



Cisco ASDM Release Notes Version 5.2(3)

August 2007

This document contains release information for Cisco ASDM Version 5.2(3) on Cisco PIX 500 series security appliance and Cisco ASA 5500 series adaptive security appliance Version 7.2(3). It includes the following sections:

- [Introduction, page 1](#)
- [New Device Manager Features for Version 5.2\(3\), 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 13](#)
- [Caveats, page 16](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 20](#)

Introduction

Cisco ASDM delivers world-class security management and monitoring services for Cisco PIX 500 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 series security appliance and Cisco ASA 5500 series adaptive security appliance software Version 7.2(3). Its secure, web-based design enables anytime, anywhere access to security appliances.



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

© 2007 Cisco Systems, Inc. All rights reserved.

New Device Manager Features for Version 5.2(3)

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



Note

These features are supported only if you are using ASA/PIX Version 7.2(3), unless otherwise noted.

- Added an option to enable or disable DNS guard. When enabled, this feature allows only one DNS response back from a DNS request. In ASDM, see Configuration > Properties > DNS > DNS Client.
- Added option to send either the fully qualified domain name (FQDN) or the IP address to the client in a VPN load balancing cluster. In ASDM, see Configuration > VPN > Load Balancing.
- Added support in Client Software Location list to allow client updates from Linux or Mac systems. In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Upload Software > Client Software.
- Added new check box Cache Static Content to allow users to cache the static content. In ASDM, see Configuration > VPN > WebVPN > Cache.
- Added two new items for the DHCP client. The first option configures DHCP Option 61 to send either the MAC or the string "cisco-<MAC>-<interface>-<hostname>" where < > represents the corresponding values as the client identifier. The second option either sets or clears the broadcast flag for DHCP discover when the DHCP request has the broadcast flag enabled.
- With the Cisco Content Security and Control (CSC) 6.2 software, ASDM provides events and statistics for the new Damage Cleanup Services (DCS) feature. DCS removes malware from clients and servers and repairs system registries and memory.
- The ASA/PIX 7.2(3) software supports an ASDM banner. If configured, when you start ASDM, this banner text will appear in a dialog with the option to continue or disconnect. In ASDM, see Configuration > Properties > Device Administration > Banner.
- Added option for ESMTP inspection to work over Transport Layer Security (TLS). In ASDM, see Configuration Global Objects > Inspect Maps > ESMTP.
- Added support for Wide Area Application Services (WAAS) inspection. WAAS gives branch and remote offices LAN-like access to WAN and MAN services. In ASDM, see Configuration > Security Policy, Service Policy Rules tab.
- Added option in the VPN group policy to specify whether tunnels stay connected or not when the Smart Card is removed. Previously, the tunnels were always disconnected.

New Security Appliance Features

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

- Smart Card Removal Disconnect—this feature allows the central site administrator to configure remote client policy for deleting active tunnels when a Smart Card is removed.
- capture Command Enhancement—the **capture** command allows the user to capture traffic and display it in real time.
- Support for ESMTP over TLS—this enhancement adds the configuration parameter allow-tls [action log] in the **esmtppolicymap** command.
- WAAS and PIX Interoperability—the **[no] inspect waas** command is added to enable WAAS inspection.

- For ASA 5510 adaptive security appliance has the Security Plus license to enable GE for port 0 and 1.
- For ASA 5505 adaptive security appliance supports VLAN IDs between 1 and 4090. Earlier, only VLAN IDs between 1 and 1001 were supported.

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\(3\)](#).

Client PC Operating System and Browser Requirements

Table 1 lists the supported and recommended PC operating systems and browsers for Version 5.2(3).

