



# Cisco ASDM Release Notes Version 5.2(4)F

---

## April 2008

This document contains release information for Cisco ASDM Version 5.2(4)F, which runs with Cisco 6500 series and Cisco 7600 series Firewall Services Module software Versions 3.1(x) and 3.2(x). This document includes the following sections:

- [Introduction, page 1](#)
- [FWSM and ASDM Release Compatibility, page 2](#)
- [New Device Manager Features Per Release, page 2](#)
- [Client PC Operating System and Browser Requirements, page 3](#)
- [Upgrading ASDM, page 4](#)
- [Getting Started with ASDM, page 6](#)
- [Unsupported Commands, page 12](#)
- [Open Caveats in Version 5.2\(4\), page 14](#)
- [Resolved Caveats in Version 5.2\(4\)F, page 16](#)
- [Resolved Caveats in Version 5.2\(3\)F, page 16](#)
- [Resolved Caveats in Version 5.2\(2\)F, page 17](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)

## Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for the FWSM through an intuitive, easy-to-use management interface. Bundled with the FWSM, the device manager accelerates FWSM deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by FWSM software Versions 3.1(x) and 3.2(x). Its secure design enables anytime, anywhere access to security appliances.



---

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

© 2008 Cisco Systems, Inc. All rights reserved.

# FWSM and ASDM Release Compatibility

Table 1 shows the ASDM or PDM versions that can be used with each FWSM release.

**Table 1** FWSM and ASDM /PDM Release Compatibility

FWSM Release	ASDM/PDM Version
3.2(x)	ASDM 5.2(x)F
3.1(x)	ASDM 5.0(3)F <sup>1</sup> , ASDM 5.2(x)F
2.3(x)	PDM 4.1(3)
2.2(x)	PDM 4.1(3)
1.1(x)	PDM 2.1(1)

1. Because ASDM 5.2(x) also supports 3.1(x), we do not plan any more maintenance releases for 5.0F.

## New Device Manager Features Per Release

This section lists the new ASDM features, and includes the following topics:

- [New Features for Version 5.2\(4\)F, page 2](#)
- [New Features for Version 5.2\(3\)F, page 2](#)
- [New Features for Version 5.2\(2\)F, page 3](#)
- [New Features for Version 5.2\(1\)F, page 3](#)

### New Features for Version 5.2(4)F

There are no new features for Version 5.2(4)F.

### New Features for Version 5.2(3)F

ASDM Version 5.2(3)F includes the following new features:

- Switch configuration—Using ASDM, you can configure the following switch functions:
  - Assign ports to a VLAN.
  - Configure port parameters such as the admin status, speed and PortFast.
  - Set the port mode to routed or switched.
  - Configure VLANs.
  - Configure SVIs
  - Configure firewall VLAN groups and assign them to the FWSM

See Configuration > Switch.

- Network objects—You can now add true network objects that you can use in firewall rules. Objects can be named, and when you edit an object, the change is inherited wherever the object is used. Also, when you create a rule, the networks that you specify in the rule are automatically added to the network object list so you can reuse them elsewhere. You can name and edit these automatic entries as well. See Configuration > Objects > Network Objects/Groups.
- Access Rules table enhancements—See the following Access Rules enhancements:
  - Support for drag and drop and inline editing.
  - Option to filter on an exact match. Previously, the filter only supported containment (for example filtering on 10.1.1.1 includes 10.1.1.0/24 or “any”).
  - Filter for source or destination address.
  - Ability to enter multiple values, such as more than one source or destination address in many fields. Input fields are more free form.
  - Fields such as the source or destination address have auto-completion so that when you type in a value, it will provide legitimate choices to choose from.

## New Features for Version 5.2(2)F

There are no new features for Version 5.2(2)F.

## New Features for Version 5.2(1)F

ASDM Version 5.2(1)F includes the following new features:

- Enhanced ASDM rules table—The ASDM rule tables have been redesigned to streamline policy creation.
- Syslogs display source IP, destination IP, syslog ID, date and time into different columns.
- Support of network, service, protocol and ICMP-type object groups.
- Search replaced by ASDM Assistant, which provides task-oriented guidance to configuring features such as AAA server, logging filters, and others features.

