

# 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, on page 1
- Requirements and Prerequisites for Licensing, on page 2
- License Requirements for Firepower Management Center, on page 2
- Evaluation License Caveats, on page 2
- Smart vs. Classic Licenses, on page 3
- License Firepower Threat Defense Devices (FTD), on page 3
- License Classic Devices ( Firepower 7000/8000 Series, ASA FirePOWER, and NGIPSv), on page 21
- How to Convert a Classic License for Use on an FTD Device, on page 29
- Assign Licenses to Managed Devices from the Device Management Page, on page 31
- Additional Information about Firepower Licensing, on page 32


# 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 (Smart or Classic) depends on the software you use, not on the hardware it runs on.

**Note** "NGFW" means different things to different people, so this documentation does not use this term.

# 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.

A single Firepower Management Center can manage both devices that require Classic licenses and devices that require Smart Licenses.

### 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. See Firepower Management Center Virtual Licenses, on page 2.

## Firepower Management Center Virtual Licenses

If a single FMCv manages Firepower Threat Defense devices that are configured in a high availability pair, you still need one entitlement for each device (*not* one entitlement for the pair of FTDs.)

This entitlement appears in Cisco Smart Software Manager as **Firepower MCv Device License** with different numbers of entitlements.

# 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.

For example, if you have Firepower Threat Defense devices configured in a cluster, and you switch from an evaluation license to Smart Licensing, service will be interrupted when you deploy the change.

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

# Smart vs. Classic Licenses

For managed devices, the licenses you need (Smart or Classic) depend on the software that runs on the device.

Any FMC can simultaneously manage devices with Smart and Classic licenses. You must configure each type of licensing separately.

| Software | License Type | More Information |
|---|---|---|
| Firepower Management Center (hardware) | None | FMC hardware models themselves require no license. |
| Firepower Management Center Virtual | Device entitlements | See Firepower Management Center Virtual Licenses, on page 2. |
| Firepower Threat Defense<br>Firepower Threat Defense Virtual | Smart | See the topics under License Firepower Threat Defense Devices (FTD), on page 3. |
| NGIPS software:<br>• Firepower 7000/8000 series<br>• ASA FirePOWER<br>• NGIPSv | Classic | See License Classic Devices ( Firepower 7000/8000 Series, ASA FirePOWER, and NGIPSv), on page 21. |
| All other software products, including those that run on Firepower hardware | See licensing information for your software product. | |

# License Firepower Threat Defense Devices (FTD)

Firepower Threat Defense devices require Smart Licensing.

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.

# Smart Software Manager (CSSM)

When you purchase one or more Smart Licenses for Firepower features, you manage them in the Cisco Smart Software Manager: http://www.cisco.com/web/ordering/smart-software-manager/index.html. The Smart Software Manager lets you create a primary account for your organization.

By default, your licenses are assigned to the Default Virtual Account under your primary 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.

You manage licenses and appliances by 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.

For each virtual account, you can create a Product Instance Registration Token. Enter this token ID when you deploy each Firepower Management Center, or when you register an existing FMC. You can create a new token if an existing token expires. An expired token does not affect a registered FMC that used this token for registration, but you cannot use an expired token to register a FMC. Also, a registered FMC becomes associated with a virtual account based on the token you use.

For more information about the Cisco Smart Software Manager, see *Cisco Smart Software Manager User Guide* or https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html or the online help in CSSM, also available from: https://www.cisco.com/web/fw/softwareworkspace/smartlicensing/SSMCompiledHelps/.

# Periodic Communication with the License Authority

In order to maintain your product license entitlement, your product must communicate periodically with the Cisco License Authority.

When you use a Product Instance Registration Token to register a Firepower Management Center, the appliance registers with the Cisco License Authority. The License Authority issues an ID certificate for communication between the Firepower Management Center 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 Firepower Management Center reverts to a deregistered state and licensed features usage become suspended.

The Firepower Management Center communicates with the License Authority on a periodic basis. If you make changes in the Smart Software Manager, you can refresh the authorization on the Firepower Management Center so the changes immediately take effect. You also can wait for the appliance to communicate as scheduled.

Your Firepower Management Center must either have direct Internet access to the License Authority through the Cisco Smart Software Manager or access through the Smart Software Satellite Server at scheduled time periods. Normal license communication occurs every 30 days, but with the grace period, your appliance will operate for up to 90 days without calling home. You must contact the License Authority before 90 days have passed.

