

Licensing the ASA FirePOWER Module

You can license a variety of features to create an optimal ASA FirePOWER deployment for your organization.

For more information, see:

- Understanding Licensing, page 36-1
- Viewing Your Licenses, page 36-4
- Adding a License to the ASA FirePOWER module, page 36-4
- Deleting a License, page 36-5

Understanding Licensing

License: Any

You can license a variety of features to create an optimal ASA FirePOWER deployment for your organization.

Licenses allow your device to perform a variety of functions including:

- intrusion detection and prevention
- Security Intelligence filtering
- file control and advanced malware protection
- application, user, and URL control

There are a few ways you may lose access to licensed features in the ASA FirePOWER module. You can remove licensed capabilities. In addition, some licenses may expire. Though there are some exceptions, you cannot use the features associated with an expired or deleted license.

This section describes the types of licenses available in an ASA FirePOWER module deployment. The licenses you can enable on an appliance can depend the other licenses enabled.

The following table summarizes ASA FirePOWER module licenses.

Table 36-1 ASA FirePOWER Module Licenses

License	Granted Capabilities	Requires
Protection	intrusion detection and prevention file control Security Intelligence filtering	none
Control	user and application control	Protection
Malware	advanced malware protection (network-based malware detection and blocking)	Protection
URL Filtering	category and reputation-based URL filtering	Protection

For more information, see:

- Protection, page 36-2
- Control, page 36-3
- Malware, page 36-3
- URL Filtering, page 36-3

Protection

License: Protection

A Protection license allows you to perform intrusion detection and prevention, file control, and Security Intelligence filtering:

- *Intrusion detection and prevention* allows you to analyze network traffic for intrusions and exploits and, optionally, drop offending packets.
- *File control* allows you to detect and, optionally, block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. With a Malware license (see Malware, page 36-3), you can also inspect and block a restricted set of those file types based on their malware dispositions.
- *Security Intelligence filtering* allows you to blacklist—deny traffic to and from—specific IP addresses, before the traffic is subjected to analysis by access control rules. Dynamic feeds allow you to immediately blacklist connections based on the latest intelligence. Optionally, you can use a "monitor-only" setting for Security Intelligence filtering.

Although you can configure an access control policy to perform Protection-related inspection without a license, you cannot apply the policy until you first add a Protection license to the ASA FirePOWER module.

If you delete your Protection license from the ASA FirePOWER module, the ASA FirePOWER module stops detecting intrusion and file events. Additionally, the ASA FirePOWER module will not contact the internet for either Cisco-provided or third-party Security Intelligence information. You cannot reapply existing policies until you re-enable Protection.

Because a Protection license is required for URL Filtering, Malware, and Control licenses, deleting or disabling a Protection license has the same effect as deleting or disabling your URL Filtering, Malware, or Control license.

Control

License: Control

A Control license allows you to implement user and application control by adding user and application conditions to access control rules. To enable Control, you must also enable Protection.

Although you can add user and application conditions to access control rules without a Control license, you cannot apply the policy until you first add a Control license to the ASA FirePOWER module.

If you delete your Control license, you cannot reapply existing access control policies if they include rules with user or application conditions.

URL Filtering

License: URL Filtering

URL filtering allows you to write access control rules that determine the traffic that can traverse your network based on URLs requested by monitored hosts, correlated with information about those URLs, which is obtained from the Cisco cloud by the ASA FirePOWER module. To enable URL Filtering, you must also enable a Protection license.

Tip Without a URL Filtering license, you can specify individual URLs or groups of URLs to allow or block. This gives you granular, custom control over web traffic, but does not allow you to use URL category and reputation data to filter network traffic.

URL filtering requires a subscription-based URL Filtering license. Although you can add category and reputation-based URL conditions to access control rules without a URL Filtering license, the ASA FirePOWER module will not contact the cloud for URL information. You cannot apply the access control policy until you first add a URL Filtering license to the ASA FirePOWER module.

