# Cisco ASDM Release Notes Version 5.0(5)

**April 2006**

This document contains release information for Cisco ASDM Version 5.0(5), which runs with Cisco PIX 500 series and Cisco ASA 5500 series security appliance software Version 7.0(5). This document includes the following sections:



# Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco PIX 500 series and ASA 5500 series adaptive security appliances through an intuitive, easy-to-use management interface. Bundled with supported security appliances, the device manager accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by software Version 7.0(5). Its secure design enables anytime, anywhere access to security appliances.


CISCO SYSTEMS

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

# Important Notes

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

# New Features

**Released: April 14, 2006**

Table 1 lists the new features for ASA and PIX Version 7.0(5)/ASDM Version 5.0(5).

***Table 1 New Features for ASA and PIX Version 7.0(5)/ASDM Version 5.0(5)***

| Feature | Description |
|---|---|
| **Application Inspection Features** | |
| Command to Control DNS Guard | You can now control the DNS guard function. In releases prior to 7.0(5), the DNS guard functions are always enabled regardless of the configuration of DNS inspection:<br>• Stateful tracking of the DNS response with DNS request to match the ID<br>• Tearing down the DNS connection when all pending requests are responded<br>This command is effective only on interfaces with DNS inspection disabled (**no inspect dns**). When DNS inspection is enabled, the DNS guard function is always performed.<br>We introduced the following command: **dns guard**. |
| Enhanced IPSEC Inspection | The ability to open specific pinholes for ESP flows based on existence of an IKE flow is provided by the enhanced IPSec inspect feature. This feature can be configured within the MPF infrastructure along with other inspects. The idle-timeout on the resulting ESP flows is statically set at 10 minutes. There is no maximum limit on number of ESP flows that can be allowed.<br>We introduced the following command: **inspect ipsec-pass-thru**. |
| **Firewall Features** | |
| Command to Disable RST for Denied TCP Packets | When a TCP packet is denied, the adaptive security appliance always sends a reset when the packet is going from a high security to a low security interface. The **service resetinbound** command is used to enable or disable sending resets when a TCP packet is denied when going from a low security to a high security interface. The **service resetinbound** command is introduced to control sending RESETs when a packet is denied when going from a high security to a low security interface. The existing **service resetinbound** command is enhanced to take an additional interface option.<br>We introduced the following commands: **service resetoutbound**, **service resetinbound**. |

*Table 1 New Features for ASA and PIX Version 7.0(5)/ASDM Version 5.0(5) (continued)*

| Feature | Description |
|---|---|
| **Platform Features** | |
| Increased Connections and VLANs | The maximum connections and VLANs is increased to the following numbers.<br>• ASA5510 base license conns 32000->50000 vlans 0->10<br>• ASA5510 plus license conns 64000->130000 vlans 10->25<br>• ASA5520 conns 130000->280000 vlans 25->100<br>• ASA5540 conns 280000->400000 vlans 100->200 |
| **Management Features** | |
| Password Increased in Local Database | Username and enable password length limits increased from 16 to 32 in the LOCAL database. |
| Enhanced **show interface** and **show traffic** Commands | The traffic statistics displayed in both the **show interface** and **show traffic** commands now support 1 minute rate and 5 minute rate for input, output and drop. The rate is calculated as the delta between the last two sampling points. For a 1 minute rate and a 5 minute rate, a 1 minute timer and a 5 minute timer are run constantly for the rates respectively. An example of the new display follows:<br>`1 minute input rate 128 pkts/sec, 15600 bytes/sec`<br>`1 minute output rate 118 pkts/sec, 13646 bytes/sec`<br>`1 minute drop rate 12 pkts/sec`<br>`5 minute input rate 112 pkts/sec, 13504 bytes/sec`<br>`5 minute output rate 101 pkts/sec, 12104 bytes/sec`<br>`5 minute drop rate 4 pkts/sec` |

# System Requirements

This section includes the following topics:



## 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 2 lists the supported and recommended PC operating systems and browsers for Version 5.0(5). While ASDM might work on other browsers and browser versions, these are the only officially supported browsers. Note that unlike earlier PDM releases, you must have the Java Plug-in or J2SE installed. The native JVM on Windows is no longer supported and does not work.

