



# Cisco ASDM Release Notes Version 5.2(2)

---

## November 2006

This document contains release information for Cisco ASDM Version 5.2(2) on Cisco PIX 500 series and Cisco ASA 5500 series security appliances Version 7.2(2). It includes the following sections:

- [Introduction, page 2](#)
- [New Device Manager Features, page 2](#)
- [New Security Appliance Features, page 2](#)
- [Client PC Operating System and Browser Requirements, page 3](#)
- [Supported Platforms and Feature Licenses, page 5](#)
- [ASDM and SSM Compatibility, page 5](#)
- [Upgrading ASDM, page 5](#)
- [Getting Started with ASDM, page 6](#)
- [ASDM Limitations, page 14](#)
- [Caveats, page 16](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, page 20](#)
- [Documentation Feedback, page 21](#)
- [Cisco Product Security Overview, page 21](#)
- [Product Alerts and Field Notices, page 22](#)
- [Obtaining Technical Assistance, page 23](#)
- [Obtaining Additional Publications and Information, page 24](#)



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

# Introduction

Cisco 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, 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 adaptive security appliance software Version 7.2(2). Its secure, web-based design enables anytime, anywhere access to security appliances.

## New Device Manager Features

The following list highlights the new device manager features in this release:

- CSC/IPS password reset, which allows you to reset the default password to “cisco” if you forget your SSM password, has been added.
- Support for the following multicast commands has been added:
  - **mfib forwarding**
  - **multicast boundary**
  - **pim bidir-neighbor-filter**
  - **pim neighbor-filter**
  - **pim old-register-checksum**
- The authorization-dn attributes for tunnel-group have been changed.
- The device manager works when it is connected to a device in a local demo mode.
- Support for an authorization server group per interface has been added.
- Support for HTTP and HTTPS inline authentication has been added.

## New Security Appliance Features

This section lists some of the new features supported by the security appliance.

- For the ASA 5505 Plus License, an increase in VLAN interfaces from three to 25 and an increase in trunk ports from one to six have been made.
- For the ASA 5510 Base License, an increase in VLAN interfaces from ten to 50 and an increase in physical interfaces from 3+1 to 4+1 have been made.
- For the ASA 5510 Plus License, an increase in VLAN interfaces from 25 to 100 has been made.
- For the ASA 5520, an increase in VLAN interfaces from 100 to 150 has been made.
- For the ASA 5550, an increase in VLAN interfaces from 200 to 250 has been made.
- Cut-through-proxy for HTTP and HTTPS traffic has been reenabled.
- Changes to the BSAFE library have been made.
- FIPS recertification has been enabled.
- A new command, **hw-module module password-reset**, which allows you to reset the default password to “cisco” on the security appliance and enables password recovery, has been added.

- The **virtual http** command has been made available again.
- If you have an ASA 5510, 5520, or 5540, you can use a 4GE card.
- Some of the ASA 5500 series security appliance performance limits have been changed.
- A new command, **aaa authentication listener**, which allows you to configure authentication for HTTP and HTTPS traffic, has been added.

For additional information, see the online help for particular features. For improvements to the ASA 5500 series adaptive security appliance software, see the [Cisco ASA 5500 Series Release Notes Version 7.2\(2\)](#).

## Client PC Operating System and Browser Requirements

Table 1 lists the supported and recommended PC operating systems and browsers for Version 5.2(2).

**Table 1** Operating System and Browser Requirements

Operating System	Version	Browser	Other Requirements
Windows <sup>1</sup>	Windows 2000 (Service Pack 4), Windows XP (English or Japanese version), Windows 2003 Server (English or Japanese versions)	Internet Explorer 6.0 with Sun Java SE <sup>2</sup> Plug-in 1.4.2 or 5.0 (1.5.0) Firefox 1.5 with Java SE Plug-in 1.4.2 or 5.0 (1.5.0) <b>Note</b> <b>HTTP 1.1</b> —Settings for <b>Internet Options &gt; Advanced &gt; HTTP 1.1</b> should use HTTP 1.1 for both proxy and non-proxy connections.	<b>SSL Encryption Settings</b> —All available encryption options are enabled for SSL in the browser preferences.
Sun SPARC	Solaris 8 or Solaris 9	Mozilla Suite 1.7 with Java SE Plug-in 1.4.2 or 5.0 (1.5.0)	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 3 running GNOME or KDE	Firefox 1.5 with Java SE Plug-in 1.4.2 or 5.0 (1.5.0) <sup>3</sup>	