# Service Subscriptions for FTD Features

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 Firepower Threat Defense device, you can continue to use the related features.

***Table 1: Service Subscriptions and Corresponding Smart Licenses***

| Subscription You Purchase | Smart Licenses You Assign in Firepower System |
|---|---|
| T | Threat |
| TC | Threat + URL Filtering |
| TM | Threat + Malware |
| TMC | Threat + URL Filtering + Malware |
| URL | URL Filtering (can be added to Threat or used without Threat) |
| AMP | Malware (the Threat license is also required) |

Your purchase of a managed device that uses Smart Licenses automatically includes a Base license. This license is perpetual and enables system updates. All service subscriptions are optional for Firepower Threat Defense devices.

# FTD License Types and Restrictions

This section describes the types of Smart Licenses available in a Firepower System deployment. The Firepower Management Center requires Smart Licenses to manage Firepower Threat Defense devices.

The following table summarizes Firepower System Smart Licenses.

***Table 2: Firepower System Smart Licenses***

| License You Assign in Firepower System | Subscription You Purchase | Duration | Granted Capabilities |
|---|---|---|---|
| Base<br>(Base licenses are automatically assigned with all Firepower Threat Defense devices) | No subscription required (license is included with device) | Perpetual | User and application control<br>Switching and routing<br>NAT<br>For details, see Base Licenses, on page 7. |
| Threat | • T<br>• TC (Threat + URL)<br>• TMC (Threat + Malware + URL) | Term-based | Intrusion detection and prevention<br>File control<br>Security Intelligence filtering<br>For details, see Threat Licenses, on page 8 |

| License You Assign in Firepower System | Subscription You Purchase | Duration | Granted Capabilities |
|---|---|---|---|
| Malware | • TM (Threat + Malware)<br>• TMC (Threat + Malware + URL)<br>• AMP | Term-based | AMP for Networks (network-based Advanced Malware Protection)<br>Cisco Threat Grid<br>File storage<br>For details, see Malware Licenses for Firepower Threat Defense Devices, on page 7 and License Requirements for File and Malware Policies. |
| URL Filtering | • TC (Threat + URL)<br>• TMC (Threat + Malware + URL)<br>• URL | Term-based | Category and reputation-based URL filtering<br>For details, see URL Filtering Licenses for Firepower Threat Defense Devices, on page 8. |
| Firepower Management Center Virtual | No subscription required. | Perpetual | The platform license determines the number of devices the virtual appliance can manage.<br>For details, see Firepower Management Center Virtual Licenses, on page 2. |
| Export-Controlled Features | No subscription required. | Perpetual | Features that are subject to national security, foreign policy, and anti-terrorism laws and regulations; see Licensing for Export-Controlled Functionality, on page 9. |
| Remote Access VPN:<br>• AnyConnect Apex<br>• AnyConnect Plus<br>• AnyConnect VPN Only | Based on license type. | Term-based or perpetual based on license type. | Remote access VPN configuration. Your base license must allow export-controlled functionality to configure Remote Access VPN. You select whether you meet export requirements when you register the device. Firepower Threat Defense can use any valid AnyConnect license. The available features do not differ based on license type.<br>For more information, see AnyConnect Licenses, on page 9 and VPN Licensing. |

## Base Licenses

A base license is automatically included with every purchase of a Firepower Threat Defense or Firepower Threat Defense Virtual device.

The Base license allows you to:

- configure your Firepower Threat Defense devices to perform switching and routing (including DHCP relay and NAT)
- configure Firepower Threat Defense devices as a high availability pair
- configure security modules as a cluster within a Firepower 9300 chassis (intra-chassis clustering)
- configure Firepower 9300 or Firepower 4100 series devices running Firepower Threat Defense as a cluster (inter-chassis clustering)
- implement user and application control by adding user and application conditions to access control rules

Threat and malware detection and URL filtering features require additional, optional licenses.

Base licenses are automatically added to the Firepower Management Center for every Firepower Threat Defense device you register.

## Malware Licenses for Firepower Threat Defense Devices

A Malware license for Firepower Threat Defense devices allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Networks and Cisco Threat Grid. With this feature, you can use Firepower Threat Defense devices to detect and block malware in files transmitted over your network. To support this feature license, you can purchase the Malware (AMP) service subscription as a stand-alone subscription or in combination with Threat (TM) or Threat and URL Filtering (TMC) subscriptions.



**Note** Firepower Threat Defense managed devices with Malware licenses enabled periodically attempt to connect 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.

