



## CHAPTER 3

# Defining Preferences and Using Configuration, Diagnostic, and File Management Tools

---

This chapter describes the preferences and tools available for configuration, problem diagnosis, and file management, and includes the following sections:

- [Preferences, page 3-1](#)
- [Configuration Tools, page 3-3](#)
- [Diagnostic Tools, page 3-6](#)
- [File Management Tools, page 3-9](#)

## Preferences

The Preferences feature lets you change the behavior of some ASDM functions between sessions.

To change various settings in ASDM, perform the following steps:

- 
- Step 1** In the main ASDM application window, choose **Tools > Preferences**.
- The Preferences dialog box appears, with three tabs: General, Rules Table, and Syslog Colors.
- Step 2** Click one of these tabs to define your settings: the **General** tab to specify general preferences; the **Rules Tables** tab to specify preferences for the Rules table; and the **Syslog Colors** tab to specify the background, foreground, and text colors for syslog messages displayed on the Home pane.
- Step 3** In the General tab, specify the following:
- a. Check the **Preview commands before sending them to the device** check box to view CLI commands generated by ASDM.
  - b. Check the **Enable cumulative (batch) CLI delivery** check box to send multiple commands in a single group to the FWSM.
  - c. Check the **Warn that configuration in ASDM is out of sync with the configuration on the FWSM** check box to be notified when the startup configuration and the running configuration are no longer in sync with each other.



---

**Note** Even if you do not choose this option, when the startup configuration changes, the Refresh button turns pink to indicate that you need to resynchronize the startup and running configurations.

---

- d. Check the **Confirm before exiting ASDM** check box to display a prompt when you try to close ASDM to confirm that you want to exit. This option is checked by default.
- e. Check the **Show configuration restriction message to read-only user** check box to display the following message to a read-only user at startup. This option is checked by default.

"You are not allowed to modify the FWSM configuration, because you do not have sufficient privileges."

- f. Check the **Enable screen reader support (requires ASDM restart)** check box to enable screen readers to work. You must restart ASDM to enable this option.

**Step 4** In the Rules Tables tab, specify the following:

- a. Display settings let you change the way rules are displayed in the Rules table.
  - Check the **Auto-expand network and service object groups with specified prefix** check box to display the network and service object groups automatically expanded based on the Auto-Expand Prefix.
  - In the Auto-Expand Prefix field, specify the prefix of the network and service object groups to expand automatically when displayed.
  - Check the **Show members of network and service object groups** check box to display members of network and service object groups and the group name in the Rules table. If the check box is not checked, only the group name is displayed.
  - In the Limit Members To field, enter the number of network and service object groups to display. When the object group members are displayed, then only the first *n* members are displayed.
  - Check the **Show all actions for service policy rules** check box to display all actions in the Rules table. When unchecked, a summary is displayed.
- b. Deployment settings let you configure the behavior of the FWSM when deploying changes to the Rules table.
  - Check the **Issue 'clear xlate' command when deploying access lists** check box to clear the NAT table when deploying new access lists. This setting ensures the access lists that are configured on the FWSM are applied to all translated addresses.
- c. Access Rule Hit Count Settings let you configure the frequency for which the hit counts are updated in the Access Rules table. Hit counts are applicable for explicit rules only. No hit count will be displayed for implicit rules in the Access Rules table.
  - Check the **Update access rule hit counts automatically** check box to have the hit counts automatically updated in the Access Rules table.
  - In the Update Frequency field, specify the frequency in seconds that the hit count column is updated in the Access Rules table. Valid values are 10 - 86400 seconds.

**Step 5** In the Syslog Colors tab, specify the following:

- To change the background text or foreground text color for messages at each severity level, click the corresponding column. The Pick a Color dialog box appears. Choose one of the following tabs:
  - On the Swatches tab, choose a color from the palette, and click **OK**.
  - On the HSB tab, specify the Hue, Strength, and Brightness settings, and click **OK**.
  - On the RGB tab, specify the Red, Green, and Blue settings, and click **OK**.

Severity is a non-editable column that lists each severity level by name and number.