# Client PC Operating System and Browser Requirements

[Table 2](#) lists the supported and recommended platforms for ASDM. While ASDM might work on other browsers and browser versions, these are the only officially supported browsers. Note that unlike earlier PDM versions, you must have Java installed. The native JVM on Windows is no longer supported and does not work.

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

Operating System	Browser	Java
<ul style="list-style-type: none"> <li>Windows Vista</li> <li>Windows XP</li> <li>Windows 2000, Service Pack 4 or higher</li> <li>Windows 2003 Server</li> </ul> (English or Japanese versions)	<ul style="list-style-type: none"> <li>Firefox 1.5</li> <li>Firefox 2.0</li> <li>Internet Explorer 6.0</li> <li>Internet Explorer 7.0</li> </ul>	<ul style="list-style-type: none"> <li>Java SE 1.4.2</li> <li>Java SE 5.0</li> <li>Java SE 6.0</li> </ul>
<ul style="list-style-type: none"> <li>Red Hat Desktop version 4</li> <li>Red Hat Enterprise Linux WS version 4</li> </ul>	<ul style="list-style-type: none"> <li>Firefox 1.5</li> <li>Firefox 2.0</li> </ul>	<ul style="list-style-type: none"> <li>Java SE 1.4.2</li> <li>Java SE 5.0</li> <li>Java SE 6.0</li> </ul>

## Upgrading ASDM

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

<http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm>

This section includes the following topics:

- [Upgrading from PDM, page 4](#)
- [Upgrading to a New ASDM Version, page 5](#)

## Upgrading from PDM

Before you upgrade your device manager, upgrade your platform software to Release 3.2. To upgrade from 2.x to 3.1, see *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*. To upgrade from 3.1 to 3.2, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide using the CLI*.

To upgrade from PDM to ASDM, perform the following steps:

---

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

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

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

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

**Step 4** Copy the ASDM binary to the FWSM using the appropriate command:

- TFTP

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

- FTP

```
hostname# copy ftp://[username:password@]server_ip/pathtofile flash:asdm
```

**Step 5** To enable the HTTPS server (if it is not already enabled), enter the following command:

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

**Step 6** To identify the IP addresses that are allowed to access ASDM, enter the following command:

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

Enter **0** for the *ip\_address* and *mask* to allow all IP addresses.

**Step 7** Save your configuration by entering the following command:

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

---

## Deleting Your Old Cache

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

Now, the cache directory for ASDM is in the following location:

- Windows—<userdir>\.asdm\cache
- Red Hat Linux —~/asdm/cache

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

## Upgrading to a New ASDM Version

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

To upgrade from ASDM to a new version of ASDM, perform the following steps:

---

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

**Step 2** Launch ASDM.

**Step 3** From the **Tools** menu, click **Upgrade Software**.

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

**Step 5** Click **Upload Image**.

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

“ASDM Image is Uploaded to Flash Successfully.”

**Step 6** To run the new ASDM image, you must quit out of ASDM and reconnect.

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

---

# Getting Started with ASDM

This section describes how to connect to ASDM and start your 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 6](#)
- [Starting ASDM from the ASDM Launcher, page 7](#)
- [Using ASDM in Demo Mode, page 7](#)
- [Starting ASDM from a Web Browser, page 9](#)
- [Using the Startup Wizard, page 9](#)
- [Configuring Failover, page 10](#)
- [Printing from ASDM, page 12](#)

## Before You Begin

If you have a new FWSM, you can enable ASDM access by sessioning into the FWSM CLI from the switch and entering the **setup** command. The **setup** command prompts you for a minimal configuration to connect to the FWSM using ASDM. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide using the CLI* to session into the FWSM. You must have an inside interface already configured to use the **setup** command. Before using the **setup** command, enter the **interface vlan *vlan\_id*** command, and then the **nameif inside** command. For multiple context mode, enter these commands in the admin context.

## Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher is an improvement over running ASDM as a Java Applet. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches faster, and caches previously-entered IP addresses and usernames.