If you disable all your Malware licenses, 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 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.

Note that 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.

## Threat Licenses

A Threat 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.

You can purchase a Threat license as a stand-alone subscription (T) or in combination with URL Filtering (TC), Malware (TM), or both (TMC).

If you disable Threat 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 intrusion policies until you re-enable Threat.

## URL Filtering Licenses for Firepower Threat Defense Devices

The URL Filtering license 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 support this feature license, you can purchase the URL Filtering (URL) service subscription as a stand-alone subscription or in combination with Threat (TC) or Threat and Malware (TMC) subscriptions.



**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.

If you disable the URL Filtering license on managed devices, you may lose access to URL filtering. If your license expires or if you 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.

# AnyConnect Licenses

You can use Firepower Threat Defense device to configure remote access VPN using the Cisco AnyConnect Secure Mobility Client (AnyConnect) and standards-based IPSec/IKEv2.

You cannot deploy the Remote Access VPN configuration to the Firepower Threat Defense device if the specified device does not have the entitlement for a minimum of one of the specified AnyConnect license types. If the registered license moves out of compliance or entitlements expire, the system displays licensing alerts and health events.

While using Remote Access VPN, your Smart License Account must have the export controlled features (strong encryption) enabled. The Firepower Threat Defense requires stronger encryption (which is higher than DES) for successfully establishing Remote Access VPN connections with AnyConnect clients. When you register the device, you must do so with a Smart Software Manager account that is enabled for export-controlled features. For more information about export-controlled features, see FTD License Types and Restrictions, on page 5.

You cannot deploy Remote Access VPN if the following are true:

- Smart Licensing on the Firepower Management Center is running in evaluation mode.
- Your Smart Account is not configured to use export-controlled features (strong encryption). Note that you need to reboot Firepower Threat Defense devices after applying a base license that has export-controlled functionality.

# Licensing for Export-Controlled Functionality

### Features that require export-controlled functionality

Certain software features are subject to national security, foreign policy, and anti-terrorism laws and regulations. These export-controlled features include:

- Security certifications compliance
- Firepower Threat Defense Remote Access VPN
- Site to Site VPN with strong encryption
- SSH platform policy with strong encryption
- SSL policy with strong encryption
- Functionality such as SNMPv3 with strong encryption

### How to determine whether export-controlled functionality is currently enabled for your system

To determine whether export-controlled functionality is currently enabled for your system: Go to **System > Licenses > Smart Licenses** and see if **Export-Controlled Features** displays **Enabled**.

### About enabling export-controlled functionality

If **Export-Controlled Features** shows **Disabled** and you want to use features that require strong encryption:

- If there is *no* option to enable export-controlled functionality when you generate a new Product Instance Registration Token in Cisco Smart Software Manager (CSSM):

  Your Smart Account is not authorized to use this functionality.

- If the option to use export-controlled functionality appears when you generate a new Product Instance Registration Token in Cisco Smart Software Manager:
  - In order to use export-controlled functionality, your Smart Account must be enabled for this functionality before you license your Firepower Management Center.
  - After export-controlled functionality is enabled for your Smart Account in Cisco Smart Software Manager (CSSM), you must re-register your Firepower Management Center using a new Product Instance Registration Token.
  - When you create the new Product Instance Registration Token, you must select the option "Allow export-controlled functionality on the products registered with this token." This option is enabled by default if this functionality is permitted for your Smart Account.
  - After you install a token with export-controlled functionality on your Firepower Management Center and assign the relevant licenses to managed Firepower Threat Defense devices:
    - Reboot each device to make the newly-enabled features available.
    - In a high availability deployment, the active and standby devices must be rebooted together to avoid an Active-Active condition.

#### More Information

For general information about export controls, see https://www.cisco.com/c/en/us/about/legal/global-export-trade.html.

## Licensing for FTD Clusters

In addition to information in this Licensing chapter, see:

- Licenses for Clustering
- FMC: Add a Cluster.

# Create a Smart Account to Hold Your Licenses

A Smart Account is required for Smart Licenses and can also hold Classic licenses.

You should set up this account before you purchase Smart Licenses.

#### Before you begin

Your account representative or reseller may have set up a Smart Account on your behalf. If so, obtain the necessary information to access the account from that person instead of using this procedure, then verify that you can access the account.

For general information about Smart Accounts, see http://www.cisco.com/go/smartaccounts.

#### Procedure

**Step 1** Request a Smart Account:

For instructions, see https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 .

For additional information, see https://communities.cisco.com/docs/DOC-57261.

