.255.255 inside
```
- where IP address 10.1.1.1 is a host that can access ASDM and which is connected via the inside interface. Refer to *Cisco Security Appliance Command Reference* for more information on the options to the `http` command.
- Step 9** Verify that ASDM is installed correctly by connecting from the client system (10.1.1.1 in the preceding example) to the security appliance, using a supported browser. For example:
- ```
https://10.1.1.254/admin/
```
- where 10.1.1.254 is the IP address of the inside interface of the device in Step 8.

**Note**

ASDM requires Java Plug-in software. After you install ASDM, download the latest Java Plug-in from the following site: <http://www.cisco.com/cgi-bin/tablebuild.pl/java2>.

## 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.

## Getting Started with ASDM

If you are using ASDM for the first time on a new security appliance, follow the instructions in this section to get started using ASDM. If you are upgrading an existing device, see [Upgrading to a New Software Release, page 5](#).

Because ASDM uses a GUI interface, it requires that you access it from a PC using a supported web browser. For the supported browsers, see the “[Client PC Operating System and Browser Requirements](#)” section on page 4.

## Before You Begin

Before using ASDM for the first time, do the following:

- 
- Step 1** Set up your security appliance.
  - Step 2** Connect your PC directly to the security appliance via the port Ethernet 1.
  - Step 3** Do one of the following:
    - Either configure your PC for DHCP, or
    - Make sure your PC is on the same subnet as the security appliance. (The default IP address for the security appliance is: 192.168.1.1. The default subnet mask is 255.255.255.0.)
  - If you want to configure transparent firewall mode on your security appliance, enter the CLI **setup** command. Refer to the [Cisco Security Appliance Command Line Configuration Guide](#) for more information.
- 

## Starting ASDM

To start ASDM for the first time, perform the following steps:

- 
- Step 1** Start ASDM from a supported web browser connected to the security appliance by entering the URL: `https://192.168.1.1/admin/`

where 192.168.1.1 is the IP address of the security appliance.



**Note** Be sure to enter **https**, not **http**.

**Step 2** Click **OK** or **Yes** to all prompts, including the name and password prompt. No name or password is required for a new device.

If ASDM does not start, check the device configuration. Your security appliance should be configured to accept ASDM configuration on its inside interface. (A new security appliance is configured this way by default.) If you need to modify the configuration to reestablish this default setting, use the CLI. Include configuration information similar to the following.



**Note** This example is of a PIX security appliance in single mode. If you are using an ASA security appliance, use the `Management0/0` interface in place of `Ethernet1`.

```
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
http server enable
http 0.0.0.0 0.0.0.0 inside
```

where the IP address 192.168.1.1 is on the same subnet as your security appliance and `inside` is the default name of the interface. (You might give your interface a different name, such as “management.”)

The **http server enable** command with the `inside` argument enables the HTTP(S) server on the security appliance interface named `inside`. The **http** command with the `0.0.0.0 0.0.0.0` arguments allows HTTP traffic from any and all IP addresses and subnet masks to the HTTP server through the interface named `inside`. For more information, see the **http** and **http server enable** commands in the [Cisco Security Appliance Command Reference](#).



**Note** Refer to the **configure factory defaults** or **setup** command in the [Cisco Security Appliance Command Line Configuration Guide](#) for more information on using the CLI to reestablish factory default settings.

## Using the Startup Wizard

The Startup Wizard helps you easily configure a single mode device or a context of a multiple mode device.

Use the Startup Wizard to configure the basic set-up of your security appliance:

- Step 1** *If your security appliance is in multi mode, for each new context, do the following:*
- 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. 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**.

*If your security appliance is in single mode:*

- a. Click **Configuration > Wizards > Startup**.
- b. Click **Launch Startup Wizard**.

- Step 2** Click **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** Click **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.

(Optional.) You can now enter other configuration details on the **Configuration > Features** panels.

## VPN Wizard

The VPN Wizard configures basic VPN access for site-to-site or remote-client access. The VPN Wizard is available only for security appliances running in single context mode with routed (not transparent) firewall mode.

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

## Bootstrapping LAN 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. Use the **configure factory defaults** or the **setup** CLI command to assign the standby IP address to the ASDM interface on the secondary device.

**Step 2** After configuration, the secondary device, has a configuration such as the following. (If you are using an ASA security device, replace the interface `Ethernet1` with `Management0/0`.)