***Table 2 Operating System, Browser, and Java Requirements***

| | Operating System | Browser with Java Applet | ASDM Launcher | Other Requirements |
|---|---|---|---|---|
| Windows[1] | Windows 2000 (Service Pack 4) or Windows XP operating systems | Internet Explorer 6.0 with Java Plug-in[2] 1.4.2 or 5.0 (1.5)<br>**Note** **HTTP 1.1**—Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections.<br>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/.

# 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/cisco/software/navigator.html

This section includes the following topics:



# Upgrading from PDM

Before you upgrade your device manager, upgrade your platform software to Version 7.0. See the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0* for more information.

To upgrade to ASDM, perform the following steps:

**Step 1** Copy the ASDM binary file to a TFTP or FTP server on your network.

**Step 2** Log in to the security appliance and enter privileged EXEC mode:

```
hostname> enable
password:
hostname#
```

**Step 3** Ensure that you have connectivity from the security appliance to the TFTP/FTP server.

**Step 4** Delete the old version of PDM by entering the following command:

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

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

- TFTP

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

- FTP

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

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

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

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

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

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

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

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

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

Enter **0** for the *ip_address* and *mask* to allow all IP addresses.

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

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

## Deleting Your Old Cache

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

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

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

## Upgrading to a New ASDM Release

If you have a previous release of ASDM on your security appliance and want to upgrade to the latest release, you can do so from within ASDM. We recommend that you upgrade the ASDM image before the platform image. ASDM is backwards compatible, so you can upgrade the platform image using the new ASDM; you cannot use an old ASDM with a new platform image.

To upgrade ASDM, perform the following steps:

**Step 1** Download the new ASDM image to your PC.

**Step 2** Launch ASDM.

**Step 3** From the Tools menu, click **Upload Image from Local PC**.

**Step 4** With the **ASDM Image** option button selected, click the **Browse Local** button to select the new ASDM image.

**Step 5** To specify the location in Flash memory where you want to install the new image, enter the directory path in the box or click the **Browse Flash** button.

If your security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifiying the same destination filename. You can reanme the image after it was uploaded using the **Tools > File Management** tool.

If you have enough memory for both versions, you can specify a different name for the new version. If you need to revert to the old version, it is still in your Flash memory.

**Step 6** Click **Upload Image**.

When ASDM is finished uploading, you see the following message:

"ASDM Image is Uploaded to Flash Successfully."

**Step 7** If the new ASDM image has a different name than the old image, then you must configure the security appliance to load the new image on the **Configuration > Features > Device Administration > Boot System/Configuration** panel.

**Step 8** To run the new ASDM image, you must quit out of ASDM and reconnect.

**Step 9** Download the new platform image using the **Tools > Upload Image from Local PC** tool.

To reload the new image, reload the security appliance using the **Tools > System Reload** tool.

# Getting Started with ASDM

This section describes how to connect to ASDM and start your configuration. If you are using the security appliance for the first time, your security appliance might include a default configuration. You can connect to a default IP address with ASDM so you can immediately start to configure the security

appliance from ASDM. If your platform does not support a default configuration, you can log in to the CLI and run the setup command to establish connectivity. See "Before You Begin" for more detailed information about networking.

This section includes the following topics:



# Before You Begin

If your security appliance includes a factory default configuration, you can connect to the default management address of 192.168.1.1 with ASDM. On the ASA 5500 series adaptive security appliance, the interface to which you connect with ASDM is Management 0/0. 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** Click **OK** or **Yes** to all prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

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

**Step 3** Click **Download ASDM Launcher and Start ASDM**.

The installer downloads to your PC.

**Step 4** Run the installer to install the ASDM Launcher.

# Starting ASDM from the ASDM Launcher

The ASDM Launcher is for Windows only.

To start ASDM from the ASDM Launcher, perform the following steps:

**Step 1** Double-click the Cisco ASDM Launcher shortcut on your desktop, or start it from the **Start** menu.

**Step 2** Enter the security appliance IP address or hostname, your username, and your password, and then click **OK**.

If there is a new version of ASDM on the security appliance, the ASDM Launcher automatically downloads it before starting ASDM.

# Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

**Step 1** From a supported web browser on the security appliance network, enter the following URL:

**https://***interface_ip_address*

In transparent firewall mode, enter the management IP address.

