



# CHAPTER 5

## Before You Start

---

This chapter includes the following sections:

- [Configuring FWSM for ASDM Access, page 5-1](#)
- [Setting Transparent or Routed Firewall Mode at the CLI, page 5-2](#)
- [Downloading the ASDM Launcher, page 5-2](#)
- [Starting ASDM, page 5-3](#)
- [Configuration Overview, page 5-5](#)

## Configuring FWSM for ASDM Access

To use ASDM, you need to enable the HTTPS server, and allow HTTPS connections to the FWSM. These tasks are completed if you use the **setup** command. This section describes how to manually configure ASDM access.

The FWSM allows a maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 80 ASDM instances between all contexts. You can control the number of ASDM sessions allowed per context using resource classes. (See the [“Configuring Resource Classes” section on page 9-16.](#))

To configure ASDM access, perform the following steps:

- 
- Step 1** To identify the IP addresses from which the FWSM accepts HTTPS connections, enter the following command for each address or subnet:

```
hostname(config)# http source_IP_address mask source_interface
```

- Step 2** To enable the HTTPS server, enter the following command:

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

---

For example, to enable the HTTPS server and let a host on the inside interface with an address of 192.168.1.2 access ASDM, enter the following commands:

```
hostname(config)# http server enable  
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

To allow all users on the 192.168.3.0 network to access ASDM on the inside interface, enter the following command:

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

## Setting Transparent or Routed Firewall Mode at the CLI

You cannot change the mode in single mode in ASDM; in multiple mode, you cannot change the mode of the admin context in ASDM. You must change the mode at the CLI.

When you change modes, the FWSM clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

If you download a text configuration to the FWSM that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the FWSM changes the mode as soon as it reads the command and then continues reading the configuration that you downloaded. If the command is later in the configuration, the FWSM clears all the preceding lines in the configuration.

- To set the mode to transparent, enter the following command in each context:

```
hostname(config)# firewall transparent
```

- To set the mode to routed, enter the following command in each context:

```
hostname(config)# no firewall transparent
```

## Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. 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

This section describes how to start ASDM according to one of the following methods:

- [Starting ASDM from the ASDM Launcher, page 5-3](#)
- [Using ASDM in Demo Mode, page 5-3](#)
- [Starting ASDM from a Web Browser, page 5-5](#)

## Starting ASDM from the ASDM Launcher

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

---

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

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

If a new version of ASDM is available 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 on Windows that uses the ASDM Launcher and pre-packaged configuration files to let you run ASDM without a live device available. In ASDM Demo Mode you can:

- 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 sys log messages. The data shown is randomly generated, but the experience is identical to what you would see when connecting to an actual device.

ASDM Demo Mode has the following limitations:

- Changes made to the configuration will appear in the GUI but are not applied to the configuration file. That is, when you click the Refresh button, it will revert back to the original configuration. The changes are never saved to the configuration file.
- File and disk operations are not supported.
- Monitoring and logging data are simulated. Historical monitoring data is not available.
- You can only log in as an admin user; you cannot log in as a monitor-only or read-only user.

ASDM 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 All Running Configurations to Flash
  - Save Internal Log Buffer to Flash
  - Clear Internal Log Buffer
- Tools menu:
  - Command Line Interface
  - Ping
  - File Management > File Transfer
  - Upgrade Software from Cisco.com
  - Upgrade Software from Local Computer
  - System Reload > Device System Reload
  - Backup Configurations
  - Restore Configurations
- 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>. Find the *asdm-version-demo.msi* file.
  - b. Double-click the installer to install the software.
- Step 2** Double-click the Cisco ASDM Launcher shortcut on your desktop, or use 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**. Then make your selections from the Demo Mode area.
- Step 5** To use new ASDM images as they are released, you can either download the most recent installer, or download the normal ASDM images and install them for Demo Mode:
- a. To download the normal ASDM image, go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm>. Find the *asdm-version.bin* file.

- 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.

A Demo Mode label appears in the title bar of the window.

---

## Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

- Step 1** From a supported web browser on the 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. By default, leave the name and password blank.

A page displays with the following options:

- **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. By default, leave the name and password blank.
- 



**Note** You cannot start ASDM on the FWSM using the Java Web Start application.

---

## Configuration Overview

To configure and monitor the FWSM, perform the following steps:

- Step 1** For initial configuration, use the Startup Wizard by choosing **Configuration > Device Setup > Startup Wizard**, and then clicking **Launch Startup Wizard**.

- Step 2** Configure advanced features by choosing either **Configuration > Device Management** or **Configuration > Firewall**. Features include:

- [Configuring Routed Interfaces](#)—Configures basic interface parameters including the IP address, name, security level, and for transparent mode, the bridge group.
- [Configuring Management Access Rules](#)—Permits or denies IP traffic through the FWSM. For transparent firewall mode, you can also apply an EtherType access list to allow non-IP traffic.

- [Configuring Ethertype Rules \(Transparent Mode Only\)](#)—Permits or denies non-IP traffic through the FWSM.
- [AAA Performance](#)—Requires authentication and/or authorization for certain types of traffic, for example, for HTTP. The FWSM also sends accounting information to a RADIUS or TACACS+ server.
- [Configuring Filtering Rules](#)—Prevents outbound access to specific websites or FTP servers. The FWSM works with a separate server running either Websense Enterprise or Sentian by N2H2. Choose **Configuration > Firewall > URL Filtering Servers** to configure the URL filtering server, which you must configure before adding a rule.
- [Service Policy Overview](#)—Applies application inspection, connection limits, and TCP normalization. Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the FWSM to do a deep packet inspection. You can also limit TCP and UDP connections, and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP normalization drops packets that do not appear normal.
- [Configuring NAT Control](#)—Translates addresses used on a protected network to addresses used on the public Internet. This lets you use private addresses, which are not routable on the Internet, on your inside networks.
- [Configuring Dynamic Routing](#) and [Configuring Static Routes](#) —(Single mode only) Configures OSPF, RIP, multicast, and asymmetric routing.
- [Using Network Objects and Groups](#)—Provides a single location where you can configure, view, and modify the reusable components that you need to implement your policy on the FWSM. These reusable components, or global objects, include the following:
  - Network Objects and Groups
  - Global Pools
  - Service Groups
  - Class Maps
  - Inspect Maps
  - Time Ranges
  - Regular Expressions

**Step 3** Monitor the FWSM by clicking **Monitoring** on the toolbar and then clicking a feature button. Features include:

- [Monitoring Interfaces](#)—Monitors the ARP table, DHCP, dynamic access list, and interface statistics.
- [Monitoring Routing](#)—Monitors routes, OSPF LSAs, and OSPF neighbors.
- [Monitoring Properties](#)—Monitors management sessions, AAA servers, failover, CRLs, the DNS cache, and system statistics.
- [Monitoring Logging](#)—Monitors syslog messages.
- [Monitoring Failover](#)—(Multiple mode) Monitors failover.