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 (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.)

In multi-instance deployments, you need one entitlement for each security module.

In standard, connected Smart Licensing, these licenses are perpetual.

In Specific License Reservation, these licenses are term-based.

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 Firepower Threat Defense Virtual	Smart	See the topics under License Firepower Threat Defense Devices (FTD), on page 3.
NGIPS software: • Firepower 7000/8000 series • ASA FirePOWER • NGIPSv	Classic	See License Classic Devices (Firepower 7000/8000 Series, ASA FirePOWER, and NGIPSv), on page 41.
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.

How to License Firepower Threat Defense Devices

Firepower Threat Defense devices require Smart Licensing.

Follow the steps outlined in this overview to license FTD devices managed by a hardware or virtual Firepower Management Center.

If your FMC also manages Classic devices (ASA FirePOWER, NGIPSv, or 7000/8000 series), you can follow this procedure for FTD devices, then follow the instructions under License Classic Devices (Firepower 7000/8000 Series, ASA FirePOWER, and NGIPSv), on page 41 for devices that use Classic licensing.

Procedure

Step 1 If you do not already have a Smart Account, create one.

We recommend you have a Smart Account before you purchase licenses. To create a new Smart Account, see Create a Smart Account to Hold Your Licenses, on page 15.

Note Your account representative may have created a Smart Account on your behalf. If so, make sure you can access the account in the Cisco Smart Software Manager (CSSM) at https://software.cisco.com/#module/SmartLicensing.

Step 2 Understand the *platform* licenses your organization needs:

- Firepower Management Center physical hardware:

  This appliance comes with the licensing it needs; you do not need to do anything to activate this.

- Firepower Management Center Virtual:

  You need additional licenses. For details, see Firepower Management Center Virtual Licenses, on page 2.

  (If your FMCv will also manage devices that use Classic licenses, those devices will also require these entitlements when you configure Classic licensing.)

- Firepower Threat Defense devices:

  Each device automatically includes a license for basic functionality. For details, see Base Licenses, on page 10.

  You do not need to do anything to activate a base license, but many features require separate licensing, which is discussed below.

Step 3 Understand the *feature* licenses (sometimes called service subscriptions) that your organization needs.

See FTD License Types and Restrictions, on page 8 and subtopics.

Step 4 Determine the *number* of feature licenses/service subscriptions that your organization needs.

- Generally, each managed device needs to be licensed for each feature you will use.

- For Firepower Management Centers in a high availability pair:

  See FMC HA License Requirements for FMC High Availability Configurations.

- For Firepower Threat Defense devices in a high availability pair:

  Each device (whether active or standby) must be licensed for each feature to be used. No additional licensing is required.

  See License Requirements for FTD Devices in a High Availability Pair.

- For inter- or intra-chassis clustered Firepower Threat Defense devices:

  See Licenses for Clustering.

- For a multi-instance deployment:

  See Licensing for Multi-Instance Deployments, on page 14.

Step 5 If you have existing licenses that you need to convert or move:

- To convert a Classic license to a license that can be used for Firepower Threat Defense:

  See How to Convert a Classic License for Use on an FTD Device, on page 49.

- To transfer Smart Licenses that are currently registered to another Firepower Management Center:

  See Transfer FTD Licenses to a Different Firepower Management Center, on page 39 and Deregister a Firepower Management Center from the Cisco Smart Software Manager, on page 40.

- To move Smart Licenses that are currently registered to another Firepower Threat Defense device:

  See Move or Remove Licenses from FTD Devices, on page 39.

Step 6 If your Firepower appliances have restricted internet access:

Determine which solution is best for your situation:

- If your Firepower Management Center is not connected to the internet, but it can connect to an internal server that can connect to Cisco's licensing authority, or can receive manual license updates:

  Deploy Smart Software Manager On-Prem (formerly known as a Smart Software Satellite Server.) For information, see Smart Software Manager On-Prem Overview, on page 21 and How to Deploy Smart Software Manager On-Prem, on page 21.

- If your deployment is completely air-gapped and cannot connect to the licensing authority or to Smart Software Manager On-Prem (which connects to the licensing authority), or receive manual license updates:

  See the options at Specific License Reservation (SLR), on page 23 and skip the rest of this procedure.

- For a comparison, see Licensing Options for Air-Gapped Deployments, on page 20.

Step 7 If you have multiple Firepower Management Center appliances and you want to connect to Cisco's licensing authority through a single proxy:

Deploy Smart Software Manager On-Prem (formerly known as a Smart Software Satellite Server.) For information, see Smart Software Manager On-Prem Overview, on page 21.

Step 8 If you want to enable features that use strong encryption and that are restricted by geographic region:

See Licensing for Export-Controlled Functionality, on page 13.

Step 9 Purchase the licenses you need:

Contact your Cisco sales representative or authorized reseller.

Step 10 Verify that your reseller or Cisco sales representative has added your licenses to your Smart Account.

Look in CSSM: https://software.cisco.com/#SmartLicensing-Inventory. Click **Inventory**, then the **Licenses** tab. Filter the list as needed. You may need your purchase confirmation in order to understand the license naming.

If you don't see the licenses you expect to see, make sure you are looking at the correct virtual account. For assistance with this, see the resource links in CSSM.

If you still don't see your licenses, or the licenses are not correct, contact the person from whom you purchased the licenses.

Step 11 After your virtual account (Smart Account) holds the licenses you expect, register your Firepower Management Center to CSSM:

You must configure licensing in the Firepower Management Center using the web interface.

- If your Firepower Management Center connects directly to CSSM:

  See the following topics:

  - Obtain a Product License Registration Token for Smart Licensing, on page 16 and
  - Register Smart Licenses, on page 18

- If your Firepower Management Center connects to Smart Software Manager On-Prem:

  See Configure the Connection to Smart Software Manager On-Prem, on page 22.

Step 12 Verify that registration was successful:

In the Firepower Management Center web interface, go to **System > Licenses > Smart Licenses**. **Product Registration** should show a green checkmark.

Step 13 If you have not yet done so, add your devices to the Firepower Management Center as managed devices.

See Add a Device to the FMC

Step 14 Assign licenses to your managed Firepower Threat Defense devices:

See Assign Licenses to Multiple Managed Devices, on page 36

Step 15 Verify that licenses have successfully been added to your devices.

See View FTD Licenses and License Status, on page 37.

Step 16 As applicable, set up licensing for high-availability and clustered deployments:

- For Firepower Management Centers in a high availability pair:

  See the prerequisites to Establishing Firepower Management Center High Availability.

  After you configure FMC high-availability pairs, device licenses are automatically transferred from the active to the standby management center. You do not need to configure anything specific for licensing.

- For Firepower Threat Defense devices in a high availability pair:

  Assign the licenses for the features that you want to use to both the active and standby device before you configure high availability. If the devices are licensed for different features, the licenses on the standby device will be replaced with the same set of licenses as the active device.