**Note**

Each time a preference is checked or unchecked, the change is saved to the .conf file and becomes available for all the other ASDM sessions running on the workstation at the time. You must restart ASDM for all changes to take effect.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## Configuration Tools

This section includes the following topics:

- [Save Running Configuration to TFTP Server, page 3-3](#)
- [Save Internal Log Buffer to Flash, page 3-4](#)
- [Command Line Interface, page 3-4](#)
- [Show Commands Ignored by ASDM on Device, page 3-5](#)

## Save Running Configuration to TFTP Server

The Save Running Configuration to TFTP Server feature stores a copy of the current running configuration file on a TFTP server.

To save the running configuration to a TFTP server, perform the following steps:

- Step 1** In the main ASDM application window, choose **File > Save Running Configuration to TFTP Server**. The Save Running Configuration to TFTP Server dialog box appears.
- Step 2** Enter the TFTP server IP address and file path on the TFTP server in which the configuration file will be saved, and then click **Save Configuration**.

**Note**

To configure default TFTP settings, choose **Configuration > Device Management > Management Access > File Access > TFTP Client**. After you have configured this setting, the TFTP server IP address and file path on the TFTP server appear automatically in this dialog box.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## Save Internal Log Buffer to Flash

The Save Internal Log Buffer to Flash feature lets you save the internal log buffer to flash memory.

To save the internal log buffer to flash memory, perform the following steps:

- 
- Step 1** In the main ASDM application window, choose **File > Save Internal Log Buffer to Flash**.  
The Enter Log File Name dialog box appears.
  - Step 2** Choose the first option to save the log buffer with the default file name, LOG-YYYY-MM-DD-hhmmss.txt.
  - Step 3** Choose the second option to specify a filename for the log buffer.
  - Step 4** Enter the filename for the log buffer, and then click **OK**.
- 

## Command Line Interface

The Command Line Interface feature provides a text-based tool for sending commands to the FWSM and viewing the results.

The commands you can enter with the CLI tool depend on your user privileges. See the [“Configuring AAA for System Administrators” section on page 15-25](#) for more information. Review your privilege level in the status bar at the bottom of the main ASDM application window to ensure that you have the required privileges to execute privileged-level CLI commands.



### Note

Commands entered via the ASDM CLI tool might function differently from those entered through a terminal connection to the FWSM.

To use the CLI tool, perform the following steps:

- 
- Step 1** In the main ASDM application window, choose **Tools > Command Line Interface**.  
The Command Line Interface dialog box appears.
  - Step 2** Choose the type of command (single line or multiple line) that you want, and then choose the command from the drop-down list, or type it in the field provided.
  - Step 3** Click **Send** to execute the command.
  - Step 4** To enter a new command, click **Clear Response**, and then choose (or type) another command to execute.
  - Step 5** Check the **Enable context-sensitive help (?)** check box to provide context-sensitive help for this feature. Uncheck this check box to disable the context-sensitive help.

- Step 6** After you have closed the Command Line Interface dialog box, if you changed the configuration, click **Refresh** to view the changes in ASDM.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## Command Errors

If an error occurs because you entered an incorrect command, the incorrect command is skipped and the remaining commands are processed. A message displays in the Response area to inform you whether any error occurred, as well as other related information.



### Note

ASDM supports almost all CLI commands. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for a list of commands.

## Interactive Commands

Interactive commands are not supported in the CLI tool. To use these commands in ASDM, use the **noconfirm** keyword if available, as shown in the following command:

```
crypto key generate rsa modulus 1024 noconfirm
```

## Avoiding Conflicts with Other Administrators

Multiple administrative users can update the running configuration of the FWSM. Before using the ASDM CLI tool to make configuration changes, check for other active administrative sessions. If more than one user is configuring the FWSM at the same time, the most recent changes take effect.

To view other administrative sessions that are currently active on the same FWSM, choose **Monitoring > Properties > Device Access**.

## Show Commands Ignored by ASDM on Device

The Show Commands Ignored by ASDM on Device feature lets you show the list of commands that ASDM does not support. Typically, ASDM ignores them. ASDM does not change or remove these commands from your running configuration. See the [“Unsupported Commands” section on page 2-2](#) for more information.

To display the list of unsupported commands for ASDM, perform the following steps:

- 
- Step 1** In the main ASDM application window, choose **Tools > Show Commands Ignored by ASDM on Device**.
- Step 2** Click **OK** when you are done.
- 

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## Diagnostic Tools

ASDM provides a set of diagnostic tools to help you in troubleshooting problems. This section includes the following topics:

- [Ping, page 3-6](#)
- [ASDM Java Console, page 3-8](#)

## Ping

The Ping tool is useful for verifying the configuration and operation of the FWSM and surrounding communications links, as well as for testing other network devices.

