Licensing the System

The following topics explain how to license the Firepower Threat Defense device.

- Smart Licensing for the Firepower System, on page 1
- Managing Smart Licenses, on page 3

Smart Licensing for the Firepower System

Cisco Smart Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, smart licenses are not tied to a specific serial number or license key. Smart licensing lets you assess your license usage and needs at a glance.

In addition, Smart Licensing does not prevent you from using product features that you have not yet purchased. You can start using a license immediately, as long as you are registered with the Cisco Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval.

Cisco Smart Software Manager

When you purchase one or more licenses for the Firepower Threat Defense device, you manage them in the Cisco Smart Software Manager: https://software.cisco.com/#SmartLicensing-Inventory. The Cisco Smart Software Manager lets you create a master account for your organization.

By default, your licenses are assigned to the Default Virtual Account under your master account. As the account administrator, you can create additional virtual accounts; for example, for regions, departments, or subsidiaries. Multiple virtual accounts help you manage large numbers of licenses and appliances.

Licenses and appliances are managed per virtual account; only that virtual account's appliances can use the licenses assigned to the account. If you need additional licenses, you can transfer an unused license from another virtual account. You can also transfer appliances between virtual accounts.

When you register a device with Cisco Smart Software Manager, you create a Product Instance Registration Token in the manager, and then enter it in Firepower Device Manager. A registered device becomes associated with a virtual account based on the token that is used.

For more information about the Cisco Smart Software Manager, see the online help for the manager.

Periodic Communication with the License Authority

When you use a Product Instance Registration Token to register a Firepower Threat Defense device, the device registers with the Cisco License Authority. The License Authority issues an ID certificate for communication between the device and the License Authority. This certificate is valid for one year, although it will be renewed every six months. If an ID certificate expires (usually in nine months or a year with no communication), the device reverts to a de-registered state and licensed feature usage is suspended.

The device communicates with the License Authority on a periodic basis. If you make changes in the Cisco Smart Software Manager, you can refresh the authorization on the device so the changes immediately take effect. You also can wait for the device to communicate as scheduled. Normal license communication occurs every 30 days, but with the grace period, your device will operate for up to 90 days without calling home. You must contact the License Authority before 90 days have passed.

Smart License Types

The following table explains the licenses available for the Firepower Threat Defense device.

Your purchase of a Firepower Threat Defense device automatically includes a Base license. All additional licenses are optional.

Table 1: Smart License Types

License	Duration	Granted Capabilities
Base (automatically included)	Perpetual	All features not covered by the optional term licenses. You must also specify whether to **Allow export-controlled functionality on the products registered with this token**. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.
Threat	Term-based	**Intrusion detection and prevention**—Intrusion policies analyze network traffic for intrusions and exploits and, optionally, drop offending packets. **File control**—File policies detect and, optionally, block users from uploading (sending) or downloading (receiving) files of specific types. AMP for Firepower, which requires a Malware license, allows you to inspect and block files that contain malware.
Malware	Term-based	File policies that check for malware, which use Cisco Advanced Malware Protection (AMP) with AMP for Firepower (network-based Advanced Malware Protection) and AMP Threat Grid. File policies can detect and block malware in files transmitted over your network.

License	Duration	Granted Capabilities
URL Filtering	Term-based	Category and reputation-based URL filtering. You can perform URL filtering on individual URLs without this license.
RA VPN: • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only	Term-based or perpetual based on license type.	Remote access VPN configuration. Your base license must allow export-controlled functionality to configure RA VPN. You select whether you meet export requirements when you register the device. Firepower Device Manager can use any valid AnyConnect license. The available features do not differ based on license type. If you have not already purchased one, see Licensing Requirements for Remote Access VPN. Also see *Cisco AnyConnect Ordering Guide*, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

Impact of Expired or Disabled Optional Licenses

If an optional license expires, you can continue using features that require the license. However, the license is marked out of compliance and you need to purchase the license and add it to your account to bring the license back into compliance.

If you disable an optional license, the system reacts as follows:

- **Malware license**—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 file policies that apply malware inspection. Note that for a very brief time after a Malware license is disabled, the system can use existing cached file dispositions. After the time window expires, the system assigns a disposition of Unavailable to those files.
- **Threat**—The system no longer applies intrusion or file-control policies. You cannot re-deploy existing policies that require the license.
- **URL Filtering**—Access control rules with URL category conditions immediately stop filtering URLs, and the system no longer downloads updates to URL data. You cannot re-deploy existing access control policies if they include rules with category and reputation-based URL conditions.
- **RA VPN**—You cannot edit the remote access VPN configuration, but you can remove it. Users can still connect using the RA VPN configuration. However, if you change the device registration so that the system is no longer export compliant, the remote access VPN configuration stops immediately and no remote users can connect through the VPN.