- For clustered Firepower Threat Defense devices:

  See Licenses for Clustering. Licensing steps are included in FMC: Add a Cluster.

What to do next

- (Optional) If your Firepower Management Center also manages Classic devices (ASA FirePOWER, NGIPSv, or 7000/8000 series), configure licensing for those devices:

  See License Classic Devices (Firepower 7000/8000 Series, ASA FirePOWER, and NGIPSv), on page 41.

- Understand validity periods and expiration. See License Expiration, on page 52.

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 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.

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 use one of the options described in Licensing Options for Air-Gapped Deployments, on page 20. In non-airgapped deployments, 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 (Except for Specific License Reservation, Base licenses are automatically assigned with all Firepower Threat Defense devices)	No subscription required (license is included with device)	Perpetual	User and application control Switching and routing NAT For details, see Base Licenses, on page 10.
Threat	• T • TC (Threat + URL) • TMC (Threat + Malware + URL)	Term-based	Intrusion detection and prevention File control Security Intelligence filtering For details, see Threat Licenses, on page 11
Malware	• TM (Threat + Malware) • TMC (Threat + Malware + URL) • AMP	Term-based	AMP for Networks (network-based Advanced Malware Protection) Cisco Threat Grid File storage For details, see Malware Licenses for Firepower Threat Defense Devices, on page 11 and License Requirements for File and Malware Policies.
URL Filtering	• TC (Threat + URL) • TMC (Threat + Malware + URL) • URL	Term-based	Category and reputation-based URL filtering For details, see URL Filtering Licenses for Firepower Threat Defense Devices, on page 12.
Firepower Management Center Virtual	Based on license type.	Term-based or perpetual based on license type.	The platform license determines the number of devices the virtual appliance can manage. For details, see Firepower Management Center Virtual Licenses, on page 2.

License You Assign in Firepower System	Subscription You Purchase	Duration	Granted Capabilities
Export-Controlled Features	Based on license type.	Term-based or perpetual based on license type.	Features that are subject to national security, foreign policy, and anti-terrorism laws and regulations; see Licensing for Export-Controlled Functionality, on page 13.
Remote Access VPN: • AnyConnect Apex • AnyConnect Plus • 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. For more information, see AnyConnect Licenses, on page 12 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 FTD devices to perform switching and routing (including DHCP relay and NAT)
- configure FTD 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.

Except in deployments using Specific License Reservation, Base licenses are automatically added to the Firepower Management Center for every Firepower Threat Defense device you register.

For multi-instance deployments, see Licensing for Multi-Instance Deployments, on page 14.

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 FTD 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 FTD 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 8.

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 FTD 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:

There are two ways to enable strong cryptographic features. Your organization may be eligible for one or the other (or neither), but not both.

- 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):

  Contact your account representative.

  The Firepower Management Center allows you to use export-controlled features if your Smart Account is eligible for export-controlled functionality. When approved by Cisco, an export control license is added to your virtual account and you can use the export-controlled features. For more information, see Enabling the Export Control Feature (for Accounts Without Global Permission), on page 19

- If the option to use export-controlled functionality appears when you generate a new Product Instance Registration Token in Cisco Smart Software Manager:
  - The entitlement is perpetual and does not require a subscription.
  - 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 High-Availability Configurations

See:

- For Firepower Management Center appliances in a high-availability pair:

  License Requirements for FMC High Availability Configurations

- For Firepower Threat Defense devices in a high-availability pair:

  License Requirements for FTD Devices in a High Availability Pair

See also the topics for specific license types under the FTD License Types and Restrictions, on page 8 topic.

Licensing for FTD Clusters

In addition to information in this Licensing chapter, see:

- Licenses for Clustering
- FMC: Add a Cluster.

Licensing for Multi-Instance Deployments

All licenses apply per security engine/chassis (for the Firepower 4100) or per security module (for the Firepower 9300), not per container instance.

Base Licenses

Each security engine or module consumes a single Base license, which is automatically assigned for all deployments except those using Specific License Reservation.

Firepower Management Center Virtual

One entitlement is required for each security engine/module managed by a Firepower Management Center virtual appliance.

Feature Licenses

Each feature you license (Malware, Threat, URL Filtering, AnyConnect Apex, AnyConnect Plus, and AnyConnect VPN Only) requires one license per security engine/module. All instances on the engine/module can share the same feature licenses.

You must assign the license to each instance.

High-Availability Deployments

Instances in a high-availability pair cannot share feature licenses with each other, but each instance may share feature licenses with other instances on its respective engine/module.

Licensing Example

To see how the above licensing requirements work together, see Licenses for Container Instances.

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.

What to do next

If you are following a longer workflow, return to the workflow:

How to License Firepower Threat Defense Devices, on page 4

How to Configure Smart Licensing with Direct Internet Access

Before you begin

If your deployment is complex or you have questions about the licenses you need, see How to License Firepower Threat Defense Devices, on page 4.

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 16.

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

See Register Smart Licenses, on page 18. 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 36.

Step 6 Verify that licenses are successfully installed.

See View FTD Licenses and License Status, on page 37.

What to do next

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

See the final steps in How to License Firepower Threat Defense Devices, on page 4.

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 18 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, and your organization has obtained a license for export-controlled functionality, you will enable this functionality later, as described in Enabling the Export Control Feature (for Accounts Without Global Permission), on page 19.

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 18.

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 22 or How to Implement Specific License Reservation, on page 24, respectively.
- 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 FTD 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 16, 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 Decide whether to send usage data to Cisco.

- **Enable Cisco Success Network** is enabled by default. You can click **sample data** to see the kind of data Cisco collects. To help you make your decision, read the Cisco Success Network information block.
- **Note**
  - When enabled, Cisco Support Diagnostics is enabled in the Firepower Threat Defense (FTD) devices in the next sync cycle. The FMC sync with the FTD runs once every 30 minutes.
  - When enabled, any new FTD registered in this FMC in the future will have Cisco Support Diagnostics enabled on it automatically.

Step 5 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 36.

Enabling the Export Control Feature (for Accounts Without Global Permission)

Important Use this procedure only if your Smart Account is not authorized for strong encryption. If your account is authorized, or you aren't sure, see Licensing for Export-Controlled Functionality, on page 13.

Before you begin

- Make sure that your deployment does **not** already support the export-controlled functionality.

Note If your deployment supports export-controlled features, you will see an option that allows you to enable export-controlled functionality in the **Create Registration Token** page in the Cisco Smart Software Manager. For more information, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html.