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

**Step 2** Click **OK** or **Yes** to all browser prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**

- **Run ASDM as a Java Applet**

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

**Step 4** Click **OK** or **Yes** to all Java prompts, including the name and password prompt. By default, leave the name and password blank.

# Using the Startup Wizard

The Startup Wizard helps you easily configure a single mode security appliance or a context in multiple context mode.

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. Click **Configuration > Wizards > Startup**.
  b. Click **Launch Startup Wizard**.
- In multiple context mode, for each new context, perform the following steps:
  a. Create a new context using the **System > Configuration > Features > Security Context** 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**.

**Step 2** Click **Next** as you proceed through the Startup Wizard screens, filling in the appropriate information in each screen, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.

**Step 3** Click **Finish** on the last 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** Click **Configuration > Wizards > VPN**.

**Step 2** 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.

# Configuring Failover

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

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

**Tip** If your security appliances are located near each other, you might prefer connecting them with a serial cable to connecting them via the LAN. Although the serial cable is slower than a LAN connection, using a cable prevents having to use an interface or having 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 7, and use a different IP address on the same network as the primary device.

**Step 2** Connect the pair of devices together and to their networks in their failover LAN cable configuration.

**Step 3** Start ASDM from the primary device through a supported web browser. (See the section Downloading the ASDM Launcher, page 7.)

**Step 4** Perform one of the following steps, depending on your context mode:

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

**Step 5** Perform one of the following steps, depending on your firewall mode:

- **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: click **System > Configuration > Features > Failover**.

b. If your device is in single mode: click **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** Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.

**Step 12** Enter the IP address of the secondary device, which you configured as the standby IP address of the ASDM interface. Wait about 60 seconds. The standby peer still could become temporarily inaccessible.

**Step 13** Click **OK**. Wait for configuration to be synchronized to the standby device over the failover LAN connection.

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

## Securing the Failover Key

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

a. If your device is in single mode, navigate to **Configuration > Features > Properties > Failover > Setup**.

b. If you device is in multiple mode, navigate to **System > Configuration > Features > Failover > Setup**.

**Step 2** Turn off failover. (The standby should switch to pseudo-standby mode.)

a. Uncheck the **Enable failover** check box.

b. Click **Apply**. (Click **OK** if CLI preview is enabled.)

**Step 3** Enter the failover key in the **Shared Key** box.

**Step 4** Reenable failover.

a. Check the **Enable failover** check box.

b. Click **Apply**. (Click **OK** if CLI preview is enabled.) A dialog box about configuring the peer appears.

**Step 5** Enter the IP address of the peer. Wait about 60 seconds. Even though the standby peer does not have the shared failover key, the standby peer still could become inaccessible.

**Step 6** Click **OK**. (Click **OK** if CLI preview is enabled.) Wait for configuration to be synchronized to the standby device over the encrypted failover LAN connection.

## Printing from ASDM

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

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

ASDM supports printing for the following features:

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

# Unsupported Commands

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

See the following sections for more information:


- Effects of Unsupported Commands, page 12
- Ignored and View-Only Commands, page 13
- ASDM Limitations, page 14
- ASDM Limitations, page 14


## Effects of Unsupported Commands

- If ASDM loads an existing running configuration and finds IPv6-related commands, ASDM displays a dialog box informing you that it does not support IPv6. You cannot configure any IPv6 commands in ASDM, but all other configuration is available.
- If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, see **Options > Show Commands Ignored by ASDM on Device**.

- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.

  Monitor-only mode allows access to the following functions:

  – The **Monitoring** area

  – The CLI tool (**Tools > Command Line Interface**), which lets you use the CLI commands.

  To exit Monitor-only mode, use the CLI tool or access the security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.