You may lose access to URL filtering if you delete the license from the ASA FirePOWER module. Also, URL Filtering licenses may expire. If your license expires or if you delete it, access control rules with URL conditions immediately stop filtering URLs, and your ASA FirePOWER module can no longer contact the cloud. You cannot reapply existing access control policies if they include rules with category and reputation-based URL conditions.

Malware

License: Malware

A Malware license allows you to perform advanced malware protection, that is, use devices to detect and block malware in files transmitted over your network. To enable Malware on a device, you must also enable Protection.

You configure malware detection as part of a file policy, which you then associate with one or more access control rules. File policies can detect your users uploading or downloading files of specific types over specific application protocols. The Malware license allows you to inspect a restricted set of those file types for malware. The Malware license also allows you to add specific files to a file list and enable the file list within a file policy, allowing those files to be automatically allowed or blocked on detection.

Although you can add a malware-detecting file policy to an access control rule without a Malware license, the file policy is marked with a warning icon ( ) in the access control rule editor. Within the file policy, Malware Cloud Lookup rules are also marked with the warning icon. Before you can apply

an access control policy that includes a malware-detecting file policy, you **must** add a Malware license. If you later delete the license, you cannot reapply an existing access control policy to those devices if it includes file policies that perform malware detection.

If you delete your Malware license or it expires, the ASA FirePOWER module stops performing malware cloud lookups, and also stops acknowledging retrospective events sent from the Cisco cloud. You cannot reapply existing access control policies if they include file policies that perform malware detection. Note that for a very brief time after a Malware license expires or is deleted, the system can use cached dispositions for files detected by Malware Cloud Lookup file rules. After the time window expires, the system assigns a disposition of `Unavailable` to those files, rather than performing a lookup.

Viewing Your Licenses

License: Any

Use the Licenses page to view the licenses for an ASA FirePOWER module.

Other than the Licenses page, there are a few other ways you can view licenses and license limits:

- The Product Licensing dashboard widget provides an at-a-glance overview of your licenses.
- The Device page (**Configuration > ASA FirePOWER Configuration > Device Management > Device**) lists the licenses.

To view your licenses:

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

The Licenses page appears.

Adding a License to the ASA FirePOWER module

License: Any

Before you add a license to the ASA FirePOWER module, make sure you have the activation key provided by Cisco when you purchased the license. You **must** add licenses before you can use licensed features.

Note If you add licenses after a backup has completed, these licenses will not be removed or overwritten if this backup is restored. To prevent a conflict on restore, remove those licenses before restoring the backup, noting where the licenses were used, and add and reconfigure them after restoring the backup. If a conflict occurs, contact Support.

To add a license:

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

The Licenses page appears.

Step 2 Click **Add New License**.

The Add License page appears.

Step 3 Did you receive an email with your license?

- If yes, copy the license from the email, paste it into the **License** field, and click **Submit License**.

  If the license is correct, the license is added. Skip the rest of the procedure.

- If no, click **Get License**.

  The Product License Registration portal appears. If you cannot access the Internet, switch to a computer that can. Note the license key at the bottom of the page and browse to https://www.cisco.com/go/license.

Step 4 Follow the on-screen instructions to obtain your license, which will be sent to you in an email.

Tip You can also request a license on the **Licenses** tab after you log into the Support Site.

Step 5 Copy the license from the email, paste it into the **License** field in the ASA FirePOWER module's web user interface, and click **Submit License**.

If the license is valid, it is added.

Deleting a License

License: Any

Use the following procedure if you need to delete a license for any reason. Keep in mind that because Cisco generates licenses based on each ASA FirePOWER module's unique license key, you cannot delete a license from one ASA FirePOWER module and then reuse it on a different ASA FirePOWER module.

In most cases, deleting a license removes your ability to use features enabled by that license. For more information, see Understanding Licensing, page 36-1.

To delete a license:

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

The Licenses page appears.

Step 2 Next to the license you want to delete, click the delete icon ( ).

Step 3 Confirm that you want to delete the license.

The license is deleted.