To download the ASDM launcher, perform the following steps:

---

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

**https://interface\_ip\_address**

In transparent firewall mode, enter the management IP address.




---

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

---

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

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**

- **Run ASDM as a Java Applet**

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

The installer downloads to your PC.

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

---

## Starting ASDM from the ASDM Launcher

The ASDM Launcher is for Windows only.

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

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

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

If there is a new version of ASDM on the FWSM, 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 under Windows. It 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:

- Perform configuration and select monitoring tasks via ASDM as though you were interacting with a real device.
- Demonstrate ASDM or FWSM features using the ASDM interface.
- Perform configuration and monitoring tasks with the Content Security and Control SSM (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 a real 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 the Refresh button, it will revert back to the original configuration. The changes are never saved to the configuration file.
- File/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 login 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 it back to the original configuration.

- 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 from <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm>.  
The filename is `asdm-version-demo.msi`.
  - b. Double-click the installer to install the software.
- Step 2** Double-click the Cisco ASDM Launcher shortcut on your desktop, or start it from the **Start** menu.
- Step 3** Click the **Run in Demo Mode** check box.
- Step 4** To set the platform, context and firewall modes, and ASDM Version, click the **Demo** button and make your selections from the Demo Mode area.
- Step 5** If you want to use new ASDM images as they come out, you can either download the latest installer, or you can download the normal ASDM images and install them for Demo Mode:
- a. Download the image from <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm>.  
The filename is `asdm-version.bin`
  - 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 Demo Mode.

You see a Demo Mode label 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 FWSM network, enter the following URL:

`https://interface_ip_address`

In transparent firewall mode, enter the management IP address.



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

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

A page displays with the following buttons:

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

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

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

## Using the Startup Wizard

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

To use the Startup Wizard to configure the basic set-up of your FWSM, perform the following steps:

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

- In single context mode, perform the following steps:
  - a. Click **Configuration > Properties > Startup**.
  - b. Click **Launch Startup Wizard**.
- In multiple context mode, for each new context, perform the following steps:
  - a. From the Mode drop-down list on the left of the toolbar, choose **System**.
  - b. Create a new context using the Configuration > Security Context panel.
  - c. Be sure to allocate interfaces to the context.
  - d. When you apply the changes, ASDM prompts you to use the Startup Wizard.
  - e. From the Mode drop-down list on the left of the toolbar, choose the context you want to configure.

- f. Click **Configuration > Properties > Startup**.
  - g. Click **Launch Startup Wizard**.
- Step 2** Click **Next** as you proceed through the Startup Wizard panels, filling in the appropriate information in each panel, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.
- Step 3** Click **Finish** on the last panel to transmit your configuration to the FWSM. Reconnect to ASDM using the new IP address, if the IP address of your connection changes.
- Step 4** You can now enter other configuration details in the Configuration panels.
- 


## Configuring Failover


This section describes how to implement failover on FWSMs.

As specified in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide using the CLI*, both devices must have appropriate licenses and have the same hardware configuration.

Before you begin, decide on active and standby IP addresses for the interfaces ASDM connects through on the primary and secondary devices. These IP addresses must be assigned to device interfaces with HTTPS access.

To configure failover on your FWSM, perform the following steps:

- 
- Step 1** Configure the secondary device for HTTPS IP connectivity. See the [“Before You Begin” section on page 6](#), and use a different IP address on the same network as the primary device.
- Step 2** If the units are in different switches, make sure the switches can communicate with each other over a trunk that includes the failover and/or state VLANs.
- Step 3** Start ASDM from the primary device.
- Step 4** Perform one of the following steps, depending on your context mode:
- a. If your device is in multiple context mode, choose the admin context from the Mode drop-down list, and click **Configuration > Properties > Failover**.
  - b. If your device is in single mode, click **Configuration > Properties > Failover**. Click the **Interfaces** tab.
- Step 5** Perform one of the following steps, depending on your firewall mode:
- a. If your device is in routed mode, configure standby addresses for all routed mode interfaces.
  - b. If your device is in transparent mode, configure a standby management IP address for each bridge group.
-  **Note** Interfaces used for failover connectivity should not have names (in single mode) or be allocated to security contexts (in multiple security context mode). In multiple context mode, other security contexts may also have standby IP addresses configured.
- 
- Step 6** Perform one of the following steps, depending on your security context mode:
- a. If your device is in multiple security context mode, choose **System** from the Mode drop-down list, and click **Configuration > Failover**.

