Licensing the Firepower System

The Licensing chapter of the Firepower Management Center Configuration Guide provides in-depth information about the different license types, service subscriptions, licensing requirements and more. The chapter also provides procedures and requirements for deploying Smart and Classic licenses and licensing for air-gapped solutions.

The following topics explain how to license Firepower.

About Firepower Licenses

Your Firepower products (Firepower Management Center and managed devices) include licenses for basic operation, but some features require separate licensing or service subscriptions, as described in this chapter.

A "right-to-use" license does not expire, but service subscriptions require periodic renewal.

The type of license your products require depends on the software you use, not on the hardware it runs on.

Requirements and Prerequisites for Licensing

Model Support

Any, but the specific licenses requires per model differ as indicated in the procedures.

Supported Domains

Global, except where indicated.

User Roles

- Admin

License Requirements for Firepower Management Center

Firepower Management Center allows you to assign licenses to managed devices and manage licenses for the system.

Hardware FMC

A hardware Firepower Management Center does not require purchase of additional licenses or service subscriptions in order to manage devices.

Virtual FMC

Firepower Management Center Virtual has additional licensing requirements. Contact your authorized representative for details.

Evaluation License Caveats

Not all functionality is available with an evaluation license, functionality under an evaluation license may be partial, and transition from evaluation licensing to standard licensing may not be seamless.

Review information about evaluation license caveats in information about particular features in this Licensing chapter and in the chapters related to deploying each feature.

Licensing All Devices

7000 and 8000 Series and NGIPSv devices and ASA FirePOWER modules require Classic licenses. These devices are frequently referred to in this documentation as Classic devices.

Important If you are running Firepower hardware but not Firepower software, see licensing information for the software product you are using. This documentation is not applicable.

Classic licenses require a product authorization key (PAK) to activate and are device-specific. Classic licensing is sometimes also referred to as "traditional licensing."

Product License Registration Portal

When you purchase one or more Classic licenses for Firepower features, you manage them in the Cisco Product License Registration Portal:

https://cisco.com/go/license

For more information on using this portal, see:

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

You will need your account credentials in order to access these links.

Service Subscriptions for Firepower Features (Classic Licensing)

Some features require a service subscription.

A service subscription enables a specific Firepower feature on a managed device for a set length of time. Service subscriptions can be purchased in one-, three-, or five-year terms. If a subscription expires, Cisco notifies you that you must renew the subscription. If a subscription expires for a Classic device, you might not be able to use the related features, depending on the feature type.

Table 1: Service Subscriptions and Corresponding Classic Licenses

Subscription You Purchase	Classic Licenses You Assign in Firepower System
TA	Control + Protection (a.k.a. "Threat & Apps," required for system updates)
TAC	Control + Protection + URL Filtering
TAM	Control + Protection + Malware
TAMC	Control + Protection + URL Filtering + Malware
URL	URL Filtering (add-on where TA is already present)
AMP	Malware (add-on where TA is already present)

Your purchase of a managed device that uses Classic licenses automatically includes Control and Protection licenses. These licenses are perpetual, but you must also purchase a TA service subscription to enable system updates. Service subscriptions for additional features are optional.

Classic License Types and Restrictions

This section describes the types of Classic licenses available in a Firepower System deployment. The licenses you can enable on a device depend on its model, version, and the other licenses enabled.

Licenses are model-specific for 7000 and 8000 Series and NGIPSv devices and for ASA FirePOWER modules. You cannot enable a license on a managed device unless the license exactly matches the device's model. For example, you cannot use a Firepower 8250 Malware license (FP8250-TAM-LIC=) to enable Malware capabilities on an 8140 device; you must purchase a Firepower 8140 Malware license (FP8140-TAM-LIC=).

Note For NGIPSv or ASA FirePOWER, the Control license allows you to perform user and application control, but these devices do not support switching, routing, stacking, or 7000 and 8000 Series device high availability.

There are a few ways you may lose access to licensed features in the Firepower System:

- You can remove Classic licenses from the Firepower Management Center, which affects all of its managed devices.

- You can disable licensed capabilities on specific managed devices.