```
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.2 255.255.255.0
 http server enable
 http 0.0.0.0 0.0.0.0 inside
```

where in this example IP address 192.168.1.2 is the standby IP address of the ASDM interface on the secondary device.

**Step 3** Configure the primary device for HTTPS IP connectivity using the active IP address for the ASDM interface.

**Step 4** Connect the pair of devices together and to their networks in their failover LAN cable configuration.

**Step 5** Start ASDM from the primary device through a supported web browser. (See the section [Starting ASDM](#), page 6.)

**Step 6** Perform one of the following steps, depending on your security context mode:

- a. If your device is in multiple security context mode, click **Context**. Choose the **admin** context from the **Context** drop-down menu, and click **Configuration > Features > Properties > Failover**.
- b. If your device is in single mode, click **Configuration > Features > Properties > Failover**. Click the **Interfaces** tab.

**Step 7** 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 8** Perform one of the following steps, depending on your security context mode:

- a. If your device is in multiple security context mode: click **System > Configuration > Features > Failover**.
- b. If your device is in single mode: click **Configuration > Features > Properties > Failover**.

**Step 9** On the **Setup** tab of the **Failover** panel under **LAN Failover**, select the interface that is cabled for LAN failover.

**Step 10** Configure the remaining **LAN Failover** fields.

- Step 11** (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 12** On the **Setup** tab, select the **Enable Failover** check box. If you are using the PIX 500 series security appliance, select the **Enable LAN rather than serial cable failover** check box.
- Step 13** Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.
- Step 14** 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 15** 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.

---

## ASA Interface Supports Either WebVPN or ASDM Admin Session

The security appliance supports either WebVPN or an ASDM administrative session on an interface, but not both simultaneously. To use ASDM and WebVPN at the same time, configure them on different interfaces.

## Unsupported Characters

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.

*Workaround:*

For work around, see CSCeh39437 under [Caveats, page 14](#).

## ASDM CLI Does Not Support Interactive User Commands

ASDM provides a CLI tool (click **Tools > Command Line Interface...**) that allows you to enter certain CLI commands from ASDM. For a list of specific commands that are not supported, see [Unsupported Commands, page 11](#).

The ASDM CLI feature also does not support *interactive* user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter “[yes/no]” but does not recognize your input. ASDM then times out waiting for your response.

For example:

1. On the ASDM **Tools** menu, click **Command Line Interface**.
2. Enter the command: `crypto key generate rsa`

ASDM generates the default 1024-bit RSA key.

3. Enter the command again: **crypto key generate rsa**

Instead of regenerating the RSA keys by overwriting the previous one, ASDM displays the following error:

```
Do you really want to replace them? [yes/no]:WARNING: You already have RSA
ke00000000000000$A key
Input line must be less than 16 characters in length.
```

```
%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:
```

```
%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

*Workaround:*

- You can configure most commands that require user interaction by means of the ASDM panels.
- For CLI commands that have a noconfirm option, use the noconfirm option when entering the CLI command. For example:

```
crypto key generate rsa noconfirm
```

## 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
- 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.

### 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                                                     |
|--------------------------------------|-------------------------------------------------------------------|
| <b>access-list</b>                   | Ignored if not used, except for use in VPN group policy screens   |
| <b>asr-group</b>                     | Ignored                                                           |
| <b>capture</b>                       | Ignored                                                           |
| <b>established</b>                   | Ignored                                                           |
| <b>failover timeout</b>              | Ignored                                                           |
| <b>ipv6</b> , any IPv6 addresses     | Ignored                                                           |
| <b>object-group icmp-type</b>        | View-only                                                         |
| <b>object-group network</b>          | Nested group is view-only                                         |
| <b>object-group protocol</b>         | View-only                                                         |
| <b>object-group service</b>          | Nested group cannot be added                                      |
| <b>pager</b>                         | Ignored                                                           |
| <b>pim accept-register route-map</b> | Ignored. Only the <b>list</b> option can be configured using ASDM |
| <b>prefix-list</b>                   | Ignored if not used in an OSPF area                               |
| <b>route-map</b>                     | Ignored                                                           |

