Cisco ASDM Release Notes Version 6.1(x)F

July 2009

This document contains release information for the following Cisco ASDM Versions:

- 6.1(5)F
- 6.1(4)F
- 6.1(3)F
- 6.1(2)F
- 6.1(1)F

ASDM 6.1(x)F runs with Cisco 6500 series and Cisco 7600 series Firewall Services Module software Release 4.0.

This document includes the following sections:

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

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 4.0.

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
4.0(x)	ASDM 6.1(x)F
3.2(x)	ASDM 5.2(x)F, ASDM 6.1(x)F
3.1(x)	ASDM 5.0(2)F, ASDM 5.2(x)F, ASDM 6.1(x)F
2.3(x)	PDM 4.1(3)
2.2(x)	PDM 4.1(3)
1.1(x)	PDM 2.1(1)

New ASDM Features

This section lists new features for each ASDM maintenance release, and includes the following topics:

New Features for ASDM Version 6.1(5)F

No features were added for 6.1(5)F.

New Features for ASDM Version 6.1(4)F

No features were added for 6.1(4)F.

New Features for ASDM Version 6.1(3)F

Support for FWSM Release 4.0(4).

New Features for ASDM Version 6.1(2)F

You can now configure Route Map properties for static connected routes. Route maps are used when redistributing routes into an OSPF, RIP, EIGRP, or Route Health Injection routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

See Configuration > Device Setup > Routing > Route Map.

New Features for ASDM Version 6.1(1)F

Support for FWSM Release 4.0(1).

New FWSM Platform Features

This section lists new features for each maintenance release, and includes the following topics:

Note This section only lists features for FWSM 4.0(x) on ASDM 6.1(x)F. ASDM 6.1(x)F also supports FWSM 3.1(x) and 3.2(x).

New Features in Release 4.0(4)

The following Cisco IOS-integrated features are now officially supported in FWSM:

Feature	Description
PISA integration	**Note** This feature depends on Cisco IOS Release 12.2(18)ZYA or later, and is only available on the Catalyst 6500 switch. The FWSM can leverage the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type.

Feature	Description
Route Health Injection	**Note** This feature depends on Cisco IOS Release 12.2(33)SXI or later, and is only available on the Catalyst 6500 switch. Route Health Injection is used for injecting the connected and static routes and NAT pools configured on the FWSM into the MSFC routing table on a per context basis. MSFC can then redistribute the route or NAT pools to other router routing tables.
Virtual Switching System (VSS) support	**Note** This feature depends on Cisco IOS Release 12.2(33)SXI or later, and is only available on the Catalyst 6500 switch. VSS is a system virtualization technology that allows the pooling of multiple Catalyst 6500 switches into a single virtual switch. If you have the FWSM installed, FWSM traffic benefits from this feature. There is no configuration required on the FWSM.

New Features in Release 4.0(3)

The SCCP (Skinny) inspection has been enhanced to do the following:

- Support registrations of SCCP version 17 phones.
- Support SCCP version 17 media related messages for opening up pinholes for video/audio streams.

The following are not supported:

- Registrations of endpoints that have IPv6 addresses. The Register messages are dropped and a debug message is generated.
- If IPv6 messages are embedded in the SCCP messages, they are not NATed or PATed; they are left untranslated.

New Features in Release 4.0(2)

There were no new features in Release 4.0(2).

New Features in Release 4.0(1)

Table 1-2 lists the new features in Release 4.0(1).

Table 1-2 New Features for FWSM Release 4.0(1)

Feature	Description
Routing	
EIGRP	The following EIGRP features are supported in this release: • Summarization • Stub-routing • Route filtering • Manual Route summarization • Redistribution See **Configuration > Device Setup > Routing**
Static route monitoring	If you configure multiple static routes to reach a network, the route monitoring feature can detect if a network goes down so that the next best route can be used. See **Monitoring > Routing > Routes**.
DHCP	
DHCP Option 82 support	When the switch is acting as relay agent, to interoperate with HSRP, the FWSM will preserve the Option 82 field set up by the switch. See the **Configuration > Device Management > DHCP**.
Modular Policy Framework	
Inspection policy maps and class maps	The following protocols support inspection policy and/or class maps: • DCERPC • ESMTP • HTTP • SIP See **Configuration > Firewall > Service Policy Rules**. or **Configuration > Firewall > Objects > Policy Maps**.
Regular expressions and regular expression class maps	You can create regular expressions and regular expression class maps for use in an inspection policy map or class map. See **Configuration > Firewall > Service Policy Rules**. or **Configuration > Firewall > Objects > Policy Maps**.
Filtering	
HTTPS support with Secure Computing SmartFilter	The FWSM now supports HTTPS filtering using Secure Computing SmartFilter. See **Configuration > Device Management> Logging > Logging Filters.**.
Adding the context name to Websense version 4 requests	Because Websense requests initiated from the FWSM use the pre-NATted IP address of clients, which can be overlapping, this can lead to problems in defining policies in the Websense server. Adding the context name to Websense queries lets the Websense server use the context name for policy lookups.