**Step 2** Wait for an email telling you that your Smart Account is ready to set up. When it arrives, click the link it contains, as directed.

**Step 3** Set up your Smart Account:

Go here: https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation.

For instructions, see https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604.

**Step 4** Verify that you can access the account in the Cisco Smart Software Manager (CSSM).

Go to https://software.cisco.com/#module/SmartLicensing and sign in.

# How to Configure Smart Licensing with Direct Internet Access

### Procedure

**Step 1** Obtain a token from the Cisco Smart Software Manager licensing portal.

See Obtain a Product License Registration Token for Smart Licensing, on page 12.

**Step 2** Register your Firepower Management Center with the Smart licensing portal.

See Register Smart Licenses, on page 13. Be sure to address the prerequisites in this topic.

**Step 3** Verify that your FMC registered successfully with the Smart licensing portal.

In the Firepower Management Center web interface, go to **System > Licenses > Smart Licenses**.

**Product Registration** should show a green checkmark.

**Step 4** If you have not yet done so, add devices to your FMC.

See Add a Device to the FMC.

**Step 5** Assign licenses to the devices that are managed by your FMC.

See Assign Licenses to Multiple Managed Devices, on page 15.

**Step 6** Verify that licenses are successfully installed.

See View FTD Licenses and License Status, on page 16.

### What to do next

If applicable, set up licensing for high-availability and clustered deployments.

# Obtain a Product License Registration Token for Smart Licensing

### Before you begin

- Create a Smart Account, if you have not already done so: Visit https://software.cisco.com/smartaccounts/setup#accountcreation-account. For information, see https://www.cisco.com/c/en/us/buy/smart-accounts.html.
- Ensure that you have purchased the type and number of licenses you require.
- Verify that the licenses you need appear in your Smart Account.

  If your licenses do not appear in your Smart Account, ask the person who ordered them (for example, your Cisco sales representative or authorized reseller) to transfer those licenses to your Smart Account.
- Ideally, check the prerequisites for Register Smart Licenses, on page 13 to ensure that your registration process goes smoothly.
- Make sure you have your credentials to sign in to the Cisco Smart Software Manager.

### Procedure

**Step 1** Go to https://software.cisco.com.

**Step 2** Click **Smart Software Licensing** (in the License section.)

**Step 3** Sign in to the Cisco Smart Software Manager.

**Step 4** Click **Inventory**.

**Step 5** Click **General**.

**Step 6** Click **New Token**.

**Step 7** For **Description**, enter a name that uniquely and clearly identifies the Firepower Management Center for which you will use this token.

**Step 8** Enter an expiration time within 365 days.

This determines how much time you have to register the token to a Firepower Management Center. (Your license entitlement term is independent of this setting but may start to count down even if you have not yet registered your token.)

**Step 9** If you see an option to enable export-controlled functionality, and you plan to use features that require strong encryption, select this option.

**Important** If you see this option, you must select it now if you plan to use this functionality. You cannot enable export-controlled functionality later.

If you do not see this option but you expect to, cancel out of this procedure now and contact your Cisco account representative.

**Step 10** Click **Create Token**.

**Step 11** Locate your new token in the list and click **Actions**, then choose **Copy** or **Download**.

**Step 12** If necessary, save your token in a safe place until you are ready to enter it into your Firepower Management Center.

### What to do next

Continue with the steps in Register Smart Licenses, on page 13.

## Register Smart Licenses

Register the Firepower Management Center with the Cisco Smart Software Manager.

### Before you begin

- If your deployment is air-gapped, do not use this procedure. Instead, see Configure the Connection to Smart Software Manager On-Prem, on page 14.
- Ensure that the Firepower Management Center can reach the Cisco Smart Software Manager (CSSM) server at tools.cisco.com:443.
- Make sure the NTP daemon is running on your Firepower Management Center. During registration, a key exchange occurs between the NTP server and the Cisco Smart Software Manager, so time must be in sync for proper registration.

  If you are deploying Firepower Threat Defense on a Firepower 4100/9300 chassis, you must configure NTP on the Firepower chassis using the same NTP server for the chassis as for the Firepower Management Center.
- If your organization has multiple Firepower Management Center appliances, make sure each FMC has a unique name that clearly identifies and distinguishes it from other Firepower Management Center appliances that may be registered to the same virtual account. This name is critical for managing your Smart License entitlements and ambiguous names will lead to problems later.
- Generate the necessary product license registration token from the Cisco Smart Software Manager. See Obtain a Product License Registration Token for Smart Licensing, on page 12, including all prerequisites. Make sure the token is accessible from the machine from which you will access your Firepower Management Center.

