



CHAPTER 8

Configuring Device Settings and Management

This section contains the following topics:

- [Management IP Address, page 8-1](#)
- [Configuring Advanced Device Management Features, page 8-2](#)
- [System Image/Configuration, page 8-3](#)
- [Device Name/Password, page 8-7](#)
- [System Software, page 8-8](#)

Management IP Address

The **Management IP** pane lets you set the management IP address for the FWSM or for a context in transparent firewall mode. A transparent firewall does not participate in IP routing. The only IP configuration required for the FWSM is the management IP address. The exception is that you can set the IP address for the Management 0/0 management-only interface, which does not pass through traffic. See the [Configuring Interfaces](#) chapter to set the IP address for Management 0/0.

This address is required because the FWSM uses this address as the source address for traffic originating on the FWSM, such as system messages or communications with AAA servers. You can also use this address for remote management access.

Fields

- **Management IP Address**—Sets the management IP address.
- **Subnet Mask**—Sets the subnet mask.

Modes

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

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

Configuring Advanced Device Management Features

The following sections describe how to configure the items in the **Advanced** menu.

Configuring HTTP Redirect

The HTTP Redirect table displays each interface on the FWSM, shows whether it is configured to redirect HTTP connections to HTTPS, and the port number from which it redirects those connections.



Note

To redirect HTTP, the interface requires an access list that permits HTTP. Otherwise the interface cannot listen to the HTTP port.

To change the HTTP redirect setting of an interface or the port from which it redirects HTTP connections, select the interface in the table and click **Edit**. You can also double-click an interface. The Edit HTTP/HTTPS Settings dialog box opens.

Fields in the Edit HTTP/HTTPS pane

The Edit HTTP/HTTPS Settings dialog box displays the following fields:

- **Interface**—Identifies the interface on which the FWSM redirects or does not redirect HTTP requests to HTTPS.
- **Redirect HTTP to HTTPS**—Check to redirect HTTP requests to HTTPS, or uncheck to not redirect HTTP requests to HTTPS.
- **HTTP Port**—Identifies the port from which the interface redirects HTTP connections. By default it listens to port 80.

Modes

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

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

History Metrics

The History Metrics pane lets you configure the adaptive FWSM to keep a history of various statistics, which ASDM can display on any Graph/Table. If you do not enable history metrics, you can only monitor statistics in real time. Enabling history metrics lets you view statistics graphs from the last 10 minutes, 60 minutes, 12 hours, and 5 days.

To configure history metrics, perform the following steps:

- Step 1** Choose **Configuration > Device Management > Advanced > History Metrics**.

The History Metrics pane appears.

Step 2 Check the **ASDM History Metrics** check box to enable history metrics, and then click **Apply**.

Modes

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

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

System Image/Configuration

This section contains the following topics:

- [Activation Key, page 8-3](#)
- [Auto Update, page 8-3](#)

Activation Key

The Activation Key pane lets you view the device serial number and activation keys in the running configuration and Flash memory. You can also update the activation key on this pane.

To update the activation key, perform the following steps:

Step 1 Go to **Configuration > Device Management > System Image/Configuration > Activation Key**.