**Note** You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to 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. |
| **asr-group** | Ignored |
| **capture** | Ignored |
| **established** | Ignored |
| **failover timeout** | Ignored |
| **ipv6**, any IPv6 addresses | Ignored |
| **logging** (in system in multiple context mode) | Ignored |
| **object-group icmp-type** | View-only |
| **object-group network** | Nested group is view-only |
| **object-group protocol** | View-only |
| **object-group service** | Nested group cannot be added |
| **pager** | Ignored |
| **pim accept-register route-map** | Ignored. Only the **list** option can be configured using ASDM. |
| **prefix-list** | Ignored if not used in an OSPF area |
| **route-map** | Ignored |

| Unsupported Commands | ASDM Behavior |
|---|---|
| **service-policy global** | Ignored if it uses a **match access-list** class. For example:<br>`access-list myacl line 1 extended permit ip any any`<br>`class-map mycm`<br>`match access-list mycl`<br>`policy-map mypm`<br>`class mycm`<br>`inspect ftp`<br>`service-policy mypm global` |
| **sysopt nodnsalias** | Ignored |
| **sysopt uauth allow-http-cache** | Ignored |
| **terminal** | Ignored |
| **virtual** | Ignored |

# ASDM Limitations

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

# Other CLI Limitations

- ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, you cannot use the following:

  ```
  ip address inside 192.168.2.1 255.255.0.255
  ```

- The ASDM CLI tool does not support interactive user commands. ASDM provides a CLI tool (click **Tools > Command Line Interface**) that lets you enter certain CLI commands from ASDM. The ASDM CLI tool does not support interactive user commands. You can configure most commands that require user interaction by means of the ASDM 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
  ke0000000000000$A key
  Input line must be less than 16 characters in length.

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

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

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

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

# Caveats for 5.0(5)

This section describes caveats for the 5.0.(5) release, and includes the following topics:



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

http://tools.cisco.com/Support/BugToolKit/

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

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

## Open Caveats

*Table 3 Open Caveats*

| ID Number | Caveat Title |
|---|---|
| CSCei47678 | SNMP packet size standards in RFC3417 not fully supported. |
| CSCek21836 | SIP: BYE embryonic connection timestamp not updated. |
| CSCsc36891 | Higher CPU utilization for url filtering in recent releases. |
| CSCsc37965 | IP-directed broadcasts no longer allowed through device. |
| CSCsc68575 | CPU usage is higher for given traffic throughput in recent releases. |
| CSCsc97602 | Traceback is sometimes observed in tmatch compile thread. |
| CSCsd00086 | ASDM connection may cause packet loss. |
| CSCsd08170 | UDP 500 not removed from pat port pool when crypto map is applied. |
| CSCsd59936 | Registering to the RP for PIM fails if fragmented in more then 12 packs. |
| CSCsd69625 | EZVPN:IOS C876 Client can't connect to ASA using digi certs and noXauth. |
| CSCsd75865 | VPN address pool overlap may cause packet drop. |
| CSCsd78428 | Traceback may occur in Checkheaps on standby unit. |
| CSCsd79596 | H245 connection going idle although traffic on RTP stream and H225. |
| CSCsd82355 | Malformed syslog packets may be generated. |
| CSCsd82714 | RTSP fails with Windows media player. |
| CSCsd84394 | IPSec: Invalid block submitted to outbound packet processing. |
| CSCsd85345 | Traceback may occur in fover_parse on 7.0.4. |
| CSCsd89503 | Traceback during failover in routing module. |
| CSCsd93207 | Show failover indicates different uptimes on devices in failover pair. |
| CSCsd93380 | Packets for VPN-l2l peer get dropped instead of encrypted. |

# Resolved Caveats

*Table 4 Resolved Caveats*

| ID Number | Caveat Title |
|---|---|
| CSCei39245 | IP address not accepted when specifying a NATed address for IPS. |
| CSCsc10806 | ASDM: VPN wizard should not create crypto ACL for remote access. |
| CSCsc59420 | ASDM hangs at 47% when loading the config due to static policy NAT entry. |
| CSCsc78337 | IPS configuration stops working. |
| 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. |
| CSCsd03819 | ASDM location not created when adding a new host to an existing group. |
| CSCsd22676 | ASDM does not allow ACL rule with same src and dst interface. |
| CSCsd38435 | ASDM stuck at 47% during loading due to access list configurations using object-groups. |
| CSCsd81155 | ASDM VPN wizard silently removes 'no sysopt connection permit-vpn. |
| CSCsd86303 | VPN Wizard: Re word sysopt connection permit  option text. |
| CSCsd86444 | ASDM: allow 32 character passwords in LOCAL user database. |
| CSCsd89515 | Live Log: Show all does not work after Filter text. |

# 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 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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