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

2. Obtain Sun Java from [java.sun.com](http://java.sun.com).

3. On Windows and Linux, Firefox 1.5 replaces Mozilla 1.7.3, which was used in previous ASDM releases.

### Memory Errors in Firefox

Firefox may stop responding or give an out of memory error message Linux and Windows if multiple instances of ASDM are running. You can use the following steps to increase the Java memory and work around the behavior.

This section describes how to increase the memory for Java on the following platforms:

- [Java Plug-In for Windows](#)
- [Java Plug-In on Linux](#)

## Java Plug-In for Windows

To change the memory settings of the Java Plug-in on Windows for Java Plug-in versions 1.4.2 and 1.5, perform the following steps:

- 
- Step 1** Close all instances of Internet Explorer or Netscape.
- Step 2** Click **Start > Settings > Control Panel**.
- Step 3** If you have Java Plug-in 1.4.2 installed:
- Click **Java Plug-in**. The Java Plug-in Control Panel appears.
  - Click the **Advanced** tab.
  - Type **-Xmx256m** in the Java RunTime Parameters field.
  - Click **Apply** and exit the Java Control Panel.
- Step 4** If you have Java Plug-in 1.5 installed:
- Click **Java**. The Java Control Panel appears.
  - Click the **Java** tab.
  - Click **View** under Java Applet Runtime Settings. The Java Runtime Settings Panel appears.
  - Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.
  - Click **OK** and exit the Java Control Panel.
- 

## Java Plug-In on Linux

To change the settings of Java Plug-in version 1.4.2 or 1.5 on Linux, perform the following steps:

- 
- Step 1** Close all instances of Netscape or Mozilla.
- Step 2** Open the Java Plug-in Control Panel by launching the Control Panel executable file.



**Note** In the Java 2 SDK, this file is located in SDK installation directory/jre/bin/ControlPanel. For example: if the Java 2 SDK is installed in /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel. In a Java 2 Runtime Environment installation, the file is located in JRE installation directory/bin/ControlPanel.

---

- Step 3** If you have Java Plug-in 1.4.2 installed:
- Click the **Advanced** tab.
  - Type **-Xmx256m** in the Java RunTime Parameters field.
  - Click **Apply** and close the Java Control Panel.
- Step 4** If you have Java Plug-in 1.5 installed:
- Click the **Java** tab.
  - Click **View** under Java Applet Runtime Settings.
  - Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.

- d. Click **OK** and exit the Java Control Panel.
- 

## Supported Platforms and Feature Licenses

This software version supports the following platforms:

- ASA 5505
- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- PIX 515/515E
- PIX 525
- PIX 535

For the feature license support of each model, see:

<http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/specs.html>

## ASDM and SSM Compatibility

For a table showing ASDM compatibility with SSMs, see:

<http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html>

## Upgrading ASDM

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

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



### Note

If you are upgrading from PIX Version 6.3, first upgrade to Version 7.0 according to *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*. Then upgrade PDM to ASDM according to the ASDM 5.0 release notes.

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.

In general, ASDM will maintain compatibility across minor versions (for example, ASDM 5.2.1 will work with ASA Versions 7.2.1 and 7.2.2, but ASDM Version 5.2.1 will not work with ASA Version 7.1.1), so you can upgrade the platform image using the new ASDM version.

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:
- In ASDM 5.0 and 5.1, click **Upload Image from Local PC**.
  - In ASDM 5.2, click **Upgrade Software**.
- Step 4** With ASDM selected, click **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 click **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 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, the following message appears:
- “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 > Properties > Device Administration > Boot System/Configuration** pane.
- Step 8** To run the new ASDM image, you must exit ASDM and reconnect.
- Step 9** Download the new platform image using the **Tools > Upgrade Software** tool.
- To reload the new image, reload the security appliance using the **Tools > System Reload** tool.
- 

## Getting Started with ASDM

This section describes how to connect to ASDM and start your configuration. If you are using the security appliance for the first time, your security appliance might include a default configuration. You can connect to a default IP address with ASDM so that you can immediately start to configure the security appliance from ASDM. If your platform does not support a default configuration, you can log in to the CLI and run the **setup** command to establish connectivity. See [Before You Begin](#) for more detailed information about networking.