### Procedure

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

**Step 2** Click **Register**.

**Step 3** Paste the token you generated from Cisco Smart Software Manager into the **Product Instance Registration Token** field.

Make sure there are no empty spaces or blank lines at the beginning or end of the text.

**Step 4** Click **Apply Changes**.

### What to do next

- Add your Firepower Threat Defense devices to the Firepower Management Center; see Add a Device to the FMC.
- Assign licenses to your Firepower Threat Defense devices; see Assign Licenses to Multiple Managed Devices, on page 15.

# Smart Software Manager On-Prem Overview

As described in Periodic Communication with the License Authority, on page 4, your system must communicate regularly with Cisco to maintain your license entitlement. If you have one of the following situations, you might want to use a Smart Software Manager On-Prem (also known as SSM On-Prem, and formerly known as "Smart Software Satellite Server") as a proxy for connections to the License Authority:

- Your Firepower Management Center is offline or otherwise has limited or no connectivity (in other words, is deployed in an air-gapped network.)
- Your Firepower Management Center has permanent connectivity, but you want to manage your Smart Licenses via a single connection from your network.

Cisco Smart Software Manager On-Prem allows you to schedule synchronization or manually synchronize Smart License authorization with the Smart Software Manager.

For more information about Smart Software Manager On-Prem, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem

## How to Deploy Smart Software Manager On-Prem

### Procedure

**Step 1** Deploy and set up Smart Software Manager On-Prem.

See the documentation for the Smart Software Manager On-Prem, available from https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem.

**Step 2** Connect the Firepower Management Center to Smart Software Manager On-Prem, obtain a registration token, and register the FMC to SSM On-Prem.

See Configure the Connection to Smart Software Manager On-Prem, on page 14.

**Step 3** Add devices to be managed.

See Add a Device to the FMC.

**Step 4** Assign licenses to managed devices

See Assign Licenses to Multiple Managed Devices, on page 15

**Step 5** Synchronize Smart Software Manager On-Prem to the Cisco Smart Software Management Server (CSSM).

See the Smart Software Manager On-Prem documentation, above.

**Step 6** Schedule ongoing synchronization times.

### Configure the Connection to Smart Software Manager On-Prem

#### Before you begin

- Set up Smart Software Manager On-Prem (SSM On-Prem). For information, see How to Deploy Smart Software Manager On-Prem, on page 14.

- Make a note of the CN of the TLS/SSL certificate on your SSM On-Prem.
- Verify that your FMC can reach your SSM On-Prem. For example, verify that the FQDN configured as the SSM On-Prem call-home URL can be resolved by your internal DNS server.
- Go to http://www.cisco.com/security/pki/certs/clrca.cer and copy the entire body of the TLS/SSL certificate (from "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE-----") into a place you can access during configuration.

### Procedure

**Step 1** Choose **System** > **Integration**.

**Step 2** Click **Smart Software Satellite**.

**Step 3** Select **Connect to Cisco Smart Software Satellite Server**.

**Step 4** Enter the **URL** of your Smart Software Manager On-Prem, using the CN value you collected in the prerequisites of this procedure, in the following format:

`https://FQDN_or_hostname_of_your_SSM_On-Prem/Transportgateway/services/DeviceRequestHandler`

The FQDN or hostname must match the CN value of the certificate presented by your SSM On-Prem.

**Step 5** Add a new **SSL Certificate** and paste the certificate text that you copied in the prerequisites for this procedure.

**Step 6** Click **Apply**.

**Step 7** Select **System > Licenses > Smart Licenses** and click **Register**.

**Step 8** Create a new token on Smart Software Manager On-Prem.

**Step 9** Copy the token.

**Step 10** Paste the token into the form on the management center page.

**Step 11** Click **Apply Changes**.

The management center is now registered to Smart Software Manager On-Prem.

### What to do next

Complete remaining steps in How to Deploy Smart Software Manager On-Prem, on page 14.

# Assign Licenses to Multiple Managed Devices

Devices managed by a Firepower Management Center obtain their licenses via the Firepower Management Center, not directly from the Cisco Smart Software Manager.

Use this procedure to enable licensing on multiple Firepower Threat Defense devices at once.

**Note** For an Firepower Threat Defense cluster, you apply the licenses to the cluster as a whole; note that each unit in the cluster consumes a separate license per feature.