Step 2 Enter the new activation key in the New Activation Key field. Enter the activation key as a four- or five-element hexadecimal string with one space between each element, for example:

```
0x00000000 0x00000000 0x00000000 0x00000000
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal. The key is not stored in the configuration file. The key is tied to the serial number.

Step 3 Click **Update Activation Key**.

You do not need to reload for the new key to take effect.

Auto Update

The Auto Update pane lets you configure the FWSM to be managed remotely from servers that support the Auto Update specification. Auto Update lets you apply configuration changes to the FWSM and receive software updates from remote locations.

Auto Update is useful in solving many of the challenges facing administrators for FWSM management:

- Overcomes dynamic addressing and NAT challenges.

- Gives ability to commit configuration changes in one atomic action.
- Provides a reliable method for updating software.
- Leverages well understood methods for high scalability.
- Open interface gives developers tremendous flexibility.
- Simplifies security solutions for Service Provider environments.
- High reliability, rich security/management features, broad support by many products.

Introduction to Auto Update

The Auto Update specification provides the infrastructure necessary for remote management applications to download FWSM configurations, software images, and to perform basic monitoring from a centralized location or multiple locations.

The Auto Update specification allows the Auto Update server to either push configuration information and send requests for information to the FWSM, or to pull configuration information by causing the FWSM to periodically poll the Auto Update server. The Auto Update server can also send a command to the FWSM to send an immediate polling request at any time. Communication between the Auto Update server and the FWSM requires a communications path and local CLI configuration on each FWSM.

The Auto Update feature on the FWSM can be used with Cisco security products, as well as products from third-party companies that want to manage the FWSM.

Important Notes

- If the FWSM configuration is updated from an Auto Update server, ASDM is not notified. You must choose **Refresh** or **File > Refresh ASDM with the Running Configuration on the Device** to get the latest configuration, and any changes to the configuration made in ASDM will be lost.
- If HTTPS is chosen as the protocol to communicate with the Auto Update server, the FWSM will use SSL. This requires the FWSM to have a DES or 3DES license.

Fields

The Auto Update pane consists of an Auto Update Servers table and two areas: the Timeout area, and the Polling area.

The Auto Update Servers table lets you view the parameters of previously-configured Auto Update servers. The FWSM polls the server listed at the top of the table first. You can change the order of the servers in the table with the Move Up and Move Down buttons. The Auto Update Servers table contains the following columns:

- Server—The name or IP address of the Auto Update server.
- User Name—The user name used to access the Auto Update server.
- Interface—The interface used when sending requests to the Auto Update server.
- Verify Certificate—Indicates whether the FWSM checks the certificate returned by the Auto Update server against the Certification Authority (CA) root certificates. This requires that the Auto Update server and the FWSM use the same CA.

Double-clicking any of the rows in the Auto Update Server table opens the Edit Auto Update Server dialog box, in which you can modify the Auto Update server parameters. These changes are immediately reflected in the table, but you must click Apply to save them to the configuration.

The Timeout area lets you set the amount of time the FWSM waits for the Auto Update server to time out. The Timeout area contains the following fields:

- **Enable Timeout Period**—Check to enable the FWSM to time out if no response is received from the Auto Update server.
- **Timeout Period (Minutes)**—Enter the number of minutes the FWSM will wait to time out if no response is received from the Auto Update server.

The Polling area lets you configure how often the FWSM will poll for information from the Auto Update server. The Polling area contains the following fields:

- **Polling Period (minutes)**—The number of minutes the FWSM will wait to poll the Auto Update server for new information.
- **Poll on Specified Days**—Allows you to specify a polling schedule.
- **Set Polling Schedule**—Displays the Set Polling Schedule dialog box where you can configure the days and time-of-day to poll the Auto Update server.
- **Retry Period (minutes)**—The number of minutes the FWSM will wait to poll the Auto Update server for new information if the attempt to poll the server fails.
- **Retry Count**—The number of times the FWSM will attempt to retry to poll the Auto Update server for new information.

Modes

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

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

Set Polling Schedule

The Set Polling Schedule dialog box lets you configure specific days, and the time-of-day for the FWSM to poll the Auto Update server.

Fields

The Set Polling Schedule dialog box contains the following fields:

Days of the Week—Check the days of the week that you want the FWSM to poll the Auto Update server.

The Daily Update pane group lets you configure the time of day when you want the FWSM to poll the Auto Update server, and contains the following fields:

- **Start Time**—Enter the hour and minute to begin the Auto Update poll.
- **Enable randomization**—Check to enable the FWSM to randomly choose a time to poll the Auto Update server.

Modes

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

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

Add/Edit Auto Update Server

The Edit Auto Update Server dialog box contains the following fields:

- URL—The protocol the Auto Update server uses to communicate with the FWSM, either http or https, and the path to the Auto Update server.
- Interface—The interface to use when sending requests to the Auto Update server.
- Verify Certificate—Select to enable the FWSM to verify the certificate returned by the Auto Update server against the Certification Authority (CA) root certificates. This requires that the Auto Update server and the FWSM use the same CA.

The User area contains the following fields:

- User Name (Optional)—Enter the user name needed to access the Auto Update server.
- Password—Enter the user password for the Auto Update server.
- Confirm Password—Reenter the user password for the Auto Update server.

Modes

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

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

Advanced Auto Update Settings

Fields

- Use Device ID to uniquely identify the ASA—Enables authentication using a Device ID. The Device ID is used to uniquely identify the FWSM to the Auto Update server.
- Device ID—Type of Device ID to use.
 - Hostname—The name of the host.
 - Serial Number—Device serial number.
 - IP Address on interface—The IP address of the selected interface, used to uniquely identify the FWSM to the Auto Update server.