Table 1 Operating System and Browser Requirements

Operating System	Version	Browser	Other Requirements
Windows	Windows Vista, Windows XP, Windows 2000 (Service Pack 4 or higher), Windows 2003 Server (English or Japanese versions)	Internet Explorer 6.0 with Sun Java SE ¹ 1.4.2, 5.0 , and 6. Firefox 1.5 or 2.0 or Internet Explorer 6.0 or 7.0 Note HTTP 1.1 —Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections.	SSL Encryption Settings —All available encryption options are enabled for SSL in the browser preferences.
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 4	Firefox 1.5 or 2.0 Java SE 1.4.2, 5.0, or 6	

1. Obtain Sun Java from java.sun.com.

Memory Errors in Firefox

Firefox may stop responding or give an out of memory error message in 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 for Windows](#)
- [Java on Linux](#)

Java for Windows

To change the memory settings of the Java on Windows for Java versions 1.4.2 and 5.0, perform the following steps:

-
- Step 1** Close all instances of Internet Explorer or Netscape.
- Step 2** Click **Start > Settings > Control Pane**.

- Step 3** If you have Java 1.4.2 installed:
- Click **Java Plug-in**. The Java Control pane appears.
 - Click the **Advanced** tab.
 - Type **-Xmx256m** in the Java RunTime Parameters field.
 - Click **Apply** and exit the Java Control pane.
- Step 4** If you have Java 5.0 installed:
- Click **Java**. The Java Control pane appears.
 - Click the **Java** tab.
 - Click **View** under Java Applet Runtime Settings. The Java Runtime Settings pane appears.
 - Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.
 - Click **OK** and exit the Java Control pane.
- Step 5** If you have Java 6 installed:
- Click **Java**. The Java Control pane appears.
 - Click the **Java** tab.
 - Click **View** under Java Applet Runtime Settings. The Java Runtime Settings pane appears.
 - Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.
 - Click **OK** and exit the Java Control pane.

Java on Linux

To change the settings of Java version 1.4.2 or 5.0 on Linux, perform the following steps:

- Step 1** Close all instances of Firefox.
- Step 2** Open the Java Control pane by launching the Control pane executable file.



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

- Step 3** If you have Java 1.4.2 installed:
- Click the **Advanced** tab.
 - Type **-Xmx256m** in the Java RunTime Parameters field.
 - Click **Apply** and close the Java Control pane.
- Step 4** If you have Java 5.0 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 pane.
-

Supported Platforms and Feature Licenses

For information on supported platforms and feature licenses, see:

- Cisco ASA 5500 series adaptive security appliance
<http://www.cisco.com/en/US/docs/security/asa/asa72/release/notes/asarn723.html>
- Cisco PIX 500 series security appliance
<http://www.cisco.com/en/US/docs/security/pix/pix72/release/notes/pixrn723.html>

ASDM and SSM Compatibility

For a table showing ASDM compatibility with SSMs, see:

<http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.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 adaptive 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. You cannot use a previous version of 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** On the Tools menu:
 - a. In ASDM 5.0 and 5.1, click **Upload Image from Local PC**.
 - b. 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 adaptive 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 adaptive security appliance to load the new image in the **Configuration > Properties > Device Administration > Boot System/Configuration** pane.

Step 8 Similar to ASDM, you need to do the same for the ASA/PIX image. Repeat steps 1, 3, 4, 5, 6 and 7 for the ASA/PIX image. Then go to Tools > System Reload and be sure to enable "Save the running configuration at time of reload" before clicking the "Schedule Reload" button.

Getting Started with ASDM

This section describes how to connect to ASDM and start your configuration. If you are using the adaptive security appliance for the first time, your adaptive 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 adaptive 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 6](#)
- [Downloading the ASDM Launcher, page 7](#)
- [Starting ASDM from the ASDM Launcher, page 7](#)
- [Using ASDM in Demo Mode, page 8](#)
- [Starting ASDM from a Web Browser, page 9](#)
- [Using the Startup Wizard, page 10](#)
- [Using the VPN Wizard, page 10](#)
- [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 Cisco 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 adaptive security appliance CLI.