Managing Smart Licenses

Use the Smart License page to view the current license status for the system. The system must be licensed.

The page shows you whether you are using the 90-day evaluation license, or if you have registered with the Cisco Smart Software Manager. Once registered, you can see the status of the connection to the Cisco Smart Software Manager as well as the status for each type of license.

Usage Authorization identifies the Smart License Agent status:

- Authorized ("Connected," "Sufficient Licenses")—The device has contacted and registered successfully with the License Authority, which has authorized the license entitlements for the appliance. The device is now In-Compliance.
- Out-of-Compliance—There is no available license entitlement for the device. Licensed features continue to work. However, you must either purchase or free up additional entitlements to become In-Compliance.
- Authorization Expired—The device has not communicated with the Licensing Authority in 90 or more days. Licensed features continue to work. In this state, the Smart License Agent retries its authorization requests. If a retry succeeds, the agent enters either an Out-of-Compliance or Authorized state, and begins a new Authorization Period. Try manually synchronizing the device.

Note Click the **i** button next to the Smart License status to view the virtual account, export-controlled features, and get a link to open the Cisco Smart Software Manager. Export-Controlled Features control software that is subject to national security, foreign policy, and anti-terrorism laws and regulations.

The following procedure provides an overview of how to manage licenses for the system.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Register the device.

You must register with the Cisco Smart Software Manager before you can assign the optional licenses. Register before the end of the evaluation period.

See Registering the Device, on page 5.

Step 3 Request and manage the optional feature licenses.

You must register the optional licenses to use the features controlled by the license. See Enabling or Disabling Optional Licenses, on page 5.

Step 4 Maintain system licensing.

You can do the following tasks:

- Synchronizing with the Cisco Smart Software Manager, on page 6
- Unregistering the Device, on page 6

Registering the Device

Your purchase of a Firepower Threat Defense device automatically includes a Base license. The Base license covers all features not covered by the optional licenses. It is a perpetual license.

During initial system setup, you are prompted to register the device with Cisco Smart Software Manager. If you instead elected to use the 90-day evaluation license, you must register the device before the end of the evaluation period.

When you register the device, your virtual account allocates the license to the device. Registering the device also registers any optional licenses that you have enabled.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Click **Request Register** and follow the instructions.

a) Click the link to open the Cisco Smart Software Manager and log into your account, or create a new one if necessary.

b) Generate a new token.

When you create the token, you specify the amount of time the token is valid for use. The recommended expiration period is 30 days. This period defines the expiration date of the token itself, and has no impact on the device that you register using the token. If the token expires before you can use it, you can simply generate a new token.

You must also specify whether to **Allow export-controlled functionality on the products registered with this token**. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.

c) Copy and paste the token into the edit box on the Smart License Registration dialog box.

d) Click **Request Register**.

Enabling or Disabling Optional Licenses

You can enable (register) or disable (release) optional licenses. You must enable a license to use the features controlled by the license.

If you no longer want to use the features covered by an optional term license, you can disable the license. Disabling the license releases it in your Cisco Smart Software Manager account, so that you can apply it to another device.

You can also enable evaluation versions of these licenses when running in evaluation mode. In evaluation mode, the licenses are not registered with Cisco Smart Software Manager until you register the device. However, you cannot enable the RA VPN license in evaluation mode.

Before you begin

Before disabling a license, ensure that you are not using it. Rewrite or delete any policies that require the license.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Click the **Enable/Disable** control for each optional license as desired.

- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.
- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.

Step 3 If you enabled the **RA VPN** license, select the type of license you have available in your account.

You can use any of the AnyConnect licenses: **Plus**, **Apex**, or **VPN Only**. You can select **Plus and Apex** if you have both licenses and you want to use them both.

Synchronizing with the Cisco Smart Software Manager

The system periodically synchronizes license information with Cisco Smart Software Manager. Normal license communication occurs every 30 days, but with the grace period, your appliance will operate for up to 90 days without calling home.

However, if you make changes in the Cisco Smart Software Manager, you can refresh the authorization on the device so the changes immediately take effect.

Synchronization gets the current status of licenses, and renews authorization and the ID certificate.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select **Resync Connection** from the gear drop-down list.

Unregistering the Device

If you no longer want to use the device, you can unregister it from the Cisco Smart Software Manager. When you unregister, the base license and all optional licenses associated with the device are freed in your virtual account. Optional licenses are available to be assigned to other devices.

After unregistering the device, the current configuration and policies on the device continue to work as-is, but you cannot make or deploy any changes.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select **Unregister Device** from the gear drop-down list.

Step 3 Read the warning and click **Unregister** if you really want to unregister the device.