Though there are some exceptions, you cannot use the features associated with an expired or deleted license.

The following table summarizes Classic licenses in the Firepower System.

Table 2: Firepower System Classic Licenses

License You Assign in Firepower System	Service Subscription You Purchase	Platforms	Granted Capabilities	Also Requires	Expire Capable?
Any	TA, TAC, TAM, or TAMC	7000 and 8000 Series ASA FirePOWER NGIPSv	host, application, and user discovery decrypting and inspecting SSL- and TLS-encrypted traffic	none	depends on license
Protection	TA (included with device)	7000 and 8000 Series ASA FirePOWER NGIPSv	intrusion detection and prevention file control Security Intelligence filtering	none	no
Control	none (included with device)	7000 and 8000 Series	user and application control switching and routing 7000 and 8000 Series device high availability 7000 and 8000 Series network address translation (NAT)	Protection	no
Control	none (included with device)	ASA FirePOWER NGIPSv	user and application control	Protection	no
Malware	TAM, TAMC, or AMP	7000 and 8000 Series ASA FirePOWER NGIPSv	AMP for Networks (network-based Advanced Malware Protection) File storage	Protection	yes
URL Filtering	TAC, TAMC, or URL	7000 and 8000 Series ASA FirePOWER NGIPSv	category and reputation-based URL filtering	Protection	yes
VPN	none (contact Sales for more information)	7000 and 8000 Series	deploying virtual private networks	Control	yes

Protection Licenses

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. *AMP for Networks*, which requires a Malware license, allows you to inspect and block a restricted set of those file types based on their dispositions.
- *Security Intelligence filtering* allows you to block —deny traffic to and from—specific IP addresses, URLs, and DNS domain names, before the traffic is subjected to analysis by access control rules. Dynamic feeds allow you to immediately block connections based on the latest intelligence. Optionally, you can use a "monitor-only" setting for Security Intelligence filtering.

A Protection license (along with a Control license) is automatically included in the purchase of any Classic managed device. This license is perpetual, but you must also purchase a TA subscription to enable system updates.

Although you can configure an access control policy to perform Protection-related inspection without a license, you cannot deploy the policy until you first add a Protection license to the Firepower Management Center, then enable it on the devices targeted by the policy.

If you delete your Protection license from the Firepower Management Center or disable Protection on managed devices, the Firepower Management Center stops acknowledging intrusion and file events from the affected devices. As a consequence, correlation rules that use those events as a trigger criteria stop firing. Additionally, the Firepower Management Center will not contact the internet for either Cisco-provided or third-party Security Intelligence information. You cannot re-deploy 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 Licenses

A Control license allows you to implement user and application control by adding user and application conditions to access control rules. For 7000 and 8000 Series devices only, this license also allows you to configure switching and routing (including DHCP relay and NAT) and device high-availability pairs. To enable a Control license on a managed device, you must also enable a Protection license. A Control license is automatically included (along with a Protection license) in the purchase of any Classic managed device. This license is perpetual, but you must also purchase a TA subscription to enable system updates.

If you do not enable a Control license for a Classic managed device, you can add user and application conditions to rules in an access control policy, but you cannot deploy the policy to the device. If you do not enable a Control license for 7000 or 8000 Series devices specifically, you also cannot:

- create switched, routed, or hybrid interfaces
- create NAT entries
- configure DHCP relay for virtual routers
- deploy a device configuration that includes switch or routing to the device

- establish high availability between devices

Note Although you can create virtual switches and routers without a Control license, they are not useful without switched and routed interfaces to populate them.

If you delete a Control license from the Firepower Management Center or disable Control on individual devices:

- The affected devices do **not** stop performing switching or routing, nor do device high-availability pairs break.
- You can continue to edit and delete existing configurations, but you cannot deploy those changes to the affected devices.
- You cannot add new switched, routed, or hybrid interfaces, nor can you add new NAT entries, configure DHCP relay, or establish 7000 or 8000 Series device high-availability.
- You cannot re-deploy existing access control policies if they include rules with user or application conditions.