This section includes the following topics:

- [Before You Begin, page 7](#)
- [Downloading the ASDM Launcher, page 7](#)
- [Starting ASDM from the ASDM Launcher, page 8](#)
- [Using ASDM in Demo Mode, page 8](#)
- [Starting ASDM from a Web Browser, page 10](#)
- [Using the Startup Wizard, page 10](#)
- [Using the VPN Wizard, page 11](#)

- [Configuring Stateful Failover, page 11](#)
- [Printing from ASDM, page 13](#)

## Before You Begin

If your security appliance includes a factory default configuration, you can connect to the default management address of 192.168.1.1 with ASDM. On the ASA 5500 series adaptive security appliance, the interface to which you connect with ASDM is Management 0/0. For the PIX 500 series security appliance, the interface to which you connect with ASDM is Ethernet 1. To restore the default configuration, enter the **configure factory-default** command at the security appliance CLI.

Make sure the PC is on the same network as the security appliance. You can use DHCP on the client to obtain an IP address from the security appliance, or you can set the IP address to a 192.168.1.0/24 network address.

If your platform does not support the factory default configuration, or you want to add to an existing configuration to make it accessible for ASDM, access the security appliance CLI according to the [Cisco Security Appliance Command Line Configuration Guide](#), and enter the **setup** command. The **setup** command prompts you for a minimal configuration to connect to the security appliance using ASDM.



### Note

You must have an inside interface already configured to use the **setup** command. The Cisco PIX security appliance default configuration includes an inside interface, but the Cisco ASA adaptive security appliance default configuration does not. Before using the **setup** command, enter the **interface gigabitethernet slot/port** command, and then the **nameif inside** command. The *slot* for interfaces that are built in to the chassis is **0**. For example, enter **interface gigabitethernet 0/1**. The Cisco PIX 500 series and the ASA 5510 adaptive security appliance have an Ethernet-type interface.

## Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher is an improvement over running ASDM in a Java Applet, because you can avoid double authentication and certificate dialog boxes, the application 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. Leave the name and password blank (default).

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 the file 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 launch 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.

## Using ASDM in Demo Mode

ASDM Demo Mode is available as a separately installed application running Windows. This mode makes use of the ASDM Launcher and pre-packaged configuration files to let you run ASDM without having a live device available. ASDM Demo Mode lets you do the following:

- Perform configuration and select monitoring tasks via ASDM as though you were interacting with an actual device.
- Demonstrate ASDM or security appliance features using the ASDM interface.
- Perform configuration and monitoring tasks with the Content Security and Control (CSC) SSM.

ASDM Demo Mode provides simulated monitoring data, including real-time system log messages. The data shown is randomly generated, but the experience is identical to what you would see when connecting to an actual device.

ASDM Demo Mode has the following limitations:

- Changes made to the configuration will appear in the GUI, but are not applied to the configuration file. That is, when you click **Refresh**, the GUI will revert to the original configuration. The changes are never saved to the configuration file.
- File and disk operations are not supported.
- Monitoring and logging data are simulated. Historical monitoring data is not available.
- You can only log in as an admin user; you cannot log in as a monitor-only or read-only user.
- Demo Mode does not support the following features:
  - File menu:
    - Save Running Configuration to Flash
    - Save Running Configuration to TFTP Server
    - Save Running Configuration to Standby Unit

- Save Internal Log Buffer to Flash
- Clear Internal Log Buffer
- Tools menu:
  - Command Line Interface
  - Ping
  - File Management
  - Update Image
  - File Transfer
  - Upload image from Local PC
  - System Reload
- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Failover—Configuring a standby device
- These operations cause a reread of the configuration and therefore will revert the configuration to the original settings.
  - Switching contexts
  - Making changes in the Interface panel
  - NAT panel changes
  - Clock panel changes

To run ASDM in Demo Mode, perform the following steps:

- 
- Step 1** If you have not yet installed the Demo Mode application, perform the following steps:
- a. Download the ASDM Demo Mode installer, `asdm-demo-version.msi`, from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
  - b. Double-click the `asdm-demo-version.msi` file to install the software.
- Step 2** Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or access it from the **Start** menu.
- Step 3** Check **Run in Demo Mode**.
- Step 4** To set the platform, context and firewall modes, and ASDM Version, click **Demo** and make your selections from the Demo Mode area.
- Step 5** To use new ASDM images as they come out, you can either download the latest installer or the normal ASDM images and install them for Demo Mode:
- a. Download the image file, `asdm-version.bin`, from the download page (see [Step 1](#)).
  - b. In the Demo Mode area, click **Install ASDM Image**.  
A file browser appears. Find the ASDM image file in the browser.
- Step 6** Click **OK** to launch ASDM in Demo Mode.  
A Demo Mode label appears in the title bar of the window.
-

## 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. Leave the name and password blank (default).

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 configure a single mode security appliance or a context in multiple context mode.

To use the Startup Wizard to configure the security appliance, perform the following steps:

---

**Step 1** Launch the wizard according to the steps for the correct security context mode.

- In single context mode, choose **Wizards > Startup Wizard**.
- In multiple context mode, for each new context, perform the following steps:
  - a. Choose **System > Configuration > Security Context**.
  - 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 **System/Contexts** icon on the toolbar, and choose the context name.
  - e. Choose **Wizards > Startup Wizard**.

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

**Step 3** Click **Finish** on the last pane to send the configuration to the security appliance.

**Step 4** If the IP address of the connection changes, reconnect to ASDM using the new IP address.

- Step 5** Enter other configuration details on the **Configuration** panes.
- 

## Using the VPN Wizard

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

To use the VPN Wizard to configure VPN, perform the following steps:

- 
- Step 1** Click **Wizards > VPN Wizard**.
- Step 2** Supply information on each wizard screen. Click **Next** to move through the VPN Wizard screens. You may use the default IPSec and IKE policies. Click **Help** for more information about each field.
- Step 3** After you complete the VPN Wizard, click **Finish** on the last screen to send the configuration to the security appliance.
- 

## Configuring Stateful Failover

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

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



**Tip**

If your security appliances are located near each other, you might prefer to connect them with a serial cable instead of via the LAN. Although a serial connection is slower than a LAN connection, using a cable obviates the need for an interface or for the LAN and Stateful Failover to 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 that ASDM connects through on the primary and secondary devices. These IP addresses must be assigned to device interfaces with HTTPS access.

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

- 
- Step 1** Configure the secondary device for HTTPS IP connectivity. See the section [Before You Begin, page 7](#), and use a different IP address on the same network as the primary device.
- Step 2** Connect the pair of devices together and to their networks in their Stateful Failover LAN cable configuration.
- Step 3** Start ASDM from the primary device through a supported web browser. See the section [Downloading the ASDM Launcher, page 7](#).
- Step 4** Perform one of the following steps, depending on the context mode:

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

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

- If your device is in routed mode, configure standby addresses for all routed mode interfaces.
- If your device is in transparent mode, configure a standby management IP address.



**Note**

Interfaces used for failover connectivity should not have names (in single mode) or be allocated to security contexts (in multiple security context mode). In multiple context mode, other security contexts may also have standby IP addresses configured.

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

- If your device is in multiple security context mode, choose **System > Configuration > Failover**.
- If your device is in single mode, choose **Configuration > Properties > Failover**.

**Step 7** On the **Setup** tab of the **Failover** pane under **LAN Failover**, select the interface that is cabled for LAN Stateful Failover.

**Step 8** Configure the remaining LAN Failover fields.

**Step 9** (Optional) Provide information for other fields in all of the failover tabs. If you are configuring Active/Active failover, you must configure failover groups in multiple security context mode. If more than one failover pair of devices coexists on a LAN in Active/Active Stateful Failover, provide failover-group MAC addresses for any interfaces on shared LAN networks.

**Step 10** On the **Setup** tab, check **Enable Failover**. If you are using the PIX 500 series security appliance, check **Enable LAN rather than serial cable failover**.