### Before you begin

- If you have not yet done so, register your devices with the Firepower Management Center. See Add a Device to the FMC.
- Prepare licenses for distribution to managed devices: See Register Smart Licenses, on page 13

### Procedure

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

**Step 2** Click **Edit Licenses**.

**Step 3** For each type of license you want to add to a device:

a) Click the tab for that type of license.
b) Click a device in the list on the left.
c) Click **Add** to move that device to the list on the right.
d) Repeat for each device to receive that type of license.

For now, don't worry about whether you have licenses for all of the devices you want to add.

e) Repeat this subprocedure for each type of license you want to add.
f) Click **Apply**.

### What to do next

- Verify that your licenses are correctly installed. Follow the procedure in View FTD Licenses and License Status, on page 16.
- If export-controlled functionality is newly enabled, reboot each device. If devices are configured in a high-availability pair, reboot both devices at the same time to avoid an Active-Active condition.
- Deploy configuration changes; see Deploy Configuration Changes.

# View FTD Licenses and License Status

To view the license status for a Firepower Management Center and its managed Firepower Threat Defense devices, use the Smart Licenses page in FMC.

For each type of license in your deployment, the page lists the total number of licenses consumed, whether the license is in compliance or out of compliance, the device type, and the domain and group where the device is deployed. You can also view the Firepower Management Center's Smart License Status.

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

- The Product Licensing dashboard widget provides an at-a-glance overview of your licenses.

  See Adding Widgets to a Dashboard and Dashboard Widget Availability by User Role and The Product Licensing Widget.

- The Device Management page (**Devices** > **Device Management**) lists the licenses applied to each of your managed devices.

- The Smart License Monitor health module communicates license status when used in a health policy.

### Procedure

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

**Step 2** In the **Smart Licenses** table, click the arrow at the left side of each **License Type** folder to expand that folder.

**Step 3** In each folder, verify that each device has a green circle with a **Check Mark** ( ) in the **License Status** column.

**Note** If you see duplicate Firepower Management Center Virtual licenses, each represents one managed device.

If all devices show a green circle with a **Check Mark** ( ), your devices are properly licensed and ready to use.

If you see any License Status other than a green circle with a **Check Mark** ( ), hover over the status icon to view the message.

### What to do next

- If you had any devices that did NOT have a green circle with a **Check Mark** ( ), you may need to purchase more licenses.

## FTD License Status

### Smart Licensing

The Smart License Status section of the **System > Licenses > Smart Licenses** page provides an overview of license usage on the Firepower Management Center, as described below.

### Usage Authorization

Possible status values are:

- **In-compliance** ( ) — All licenses assigned to managed devices are in compliance and the Firepower Management Center is communicating successfully with the Cisco licensing authority.
- **License is in compliance but communication with licensing authority has failed**— Device licenses are in compliance, but the Firepower Management Center is not able to communicate with the Cisco licensing authority.
- **Out-of-compliance icon or unable to communicate with License Authority**— One or more managed devices is using a license that is out of compliance, or the Firepower Management Center has not communicated with the Cisco licensing authority in more than 90 days.

### Product Registration

Specifies the last date when the Firepower Management Center contacted the License Authority and registered.

### Assigned Virtual Account

Specifies the Virtual Account under the Smart Account that you used to generate the Product Instance Registration Token and register the Firepower Management Center. If this deployment is not associated with a particular virtual account within your Smart Account, this information is not displayed.

### Export-Controlled Features

If this option is enabled, you can deploy restricted features. For details, see Licensing for Export-Controlled Functionality, on page 9.

# Move or Remove Licenses from FTD Devices

Use this procedure to manage licenses for Firepower Threat Defense devices managed by an Firepower Management Center.

For example, you can move a license from one FTD device to another device registered to the same FMC, or to remove a license from a device.

If you remove (disable) a license for a device, you cannot use the features associated with that license on that device.

**Important** If you need to move a license to a device managed by a *different* Firepower Management Center, see Transfer FTD Licenses to a Different Firepower Management Center, on page 19.

### Procedure

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

**Step 2** Click **Edit Licenses**.

**Step 3** Click either the **Malware**, **Threat**, **URL Filtering**, **AnyConnect Plus**, **AnyConnect Apex**, or **AnyConnect VPN Only**.

**Step 4** Choose the devices you want to license, then click **Add**, and/or click each device form which you want to remove a license and click the **Delete** ( ).