 - MAC Address on interface—The MAC address of the selected interface, used to uniquely identify the FWSM to the Auto Update server.
 - User-defined value—A unique user ID.

Modes

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

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

Device Name/Password

The **Device Name/Password** pane lets you set the hostname and domain name for the FWSM and set the enable and telnet passwords..

The hostname appears in the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. The hostname is also used in system messages.

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line; it can be used for a banner.

The FWSM appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name of “jupiter,” then the FWSM qualifies the name to “jupiter.example.com.”

The Telnet Password sets the login password. By default, it is “cisco.” Although this area is called Telnet Password, this password applies to Telnet and SSH access. The login password lets you access EXEC mode if you connect to the FWSM using a Telnet or SSH session. (If you configure user authentication for Telnet or SSH access, then each user has their own password, and this login password is not used; see the [“Configuring AAA for System Administrators” section on page 16-25.](#))

The enable password lets you access privileged EXEC mode after you log in. Also, this password is used to access ASDM as the default user, which is blank. The default user shows as “enable_15” in the [User Accounts](#) pane. (If you configure user authentication for enable access, then each user has their own password, and this enable password is not used; see the [“Configuring AAA for System Administrators” section on page 16-25.](#) In addition, you can configure authentication for HTTP/ASDM access.)

Fields

The Hostname and Domain Name areas contain the following fields:

- **Primary Hostname**—Sets the hostname on the primary unit in a failover pair. The default hostname depends upon on your platform.
- **Secondary Hostname**—Sets the hostname on the secondary unit in a failover pair. By default, the hostname for the secondary unit is the same as the hostname for the primary unit; however, if you configure a secondary hostname, it must be different from the primary hostname.
- **Domain Name**—Sets the domain name. The default domain name is default.domain.invalid.

The Enable Password area contains the following fields. In multiple context mode, the Enable Password area only appears in contexts; it does not appear in the system execution space.

- **Change the privileged mode password**—Lets you change the enable password.
- **Old Password**—Enter the old password.

- New Password—Enter the new password.
- Confirm New Password—Confirm the new password.

The Telnet Password area contains the following fields. In multiple context mode, the Telnet Password area only appears in contexts; it does not appear in the system execution space.

- Change the password to access the console—Lets you change the login password.
- Old Password—Enter the old password.
- New Password—Enter the new password.
- Confirm New Password—Confirm the new password.

Modes

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

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

System Software

The System Software pane lets you configure the parameters of FWSMs configured as Auto Update clients when this FWSM is acting as an Auto Update server.

As an Auto Update server, you can specify the platform and ASDM images for FWSMs configured as Auto Update clients, including image revision numbers and locations, according to the device ID, device family, or device type of the client.

Introduction to Auto Update Server and Client Update

The Auto Update specification provides the infrastructure necessary for remote management applications to download FWSM configurations, software Images, and to perform basic monitoring from a centralized location.

As an Auto Update server, the specification allows the Auto Update server to either push configuration information and send requests for information to the FWSM, or to pull configuration information by causing the FWSM to periodically poll the Auto Update server. The Auto Update server can also send a command to the FWSM to send an immediate polling request at any time. Communication between the Auto Update server and the FWSM requires a communications path and local CLI configuration on each FWSM.

Fields

The Client Update pane consists of the following fields:

- Enable Client Update—Check to allow the FWSM to update the images used by other FWSMs that are configured as Auto Update clients.
- Client Images table—lets you view previously-configured Client Update entries and includes the following columns:
 - Device—Displays a text string corresponding to a device-id of the client.

- Device Family—Displays the family name of a client, either asa, pix, or a text string.
- Device Type—Displays the type name of a client.
- Image Type—Specifies the type of image, either ASDM image or Boot image.
- Image URL—Specifies the URL for the software component.
- Client Revision—Specifies the revision number(s) of the software component.

Double-clicking any of the rows in the Client Images table opens the Edit Client Update Entry dialog box, in which you can modify the client parameters. These changes are immediately reflected in the table, but you must click Apply to save them to the configuration.

- Live Client Update area—Lets you immediately update Auto Update clients that are currently connected to the FWSM through a tunnel.
 - Tunnel Group—Select “all” to update all Auto Update clients connected over all tunnel groups, or specify a tunnel group for clients that you want to update.
 - Update Now—Click to begin an immediate update.



Note Live Client Update is only available when the FWSM is configured in routed mode.

Modes

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

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

Add/Edit Client Update

Fields

The Add/Edit Client Update dialog box displays the following fields:

- Device Identification group:
 - Device ID—Enable if the client is configured to identify itself with a unique string, and specify the same string that the client uses. The maximum length is 63 characters.
 - Device Family—Enable if the client is configured to identify itself by device family, and specify the same device family that the client uses. It can be asa, pix, or a text string with a maximum length of 7 characters.
 - Device Type—Enable if the client is configured to identify itself by device type, and specify the same device type that the client uses. It can be pix-515, pix-515e, pix-525, pix-535, asa5505, asa5510, asa5520, or asa5540. It can also be a text string with a maximum length of 15 characters.
 - Not Specified—Select for clients that do not match the above.
- Image Type—Specifies an image type, either ASDM or boot image. This URL must point to a file appropriate for this client. Maximum length of 255 characters.

- Client Revision—Specifies a text string corresponding to the revision number(s) of the software component. For example: 7.1(0)22.
- Image URL—Specifies the URL for the software component. This URL must point to a file appropriate for this client.

Modes

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

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