

Configuring ASA FirePOWER Module Settings

The following table summarizes an ASA FirePOWER module's local configuration.

Table 35-1 Local Configuration Options

Option	Description	For more information, see...
Information	Allows you to view current information about the appliance. You can also change the appliance name.	Viewing and Modifying the Appliance Information, page 35-1
Cloud Services	Allows you to download URL filtering data from the Collective Security Intelligence Cloud, perform lookups for uncategorized URLs, and send diagnostic information on detected files to Cisco.	Enabling Cloud Communications, page 35-2

Viewing and Modifying the Appliance Information

License: Any

The Information page provides you with information about your ASA FirePOWER module. The information includes read-only information, such as the product name and model number, the operating system and version, and the current system policy. The page also provides you with an option to change the name of the appliance.

The following table describes each field.

Table 35-2 Appliance Information

Field	Description
Name	A name you assign to the appliance. Note that this name is only used within the context of the ASA FirePOWER module. Although you can use the hostname as the name of the appliance, entering a different name in this field does not change the hostname.
Product Model	The model name for the appliance.
Serial Number	The chassis serial number of the appliance.
Software Version	The version of the software currently installed.
Operating System	The operating system currently running on the appliance.
Operating System Version	The version of the operating system currently running on the appliance.

Table 35-2 Appliance Information (continued)

Field	Description
IPv4 Address	The IPv4 address of the default (`eth0`) management interface of the appliance. If IPv4 management is disabled for the appliance, this field indicates that.
IPv6 Address	The IPv6 address of the default (`eth0`) management interface of the appliance. If IPv6 management is disabled for the appliance, this field indicates that.
Current Policies	The appliance-level policies currently applied. If a policy has been updated since it was last applied, the name of the policy appears in italics.
Model Number	The model number for the appliance. This number may be important for troubleshooting.

To modify the appliance information:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > Configuration**.

The Information page appears.

Step 2 To change the appliance name, type a new name in the **Name** field.

The name **must** be alphanumeric characters and cannot be composed of numeric characters only.

Step 3 To save your changes, click **Save**.

The page refreshes and your changes are saved.

Enabling Cloud Communications

License: URL Filtering or Malware

The ASA FirePOWER module contacts Cisco's Collective Security Intelligence Cloud to obtain various types of information:

- File policies associated with access control rules allow devices to detect files transmitted in network traffic. The ASA FirePOWER module uses data from the Cisco cloud to determine if the files represent malware; see Understanding and Creating File Policies, page 26-4.
- When you enable URL filtering, the ASA FirePOWER module can retrieve category and reputation data for many commonly visited URLs, as well as perform lookups for uncategorized URLs. You can then quickly create URL conditions for access control rules; see Performing Reputation-Based URL Blocking, page 8-8.

Use the ASA FirePOWER module's local configuration to specify the following options:

Enable URL Filtering

You must enable this option to perform category and reputation-based URL filtering.

Query Cloud for Unknown URL

Allows the system to query the cloud when someone on your monitored network attempts to browse to a URL that is not in the local data set.

If the cloud does not know the category or reputation of a URL, or if the ASA FirePOWER module cannot contact the cloud, the URL does **not** match access control rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually.

Disable this option if you do not want your uncategorized URLs to be cataloged by the Cisco cloud, for example, for privacy reasons.

Enable Automatic Updates

Allows the system to contact the cloud on a regular basis to obtain updates to the URL data in your appliances' local data sets. Although the cloud typically updates its data once per day, enabling automatic updates forces the ASA FirePOWER module to check every 30 minutes to make sure that you always have up-to-date information.

Although daily updates tend to be small, if it has been more than five days since your last update, new URL filtering data may take up to 20 minutes to download, depending on your bandwidth. Then, it may take up to 30 minutes to perform the update itself.

If you want to have strict control of when the system contacts the cloud, you can disable automatic updates and use the scheduler instead, as described in Automating URL Filtering Updates, page 33-8.

Note Cisco recommends that you either enable automatic updates or use the scheduler to schedule updates. Although you can manually perform on-demand updates, allowing the system to automatically contact the cloud on a regular basis provides you with the most up-to-date, relevant URL data.

Licensing

Performing category and reputation-based URL filtering and device-based malware detection require that you enable the appropriate licenses on your ASA FirePOWER module; see Licensing the ASA FirePOWER Module, page 36-1.

You **cannot** configure cloud connection options if you have no URL Filtering license on the ASA FirePOWER module. The Cloud Services local configuration page displays only the options for which you are licensed. ASA FirePOWER modules with expired licenses cannot contact the cloud.

Note that, in addition to causing the URL Filtering configuration options to appear, adding a URL Filtering license to your ASA FirePOWER module automatically enables **Enable URL Filtering** and **Enable Automatic Updates**. You can manually disable the options if needed.

Internet Access

The system uses ports 80/HTTP and 443/HTTPS to contact the Cisco cloud.

The following procedures explain how to enable communications the Cisco cloud, and how to perform an on-demand update of URL data. Note that you cannot start an on-demand update if an update is already in progress.

To enable communications with the cloud:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > Configuration**.

The Information page appears.

Step 2 Click **Cloud Services**.

The Cloud Services page appears. If you have a URL Filtering license, the page displays the last time URL data was updated.

Step 3 Configure cloud connection options as described above.

You must **Enable URL Filtering** before you can **Enable Automatic Updates** or **Query Cloud for Unknown URLs**.

Step 4 Click **Save**.

Your settings are saved. If you enabled URL filtering, depending on how long it has been since URL filtering was last enabled, or if this is the first time you enabled URL filtering, the ASA FirePOWER moduleretrieves URL filtering data from the cloud.

To perform an on-demand update of the system's URL data:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration > Cisco CSI**.

The Information page appears.

Step 2 Click **URL Filtering**.

The URL Filtering page appears.

Step 3 Click **Update Now**.

The ASA FirePOWER module contacts the cloud and updates its URL filtering data if an update is available.

Time

You can view the current time and time source on the ASA FirePOWER module using the Time page.