**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 the configuration to be synchronized to the standby device over the failover LAN connection.

The secondary device should 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.

## Reenabling Stateful Failover and Securing the Failover Key

To prevent the failover key from being replicated to the peer unit in clear text for an existing failover configuration, perform the following steps:

**Step 1** Disable failover on the active unit (or in the system execution space on the unit that has failover group 1 in the active state).

**Step 2** Enter the failover key on both units.

- Step 3** Reenable failover.  
When Stateful Failover is reenabled, the failover communication is encrypted with the key.
- 

To secure the failover key on the active device, perform the following steps:

---

- Step 1** Perform one of the following steps, according to the security context mode:
- a. If your device is in single mode, choose **Configuration > Properties > Failover > Setup**.
  - b. If your device is in multiple mode, choose **System > Configuration > 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** field.
- 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. Although the standby peer does not have the shared failover key, the standby peer still could become inaccessible.
- Step 6** Click **OK**. Wait for the 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. There is a known caveat ([CSCse15764](#)) for printing from Windows XP that causes printing to be extremely slow.

---

ASDM supports printing for the following features:

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

# ASDM Limitations

This section describes ASDM limitations, and includes the following:

- [Unsupported Commands](#), page 14
- [One-Time Password Not Supported](#), page 14
- [Interactive User Commands Not Supported in ASDM CLI Tool](#), page 15
- [Unsupported Characters](#), page 16

## 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 the configuration.

## One-Time Password Not Supported

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

## 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, choose **Options > Show Commands Ignored by ASDM on Device**.
- If ASDM loads an existing running configuration and reads the **alias** command, it enters Monitor-only mode.

Monitor-only mode allows access to the following functions:

- The Monitoring area
- The CLI tool (choose **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. For more information, see the [Cisco Security Appliance Command Reference](#).



### Note

You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to three by your system administrator, which allows Monitor-only mode. For more information, choose **Configuration > Properties > Device Administration > User Accounts and Configuration > Properties > Device Administration > AAA Access**.

## Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when you add them through the CLI, but that you cannot add or edit in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If the command is view-only, then it 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>capture</b>	Ignored
<b>established</b>	Ignored
<b>failover timeout</b>	Ignored
<b>ipv6</b> , any IPv6 addresses	Ignored
<b>pager</b>	Ignored
<b>pim accept-register route-map</b>	Ignored. You can only configure the <b>list</b> option using ASDM.
<b>prefix-list</b>	Ignored if not used in an OSPF area
<b>route-map</b>	Ignored
<b>service-policy global</b>	Ignored if it uses a <b>match access-list</b> class. For example: <pre>access-list myacl line 1 extended permit ip any any class-map mycm match access-list mycl policy-map mypm class mycm inspect ftp service-policy mypm global</pre>
<b>sysopt nodnsalias</b>	Ignored
<b>sysopt uauth allow-http-cache</b>	Ignored
<b>terminal</b>	Ignored
<b>virtual</b>	Ignored

## 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
```

## Interactive User Commands Not Supported in ASDM CLI Tool

The ASDM CLI tool does not support interactive user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter “Yes” or “No,” but does not recognize your input. ASDM then times out waiting for your response.

For example:

- From the ASDM Tools menu, click **Command Line Interface**.
- Enter the `crypto key generate rsa` command.

ASDM generates the default 1024-bit RSA key.

3. Reenter the **crypto key generate rsa** command.

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 through ASDM.
- For CLI commands that have a **noconfirm** option, use this option when entering the CLI command. For example:

