Cisco ASDM Release Notes Version 5.0(2)F

June 2006

This document contains release information for Cisco ASDM Version 5.0(2)F, which runs with Cisco 6500 series and Cisco 7600 series Firewall Services Module software Version 3.1. This document includes the following sections:

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 Release 3.1. Its secure design enables anytime, anywhere access to security appliances.

ASDM 5.0(2)F is the next generation release of PDM, which was the device manager compatible with earlier versions of FWSM.

CISCO SYSTEMS

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

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
3.1(x)	ASDM 5.0(2)F[1]
2.3(x)	PDM 4.1(3)
2.2(x)	PDM 4.1(3)
1.1(x)	PDM 2.1(1)

1. This ASDM version only works with FWSM; it is not compatible with ASA or PIX security appliances.

New Device Manager Features

ASDM Version 5.0(2)F includes the following new features:

- Supports all new FWSM Release 3.1 features. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Release Notes* for a list of platform features.
- New GUI look-and-feel

  The overall look-and-feel of the application has changed from PDM 4.1. There is a sidebar that highlights the high-level features. The Home Page has a live system log message section at the bottom of the panel. The categories (for example, **Configuration > Properties**) have been reorganized and are in alphabetical order.
- (Windows only) Demo mode

  If you use the ASDM Launcher to start ASDM, there is a Run in Demo Mode option. This option allows you to use ASDM without actually having a real FWSM. You must install the ASDM demo image to get the demo mode feature.
- **Back** and **Forward** buttons

  The Back and Forward buttons allow you to move back and forth between categories much like the browser **Back** and **Forward** buttons.

  See the **Toolbar**.
- **Search** button

  This allows you to search for a category in ASDM. For example, you can do a search on SIP to find out where to configure SIP.

  See the **Toolbar**.
- Real-time Log Viewer

  The Real-time Log Viewer shows you real-time system log messages. The system log message information is transferred over HTTPS.

  See **Monitoring > Logging > Real-time Log Viewer**.
- System log message enhancements
  - Identify the access rule that generated the syslog.

Using the **Log Buffer** or **Real-time Log Viewer** for system log messages 106100 and 106023, you can click this rule and click the **Show Rule** button. This shows you the Access Rules table and highlights the rule that triggered this system log message.

See **Monitoring > Logging > Log Buffer** > **View** button and **Show Rule** button.

See **Monitoring > Logging > Real-time Log Viewer** > **View** button and **Show Rule** button.

- Filter system log messages.

  You can filter the system log messages shown on any output device, including ASDM.

  See **Configuration > Properties > Logging** > **Logging Filters**.

- Create the opposite access rule to permit or deny the traffic from the system log message

  Using the Log Buffer or Live Log for system log messages 106100 and 106023, you can click this rule and click the **Create Rule** button. This brings up an **Add Rule** dialog box to create the rule to permit or deny the traffic. The rule is placed at the beginning of the access list.

  See **Monitoring > Logging > Log Buffer** > **View** button and **Create Rule** button.

  See **Monitoring > Logging > Real-time Log Viewer** > View button and **Create Rule** button.

- Color Settings

  You can set different colors for different syslog levels.

  See **Monitoring > Logging > Real-time Log Viewer > View** button and **Color Settings** button.

- Find

  You can search on any text in the syslog table.

  See **Monitoring > Logging > Log Buffer > View** button and **Find** field.

  See **Monitoring > Logging > Real-time Log Viewer > View** button and **Find** field.

- (Windows only) You can run ASDM without a browser using the Cisco ASDM Launcher.
  - The ASDM Launcher lets you download and run ASDM locally on your PC.
  - Multiple instances of the ASDM Launcher provide administrative access to multiple FWSMs simultaneously, from the same management workstation.
  - The ASDM Launcher automatically updates the software based on the installed version on the FWSM, enabling consistent security management throughout the network.
- File Management

  This allows you to view, cut, copy, paste, delete, and rename files on the Flash file system. You can create directories and transfer files to and from other systems using HTTP, HTTPS, FTP, or TFTP.

  See **Tools > File Management**

  In multiple context mode, you must be in System mode to access this menu item.
- Upgrade Software

  You can upgrade the FWSM image or the ASDM image.

  See **Tools > Upgrade Software**

  In multiple context mode, you must be in System mode to access this menu item.
- System Reload

  You can reload the FWSM now or schedule a reload at a later time.

  See **Tools > System Reload**

  In multiple context mode, you must be in System mode to access this menu item.

- Context Caching

  Up to two contexts can be cached in memory. This allows switching between contexts without having to reread the configuration each time. It takes about ten seconds before the caching takes effect so if you switch between contexts rapidly, it does not cache the context.

- Better support for handling large number of contexts

  If you click the down arrow button from the **File** menu, it changes the context choice list to a list shown on the left-hand side. This allows you to view many contexts at once.

  If you now click the **<** button, it shifts the context panel to the edge. If you mouse over the vertical text labeled **Mode: Refresh**, it expands the context choice list so you can click an item.

- Online Help

  The online help has been revised and has a new look-and-feel. It also supports searching.