- b. If your device is in single mode, click **Configuration > Properties > Failover**.
- Step 7** On the Setup tab of the Failover panel under LAN Failover, choose the VLAN you want to use for the failover link.
-  **Note** In single mode, be sure to first add the failover link VLAN in the Configuration > Interfaces pane. Do not configure any parameters for the interface when you add it; all parameters are configured in the Configuration > Properties > Failover pane.
- Step 8** Configure the remaining LAN Failover fields.
- Step 9** (Optional) Provide information for other fields in all of the failover tabs. If you are configuring Active/Active failover, you must configure failover groups in multiple security context mode. If more than one failover pair of devices coexist on a LAN in Active/Active failover, provide failover-group MAC addresses for any interfaces on shared LAN networks.
- Step 10** On the Setup tab, check the **Enable Failover** check box.
- Step 11** Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.
- Step 12** Enter the IP address of the secondary device, which you configured as the standby IP address of the ASDM interface. Wait about 60 seconds. The standby peer still could become temporarily inaccessible.
- Step 13** Click **OK**. Wait for configuration to be synchronized to the standby device over the failover LAN connection.
- The secondary device should now enter standby failover state using the standby IP addresses. Any further configuration of the active device or an active context is replicated to the standby device or the corresponding standby context.

## Securing the Failover Key

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

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

- Step 1** Perform one of the following steps, depending on your security context mode:
- If your device is in single mode, navigate to Configuration > Properties > Failover > Setup.
  - If your device is in multiple mode, choose **System** from the Mode drop-down list, and navigate to 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.

- b. Click **Apply**. (Click **OK** if CLI preview is enabled.) A dialog box about configuring the peer appears.
- Step 5** Enter the IP address of the peer. Wait about 60 seconds. Even though the standby peer does not have the shared failover key, the standby peer still could become inaccessible.
- Step 6** Click **OK**. Wait for configuration to be synchronized to the standby device over the encrypted failover connection.
- 

## Printing from ASDM

ASDM supports printing for the following features:

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

## Unsupported Commands

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

See the following sections for more information:

- [Effects of Unsupported Commands, page 12](#)
- [Ignored and View-Only Commands, page 13](#)
- [ASDM Limitations, page 14](#)
- [Other CLI Limitations, page 14](#)

## Effects of Unsupported Commands

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

Monitor-only mode allows access to the following functions:

- The Monitoring area
- The CLI tool (Tools > Command Line Interface), which lets you use the CLI commands.

To exit Monitor-only mode, use the CLI tool or access the FWSM console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for more information.



**Note** You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to 3 by your system administrator, which allows Monitor-only mode. For more information, see Configuration > Device Administration > User Accounts and Configuration > Device Administration > AAA Access.

## Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when added by the CLI, but that cannot be added or edited in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If it is view-only, then the command appears in the GUI, but you cannot edit it.

Unsupported Commands	ASDM Behavior
<b>capture</b>	Ignored.
<b>control-point tcp-normalizer</b>	Ignored.
<b>established</b>	Ignored.
<b>failover timeout</b>	Ignored.
<b>ipv6</b> , any IPv6 addresses	Ignored.
<b>logging</b> (in system in multiple context mode)	Ignored.
<b>pager</b>	Ignored.
<b>pim accept-register route-map</b>	Ignored. Only the <b>list</b> option can be configured using ASDM.
<b>prefix-list</b>	Ignored if not used in an OSPF area.
<b>route-map</b>	Ignored.
<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 uauth allow-http-cache</b>	Ignored.
<b>terminal</b>	Ignored.
<b>virtual</b>	Ignored.