- Make sure your deployment is not using an evaluation license.
- In Cisco Smart Software Manager, on the **Inventory** > **Licenses** page, verify that you have the license that corresponds to your Firepower Management Center:

Export Control License	Firepower Management Center Model
Cisco Virtual FMC Series Strong Encryption (3DES/AES)	All virtual Firepower Management Centers
Cisco FMC 1K Series Strong Encryption (3DES/AES)	750, 1000, 1500, 1600
Cisco FMC 2K Series Strong Encryption (3DES/AES)	2000, 2500, 2600
Cisco FMC 4K Series Strong Encryption (3DES/AES)	3500, 4000, 4500, 4600

Procedure

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

Note If you see the **Request Export Key**, your account is approved for the export-controlled functionality and you can proceed to use the required feature.

Step 2 Click **Request Export Key** to generate an export key.

Tip If the export control key request fails, make sure that your virtual account has a valid Export Control license.

What to do next

You can now deploy configurations or policies that use the export-controlled features.

Remember The new export-controlled licenses and all features enabled by it do not take effect on the Firepower Threat Defense devices until the devices are rebooted. Until then, only the features supported by the older license will be active.

In high-availability deployments both the Firepower Threat Defense devices need to be rebooted simultaneously, to avoid an Active-Active condition.

Disabling the Export Control Feature (for Accounts without Global Permission)

If you enabled the export-controlled functionality using the feature described in Enabling the Export Control Feature (for Accounts Without Global Permission), on page 19, you can disable this functionality using this procedure.

Procedure

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

This releases the license back into the pool of available licenses in your virtual account, where it is now available for reuse.

Step 2 Disable the export control license by clicking **Return Export Key**.

Licensing Options for Air-Gapped Deployments

The following table compares the available licensing options for environments without internet access. Your sales representative may have additional advice for your specific situation.

Table 3: Comparison of Licensing Options for Air-Gapped Networks

Smart Software Manager On-Prem	Specific License Reservation
Scalable for a large number of products	Best for a small number of devices
Automated licensing management, usage and asset management visibility	Limited usage and asset management visibility
No incremental operational costs to add devices	Linear operational costs over time to add devices
Flexible, easier to use, less overhead	Significant administrative and manual overhead for moves, adds, and changes
Out-of-compliance status is allowed initially and at various expiration states	Out-of-compliance status impacts system functioning
For more information, see Smart Software Manager On-Prem Overview, on page 21	For more information, see Specific License Reservation (SLR), on page 23

Smart Software Manager On-Prem Overview

As described in Periodic Communication with the License Authority, on page 7, 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.)

  (For an alternate solution for air-gapped networks, see Licensing Options for Air-Gapped Deployments, on page 20.)

- 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

Before you begin

If your network is air-gapped, determine the best solution for license management for your deployment. See Licensing Options for Air-Gapped Deployments, on page 20.

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 22.

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 36

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 21.
- 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 21.

Specific License Reservation (SLR)

You can use the Specific License Reservation feature to deploy Smart Licensing in an air-gapped network.

Note Various names are used at Cisco for Specific License Reservation, including SLR, SPLR, PLR, and Permanent License Reservation. These terms may also be used at Cisco to refer to similar but not necessarily identical licensing models.

When Specific License Reservation is enabled, the Firepower Management Center reserves licenses from your virtual account for a specified duration without accessing the Cisco Smart Software Manager or using Smart Software Manager On-Prem.

Your Firepower Management Center can also simultaneously manage devices that use standard Classic licenses. However, those devices do not use Specific License Reservation.

Features that require access to the internet, such as URL Lookups or contextual cross-launch to public web sites, will not work.

Cisco does not collect web analytics or telemetry data for deployments that use Specific License Reservation.

Related Topics:

- Best Practices for Specific License Reservation, on page 24
- Requirements for Specific License Reservation, on page 24
- How to Implement Specific License Reservation, on page 24
- Specific License Reservation Status, on page 31
- Update a Specific License Reservation, on page 29
- Deactivate and Return the Specific License Reservation, on page 33
- Troubleshoot Specific License Reservation, on page 35

Best Practices for Specific License Reservation

You will not be able to successfully implement Specific License Reservation without reading this documentation.

An unsuccessful attempt is likely to result in the need to contact TAC.

To avoid problems, follow the instructions carefully, including the prerequisites and verification procedures.

Requirements for Specific License Reservation

Usage of Specific License Reservation requires approval and authorization from Cisco.

See also Prerequisites for Specific License Reservation, on page 24.

How to Implement Specific License Reservation

	Do This	More Information
Step 1	Complete the prerequisites for this feature.	Prerequisites for Specific License Reservation, on page 24
Step 2	Verify that your Smart Account is ready to deploy Specific License Reservation.	Verify that your Smart Account is Ready to Deploy Specific License Reservation, on page 25
Step 3	Enable Specific License Reservation using the Firepower Management Center	Enable the Specific Licensing Menu Option, on page 26
Step 4	Generate a Reservation Request Code from the Firepower Management Center	Generate a Reservation Request Code from the Firepower Management Center, on page 27
Step 5	Use the Reservation Request Code to Generate a Reservation Authorization Code from Cisco Smart Software Manager	Generate a Reservation Authorization Code from Cisco Smart Software Manager, on page 27
Step 6	Enter the Reservation Authorization Code into the Firepower Management Center	Enter the Specific License Reservation Authorization Code into the Firepower Management Center, on page 28
Step 7	Assign Specific Licenses to managed Firepower Threat Defence devices	Assign Specific Licenses to Managed Devices, on page 28
Step 9	(Outside of your Firepower Management Center) Schedule reminders for ongoing maintenance tasks	Maintain Your Air-Gapped Deployment

Prerequisites for Specific License Reservation

- Set up your Smart Account.

  See Create a Smart Account to Hold Your Licenses, on page 15.

- If you are currently using standard Smart Licensing on your Firepower Management Center, de-register the Firepower Management Center before you implement Specific License Reservation. For information, see Deregister a Firepower Management Center from the Cisco Smart Software Manager, on page 40.

All Smart Licenses that are currently deployed to your Firepower Management Center will be returned to the pool of available licenses in your account, and you can re-use them when you implement Specific License Reservation.

- Specific License Reservation requires the same number and types of licenses as standard Smart Licensing. Determine how many standard licenses and service subscriptions you need for the devices and features you will deploy. Be sure to include entitlements for Firepower Management Center Virtual if applicable.

  For descriptions of Firepower licenses and service subscriptions, see FTD License Types and Restrictions, on page 8 and its subtopics, especially Firepower Management Center Virtual Licenses, on page 2.

- Purchase the licenses you need.

- Arrange for export-controlled strong cryptographic functionality, if required and if your organization is eligible. Confirm that your account is enabled to use it, or the required per-Firepower Management Center licenses appear in your virtual account. Your account representative can assist you with this.

  For more information, see Licensing for Export-Controlled Functionality, on page 13.

- Work with your account representative to obtain approval for Specific License Reservation (SLR) for your Firepower products.

- Obtain confirmation from your account representative that the Specific License Reservation is ready for use and reflected in your Smart Account.