Table 1-2 New Features for FWSM Release 4.0(1) (continued)

Feature	Description
Application Inspection	
DNS Guard configurability	You can now disable DNS Guard at the CLI. See **Configuration > Device Management> DNS > DNS Client.**
SIP inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map. See **Configuration > Firewall > Objects > Inspect Maps > SIP**.
HTTP inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map. See **Configuration > Firewall > Objects > Inspect Maps > HTTP**.
ESMTP inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map. See **Configuration > Firewall > Objects > Inspect Maps > ESMTP**.
DCERPC inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map. See **Configuration > Firewall > Objects > Inspect Maps > DCERPC**.
Access Lists	
Customizable memory partition sizes	In multiple context mode, you can change the size of memory partitions for rule use, so you can reallocate memory from one partition to another. See **System > Configuration > Device Management > Resource Allocation**.
Rule reallocation per feature per partition	You can reallocate rules between features on a per-partition basis instead of just globally. See **System > Configuration > Device Management > Resource Allocation** or in Single routed mode **Context > Configuration > Device Management > Dynamic Resource Allocation**.
Access list optimization	The access list group optimization feature reduces the number of ACEs per group by merging and/or deleting redundant and conflicting ACEs without affecting the semantics of the access list. See **Configuration > Firewall > Access Rules**.
Connections and Switch Integration	
Connection rate limiting	You can limit the connection rate for TCP and UDP traffic. See **Configuration > Firewall > Service PolicyRules**.
Monitoring	
New SNMP MIBs	For ACL entries and ACL hit counters (CISCO-IP-PROTOCOL-FILTER-MIB), and ARP table entries (IP-MIB).

Client PC Operating System and Browser Requirements

Table 3 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 3 Operating System and Browser Requirements

Operating System	Browser	Java
• Windows Vista • Windows XP • Windows 2000, Service Pack 4 or higher • Windows 2003 Server (English or Japanese versions)	• Firefox 1.5 • Firefox 2.0 • Internet Explorer 6.0 • Internet Explorer 7.0	• Java SE 5.0 • Java SE 6.0
• Red Hat Desktop version 4 • Red Hat Enterprise Linux WS version 4	• Firefox 1.5 • Firefox 2.0	• Java SE 5.0 • Java SE 6.0

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

Before you upgrade your device manager, upgrade your platform software to Release4.0(1). To upgrade from 3.x to 4.0(1), see *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 4.0*. To upgrade from 3.2 to 4.0(1) , see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

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.

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 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 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 Check the **Run in Demo Mode** check box.

Step 4 To set the platform, context and firewall modes, and ASDM Version, click **Demo** and make your selections in 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. Choose **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 pane.
  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. Choose **Configuration > Properties > Startup**.
  g. Click **Launch Startup Wizard**.

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

Step 3 Click **Finish** on the last pane 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 panes.

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 10, 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 pane 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 16
- Ignored and View-Only Commands, page 17
- Other CLI Limitations, page 18

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.
control-point tcp-normalizer	Ignored.
established	Ignored.
failover timeout	Ignored.
ipv6, any IPv6 addresses	Ignored.
logging (in system in multiple context mode)	Ignored.
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`