URL Filtering Licenses for Classic Devices

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. To enable a URL Filtering license, you must also enable a Protection license. You can purchase a URL Filtering license for Classic devices as a services subscription combined with Threat & Apps (TAC) or Threat & Apps and Malware (TAMC) subscriptions, or as an add-on subscription (URL) for a system where Threat & Apps (TA) is already enabled.

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.

Although you can add category and reputation-based URL conditions to access control rules without a URL Filtering license, the Firepower Management Center will not download URL information. You cannot deploy the access control policy until you first add a URL Filtering license to the Firepower Management Center, then enable it on the devices targeted by the policy.

You may lose access to URL filtering if you delete the license from the Firepower Management Center or disable URL Filtering on managed devices. Also, URL Filtering licenses may expire. If your license expires or if you delete or disable it, access control rules with URL conditions immediately stop filtering URLs, and your Firepower Management Center can no longer download updates to URL data. You cannot re-deploy existing access control policies if they include rules with category and reputation-based URL conditions.

Malware Licenses for Classic Devices

A Malware license allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Networks and Cisco Threat Grid. You can use managed devices to detect and block malware in files transmitted over your network. To enable a Malware license, you must also enable Protection. You can purchase a Malware

license as a subscription combined with Threat & Apps (TAM) or Threat & Apps and URL Filtering (TAMC) subscriptions, or as an add-on subscription (AMP) for a system where Threat & Apps (TA) is already enabled.

Note 7000 and 8000 Series managed devices with Malware licenses enabled attempt to connect periodically to the AMP cloud even if you have not configured dynamic analysis. Because of this, the device's Interface Traffic dashboard widget shows transmitted traffic; this is expected behavior.

You configure AMP for Networks 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. AMP for Networks allows you to use local malware analysis and file preclassification to inspect a restricted set of those file types for malware. You can also download and submit specific file types to the Cisco Threat Grid cloud for dynamic and Spero analysis to determine whether they contain malware. For these files, you can view the network file trajectory, which details the path the file has taken through your network. 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.

Before you can deploy an access control policy that includes AMP for Networks configurations, you **must** add a Malware license, then enable it on the devices targeted by the policy. If you later disable the license on the devices, you cannot re-deploy the existing access control policy to those devices.

If you delete all your Malware licenses or they all expire, the system stops querying the AMP cloud, and also stops acknowledging retrospective events sent from the AMP cloud. You cannot re-deploy existing access control policies if they include AMP for Networks configurations. Note that for a very brief time after a Malware license expires or is deleted, the system can use existing cached file dispositions. After the time window expires, the system assigns a disposition of `Unavailable` to those files.

A Malware license is required only if you deploy AMP for Networks and Cisco Threat Grid. Without a Malware license, the Firepower Management Center can receive AMP for Endpoints malware events and indications of compromise (IOC) from the AMP cloud.

See also important information at License Requirements for File and Malware Policies.

VPN Licenses for 7000 and 8000 Series Devices

VPN allows you to establish secure tunnels between endpoints via a public source, such as the Internet or other network. You can configure the Firepower System to build secure VPN tunnels between the virtual routers of 7000 and 8000 Series devices. To enable VPN, you must also enable Protection and Control licenses. To purchase a VPN license, contact Sales.

Without a VPN license, you cannot configure a VPN deployment with your 7000 and 8000 Series devices. Although you can create deployments, they are not useful without at least one VPN-enabled routed interface to populate them.

If you delete your VPN license from the Firepower Management Center or disable VPN on individual devices, the affected devices do **not** break the current VPN deployments. Although you can edit and delete existing deployments, you cannot deploy your changes to the affected devices.

Classic Licenses in Device Stacks and High-Availability Pairs

Individual devices must have equivalent licenses before they can be stacked or configured into 7000 or 8000 Series device high-availability pairs. After you stack devices, you can change the licenses for the entire stack. However, you cannot change the enabled licenses on a 7000 or 8000 Series device high-availability pair.

See also About Device Stacks and Device High Availability Requirements.