## ASDM Limitations

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

## Other CLI Limitations

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

```
ip address inside 192.168.2.1 255.255.0.255
```

- The ASDM CLI tool does not support interactive user commands. ASDM provides a CLI tool (choose **Tools > Command Line Interface**) that lets you enter certain CLI commands from ASDM. The ASDM CLI tool does not support interactive user commands. You can configure most commands that require user interaction by means of the ASDM panels. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter “[yes/no]” but does not recognize your input. ASDM then times out waiting for your response. For example, if you enter the **crypto key generate rsa** command, ASDM displays the following prompt and error:

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

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

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

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

## Open Caveats in Version 5.2(4)

This section contains open caveats in software Version 5.2(4)F.

- CSCsj24279
 

When running ASDM in demo mode, the Dynamic Resource Allocation pane only shows 0 for all the values. The user cannot configure any value from this panel.

**Workaround:** None.
- CSCsk65606
 

In the Configuration > Switch > Interfaces pane, the speed drop-down list values do not match the actual speed values for the interface. Fast Ethernet interfaces allow an auto setting that lets the switch hardware to auto-negotiate the speed, but auto is not available in ASDM. Fast Ethernet interfaces do not support 1000 Mbps, but that is given as an option. Gigabit Ethernet interfaces show the possibility of changing the speed (the Modify button is not grayed out when a Gigabit interface is selected) even though speed and other changes are not permitted. For the Ten-Gigabit Ethernet module WS-X6708-10GE, the value of speed as seen on the interface table is incorrectly shown as 4294.

**Workaround:** Use only supported speeds and access the switch supervisor CLI directly for configuration of auto speeds.

- CSCsl07293  
The ASDM dashboard might incorrectly show all interface status as unknown with a question mark.  
**Workaround:** None.
- CSCsl09988  
In multiple context mode, if you make any changes to the context setup (such as allocating interfaces) in the Configuration > Switch panes, then the **write memory all** command is sent implicitly. The **write memory all** command saves *all* context configurations. The time to save the configurations depends on the configuration sizes. This command is not seen in the preview CLI window. If you make any other changes (unrelated to the context setup), then the **write memory** command is sent implicitly. Normally, ASDM does not send the **write memory** command unless you specifically click the **Save** button on the toolbar.  
**Workaround:** None.
- CSCsl11244  
ASDM might show an incorrect interface packet rate graph.  
**Workaround:** None.
- CSCsl29949  
When you add a new context and set the mode to transparent, and then click **Apply**, ASDM might set the mode to transparent before creating the context; therefore the mode defaults to routed mode. The actual mode can be seen if you refresh the configuration; prior to refreshing, ASDM displays the mode as transparent.  
**Workaround:** Reset the mode to transparent after the context is created.
- CSCsl65027  
Deleting a VLAN from the Configuration > Switch > Vlans table also removes the SVI of that VLAN and its association from the VLAN group.  
**Workaround:** None.
- CSCsl85050  
If you delete all IGMP access groups from the Configuration > Routing > Multicast > IGMP > Access Groups pane, and then go to add a new one, ASDM fails to display the Add dialog box.  
**Workaround:** Restart ASDM.
- CSCsl87131  
After adding a multicast group on the Configuration > Routing > Multicast > PIM > Route Tree pane, when you try to add another group, the Apply button is disabled.  
**Workaround:** Restart ASDM.
- CSCsm00593  
If you enable failover after you assign VLAN groups to an FWSM, then ASDM does not support adding the groups to the standby unit; similarly, if you later disable failover, ASDM does not support removing VLAN groups from a standby unit.  
**Workaround:** Use the **firewall module *module\_number* vlan-group *firewall\_group*** command on the switch to assign the VLAN group to the standby FWSM or use the **no** form of the command to remove the group.

- CSCso21565

When ASDM is running as an applet using Java version 6 from an FWSM failover pair, ASDM cannot reconnect to the failover peer after sending the **no failover active** command, which fails over an active device. After being unable to communicate with the peer, ASDM may be able to reconnect with the original device if there is a return failover through an alternate method, but the peer is permanently unreachable for the session.