- Add managed devices to your Firepower Management Center. For instructions, see Add a Device to the FMC. (You can add managed devices at any time, but adding them now simplifes this process.) You will need to enable the evaluation license in order to do this (under **System > Licenses > Smart Licenses**). Evaluation licensing does not require a connection to the License Authority.

- Make sure NTP is configured on the Firepower Management Center and managed devices. Time must be synchronized for registration to succeed.

  If you are deploying FTD 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.

- (Recommended) If you will deploy a Firepower Management Center pair in a high availability configuration, configure that before you assign licenses. (FMCs in a high availability configuration require the same number of licenses as a single FMC.) If you have already deployed licenses to the secondary appliance, de-register licensing from that appliance.

Verify that your Smart Account is Ready to Deploy Specific License Reservation

In order to prevent problems when deploying your Specific License Reservation, complete this procedure before you make any changes in your Firepower Management Center.

Before you begin

- Ensure that you have met the requirements described in Prerequisites for Specific License Reservation, on page 24.

- Make sure you have your Cisco Smart Software Manager credentials.

Procedure

Step 1 Sign in to the Cisco Smart Software Manager:

https://software.cisco.com/#SmartLicensing-Inventory

Step 2 If applicable, select the correct account from the top right corner of the page.

Step 3 If necessary, click **Inventory**.

Step 4 Click **Licenses**.

Step 5 Verify the following:

- There is a **License Reservation** button.
- There are enough platform and feature licenses for the devices and features you will deploy, including Firepower Management Center Virtual entitlements for your devices, if applicable.

Step 6 If any of these items is missing or incorrect, contact your account representative to resolve the problem.

Important Do **not** continue with this process until any problems are corrected.

Enable the Specific Licensing Menu Option

This procedure changes the "Smart Licenses" menu option to "Specific Licenses" in Firepower Management Center.

Procedure

Step 1 Access the Firepower Management Center console using a USB keyboard and VGA monitor, or use SSH to access the management interface.

Step 2 Log into the Firepower Management Center using the CLI**admin** account. If the Firepower Management Center CLI is not enabled, this gives you direct access to the Linux shell. If your Firepower Management Center is enabled, this give you access to the Firepower Management Center CLI.

Step 3 If the Firepower Management Center CLI is enabled, enter the **expert** command to access the Linux shell.

Step 4 Execute the following command to access the Specific License Reservation options:

sudo manage_slr.pl

Example:

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

Step 5 Enable Specific License Reservation by selecting option 2.

Step 6 Select option 0 to exit the manage_slr utility.

Step 7 Type **exit** to exit the Linux shell.

Step 8 On a Firepower Management Center with the CLI enabled, enter **exit** to exit the command line interface.

Step 9 Verify that you can access the **Specific License Reservation** page in the Firepower Management Center web interface:

- If the **System** > **Licenses** > **Smart Licenses** page is currently displayed, refresh the page.
- Otherwise, choose **System** > **Licenses** > **Specific Licenses**.

Generate a Reservation Request Code from the Firepower Management Center

Procedure

Step 1 If you are not already viewing the **Specific License Reservation** page, choose **System** > **Licenses** > **Specific Licenses**.

Step 2 Click **Generate**.

Step 3 Make a note of the **Reservation Request Code**.

Generate a Reservation Authorization Code from Cisco Smart Software Manager

Procedure

Step 1 Go to the Cisco Smart Software Manager:

https://software.cisco.com/#SmartLicensing-Inventory

Step 2 If necessary, select the correct account from the top right of the page.

Step 3 If necessary, click **Inventory**.

(This page may display automatically.)

Step 4 Click **Licenses**.

Step 5 Click **License Reservation**.

Step 6 Enter the code that you generated from Firepower Management Center into the **Reservation Request Code** box.

Step 7 Click **Next**.

Step 8 Select **Reserve a specific license**.

Step 9 Scroll down to display the entire License grid.

Step 10 Under **Quantity To Reserve**, enter the number of each platform and feature license needed for your deployment.

Important

- You must explicitly include a **Firepower Threat Defense Base Features** license for each managed device, or, for multi-instance deployments, a **Firepower Threat Defense Base Features** license for each module.
- If you are using a virtual management center, you must include a **Firepower MCv Device License** entitlement for each module (in multi-instance deployments) or each managed device (all other deployments).
- If you use strong cryptographic functionality:
  - If your entire Smart Account is enabled for export-controlled functionality, you do not need to do anything here.
  - If your organization's entitlement is per-Firepower Management Center, you must select the appropriate license for your appliance.

    For the correct license name to choose for your device, see the prerequisites in Enabling the Export Control Feature (for Accounts Without Global Permission), on page 19.

Step 11 Click **Next**.

Step 12 Click **Generate Authorization Code**.

At this point, the license is now in use according to the Smart Software Manager.

Step 13 Download the Authorization Code in preparation for entering it into the Firepower Management Center.

Enter the Specific License Reservation Authorization Code into the Firepower Management Center

Procedure

Step 1 If you are not already viewing the **Specific License Reservation** page, in the Firepower management center web interface, choose **System** > **Licenses** > **Specific Licenses**.

Step 2 Click **Browse** to upload the text file with the authorization code that you generated from CSSM.

Step 3 Click **Install**.

Step 4 Verify that the **Specific License Reservation** page shows the **Usage Authorization** status as authorized.

Step 5 Click the **Reserved License** tab to verify the licenses selected while generating the **Authorization Code**.

If you do not see the licenses you require, then add the necessary licenses. For more info, see Update a Specific License Reservation.

Assign Specific Licenses to Managed Devices

Use this procedure to quickly assign licenses to multiple managed devices at one time.

You can also use this procedure to disable or move licenses from one Firepower Threat Defense device to another. If you disable a license for a device, you cannot use the features associated with that license on that device.

Procedure

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

Step 2 Click **Edit Licenses**.

Step 3 Click each tab and assign licenses to devices as needed.

Step 4 Click **Apply**.

Step 5 Click the **Assigned Licenses** tab and verify that your licenses are correctly installed on each device.

What to do next

- If export-controlled functionality is 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.

Update a Specific License Reservation

After you have successfully deployed Specific Licenses on your Firepower Management Center, you can add or remove entitlements at any time using this procedure.

Procedure

Step 1 In Firepower Management Center, obtain the unique product instance identifier of this appliance:

a) Select **System** > **Licenses** > **Specific Licenses**.

b) Make a note of the **Product Instance** value.

You will need this value several times during this process.

Step 2 In Cisco Smart Software Manager, identify the Firepower Management Center appliance to update:

a) Go to the Cisco Smart Software Manager:

https://software.cisco.com/#SmartLicensing-Inventory

b) If necessary, click **Inventory**.