A ping is sent to an IP address and it returns a reply. This process enables network devices to discover, identify, and test each other.

The Ping tool uses ICMP (as described in RFC 777 and RFC 792) to define an echo request and reply transaction between two network devices. The echo request packet is sent to the IP address of a network device. The receiving device reverses the source and destination address and sends the packet back as the echo reply.

To use the Ping tool, perform the following steps:

- 
- Step 1** In the main ASDM application window, choose **Tools > Ping**.  
The Ping dialog box appears.
- Step 2** Enter the destination IP address for the ICMP echo request packets in the IP Address field.




---

**Note** If a hostname has been assigned in the **Configuration > Firewall > Objects > Network Objects/Groups** pane, you can use the hostname instead of the IP address.

---

**Step 3** (Optional) Choose the FWSM interface that transmits the echo request packets from the drop-down list. If it is not specified, the FWSM checks the routing table to find the destination address and uses the required interface.

**Step 4** Click **Ping** to send an ICMP echo request packet from the specified or default interface to the specified IP address and start the response timer.

The response appears in the Ping Output area. Three attempts are made to ping the IP address, and results display the following fields:

- The IP address of the device pinged or a device name, if available. The name of the device, if assigned Hosts/Networks, may be displayed, even if **NO response** is the result.
- When the ping is transmitted, a millisecond timer starts with a specified maximum, or timeout value. This timer is useful for testing the relative response times of different routes or activity levels.

- Example Ping Output:

```

Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
If the ping fails, the output is as follows:
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
????
Success rate is 0 percent (0/5)

```

**Step 5** To enter a new IP address, click **Clear Screen** to remove the previous response from the Ping Output area.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## Using the Ping Tool

Administrators can use the ASDM Ping interactive diagnostic tool in these ways:

- Loopback testing of two interfaces—A ping may be initiated from one interface to another on the same FWSM, as an external loopback test to verify basic “up” status and operation of each interface.
- Pinging to an FWSM—The Ping tool can ping an interface on another FWSM to verify that it is up and responding.
- Pinging through an FWSM—Ping packets originating from the Ping tool may pass through an intermediate FWSM on their way to a device. The echo packets will also pass through two of its interfaces as they return. This procedure can be used to perform a basic test of the interfaces, operation, and response time of the intermediate unit.
- Pinging to test questionable operation of a network device—A ping may be initiated from an FWSM interface to a network device that is suspected to be functioning incorrectly. If the interface is configured correctly and an echo is not received, there may be problems with the device.

- Pinging to test intermediate communications—A ping may be initiated from an FWSM interface to a network device that is known to be functioning correctly and returning echo requests. If the echo is received, the correct operation of any intermediate devices and physical connectivity is confirmed.

## Troubleshooting the Ping Tool

When pings fail to receive an echo, it may be the result of a configuration or operational error in an FWSM, and not necessarily because of no response from the IP address being pinged. Before using the Ping tool to ping from, to, or through an FWSM interface, perform the following basic checks:

- Verify that interfaces are configured by choosing **Configuration > Device Setup > Interfaces**.
- Verify that devices in the intermediate communications path, such as switches or routers, are correctly delivering other types of network traffic.
- Make sure that traffic of other types from “known good” sources is being passed by choosing **Monitoring > Interfaces > Interface Graphs**.

### Pinging from an FWSM Interface

For basic testing of an interface, you can initiate a ping from an FWSM interface to a network device that you know is functioning correctly and returning replies via the intermediate communications path. For basic testing, make sure you do the following:

- Verify receipt of the ping from the FWSM interface by the “known good” device. If the ping is not received, a problem with the transmitting hardware or interface configuration may exist.
- If the FWSM interface is configured correctly and it does not receive an echo reply from the “known good” device, problems with the interface hardware receiving function may exist. If a different interface with “known good” receiving capability can receive an echo after pinging the same “known good” device, the hardware receiving problem of the first interface is confirmed.

### Pinging to a FWSM Interface

When you try to ping to an FWSM interface, verify that the ping response (ICMP echo reply) is enabled for that interface by choosing **Tools > Ping**. When ping is disabled, the FWSM cannot be detected by other devices or software applications, and will not respond to the ASDM Ping tool.