Make sure the PC is on the same network as the adaptive security appliance. You can use DHCP on the client to obtain an IP address from the adaptive 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 adaptive 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 adaptive security appliance using ASDM.

**Note**

You must have an inside interface already configured to use the **setup** command. The Cisco PIX 500 series 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 security appliance 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 adaptive 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 adaptive 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 adaptive 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 adaptive 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 pane
 - NAT pane changes
 - Clock pane 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** 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 adaptive 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.
- 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 adaptive security appliance or a context in multiple context mode.

To use the Startup Wizard to configure the adaptive 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** in the last pane to send the configuration to the adaptive 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 in 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 adaptive 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 in 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** in the last screen to send the configuration to the adaptive security appliance.
-

Configuring Stateful Failover

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

If you are connecting two adaptive security appliance for failover, you must connect them via a LAN. If you are connecting two adaptive security appliance, 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 6](#), 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:
- a. If your device is in multiple security context mode, choose **System > Configuration > Failover**.
 - b. If your device is in single mode, choose **Configuration > Properties > Failover**.
- Step 7** In 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** In 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 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 in 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:
- If your device is in single mode, choose **Configuration > Properties > Failover > Setup**.
 - 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.
- Uncheck the **Enable failover** check box.
 - Click **Apply**. (Click **OK** if CLI preview is enabled.)
- Step 3** Enter the failover key in the **Shared Key** field.
- Step 4** Reenable failover.
- Check the **Enable failover** check box.
 - 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 13](#)
- [One-Time Password Not Supported, page 13](#)
- [Interactive User Commands Not Supported in ASDM CLI Tool, page 15](#)

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 adaptive 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
access-list	Ignored if not used, except for use in VPN group policy screens
capture	Ignored
established	Ignored
failover timeout	Ignored
ipv6 , any IPv6 addresses	Ignored
pager	Ignored
pim accept-register route-map	Ignored. You can only configure the list option using ASDM.
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored
service-policy global	Ignored if it uses a match access-list class. For example: <pre>access-list myacl line 1 extended permit ip any any class-map mycm match access-list myacl policy-map mypm class mycm inspect ftp service-policy mypm global</pre>
sysopt nodnsalias	Ignored