```
crypto key generate rsa noconfirm
```

## 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 a language other than English, be careful not to enter non-English characters accidentally.

*Workaround:*

For workarounds, see CSCeh39437 under [Caveats, page 16](#).

## Caveats

The following sections describe caveats for the Version 5.2(2) release.

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

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling and typographical errors 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](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 5.2(2)

**Table 2** Open Caveats

ID Number	Caveat Title
CSCeh39437	ASDM: Non-English characters do not display properly in some screens.
CSCsd75599	Modifying a shared extended ACL should warn user of sharing implications.
CSCse07045	Service policy classes not listed in same order as the CLI.
CSCse15764	ASDM: File > Print very slow to execute.
CSCse15764	ASDM: File > Print very slow to execute.
CSCse23663	Status window and command preview window pop up at same time on Linux.
CSCse24255	Help does not exist for EZVPN Advanced Tab and screen.
CSCse30268	ASDM does not show WebVPN historical graph for active sessions.
CSCse43201	HTTP map Advanced View Inspection Tab causes error.
CSCse52465	File transfer dialog box goes behind File Management window.
CSCse53604	ASDM is not detecting FTP inspection disabled scenario.
CSCse54801	ASDM hard codes some colors instead of using system defaults.
CSCse74616	HAS Wizard, Load Balancing: Wrong error order.
CSCse74662	HAS Wizard: Cancelling multi-mode change causes ASDM to quit.
CSCse81738	ASDM 5.2 performance very slow when ASDM system log message severity level is 6 or 7.
CSCse93458	Existing network object group name for service group is allowed.
CSCsf05395	Error in configuring aaa authentication include.
CSCsf10418	Inactivity/absolute time of aaa is not shown in monitoring.
CSCsf16560	File Management: Cut and Paste Flash file hangs the dialog box.
CSCsf16770	Adding a tunnel group with text in L2L VPN is allowed without warning.
CSCsf18287	POST error message occurs due to deprecated authentication-server-group none.
CSCsf18305	Wrong CLI generation in dynamic crypto map, IPSec rules panel.
CSCsf19100	No error message when upload ASDM Assistant Guide with invalid XML file.
CSCsf26114	Deleting an IP pool, coupled with group policy, is allowed by ASDM.
CSCsf26202	Deleting VPN > IP pool is allowed by device when no client is connected.
CSCsf27282	Spaces are accepted in the Easy VPN Remote panel.
CSCsf27289	Enabling EasyVPN generates POST error message.
CSCsf28179	Name string/URL list is not displayed correctly from ASDM after clicking Apply.
CSCsf28671	Changing DHCP server to DHCP client produces a POST warning message.

**Table 2** *Open Caveats (continued)*

<b>ID Number</b>	<b>Caveat Title</b>
CSCsf32361	MPF: Direction check box in policy should not have input value.
CSCsf32406	MPF: Protocol inspection should be disabled when tunnel group is enabled.
CSCsf32419	MPF: Enabling priority action without a priority queue is allowed by ASDM.
CSCsf32438	MPF: A warning message appears even after a priority queue is configured.
CSCsf32446	Wrong CLI generation in MPF, while editing a service policy.
CSCsg16688	ASDM hangs at 56% when switching from context to no configuration context.
CSCsg17928	Multiple mode: Non-Flash options are available for an admin context.
CSCsg17959	Multiple mode: Commands ignored by the device are shown as POST error messages.
CSCsg60594	Startup Wizard Auto Update screen not seeing changes.
CSCsg64625	5505 Startup Wizard PPPoE Finish button enabled in error.
CSCsg68119	Monitoring/Routing/RIP Type is set to blank for RIP/Conn/Static.
CSCsg68303	Boot system: ASDM allows more than four boot entries.
CSCsg68633	HAS Wizard confusing intro message on standby IP page.
CSCsg69530	Help for Gateways and Call Agents panel is not present.
CSCsg70068	Displays wrong associated VLANs information on trunk port.
CSCsg71143	Reset in VPN > IPsec Rules panel is not working correctly.
CSCsg71164	POST error message occurs in service group due to looping of service groups.
CSCsg71825	Network Object Groups should be removed from browser real address.
CSCsg73174	ASDM: "Page not found" error occurs when Help button selected for EZVPN Con stat.
CSCsg73576	5505: Step 8 of Startup Wizard needs return character.
CSCsg73712	Startup Wizard: Information window needs updated 5.2.2 logo.
CSCsg76794	Last 30-day counter is not updating correctly.
CSCsg76796	Interactive authentication subpanel note needs to be reworded.