**Step 5** Click **Apply**.

### What to do next

Deploy the changes to the managed devices.

# Transfer FTD Licenses to a Different Firepower Management Center

When you register a Smart License to a Firepower Management Center, your virtual account allocates the license to the FMC. If you need to transfer your Smart Licenses to another Firepower Management Center, you must deregister the currently licensed FMC. This removes it from your virtual account and frees your existing licenses, so you can register the licenses to the new FMC. Otherwise, you cannot reuse these licenses, and you may receive an Out-of-Compliance notification because your virtual account does not have enough free licenses. For instructions, see Deregister a Firepower Management Center from the Cisco Smart Software Manager, on page 19.

Then you can register the licenses to the destination Firepower Management Center.

# If FTD License Status is Out of Compliance

If the Usage Authorization status on the Smart Licenses page (**System** > **Licenses** > **Smart Licenses**) shows Out of Compliance, you must take action.

### Procedure

**Step 1** Look at the Smart Licenses section at the bottom of the page to determine which licenses are needed.

**Step 2** Purchase the required licenses through your usual channels.

**Step 3** In Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory), verify that the licenses appear in your virtual account.

If the expected licenses are not present, see Troubleshoot FTD Licensing, on page 20.

**Step 4** In Firepower Management Center, select **System** > **Licenses** > **Smart Licenses**.

**Step 5** Click **Re-Authorize**.

# Deregister a Firepower Management Center from the Cisco Smart Software Manager

Deregister (unregister) your Firepower Management Center from the Cisco Smart Software Manager before you reinstall (reimage) the appliance, or if you need to release all of the license entitlements back to your Smart Account for any reason.

Deregistering removes the FMC from your virtual account. All license entitlements associated with the Firepower Management Center release back to your virtual account. After deregistration, the Firepower Management Center enters Enforcement mode where no update or changes on licensed features are allowed.

If you need to remove the licenses from a subset of managed Firepower Threat Defense devices, see Assign Licenses to Multiple Managed Devices, on page 15 or Assign Licenses to Managed Devices from the Device Management Page, on page 31.

### Procedure

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

**Step 2** Click **Deregister** ( ).

# Synchronize a Firepower Management Center with the Cisco Smart Software Manager

If you make changes in the Cisco Smart Software Manager, you can refresh the authorization on the Firepower Management Center so the changes immediately take effect.

**Procedure**

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

**Step 2** Click **Refresh** ( ).

# Troubleshoot FTD Licensing

### Expected Licenses Do Not Appear in My Smart Account

If the licenses you expect to see are not in your Smart Account, try the following:

- Make sure they are not in a different Virtual Account. Your organization's license administrator may need to assist you with this.
- Check with the person who sold you the licenses to be sure that transfer to your account is complete.

### Unable to Connect to Smart License Server

Check the obvious causes first. For example, make sure your Firepower system has outside connectivity. See Internet Access Requirements.

### Unexpected Out-of-Compliance Notification or Other Error

- If a device is already registered to a different FMC, you need to deregister the original FMC before you can license the device under a new FMC. See Deregister a Firepower Management Center from the Cisco Smart Software Manager, on page 19.
- Try synchronizing: Synchronize a Firepower Management Center with the Cisco Smart Software Manager, on page 20.

### Troubleshoot Other Issues

For solutions to other common issues, see https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

# License Classic Devices ( Firepower 7000/8000 Series, ASA FirePOWER, and NGIPSv)

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 3: 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 4: 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<br>ASA FirePOWER<br>NGIPSv | host, application, and user discovery<br>decrypting and inspecting SSL- and TLS-encrypted traffic | none | depends on license |
| Protection | TA (included with device) | 7000 and 8000 Series<br>ASA FirePOWER<br>NGIPSv | intrusion detection and prevention<br>file control<br>Security Intelligence filtering | none | no |

| License You Assign in Firepower System | Service Subscription You Purchase | Platforms | Granted Capabilities | Also Requires | Expire Capable? |
|---|---|---|---|---|---|
| Control | none (included with device) | 7000 and 8000 Series | user and application control<br>switching and routing<br>7000 and 8000 Series device high availability<br>7000 and 8000 Series network address translation (NAT) | Protection | no |
| Control | none (included with device) | ASA FirePOWER<br>NGIPSv | user and application control | Protection | no |
| Malware | TAM, TAMC, or AMP | 7000 and 8000 Series<br>ASA FirePOWER<br>NGIPSv | AMP for Networks (network-based Advanced Malware Protection)<br>File storage | Protection | yes |
| URL Filtering | TAC, TAMC, or URL | 7000 and 8000 Series<br>ASA FirePOWER<br>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**.<br>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**. |

| To View | Do This |
|---|---|
| License status in the Health Monitor | Use the Classic License Monitor health module in a health policy. For information, see Health Monitoring, including #unique_233 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 27.