Unsupported Commands	ASDM Behavior (continued)
<code>sysopt uauth allow-http-cache</code>	Ignored
<code>terminal</code>	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, Tools > Command Line Interface, 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.
- 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
```

Caveats

The following sections describe caveats for Version 5.2(3).

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

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

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

Open Caveats - Version 5.2(3)

Table 2 lists the open caveats for Version 5.2(3):

Table 2 *Open Caveats*

ID Number	Caveat Title
CSCsd75599	Modifying a shared extended ACL should warn user of sharing implications
CSCse07045	Service policy classes not listed in same order as the CLI
CSCse23663	Status window and command preview window pop up at same time on Linux
CSCse43201	HTTP map advanced view inspection tab causes error
CSCse53604	ASDM is not detecting FTP inspection not enabled scenario
CSCse74616	HAS Wizard, Load Balancing: Wrong error order
CSCse74662	HAS Wizard: Cancelling multi-mode change cause ASDM to quit
CSCse81738	ASDM 5.2 performance very slow when ASDM syslog level is 6 or 7
CSCse93458	Existing network object group name for service group is allowed.
CSCsf05395	Error in configuring aaa authentication include
CSCsf18305	Wrong cli generation in dynamic crypto map, IPSec rules panel
CSCsf28179	Name string/URL list is not displayed correctly from ASDM after 'Apply'
CSCsg64625	5505 Startup Wizard PPPoE finish button enabled in error
CSCsg71825	Network Object Groups should be removed from browse real address
CSCsg82384	Global Policy ACL cannot be added to like interface policy acl

Table 2 *Open Caveats (continued)*

ID Number	Caveat Title
CSCsh16092	ASDM 5.2(2) not generating correct error for wrong CSC password
CSCsh24222	Multiple networks cannot be defined in the ASDM VPN wizard
CSCsh39808	PFS group 2 added in ASDM VPN Wizard - no option to remove
CSCsh84513	Add/Edit Regex Class Map - wrong topic ID
CSCsi65804	CSC SSM failed to login through ASDM
CSCsj61215	display incorrect Interface Status on active secondary unit
CSCsj61309	Routing/Static: Editing metric value - one failure case
CSCsj61586	Hit return in single line of Command Line Interface closes the window
CSCsj70866	Packet-tracer: change default value of icmp identifier to non-zero
CSCsj74335	ASDM: trustpoint fields become editable after clicking New
CSCsj81132	refresh function for "show wccp web hash" is not working
CSCsj85297	Cannot set sla mon timeout to greater than 60000
CSCsj90600	Obj-gp:Exception when delete obj-gp which associated with ACL w/o AG
CSCsj90833	PPPoE:When switch from Specify to Obtain address, asdm sends the addr
CSCsj96262	Startup Wiz:When switch from static IP to PPPoE, sends ip addr also

Resolved Caveats - Version 5.2(3)

Table 3 lists the resolved caveats for Version 5.2(3):

Table 3 *Resolved Caveats*

ID Number	Caveat Title
CSCsb90798	Time Set is off on the main page graphs.
CSCse26266	RIP/Default Setup: Deletion of default-info originate has some issues
CSCse85179	ASDM:hide LDAP aaa-server Login DN Password
CSCsf10418	Inactivity/absolute time of aaa is not shown in Monitoring.
CSCsf16560	File Management: Cut and Paste flash file hangs the dailog
CSCsf18287	Post error message due to deprecated authentication-server-group none
CSCsf32361	MPF: Direction check box in Police should't have input value
CSCsf32446	Wrong CLI Generation in MPF, while editing a service policy.
CSCsg16688	ASDM hangs at 56%: switching from context to no configuration context
CSCsg29740	ASDM should not allow non-ascii chars to be entered into desc
CSCsg40595	ASDM unable to show already configured rule actions/connection settings
CSCsg47138	ASDM Configuration of DHCP Option 2 Will not accept values > 0xFFFF
CSCsg47162	ASDM will not take a DHCP option 2 hex value greater than 0xFFFF
CSCsg48207	'Hardware' shows different in 'show version' between like devices.

Table 3 **Resolved Caveats (continued)**

ID Number	Caveat Title
CSCsg68119	Monitoring/Routing/RIP Type is set to blank for RIP/Conn/Static
CSCsg68633	HAS wizard confusing intro message on standby IP page
CSCsg69530	Help for Gateways and Call Agents panel is not present
CSCsg71388	HTTP server enable command incorrect in multiple mode
CSCsg76794	Last 30 day counter is not updating correctly
CSCsg76796	Interactive authentication sub-panel note needs to be reworded.