## Resolved Caveats - Release 5.2(2)

The following list shows caveats that are resolved for Version 5.2(2):

**Table 3** *Resolved Caveats*

<b>ID Number</b>	<b>Caveat Title</b>
CSCsd54213	Errors in connectivity compatibility status initial display.
CSCsd54227	Test compatibility button should include connectivity too.
CSCsd55728	Add Network Object Group produces duplicates in existing address list.
CSCsd69687	Last line in General/License panels on home page cut off.
CSCsd79930	Startup Wizard, EZVPN Remote Configuration changes.
CSCsd93317	Some multicast commands are not supported by ASDM.

**Table 3** *Resolved Caveats (continued)*

<b>ID Number</b>	<b>Caveat Title</b>
CSCse02013	Cannot delete failover group 2 if it is in the first row of the table.
CSCse09942	Appears that NAT exemption rules have other NAT options when they do not.
CSCse12571	Need to adjust page sequence number display for HAS Wizard.
CSCse13173	Startup Wizard has box for same interface traffic in transparent modes.
CSCse16117	ACE Edit dialog box when expanded does not expand the Description field.
CSCse16317	Remove Apply and Reset buttons on Configuration Properties HAS Wizard page.
CSCse16931	HAS Wizard Progress dialog box covers up Wizard page.
CSCse17991	Unable to delete filter rule with 0.0.0.0 and no default subnet mask.
CSCse19764	ASDM gives error when setting poll rate with retry count in Auto Update.
CSCse25002	HAS Wizard does not catch same active/standby IP for fail and state links.
CSCse25053	HAS Wizard change peer to multi mode message always says A/A failover.
CSCse25997	HAS Wizard send failover reset unnecessarily for A/A failover.
CSCse26186	ESMTP match on body or header length greater than 4294967295 cannot be configured.
CSCse26411	DNS Type Value controls not disabled when Multiple Matches selected.
CSCse26414	HAS Wizard does not catch ASDM version mismatch.
CSCse27198	Esp and gre appear twice in protocols list under Services Tab.
CSCse27235	IM match warning for voice-chat not suppressed during delivery.
CSCse27259	RADIUS Accounting Attribute No. list clipped in Other Parameters tab.
CSCse30073	Pasting after in-filter rules does not work.
CSCse30432	RIP routes is displaying route time in the interface field.
CSCse30449	ASDM Launcher user authentication fails first time.
CSCse32399	Apply button enabled after Save in any rules table with no changes made.
CSCse33796	VPN Monitoring Sessions: Peer IP not filled in when using VPN Server name.
CSCse33814	SIP map: if log-only action configured, does not show for some field commands.
CSCse33948	Startup Wizard does not recognize or save PPPoE IP address setting.
CSCse34044	Startup Wizard cannot configure or read static route monitoring options.
CSCse35416	HAS Wizard command summary shows wrong state interface for same failover-state link.
CSCse38624	Exception thrown in monitor-only access on ASA 5505.
CSCse41659	ASDM needs to change order of mode change commands; otherwise, traffic is blocked.
CSCse45560	Showing details in Monitor > VPN Statistics > Sessions corrupts popup menu.
CSCse47359	Change authorization-dn-attributes for tunnel-group.
CSCse47360	Provide a link to launch IDM in separate browser if IPS release is lower than 6.0.
CSCse55963	Password created with 13 or more characters in ASDM does not work.
CSCse57451	Unable to create a static NAT using the interface IP.
CSCse59099	Subject Alternate Name need to be correctly identified.
CSCse60278	LDAP-attribute map-value should be allowed with spaces if quote delimited.

**Table 3** *Resolved Caveats (continued)*

ID Number	Caveat Title
CSCse61460	Category trees are not accessible via keyboard.
CSCse67889	Use system fonts.
CSCse68161	ASDM will not show VPN statistics for tunnel groups with spaces in name.
CSCse68285	CSC home page should not show scroll bar by default.
CSCse71477	CSC CPU and node counters are not displayed correctly on Japanese OS.
CSCse74566	ASDM places certain match criteria under wrong match rule.
CSCse81766	Table Sort Order function on ASDM 5.2 not working.
CSCse86318	Wrong delta when changing ACE order.
CSCse88692	IPS screen is empty in unsupported scenarios.

## 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*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*

## Obtaining Documentation

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

### Cisco.com

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

<http://www.cisco.com>

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>

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 the “Related Documentation” section.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.