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, Browser, and Java Requirements

	Operating System	Browser with Java Applet	ASDM Launcher	Other Requirements
Windows[1] Processor: Intel Pentium IV, AMD Athlon or equivalent Memory: Min. 512 MB RAM Display: Min. 1024x768 resolution and 256 colors	Windows 2000 (Service Pack 4) or Windows XP operating systems, English or Japanese	Internet Explorer 6.0 with Java Plug-in[2] 1.4.2 or 5.0 (1.5) **Note** **HTTP 1.1**—Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections. Firefox 1.5 with Java Plug-in[2] 1.4.2 or 5.0 (1.5)	Java 1.4.2 or 5.0 (1.5)[2]	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Sun SPARC Solaris Memory: Min. 512 MB RAM Display: Min. 1024x768 resolution and 256 colors	Sun Solaris 8 or 9	Firefox 1.5 with Java Plug-in[2] 1.4.2 or 5.0 (1.5)	Not available.	
Linux Memory: Min. 256 MB RAM Display: Min. 1024x768 resolution and 256 colors	Red Hat Linux Desktop or Red Hat Linux Enterprise WS, Version 3 GNOME or KDE desktop environment	Firefox 1.5 with Java Plug-in[2] 1.4.2 or 5.0 (1.5)	Not available.	

1. ASDM is not supported on Windows 3.1, 95, 98, ME or Windows NT4.
2. Download the latest Java from http://java.sun.com/.

Upgrading ASDM

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

http://www.cisco.com/cisco/software/navigator.html

This section includes the following topics:

Upgrading from PDM

Before you upgrade your device manager, upgrade your platform software to Version 3.1. See *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1* for more information.

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
  ```

For more information on the **copy** command and its options, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*.

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 beta 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 and Solaris). 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 and Sun Solaris—~/.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.

Step 7 Download the new platform image using the **Tools > Upgrade Software** tool.

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

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* 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/cisco/software/navigator.html.

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/cisco/software/navigator.html.

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,* 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 7, 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 reenable failover. When failover is reenabled, 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:

- **a.** If your device is in single mode, navigate to Configuration > Properties > Failover > Setup.
- **b.** If you 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.)

- **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. 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 13
- Ignored and View-Only Commands, page 14
- ASDM Limitations, page 15
- ASDM Limitations, page 15

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
access-list	Ignored if not used.
capture	Ignored.
established	Ignored.
failover timeout	Ignored.
ipv6, any IPv6 addresses	Ignored.
logging (in system in multiple context mode)	Ignored.
object-group icmp-type	View-only.
object-group network	Nested group is view-only.
object-group protocol	View-only.
object-group service	You can view, edit, and delete nested service object groups. However, you cannot add a nested group.
pager	Ignored.
pim accept-register route-map	Ignored. Only the **list** option can be configured using ASDM.
prefix-list	Ignored if not used in an OSPF area.
route-map	Ignored.

service-policy global	Ignored if it uses a **match access-list** class. For example:
	`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`

Unsupported Commands	ASDM Behavior
sysopt uauth allow-http-cache	Ignored.
terminal	Ignored.
virtual	Ignored.

ASDM Limitations

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

Other CLI Limitations

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

  ```
  ip address inside 192.168.2.1 255.255.0.255
  ```

- The ASDM CLI tool does not support interactive user commands. ASDM provides a CLI tool (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
  ke0000000000000$A key
  Input line must be less than 16 characters in length.

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

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

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

Open Caveats

This section lists the open caveats, and includes the following topics:

Open Caveats in ASDM 5.0(2)F

This section describes open caveats in the 5.0(2)F version.

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

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

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

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

Open Caveats

Table 3 Open Caveats

ID Number	Caveat Title
CSCei84173	Service policy rules are created before validation is complete
CSCei87803	Service Policy dialog doesnt warn about loss of settings
CSCsd66311	All graph in the Home page reflect the same data
CSCsd77211	Failure to remove Static PAT translation via ASDM
CSCsd83057	Can't add failover interface in ASDM
CSCse40315	Unexpected IP address conflict error message when adding SNMP host
CSCse56046	NAT rule cannot be deleted from ASDM
CSCse56828	ASDM hangs at 47% while loading FWSM config
CSCse58612	Access-rules require NAT for communication between same-security intfs
CSCse61699	The Access Rules table does not show the correct service icon

Resolved Caveats

Table 4 Resolved Caveats

ID Number	Caveat Title
CSCeh96630	ASDM hardcodes some colors instead of using system defaults
CSCsc99674	Access rule is incomplete for network groups
CSCse17618	ACL commit feature preference is missing
CSCse29994	ASDM edit address translation window does not default to existing pool
CSCse30449	ASDM launcher user authentication fails first time
CSCse31288	ASDM does not add new access-list without creating a translation rule
CSCse35257	Default to better syslog colors
CSCse51471	Port the bug fix CSCsc99674 to 5.0.2.F

Open Caveats in FWSM 3.1(1) that Affect ASDM

This section describes open caveats in FWSM Release 3.1(1) that affects the ASDM operation.

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

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

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

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

- CSCsc70975

  Names are used instead of port numbers while calculating ACE hash.

  Effect on ASDM: Due to this defect, a change was made in ASDM to disable the Show Rule feature in Monitoring > Logging > Real-time Log Viewer and Monitoring > Logging > Log Buffer unless you use FWSM Release 3.1(1.5) or later.

  Workaround: Upgrade to FWSM Release 3.1(1.5) or later.

- CSCsd47160

  With 100 contexts configured, when you switch between contexts using ASDM, the FWSM tells ASDM that the session limit was reached; but in this case the session limit was not reached. When the session limit is reached, ASDM shows an error dialog box.

  Effect on ASDM: Due to this defect, a change was made in ASDM to not display an error message when the ASDM session limit is reached.

  Workaround: None.

Related Documentation

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

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Release Notes*
- *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*

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.