  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 27.
- 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 21.

**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 31. You **must** assign licenses to your managed devices before you can use licensed features on those devices.

# How to Convert a Classic License for Use on an FTD Device

You can convert licenses using either the License Registration Portal (LRP) or the Cisco Smart Software Manager (CSSM), and you can convert an unused Product Authorization Key (PAK) or a Classic license that has already been assigned to a device.



**Important** You cannot undo this process. You cannot convert a Smart License to a Classic license, even if the license was originally a Classic license.

In documentation on Cisco.com, Classic licenses may also be referred to as "traditional" licenses.

### Before you begin

- It is easiest to convert a Classic license to a Smart License when it is still an unused PAK that has not yet been assigned to a product instance.
- Your hardware must be able to run Firepower Threat Defense. See the *Cisco Firepower Compatibility Guide* at https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html.
- You must have a Smart Account. If you do not have one, create one. See Create a Smart Account to Hold Your Licenses, on page 10.
- The PAKs or licenses that you want to convert must appear in your Smart Account.
- If you convert using the License Registration Portal instead of the Cisco Smart Software Manager, you must have your Smart Account credentials in order to initiate the conversion process.

### Procedure

**Step 1** The conversion process you will follow depends on whether or not the license has been consumed:

- If the PAK that you want to convert has never been used, follow instructions for converting a PAK.
- If the PAK you want to convert has already been assigned to a device, follow instructions for converting a Classic license.

  Make sure your existing classic license is still registered to your device.

**Step 2** See instructions for your type of conversion (PAK or installed Classic license) in the following documentation:

- To convert PAKs or licenses using the LRP:

- To view a video that steps you through the License Registration Portal part of the conversion process, click https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780.
- Search for "Convert" in the following document: https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu.

  There are three conversion procedures. Choose the conversion procedure applicable to your situation.
- Sign in to the License Registration Portal (LRP) at https://tools.cisco.com/SWIFT/LicensingUI/Home and follow the instructions in the documentation above.

- To convert PAKs or licenses using CSSM:
  - *Converting Hybrid Licenses to Smart Software Licenses QRG*:

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - Sign in to CSSM at https://software.cisco.com/#SmartLicensing-LicenseConversion and follow the instructions for your type of conversion (PAK or installed Classic license) in the documentation above.

**Step 3** Freshly install Firepower Threat Defense on your hardware.

See the instructions for your hardware at https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html.

**Step 4** If you will use Firepower Device Manager to manage this device as a standalone device:

See information about licensing the device in the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager* at https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html.

Skip the rest of this procedure.

**Step 5** If you have already deployed Smart Licensing on your Firepower Management Center:

a) Set up Smart Licensing on your new Firepower Threat Defense device.

   See Assign Licenses to Multiple Managed Devices, on page 15.

b) Verify that the new Smart License has been successfully applied to the device.

   See View FTD Licenses and License Status, on page 16.

**Step 6** If you have not yet deployed Smart Licensing on your Firepower Management Center:

See Register Smart Licenses, on page 13.

# 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.

**Note** For an Firepower Threat Defense cluster, you apply the licenses to the cluster as a whole; note that each unit in the cluster consumes a separate license per feature.

### 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.
- If you will assign Smart Licenses:
  - If you need to apply Smart Licenses to many devices at one time, use the Smart Licenses page instead of following this procedure. See Assign Licenses to Multiple Managed Devices, on page 15
  - Prepare Smart Licenses for distribution to managed devices: See Register Smart Licenses, on page 13

### 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

- If you assigned Smart Licenses, verify license status:

  Go to **System** > **Licenses** > **Smart Licenses**, enter the hostname or IP address of the device into the filter at the top of the Smart Licenses table, and verify that only a green circle with a **Check Mark** ( )

appears for each device, for each license type. If you see any other icon, hover over the icon for more information.

- Deploy configuration changes; see Deploy Configuration Changes.
- If you are licensing Firepower Threat Defense devices and you applied a Base license with export-controlled functionality enabled, reboot each device. For devices configured in a high-availability pair, reboot both devices at the same time to avoid an Active-Active condition.

# 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