CSCsg78913	Clock: timezone modifications have caused regression
CSCsg80019	Unable to Add/modify/delete limits set to default class from ASDM
CSCsg80675	ASDM: Authorization-DN Email attribute incorrectly set as DNQ attribute
CSCsg80846	ASDM fails to remove certian DHCP options (2 and 15)
CSCsg81046	ASDM fails to show DHCP Options that were configured via the CLI
CSCsg87965	Enable password set incorrectly
CSCsg92142	The authorization tab for the vpn tunnel groups is blank
CSCsg97395	ASDM Err Management interface cannot be the lowest security interface
CSCsh18165	HAS wizard complains VPN-3DES-AES license incompatible incorrectly
CSCsh27751	Network Reputation Service (NRS) Messages Are Not Displayed in ASDM
CSCsh30718	ASDM: Add new user fails when modifying VPN Group Policy
CSCsh33301	Font used to display DHCP option Information is hard to read
CSCsh38434	'clear configure crypto map' cmd not sent if IPSec rule deleted in ASDM
CSCsh40144	SSM Password Recovery is missing under System > Tools in 5.2(2)
CSCsh40324	ASDM: second certificate prompt seen when using client cert authenticati
CSCsh56326	Need asdm support of redirect-fqdn cli
CSCsh58108	Unable to create custom time range in ASDM
CSCsh60259	ASDM 5.2.2 HAS wizard reports license mismatch
CSCsh62831	Default for WebVPN Cache on7.1/7.2 should be 'disabled'
CSCsh66442	VPN wiz not creating static tunnel if last entry is dynamic vpn tunnel
CSCsh74700	ASDM not updating correctly DefaultRAGroup authentication ppp-attributes
CSCsh75120	HAS Wizard check compatibilty may fail with -K8 string in PID
CSCsh85087	ASDM - Getting Events Connection Started events
CSCsh86539	Feature search for IPS is wrong
CSCsh97080	Unable to login to CSC module when using Java version 1.6.0
CSCsi10406	ASDM - a page to configure PPPoE info is missing on Startup Wizard
CSCsi26290	Unable to delete activex/java filter rules after adding duplicate entrie
CSCsi43650	ASDM: add configuration check for WebVPN memory size config
CSCsi43660	ASDM error when adding SNMP server
CSCsi58878	Change the allowed VLAN range on an ASA 5505

Table 3 **Resolved Caveats (continued)**

ID Number	Caveat Title
CSCsi61378	ASDM: comma cannot be used in certificate parameters
CSCsi61555	VPN wizard to create RA makes incorrect ACLs and NATs for NAT exemption.
CSCsi64723	ASDM: cannot select existing class-map in service-policy
CSCsi71458	JRE 6.0 shows ASDM signed jar certificate as expired
CSCsi82833	HAS wizard does not send vlan command when fail links are subinterfaces
CSCsi87860	ASDM is missing Linux and Mac support for client update
CSCsi88121	IPSec VPN Wizard: cannot add Site-to-Site if Remote Access is configured
CSCsj01003	New cache static content parameter added to webVPN cache
CSCsj22131	Support new dhcp-client options in ASA 7.2(3)
CSCsj36806	ASDM 5.0 does not allow spaces in group-policy names
CSCsj37968	DHCP server issues
CSCsj40666	ASDM: no control for configuring vpn load-balancing trustpoint
CSCsj41931	Implement ASDM banner
CSCsj45755	CSC ASDM not reporting Damage Cleanup Services events and statistics
CSCsj50266	ASDM stop at loading current configuration while there is regexp
CSCsj51135	Support ESMTP over TLS in ASDM
CSCsj51143	Add WAAS inspection support in ASDM
CSCsj56815	Startup Wizard Auto Update User and Device Identity problems
CSCsj57083	Authentication test fails when using ASDM and FQDN is configured.
CSCsj60413	Exception in VPN Wizard prevents config completion
CSCsj62045	Support DNS Guard function
CSCsj62776	Invalid vlan id for an added vlan interface
CSCsj62928	ASDM reads wrong 5505 vlan configuration
CSCsj66280	new CLI for smartcard-removal-disconnect not configurable in ASDM
CSCsj67420	ASDM Monitor mode displays failover interface in Interface Status
CSCsj69181	Config Modified dialog displayed/not displayed incorrectly
CSCsj74510	Menu separators have a white background
CSCsj75235	Enhancement: show PFS config in the VPN Wizard summary page
CSCsj77373	Help for File Transfer displays wrong content
CSCsj78672	ASDM Null Pointer exception when trying to delete a trustpoint
CSCsj83806	Add DNS Inspect:adding "no match criteria for domain name" fails on ASDM
CSCsj89744	ASDM listing object-group by IP selects wrong objects to be added

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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

This document is to be used in conjunction with the documents listed in the “[Obtaining Documentation, Obtaining Support, and Security Guidelines](#)” section.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)