sysopt uauth allow-http-cache	Ignored.
terminal	Ignored.
virtual	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
  ```

- 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 panes. 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 in Release 6.1(x)F

The caveats listed in Table 4 are open caveats in software release 6.1(x)F. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 4 Caveats Open in Release 6.1(x)F

Caveat ID	Title
CSCsq17298	The File Management tab shows the file name as a process.
CSCsq98074	The link on the main ASDM pane for Configuration > Switch > Interface becomes a field.
CSCsq98074	Avior 3: link for Configuration > Switch > Interface becomes a text box
CSCsy68911	FWSM: ASDM may report an error about incorrect version number
CSCsy68943	FWSM: ASDM may report incorrect version number in the GUI help about.
CSCsy93819	FWSM: ASDM java error while editing rules - amq cannot be cast to bxw
CSCsy98391	Incorrect configurable parameters shown on changing context mode
CSCsz48612	ASDM Should not Push 'NFS' Port-Objects to FWSM
CSCsz90779	ASDM Should Allow to Configure ICMP Error Inspection in Transparent FWSM
CSCsz96668	Object-groups cannot be edited in ASDM if the filter option is used

Resolved Caveats in Release 6.1(5)F

The following caveat was resolved in software Release 6.1(5)F. If you are a registered Cisco.com user, view more information about this caveat using the Bug Toolkit at the following website:

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

- CSCsy68943—FWSM: ASDM may report incorrect version number in the GUI help about
- CSCsz38889—SSL setting links in Identity Cert node in ASDM goes to "page not found"
- CSCsz48612—ASDM Should not Push 'NFS' Port-Objects to FWSM and Earlier ASA/PIX SW
- CSCsz90779—ASDM Should Allow to Configure ICMP Error Inspection in Transparent FWSM
- CSCsz96668—Object-groups cannot be edited in ASDM if the filter option is used
- CSCta13036—ASDM for FWSM 6.1.3F change firewall mode doesnt change correctly on err

Resolved Caveats in Release 6.1(4)F

The following caveat was resolved in software Release 6.1(3)F. If you are a registered Cisco.com user, view more information about this caveat using the Bug Toolkit at the following website:

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

- CSCsz84762—port changes of CSCsx24433 to 61f branch

Resolved Caveats in Release 6.1(3)F

The caveats listed in Table 5 were resolved in software Release 6.1(3)F. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 5 Caveats Fixed in Release 6.1(3)F

Caveat ID	Title
CSCsf19215	ASDM hard timeout for device i/o causes disconnect with large ACLs
CSCsl61523	No provision to remove ip add of interface from interface table of ASDM
CSCsr89144	ASDM: java.lang.NumberFormatException: For input string: "1 year 0"
CSCsv05945	Second vlan range is grayed out in Add Interface Allocation
CSCsv35312	FWSM: ASDM will not allow to "disable" interface on context.
CSCsv58991	ASDM: Description field in "Add Network Object" depends on Name field
CSCsv67531	Hit count does not work while changing the contexts
CSCsw22005	Service-acceleration not replicated from FWSM to ASDM when confgd by CLI
CSCsw30020	Service-acceleration not displayed on configuration window when enabled
CSCsw30480	Add 'service-acceleration timeout idle' support
CSCsw40957	ASDM java null pointer exception on Vista SP1
CSCsx58798	ASDM: Monitoring -> Routing -> Routes window is empty

Table 5 Caveats Fixed in Release 6.1(3)F

Caveat ID	Title
CSCsy31516	Admin context changes to transparent when some other context is cfg so
CSCsy31528	ASDM Refresh : Wrong dialog (ASDM is delivering commands to FWSM)
CSCsy39477	Unknown command 'access-list rename' in ASDM for FWSM

Resolved Caveats in Release 6.1(2)F

The caveats listed in Table 6 were resolved in software Release 6.1(2)F. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 6 Caveats Fixed in Release 6.1(2)F

Caveat ID	Title
CSCsu00870	ASDM webpage does not load and produces a 404.
CSCsu64769	ASDM 6.1F is allowing >,<,!=, operators for port-object of Object-group.
CSCsu66972	Add the Hit Count column for 4.0.
CSCsu28757	Privilege level checking in ASDM6.1F eventhough no command autorization.
CSCsu30657	Management Access Rule is not applicable in ASDM for FWSM.
CSCsu04242	Creating rule from the log is not working (6.1.1.2.F).
CSCsu01898	System config is not show in FWSM 3.2.
CSCsr74484	"Clear and Save Content" menu do not work on syslog viewer on homepage.
CSCsu00699	ASDM 6.1(1)f does not show context drop-down for multi-context firewalls.
CSCsu49365	Can't delete ACL with time-range.
CSCsu00498	ASDM fails to add ACLs when access rules are filtered.
CSCsu30862	Unable to add server to AAAserver group.
CSCsv21256	ASDM may throw an error about the image version being incorrect.
CSCsv07777	ASDM, in Demo mode, is timing out.

Resolved Caveats in Release 6.1(1)F

The caveats listed in Table 7 were resolved in software Release 6.1(1)F. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 7 Caveats Fixed in Release 6.1(1)F

Caveat ID	Title
CSCsq10143	Edit Static NAT Rule dialog is overlapping other text.
CSCsq94285	ASDM not defining inline service groups properly.

Table 7 Caveats Fixed in Release 6.1(1)F

Caveat ID	Title
CSCsq71857	ASDM will may freeze for 3 to 4 minutes after an ACL is edited.
CSCsq85965	ASDM "where used" on network objects shows duplicated results.
CSCso76109	Add Dynamic NAT Rule is not responding and hanging ASDM.
CSCso49954	Gives error "brs" when filtering for object-group.
CSCso33359	In the network object group, IP address column displays name.
CSCso45991	Changing address of network object removes it from the object group.
CSCsm88085	Filtering doesn't work in Syslog Buffer Viewer.

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