| Unsupported Commands                       | ASDM Behavior                                                                                                                                                                                                                               |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>service-policy global</code>         | Ignored if it uses a <b>match access-list</b> class. For example:<br><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> |
| <code>sysopt nodnsalias</code>             | Ignored                                                                                                                                                                                                                                     |
| <code>sysopt uauth allow-http-cache</code> | Ignored                                                                                                                                                                                                                                     |
| <code>terminal</code>                      | Ignored                                                                                                                                                                                                                                     |
| <code>virtual</code>                       | 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
```

## 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.)
- Clear the **Enable failover** check box.
  - Click **Apply**. (Click **OK** if CLI preview is enabled.)
- Step 3** Enter the failover key in the **Shared Key** box.

- Step 4** Reenable failover.
- a. Select 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.

## Caveats

The following sections describe caveats for the 5.0 release.



### 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](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(2)

**Table 2** Open Caveats

| ID Number  | Software Release 5.0(2) |                                                                      |
|------------|-------------------------|----------------------------------------------------------------------|
|            | Corrected               | Caveat Title                                                         |
| CSCeg14905 | No                      | Applying service group change causes no ACL CLI to be generated      |
| CSCeg67083 | No                      | failover panel lock after apply config will need reset to input data |
| CSCeg69476 | No                      | ASDM can not take any input from keyboard from SunOS 5.8 / Mozilla   |
| CSCeh06459 | No                      | ASDM can not create appropriate ACL for QoS on outbound interface    |
| CSCeh20409 | No                      | Startup Wizard allows not naming any interface                       |
| CSCeh24529 | No                      | ASDM sometimes allows more than 2 traffic match criteria             |
| CSCeh24609 | No                      | Live Log: live log on Monitoring/Home don't work after disconn/conn  |
| CSCeh33941 | No                      | ASDM: Webtype ACL port checking does not match supported values      |
| CSCeh39437 | No                      | Non-English characters do not display properly in some screens       |
| CSCeh39531 | No                      | ASDM allows user to configure same static for different networks     |
| CSCeh41391 | No                      | Priority Queue screen - range limits for Add are not correct         |
| CSCeh42043 | No                      | ASDM-IP AUDIT Policy-to-interface pull-down don't track mouse motion |

**Table 2**      *Open Caveats*

| ID Number  | Software Release 5.0(2) |                                                                      |
|------------|-------------------------|----------------------------------------------------------------------|
|            | Corrected               | Caveat Title                                                         |
| CSCeh43422 | No                      | edit nssa for default-info, metric and metric-type ignored           |
| CSCeh43569 | No                      | ASDM: Logging fails-> Exception occurred during event dispatching    |
| CSCeh52524 | No                      | Check logging permit when syslog server is down doesn't enable apply |
| CSCeh53158 | No                      | Wrong cmds sent when objgp w/ PNAT is edited to add net-obj with NAT |
| CSCeh66856 | No                      | ASDM crashes IE and launcher after socket timeout                    |
| CSCei56371 | No                      | MTU minimum size can not be set below 300                            |
| CSCei58507 | No                      | ASDM: missing enhanced split tunnel functionality - extended ACLs    |

## Resolved Caveats - Release 5.0(2)

**Table 3**      *Resolved Caveats*

| ID Number  | Software Release 5.0(2) |                                                                      |
|------------|-------------------------|----------------------------------------------------------------------|
|            | Corrected               | Caveat Title                                                         |
| CSCei16647 | Yes                     | Cannot read iplog file downloaded from ASDM                          |
| CSCeh53516 | Yes                     | ASDM displays in-complete rule in error in some configurations       |
| CSCeh78270 | Yes                     | IKE policy configuration should include infinite lifetime option     |
| CSCeh91338 | Yes                     | ASDM Home Page is blank if authenticated username is 3 chars or less |
| CSCeh93183 | Yes                     | Destination IP is not correctly set in the CLI                       |
| CSCeh95237 | Yes                     | Dynamic Crypto Maps unattached to static crypto maps crash ASDM      |
| CSCei23118 | Yes                     | Show past events with large number of hours gives blank screen       |
| CSCei25996 | Yes                     | Operator having trouble changing Global Variable                     |
| CSCei27394 | Yes                     | ASDM is not displaying VPN IKE tunnel summary on home page           |
| CSCei38991 | Yes                     | Blocking property panel delete button not visible in multi-mode      |
| CSCei10049 | Yes                     | Error displayed when trying to edit inline interface pair            |
| CSCei08437 | Yes                     | Stopping IP Logging giving java.lang.Exception                       |
| CSCei34740 | Yes                     | Need to disable Use Additional Data option for Add Rate Limit        |
| CSCei37660 | Yes                     | Help page didn't popup in Add Rate Limit panel                       |
| CSCei38088 | Yes                     | Add support for IPS 5.1 sensor                                       |
| CSCeh22246 | Yes                     | asdm_handler: After Tearing down overnight testing ASDM rep 114 tun  |
| CSCeg85016 | Yes                     | Can't login to ASDM when authentication required (Linux, JRE 1.5.0)  |
| CSCeh01635 | Yes                     | Printing from ASDM invoked as an applet is not supported             |
| CSCeh43624 | Yes                     | NTP:unable to edit key value and number                              |
| CSCeh49697 | Yes                     | ASDM IPSec/IKE graphs reporting tunnel count incorrectly.            |

**Table 3**      **Resolved Caveats**

| <b>Software Release 5.0(2)</b> |                  |                                                               |
|--------------------------------|------------------|---------------------------------------------------------------|
| <b>ID Number</b>               | <b>Corrected</b> | <b>Caveat Title</b>                                           |
| CSCeh50535                     | Yes              | Can't edit a route summarization entry in second ospf process |
| CSCeh39560                     | Yes              | ASDM cannot switch from serial to LAN failover                |

## Related Documentation

For additional information on ASDM or its platforms, refer to the ASDM online Help or the following documentation found on Cisco.com:

- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start 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. 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/univercd/home/home.htm>

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](http://www.cisco.com/public/countries_languages.shtml)

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/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/partner/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](mailto: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/techsupport>

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/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 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/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)—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/go/marketplace/>

- 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://cisco.com/univercd/cc/td/doc/pcat/>

- *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 “[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, ASIST, 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, Empowering the Internet Generation, 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, StrataView Plus, TeleRouter, 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. (0502R)

Copyright © 2005 Cisco Systems, Inc.  
All rights reserved.