(This page may display automatically.)

c) Click **Product Instances**.

d) Look for a product instance that has **FP** in the **Type** column and a generic SKU (not a hostname) in the **Name** column. You may also be able to use the values in other table columns to help determine which Firepower Management Center is the correct Firepower Management Center. Click the name.

e) Look at the **UUID** and see if it is the UUID of the Firepower Management Center that you are trying to modify.

If not, you must repeat these steps until you find the correct Firepower Management Center.

Step 3 When you have located the correct Firepower Management Center appliance in Cisco Smart Software Manager, update the reserved licenses and generate a new authorization code:

a) On the page that shows the correct UUID, choose **Actions** > **Update Reserved Licenses**.
b) Update the reserved licenses as needed.

Important
- You must explicitly include a **Firepower Threat Defense Base Features** license for each managed device, or, for multi-instance deployments, a **Firepower Threat Defense Base Features** license for each module.
- If you are using a virtual management center, you must include a **Firepower MCv Device License** entitlement for each module (in multi-instance deployments) or each managed device (all other deployments).
- If you use strong cryptographic functionality:
  - If your entire Smart Account is enabled for export-controlled functionality, you do not need to do anything here.
  - If your organization's entitlement is per-Firepower Management Center, you must select the appropriate license for your appliance.

    For the correct license name to choose for your device, see the prerequisites in Enabling the Export Control Feature (for Accounts Without Global Permission), on page 19.

c) Click **Next** and verify the details.
d) Click **Generate Authorization Code**.
e) Download the Authorization Code in preparation for entering it into the Firepower Management Center.
f) Leave the Update Reservation page open. You will return to it later in this procedure.

Step 4 Update the Specific Licenses in Firepower Management Center:

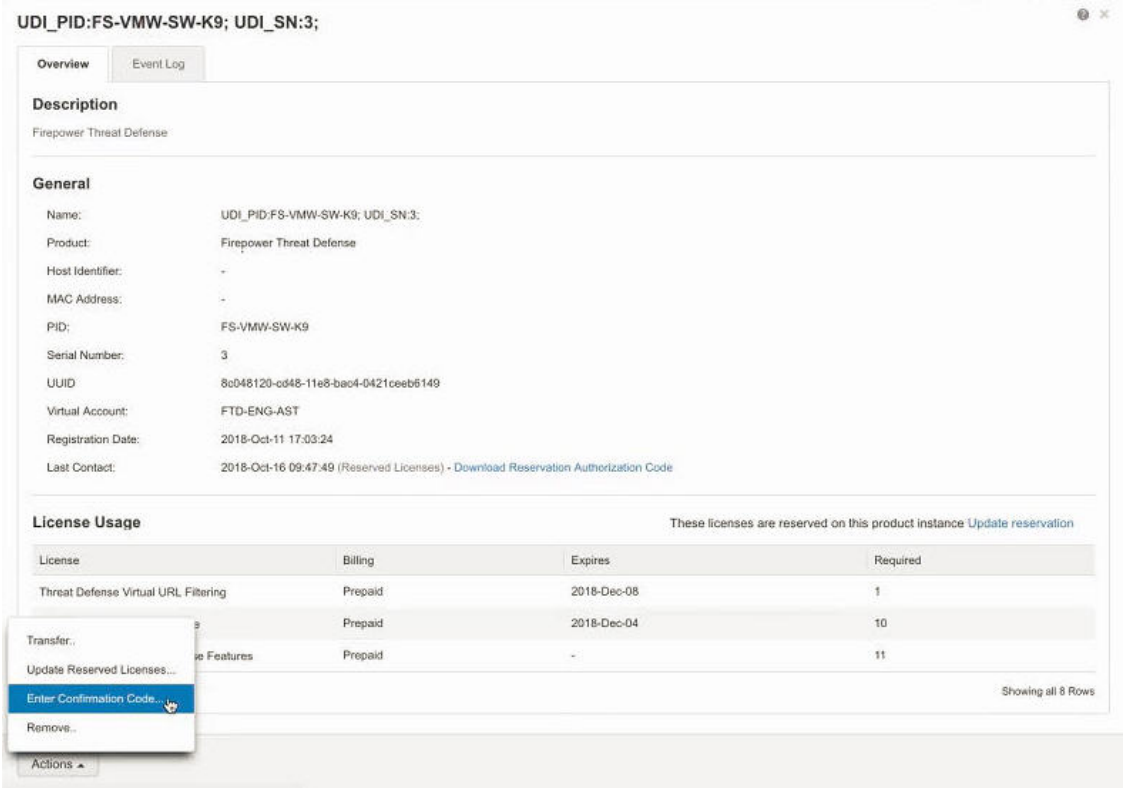
a) Choose **System** > **Licenses** > **Specific Licenses**.
b) Click **Edit SLR**.
c) Click **Browse** to upload the newly generated authorization code.
d) Click **Install** to update the licenses.

   After successful installation of the authorization code, ensure that the licenses shown in the Reserved column of Firepower Management Center, matches with the licenses that you have reserved in Cisco Smart Software Manager.

e) Make a note of the **Confirmation Code**.

Step 5 Enter the confirmation code in Cisco Smart Software Manager:

a) Return to the Cisco Smart Software Manager page that you left open earlier in this procedure.
b) Choose **Actions** > **Enter Confirmation Code**:



c) Enter the confirmation code that you generated from the Firepower Management Center.

Step 6 In Firepower Management Center, verify that your licenses are reserved as you expect them, and that each feature for each managed device shows a green circle with a **Check Mark** ( ).

If necessary, see Specific License Reservation Status, on page 31 for more information.

What to do next

If your deployment includes export-controlled functionality, 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.

Important! Maintain Your SLR Deployment

To update the threat data and software that keep your deployment effective, see Maintain Your Air-Gapped Deployment.

To ensure that all functionality continues to work without interruption, monitor your license expiration dates (on the **Reserved Licenses** tab).

Specific License Reservation Status

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

Usage Authorization

Possible status values are:

- **Authorized** — The Firepower Management Center is in compliance and registered successfully with the License Authority, which has authorized the license entitlements for the appliance.
- **Out-of-compliance** — If licenses are expired or if the Firepower Management Center has overused licenses even though they are not reserved, status shows as Out-of-Compliance. License entitlements are enforced in Specific License Reservation, so you must take action.

Product Registration

Specifies registration status and the date that an authorization code was last installed or renewed on the Firepower Management Center.

Export-Controlled Features

Specifies whether you have enabled export-controlled functionality for the Firepower Management Center.

For more information about Export-Controlled Features, see Licensing for Export-Controlled Functionality, on page 13.

Product Instance

The Universally Unique Identifier (UUID) of this Firepower Management Center. This value identifies this device in Cisco Smart Software Manager.

Confirmation Code

The **Confirmation Code** is needed if you update or deactivate and return Specific Licenses.

Assigned Licenses Tab

Shows the licenses assigned to each device and the status of each.