View Your Classic Licenses

Procedure

Do one of the following, depending on your needs:

To View	Do This
The Classic licenses that you have added to the Firepower Management Center and details including their type, status, usage, expiration dates, and the managed devices to which they are applied.	Choose **System** > **Licenses** > **Classic Licenses**. The summary shows the number of licenses you have purchased, followed by the number of licenses that are in used in parentheses.
The licenses applied to each of your managed devices	Choose **Devices** > **Device Management**.
License status in the Health Monitor	Use the Classic License Monitor health module in a health policy. For information, see Health Monitoring, including #unique_149 and Creating Health Policies.
An overview of your licenses in the Dashboard	Add the Product Licensing widget to the dashboard of your choice. For instructions, see The Product Licensing Widget and Adding Widgets to a Dashboard and Dashboard Widget Availability by User Role.

Identify the License Key

The license key uniquely identifies the Firepower Management Center in the Cisco License Registration Portal. It is composed of a product code (for example, 66) and the MAC address of the management port (eth0) of the Firepower Management Center; for example, 66:00:00:77:FF:CC:88.

You will use the license key in the Cisco License Registration Portal to obtain the license text required to add licenses to the Firepower Management Center.

Procedure

Step 1 Choose **System** > **Licenses** > **Classic Licenses**.

Step 2 Click **Add New License**.

Step 3 Note the value in the **License Key** field at the top of the **Add Feature License** dialog.

What to do next

- Add a license to the Firepower Management Center; see Generate a Classic License and Add It to the Firepower Management Center, on page 9.

  This procedure includes the process of generating the actual license text using the license key.

Generate a Classic License and Add It to the Firepower Management Center

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.

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

Before you begin

- Make sure you have the product activation key (PAK) from the Software Claim Certificate that Cisco provided when you purchased the license. If you have a legacy, pre-Cisco license, contact Support.
- Identify the license key for the Firepower Management Center; see Identify the License Key, on page 8.
- You will need your account credentials to complete this procedure.

Procedure

Step 1 Choose **System** > **Licenses** > **Classic Licenses**.

Step 2 Click **Add New License**.

Step 3 Continue as appropriate:

- If you have already obtained the license text, skip to Step 8.
- If you still need to obtain the license text, go to the next step.

Step 4 Click **Get License** to open the Cisco License Registration Portal.

Note If you cannot access the Internet using your current computer, switch to a computer that can, and browse to http://cisco.com/go/license.

Step 5 Generate a license from the PAK in the License Registration Portal.

This step requires the PAK you received during the purchase process, as well as the license key for the Firepower Management Center.

For information, see Product License Registration Portal, on page 2.

Step 6 Copy the license text from either the License Registration Portal display, or the email the License Registration Portal sends you.

Important The licensing text block in the portal or email message may include more than one license. Each license is bounded by a BEGIN LICENSE line and an END LICENSE line. Make sure that you copy and paste only one license at a time.

Step 7 Return to the **Add Feature License** page in the Firepower Management Center's web interface.

Step 8 Paste the license text into the **License** field.

Step 9 Click **Verify License**.

If the license is invalid, make sure that you correctly copied the license text.

Step 10 Click **Submit License**.

What to do next

- Assign the license to a managed device; see Assign Licenses to Managed Devices from the Device Management Page, on page 10. You **must** assign licenses to your managed devices before you can use licensed features on those devices.

Assign Licenses to Managed Devices from the Device Management Page

Although there are some exceptions, you cannot use the features associated with a license if you disable it on a managed device.

Before you begin

- Add your devices to the Firepower Management Center. See Add a Device to the FMC.
- You must have Admin or Network Admin privileges to perform this task. When operating with multiple domains, you must do this task in leaf domains.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to assign or disable a license, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Device**.

Step 4 Next to the License section, click **Edit** ( ).

Step 5 Check or clear the appropriate check boxes to assign or disable licenses for the device.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Additional Information about Firepower Licensing

For additional information to help resolve common licensing questions, see the following documents:

- The *Frequently Asked Questions (FAQ) about Firepower Licensing* document at:
  https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html
- The *Cisco Firepower System Feature Licenses* document at:
  https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html