**Workaround:** Use one of the following workarounds:

- Use the ASDM launcher instead.
- Use a Java Runtime Environment (JRE) earlier than version 6 and its updates.
- Fail over the FWSM pair by sending the **no failover active** command through the Command Line Interface menu item, which may work sometimes.

## Resolved Caveats in Version 5.2(4)F

The caveats listed in [Table 3](#) were resolved in software Release 5.2(4)F, and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

<http://www.cisco.com/support/bugtools>

**Table 3** *Caveats Resolved in Version 5.2(4)F*

Caveat ID	Title
CSCsm13051	Log Viewer cleared when you launch it from Access Rules, Show Log
CSCsm25784	TCP Service Group " named" http-https acts as range
CSCsm76473	Name entries in ASA not showing as Network Objects in ASDM
CSCsm88085	Filtering doesn't work in Syslog Buffer Viewer
CSCsm88523	Failover tab not working on ASDM 5.2(3)F, multiple context mode
CSCso19310	Startup wizard causes exception.
CSCso19318	Access-rule for tcp/http cannot be created.
CSCso33359	In the network object grp IP address column displays name.
CSCso41215	ASDM system context user management panel missing

## Resolved Caveats in Version 5.2(3)F

- CSCsk76214

When you add VLANs from the switch to the FWSM, and refresh ASDM, ASDM hangs at 71%. This only happens using Internet Explorer.

**Workaround:** Use the ASDM Launcher or another browser.

The caveats listed in [Table 4](#) were resolved in software Release 5.2(3)F, and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

<http://www.cisco.com/support/bugtools>

**Table 4** *Caveats Resolved in Version 5.2(3)F*

Caveat ID	Title
CSCeg54076	Failover enabled popup incorrect or misleading
CSCsi07079	Need to warn the user when static interface PAT is changed.
CSCsj24938	Error message "mtu configurable between 300 to 65535"
CSCsk05283	5.2.2.F: Unable to remove Failover vlan
CSCsk09308	Missing host/network concept in ASDM 5.2 and above
CSCsk13991	nameif is not configured on FWSM when int is added
CSCsk17582	window hangs while configuring country code in GTP map
CSCsk23203	Command queue size text-box size in Add&Edit MGCPmap window is too small
CSCsk24905	"ADD/Edit-http-map" window hangs while configuring the http-map
CSCsk25119	ASDM showing wrong Entity Lengths in HTTP-map
CSCsk28917	Inconsistent behavior of ASDM while config DR priority value in PIM
CSCsk56801	ASDM:5.2(2)F:Unable to save AAA authentication configs through ASDM
CSCsk65650	Unable to delete rules from ASDM when 'log' is specified in access-list
CSCsl06662	ACL commit feature preference is missing in ASDM 5.2F
CSCsl18491	ASDM connection fails with %ERROR: (Poller) message. No Java traceback
CSCsl20317	No changes when click security context after creating context.
CSCsl32325	ASDM Real-Time Log Viewer does not filter with Filter button
CSCsl58489	Inconsistency in displaying "Config Modified" dialog
CSCsl61523	No provision to remove ip add of interface from interface table of ASDM
CSCsl90286	Menu separators have a white background
CSCsl90595	Manual commit setting in ASDM is not being read on startup

## Resolved Caveats in Version 5.2(2)F

The caveats listed in [Table 5](#) were resolved in software Release 5.2(2)F, and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

<http://www.cisco.com/support/bugtools>

**Table 5** *Caveats Resolved in Version 5.2(2)F*

Caveat ID	Title
CSCsd83057	Can't add failover interface in ASDM
CSCsi05228	ASDM Monitor mode displays failover interface in Interface Status

**Table 5**      **Caveats Resolved in Version 5.2(2)F**

Caveat ID	Title
CSCsj51860	5.2: In multi context, default dynamic resource show a -4 value
CSCsj85212	ASDM 5.2F refresh button does not re-read configuration
CSCsj89744	ASDM listing object-group by IP selects wrong objects to be added

## Obtaining Documentation and Submitting a Service Request

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0804R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.