### Pinging Through the FWSM

To verify that other types of network traffic from “known good” sources is being passed through the FWSM, choose **Monitoring > Interfaces > Interface Graphs** or an SNMP management station.

To enable internal hosts to ping external hosts, configure ICMP access correctly for both the inside and outside interfaces by choosing **Configuration > Firewall > Objects > Service Groups**.

## ASDM Java Console

You can use the ASDM Java console to view and copy logged entries in a text format, which can help you troubleshoot ASDM errors. To access this tool, in the main ASDM application window, choose **Tools > ASDM Java Console**.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## File Management Tools

ASDM provides a set of file management tools to help you perform basic file management tasks. This section includes the following topics:

- [File Management, page 3-9](#)
- [Upgrade Software from Local Computer, page 3-10](#)
- [File Transfer, page 3-11](#)
- [Upgrade Software from Cisco.com Wizard, page 3-12](#)
- [ASDM Assistant, page 3-13](#)
- [System Reload, page 3-14](#)

## File Management

The File Management tool lets you view, move, copy, and delete files stored in flash memory, transfer files, and manage files on remote storage devices (mount points).



### Note

In multiple context mode, this tool is only available in the system security context.

To use the file management tools, perform the following steps:

**Step 1** In the main ASDM application window, choose **Tools > File Management**.

The File Management dialog box appears.

- The Folders pane displays the available folders on disk.
- Flash Space shows the total amount of flash memory and how much memory is available.
- The Files area displays the following information about files in the selected folder:
  - Path
  - Filename
  - Size (bytes)
  - Time Modified
  - Status (Not Used)

**Step 2** Click **View** to display the selected file in your browser.

**Step 3** Click **Cut** to cut the selected file for pasting to another directory.

**Step 4** Click **Copy** to copy the selected file for pasting to another directory.

- Step 5** Click **Paste** to paste the copied file to the selected destination.
- Step 6** Click **Delete** to remove the selected file from flash memory.
- Step 7** Click **Rename** to rename a file.
- Step 8** Click **New Directory** to create a new directory for storing files.
- Step 9** Click **File Transfer** to open the File Transfer dialog box. See the [“File Transfer” section on page 3-11](#) for more information.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

## Upgrade Software from Local Computer

The Upgrade Software from Local Computer tool lets you upload an image file from your PC to the flash file system to upgrade the FWSM.

To upgrade software from your PC, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software from Local Computer dialog box appears.
- Step 2** Choose the image file to upload from the drop-down list.
- Step 3** Enter the local path to the file on your PC or click **Browse Local Files** to find the file on your PC.
- Step 4** Enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 5** Click **Image to Upload**. The uploading process might take a few minutes; make sure you wait until it is finished.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## File Transfer

The File Transfer tool lets you copy a local file on your PC or a flash file system to and from your FWSM using HTTP, HTTP over SSL, TFTP, FTP, or SMB.

To transfer files, perform the following steps:

- 
- Step 1** To transfer a file from a remote server, choose the **Remote server** option.
  - Step 2** Define the source file to be transferred.
    - a. Choose the path to the location of the file, including the IP address of the server.
    - b. Enter the port number or type (if FTP) of the remote server. Valid FTP types are the following:
      - ap—ASCII files in passive mode
      - an—ASCII files in non-passive mode
      - ip—Binary image files in passive mode
      - in—Binary image files in non-passive mode
  - Step 3** To copy the file from the flash file system, choose the **Flash file system** option.
  - Step 4** Enter the path to the location of the file or click **Browse Flash** to find the file location.
  - Step 5** To copy the file from your local PC, choose the **Local Computer** option.
  - Step 6** Enter the path to the location of the file or click **Browse Local Files** to find the file.
  - Step 7** In addition, you can copy a file from your startup configuration, running configuration, and an SMB file system through the CLI. For instructions about using the **copy** command, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.
  - Step 8** Define the destination of the file to be transferred.
    - a. To transfer the file to the flash file system, choose the **Flash file system** option.
    - b. Enter the path to the location of the file or click **Browse Flash** to find the file location.
  - Step 9** To transfer a file to a remote server, choose the **Remote server** option.
    - a. Enter the path to the location of the file.
    - b. For FTP transfers, enter the type. Valid types are the following:
      - ap—ASCII files in passive mode
      - an—ASCII files in non-passive mode
      - ip—Binary image files in passive mode
      - in—Binary image files in non-passive mode
  - Step 10** Click **Transfer File** to start the file transfer. The file transfer process might take a few minutes; make sure you wait until it is finished.
- 

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

## Upgrade Software from Cisco.com Wizard

The Upgrade Software from Cisco.com Wizard lets you automatically upgrade the ASDM and FWSM to more current versions.