Reserved Licenses Tab

Shows the number of licenses used and available to be assigned, and license expiration dates.

Expired Specific License Reservation

If required licenses are unavailable or expired, the following actions are restricted:

- Device registration
- Policy deployment

To renew your Specific License Reservation entitlements, purchase the necessary licenses, then follow the procedure in Update a Specific License Reservation, on page 29.

Renew Specific License Reservation Entitlements

When it is time to renew your Specific License Reservation entitlements, purchase the necessary licenses, then follow the procedure in Update a Specific License Reservation, on page 29.

Deactivate and Return the Specific License Reservation

If you no longer need a specific license, you must return it to your Smart Account.

Important If you do not follow all of the steps in this procedure, the license remains in an in-use state and cannot be re-used.

This procedure releases all license entitlements associated with the Firepower Management Center back to your virtual account. After you de-register, no updates or changes on licensed features are allowed.

Procedure

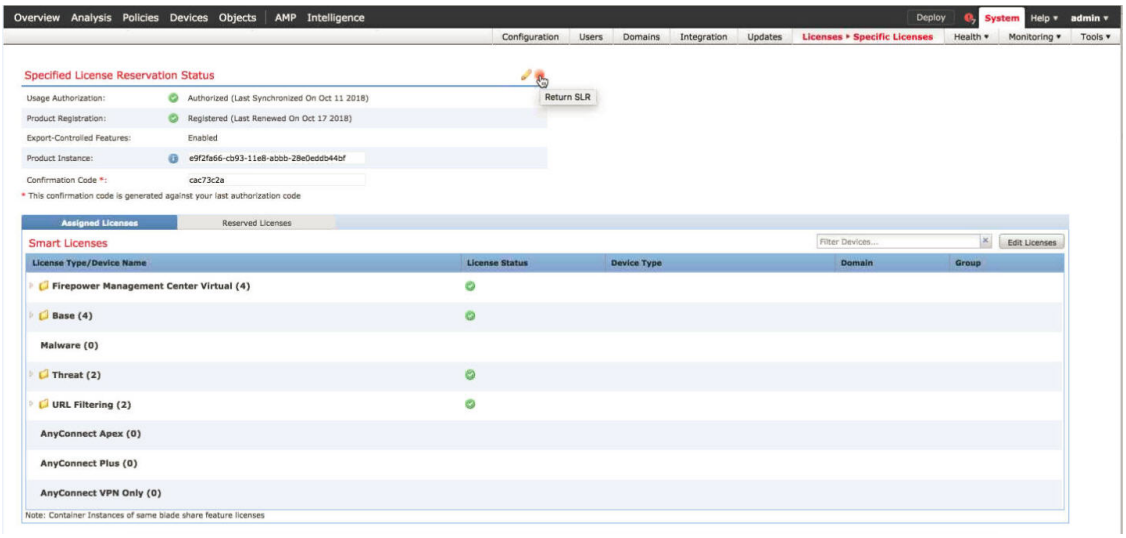
Step 1 In the Firepower Management Center Web interface, select **System** > **Licenses** > **Specific Licenses**.

Step 2 Make a note of the **Product Instance** identifier for this Firepower Management Center.

Step 3 Generate a return code from Firepower Management Center:

a) Click **Return SLR**.

The following figure shows Return SLR.



Firepower Threat Defense devices become unlicensed and Firepower Management Center moves to the de-registered state.

b) Make a note of the **Return Code**.

Step 4 In Cisco Smart Software Manager, identify the Firepower Management Center appliance to deregister:

a) Go to the Cisco Smart Software Manager:

https://software.cisco.com/#SmartLicensing-Inventory

b) If necessary, click **Inventory**.

(This page may display automatically.)

c) Click **Product Instances**.

d) Look for a product instance that has **FP** in the **Type** column and a generic SKU (not a hostname) in the **Name** column. You may also be able to use the values in other table columns to help determine which Firepower Management Center is the correct Firepower Management Center. Click the name.
e) Look at the **UUID** and see if it is the UUID of the Firepower Management Center that you are trying to modify.

   If not, you must repeat these steps until you find the correct Firepower Management Center.

Step 5 When you have identified the correct Firepower Management Center, return the licenses to your Smart Account:

a) On the page that shows the correct UUID, choose **Actions** > **Remove**.
b) Enter the reservation return code that you generated from the Firepower Management Center into the **Remove Product Instance** dialog box.
c) Click **Remove Product Instance**.

   The specific reserved licenses are returned to the available pool in your Smart Account and this Firepower Management Center is removed from the Cisco Smart Software Manager Product Instances list.

Step 6 Disable the Specific License in the Firepower Management Center Linux shell:

a) Access the Firepower Management Center console using a USB keyboard and VGA monitor, or use SSH to access the management interface.
b) Log in to the Firepower Management Center **admin** account. If the Firepower Management Center CLI is not enabled, this gives you direct access to the Linux shell. If your Firepower Management Center is enabled, this give you access to the Firepower Management Center CLI..
c) If the Firepower Management Center CLI is enabled, enter the **expert** command to access the Linux shell.For a Firepower Management Center with the CLI enabled, enter
d) Execute the following command:

```
sudo manage_slr.pl
```

Example:

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) Select menu option 3 to disable the Specific License Reservation.
f) Select option 0 to exit the manage_slr utility.
g) Enter **exit** to exit the Linux shell.
h) On a Firepower Management Center with the CLI enabled, enter **exit** to exit the command line interface.

Troubleshoot Specific License Reservation

How do I identify a particular Firepower Management Center in the Product Instance list in Cisco Smart Software Manager?

On the Product Instances page in Cisco Smart Software Manager, if you cannot identify the product instance based on a value in one of the columns in the table, you must click the name of each generic product instance of type **FP** to view the product instance details page. The **UUID** value on this page uniquely identifies one Firepower Management Center.

In the Firepower Management Center web interface, the UUID for a Firepower Management Center is the **Product Instance** value displayed on the **System > Licenses > Specific Licenses** page.

I do not see a License Reservation button in Cisco Smart Software Manager

If you do not see the **License Reservation** button, then your account is not authorized for specific license reservation. If you have already enabled Specific License Reservation in the Linux shell and generated a request code, perform the following:

1. If you have already generated a **Request Code** in the Firepower Management Center web interface, cancel the request code.
2. Disable Specific License Reservation in the Firepower Management Center Linux shell as described within the section Deactivate and Return the Specific License Reservation, on page 33.
3. Register a Firepower Management Center with Cisco Smart Software Manager in regular mode using smart token.
4. Contact Cisco TAC to enable Specific License for your smart account.

I was interrupted in the middle of the licensing process. How can I pick up where I left off?

If you have generated but not yet downloaded an Authorization code from Cisco Smart Software Manager, you can go to the **Product Instance** page in Cisco Smart Software Manager, click the product instance, then click **Download Reservation Authorization Code**.