**Note** This feature is not available in the context mode.

In this wizard, you can do the following:

- Download the list of available releases from Cisco.com.
- Select an ASDM image file or software image file for upgrade.
- Upgrade the images you have selected.
- Reload the firewall if you have upgraded the software image (optional).




**Note** You must upgrade incrementally from one version to the next (for example, from Version 5.1 to 5.2, from Version 5.2 to 6.1(F), and so on). You cannot upgrade from Version 5.1 to 6.0(F).

To complete the Upgrade Software from Cisco.com Wizard, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Upgrade Software from Cisco.com**.  
The Upgrade Software from Cisco.com Wizard appears. The Overview screen describes the steps in the image upgrade process.
- Step 2** Click **Next** to continue.  
The Authentication screen appears.
- Step 3** Enter your assigned Cisco.com user name and the Cisco.com password, and then click **Next**.  
The Image Selection screen appears.
- Step 4** Choose one or both of the two options listed.
- Check the **Upgrade the FWSM version** check box to specify the most current FWSM image to which you want to upgrade.
  - Check the **Upgrade the ASDM version** check box to specify the most current ASDM version to which you want to upgrade.



**Note** If the image version list or the ASDM version list is empty, a statement appears informing you that no new image or ASDM images are available. If you see this statement, you can exit the wizard.

- Step 5** Click **Next** to continue.  
The Selected Images screen appears.
- Step 6** Verify that the image file you have selected is the correct one, and then click **Next** to start the upgrade.  
The wizard indicates that the upgrade will take a few minutes. You can then view the status of the upgrade as it progresses.  
The Results screen appears. This screen provides additional details, such as whether the upgrade failed or whether you want to save the configuration and reload the FWSM.  
If you upgraded the FWSM version and the upgrade succeeded, an option to save the configuration and reload the FWSM appears.
- Step 7** Click **Yes**.  
For the upgrade versions to take effect, you must save the configuration, reload the FWSM, and restart ASDM.
-  **Note** You do not need to restart the wizard after you have completed one incremental upgrade. You can return to Step 3 of the wizard to upgrade to the next higher version, if any.
- Step 8** Click **Finish** to exit the wizard when the upgrade is finished.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

## ASDM Assistant

The ASDM Assistant tool lets you search and view useful ASDM procedural help about certain tasks. Alternatively, you can search for information by entering text in the Look For box next to the toolbar, and then pressing **Go**.

To view the ASDM Assistant, perform the following steps:

- Step 1** In the main ASDM application window, choose **View > ASDM Assistant**.  
The ASDM Assistant pane appears.
- Step 2** In the Search box, enter the information that you want to find, and click **Go**.  
The requested information appears in the Search Results pane.
- Step 3** Click any links that appear in the How Do I? or Features sections to obtain more details.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

## System Reload

The System Reload tool lets you schedule a system reload or cancel a pending reload.

To schedule a reload, perform the following steps:

- 
- Step 1** In the Reload Scheduling section, define the following reload scheduling settings:
- For the Configuration State, choose either to save the running configuration at reload time or to discard configuration changes to the running configuration at reload time.
  - For the Reload Start Time, you can select from the following options:
    - Click **Now** to perform an immediate reload.
    - Click **Delay by** to delay the reload by a specified amount of time. Enter the time to elapse before the reload in hours and minutes or only minutes.
    - Click **Schedule at** to schedule the reload to occur at a specific time and date. Enter the time of day the reload is to occur, and select the date of the scheduled reload.
  - In the Reload Message field, enter a message to send to open instances of ASDM at reload time.
  - Check the **On reload failure force immediate reload after** check box to show the amount of time elapsed in hours and minutes or minutes only before a reload is attempted again.
  - Click **Schedule Reload** to schedule the reload as configured.
 

The Confirm Schedule Reload dialog box appears. Click **Yes** to schedule the reload. Click **No** to bypass the reload.

The Reload Status area displays the status of the reload.

Click **Cancel Reload** to stop a scheduled reload.

Click **Refresh** to refresh the Reload Status display after a scheduled reload is finished.

Click **Details** to display the details of a scheduled reload.
- 

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