I am unable to register Firepower Threat Defense devices to Firepower Management Center Virtual

Make sure you have enough MCv entitlements in your Smart Account to cover the devices you want to register, then update your deployment to add the necessary entitlements.

See Update a Specific License Reservation, on page 29.

I have enabled Specific Licensing, but now I do not see a Smart License page.

This is the expected behavior. When you enable Specific Licensing, Smart Licensing is disabled. You can use the Specific License page to perform licensing operations.

If you want to use Smart Licensing, you must return the Specific License. For more information see, Deactivate and Return the Specific License Reservation, on page 33.

What if I do not see a Specific License page in Firepower Management Center?

You need to enable Specific License to view the Specific License page. For more information see, Enable the Specific Licensing Menu Option, on page 26.

I have disabled Specific Licensing, but forgot to copy the Return Code. What should I do?

The **Return Code** is saved in Firepower Management Center. You must re-enable the Specific License from the Linux shell (see Enable the Specific Licensing Menu Option, on page 26), then refresh the Firepower Management Center web interface. Your **Return Code** will be displayed.

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 container instances on the same security module/engine, you apply the license to each instance; note that the security module/engine consumes only one license per feature for all instances on the security module/engine.

Note For an FTD 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 18

Procedure

Step 1 Choose **System** > **Licenses** > **Smart Licenses** or **Specific 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 37.
- 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. Container instances on the same security module/engine only consume one license per security module/engine. Therefore, even though the FMC lists each container instance separately under each license type, the number of licenses consumed for feature license types will only be one.

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

Permanent License Reservation

See Specific License Reservation Status, on page 31

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 13.

Cisco Success Network

Specifies whether you have enabled Cisco Success Network for the Firepower Management Center. If this option is enabled, you provide usage information and statistics to Cisco which are essential to provide you with technical support. This information also allows Cisco to improve the product and make you aware of unused available features so that you can maximize the value of the product in your network. See Cisco Success Network, on page 57 for more information.

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 39.

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 40.

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 41.

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 36 or Assign Licenses to Managed Devices from the Device Management Page, on page 51.

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 40.
- Try synchronizing: Synchronize a Firepower Management Center with the Cisco Smart Software Manager, on page 40.

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 4: 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 5: 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

License You Assign in Firepower System	Service Subscription You Purchase	Platforms	Granted Capabilities	Also Requires	Expire Capable?
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_245 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 48.

  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 47.
- 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 42.

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 51. 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 15.
- 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 36.

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

See View FTD Licenses and License Status, on page 37.

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

See How to License Firepower Threat Defense Devices, on page 4. (Skip any steps that do not apply or that you have already completed.)

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 container instances on the same security module/engine, you apply the license to each instance; note that the security module/engine consumes only one license per feature for all instances on the security module/engine.

Note For an FTD 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 36
- Prepare Smart Licenses for distribution to managed devices: See Register Smart Licenses, on page 18

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.

License Expiration

License Expiration vs. Service Subscription Expiration

Q. Do feature licenses expire?

A. Strictly speaking, feature licenses do not expire. Instead, the service subscriptions that support those licenses expire. For details about service subscriptions, see "Service Subscriptions for Firepower Features" in the *Firepower Management Center Configuration Guide* available from https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html.

Smart Licensing

Q. Can a Product Instance Registration Token expire?

A. A token can expire if it is not used to register a product within the specified validity period. You set the number of days that the token is valid when you create the token in the Cisco Smart Software Manager. If the token expires before you use it to register a FMC, you must create a new token.

After you use the token to register a FMC, the token expiration date is no longer relevant. When the token expiration date elapses, there is no impact on the FMC that you used the token to register.

Token expiration dates do not affect subscription expiration dates.

For more information, see the *Cisco Smart Software Manager User Guide*.

Q. How can I tell if my Smart Licenses/service subscriptions are expired or about to expire?

A. To determine when a service subscription will expire (or when it expired), review your entitlements in the Cisco Smart Software Manager.

On the FMC, you can determine whether a service subscription for a feature license is currently in compliance by choosing **System** (⚙) > **Licenses** > **Smart Licenses**. On this page, a table summarizes the Smart License entitlements associated with this FMC via its product registration token. You can determine whether the service subscription for the license is currently in compliance based on the **License Status** field.

On FDM, use the Smart License page to view the current license status for the system: Click **Device**, then click **View Configuration** in the Smart License summary.

In addition, the Cisco Smart Software Manager will send you a notification 3 months before a license expires.

Q. What happens if my Smart License/subscription expires?

A. If a purchased service subscription expires, you can see in FMC and in your Smart Account that your account is out of compliance. Cisco notifies you that you must renew the subscription; see Subscription Renewals. There is no other impact.

Specific License Reservation

Q. What happens if my Specific License Reservation expires?

A. SLR licenses are term-based.

If required licenses are unavailable or expired, the following actions are restricted:

- Device registration

- Policy deployment

Classic Licensing

Q. How can I tell if my Classic licenses/service subscriptions are expired or about to expire?

A. On the FMC, choose **System** (⚙) > **Licenses** > **Classic Licenses**.

On this page, a table summarizes the Classic licenses you have added to this FMC.

You can determine whether the service subscription for the license is currently in compliance based on the **Status** field.

You can determine when the service subscription will expire (or when it expired) by the date in the **Expires** field.

You can also obtain this information by reviewing your license information in the Cisco Product License Registration Portal.

Q. What does this mean: 'IPS Term Subscription is still required for IPS'?

A. This message merely informs you that Protect and Control functionality requires not only a right-to-use license (which never expires), but also one or more associated service subscriptions, which must be renewed periodically. If the service subscriptions you want to use are current and will not expire soon, no action is required.

Q. What happens if my Classic license/subscription expires?

A. If a service subscription supporting a Classic license expires, Cisco notifies you that you must renew the subscription; see Subscription Renewals.

You might not be able to use the related features, depending on the feature type:

Table 6: Expiration Impact for Classic Licenses/Subscriptions

Classic License	Possible Supporting Subscriptions	Expiration Impact
Control	TA, TAC, TAM, TAMC	You can continue to use existing functionality, but you cannot download VDB updates, including application signature updates.
Protection	TA, TAC, TAM, TAMC	You can continue to perform intrusion inspection, but you cannot download intrusion rule updates.
URL Filtering	URL, TAC, TAMC	• Access control rules with URL conditions immediately stop filtering URLs. • Other policies (such as SSL policies) that filter traffic based on URL category and reputation immediately stop doing so. • The FMC can no longer download updates to URL data. • You cannot re-deploy existing policies that perform URL category and reputation filtering.

Classic License	Possible Supporting Subscriptions	Expiration Impact
Malware	AMP, TAM, TAMC	• For a very brief time, the system can use existing cached file dispositions. After the time window expires, the system assigns a disposition of `Unavailable` to those files. • The system stops querying the AMP Cloud, and stops acknowledging retrospective events sent from the AMP Cloud • You cannot re-deploy existing access control policies if they include AMP for FTD configurations.

Subscription Renewals

Q. How do I renew an expiring Classic license?

A. To renew an expiring Classic license, simply purchase a new PAK key and follow the same process as for implementing a new subscription.

Q. Can I renew a service subscription from the FMC?

A. No. To renew a service subscription (Classic or Smart), purchase a new subscription using either the Cisco Commerce Workspace or the Cisco Service Contract Center.

Other Licensing Information in This Guide

For	See
Information about the interface for FMC communications with the Smart Licensing authority	About Device Management Interfaces and subtopics
Firewall requirements for licensing	Internet Access Requirements
An explanation of the licensing information in tables at the beginning of each procedure in this document.	License Statements in the Documentation
Important licensing considerations when restoring from a backup	Backup and Restore

For	See
Effects of licensing on the way rules and policies are applied and how they trigger.	Policy and rule information, including but not limited to: • Access Control Rule Management • Access Control Rule Components, information about Conditions • TLS/SSL Rule Guidelines and Limitations • TLS/SSL Rule Components • Rate Limiting with QoS Policies
Deployment and policy or rule management errors related to Licensing	Policy and rule information throughout this guide, including but not limited to: • Rule and Other Policy Warnings • Rate Limiting with QoS Policies
Licensing requirements for SSL	Prerequisites in Configure SSL Settings for Firepower Threat Defense
Licensing requirements for SSL preprocessor functionality	The SSL Preprocessor
Licensing for AMP for Endpoints integrations	Comparison of Malware Protection: Firepower vs. AMP for Endpoints
Licensing and stream reassembly on client and server services	TCP Stream Preprocessing Options
Licensing and Threat Intelligence Director	Platform, Element, and License Requirements
Licensing impacts on connection events	Requirements for Populating Connection Event Fields
Information about the Licensing and other dashboard widgets	Dashboard Widget Availability by User Role The Custom Analysis Widget
Information about the Health Monitor for licensing.	Information about the Smart License Monitor and the Classic License Monitor in #unique_245

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

Cisco Success Network

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Firepower Management Center and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism to select data of interest from the Firepower System and to transmit it in a structured format to remote management stations for the following benefits:

- To inform you of available unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that might be available for your product.
- (If you integrate with SecureX) To summarize appliance and device status in SecureX tiles. This lets you see at a glance, for example, whether all of your devices are running optimal software versions.

  For more information about SecureX, see Integrate with Cisco SecureX.
- To help Cisco improve our products.

The Firepower Management Center establishes and maintains the secure connection at all times, and allows you to enroll in the Cisco Success Network. You can turn off this connection at any time by disabling Cisco Success Network, which disconnects the device from the Cisco Success Network cloud.

Enabling Cisco Success Network

You enable Cisco Success Network when you register the Firepower Management Center with the Cisco Smart Software Manager. See Register Smart Licenses, on page 18.

You can view your current Cisco Success Network enrollment status on the **Licences** > **Smart Licenses** page, and you can change your enrollment status. See Changing Cisco Success Network Enrollment, on page 66.

Note The Cisco Success Network feature is disabled if the Firepower Management Center has a valid Smart Software Manager On-Prem (formerly known as Smart Software Satellite Server) configuration, or uses Specific License Reservation.

Cisco Success Network Telemetry Data

Cisco Success Network allows enrolled Firepower Management Centers to continuously stream real time configuration and operating state information to the Cisco Success Network cloud. Collected and monitored data include the following:

- **Enrolled device information**—This includes the Firepower Management Center device name, model, serial number, UUID, system uptime, and Smart Licensing information; see Enrolled Device Data, on page 58.

- **Software information**—This includes software information about the enrolled Firepower Management Center, such as version number, rule update version, geolocation database version, and vulnerability database (VDB) version information; see Software Version Data, on page 59.
- **Managed device information**—This includes information about all the managed devices associated with the enrolled Firepower Management Center, including device names, device models, serial numbers, software versions, and licenses in use per device; see Managed Device Data, on page 59.
- **Deployment information**—This includes information about policy deploymnents. After you configure your deployment, and any time you change that configuration, you must deploy the changes to affected devices; see Deployment Information, on page 60.
- **Feature usage**—This includes feature-specific policy and licensing information:
  - **URL filtering**—This includes how many URL filtering licenses are configured and deployed to devices, and how many devices have policies deployed that are using the URL filtering capability.
  - **Intrusion prevention**—This includes how many managed devices are configured for intrusion prevention,and whether a device has been enabled for Threat Intelligence Director (TID).
  - **Malware detection**— This includes how many malware licenses are configured and deployed to devices, and how many devices have policies deployed that are using the malware detection capability.

Enrolled Device Data

Once you enroll the Firepower Management Center in Cisco Success Network, select telemetry data about the enrolled Firepower Management Center device is streamed to the Cisco cloud. The following table describes the collected and monitored data about the enrolled device. This includes feature-specific information about instrusion policies (both system-provided and custom) and malware detection for enrolled Firepower Management Centers.

Table 7: Enrolled Device Telemetry Data

Data Point	Example Value
Device Name	Management Center East
Device UUID	24fd0ccf-1464- 491f-a503- d241317bb327
HA Peer UUID	24fe0ccd-1564- 491h-b802- d321317cc827
Device Model	Cisco Firepower Management Center 4000 Cisco Firepower Management Center for VMWare
Serial Number	9AMDESQP6UN
System Uptime	99700000
Product Identifier	FMC4000-K9 FS-VMW-SW-K9
Smart License PIID	24fd0ccf-1464- 491f-a503- d241317bb327
Virtual Account Identifier	CiscoSVStemp

Software Version Data

Cisco Success Network collects software information that pertains to the enrolled Firepower Management Center device, including software version, rule update version, geolocation database version, and vulnerability database version information. The following table describes the collected and monitored software information about the enrolled device.

Table 8: Software Version Telemetry Data

Data Point	Example Value
Firepower Management Center Software Version	{ type: "SOFTWARE", version: "6.2.3-10517" }
Rule Update Version	{ type: "SNORT_RULES_DB", version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }
Vulnerability Database (VDB) Version	{ type: "VULNERABILITY_DB", version: "271", lastUpdated: 1468606837000 }
Geolocation Database Version	{ type: "GEOLOCATION_DB", version: "850" }

Managed Device Data

Cisco Success Network collects information about all the managed devices associated with an enrolled Firepower Management Center. The following table describes the collected and monitored information about managed devices. This includes feature-specific policy and licensing information, such as URL filtering, intrusion prevention, and malware detection for managed devices.

Table 9: Managed Device Telemetry Data

Data Point	Example Value
Managed Device Name	firepower
Managed Device Version	6.2.3-10616
Managed Device Manager	FMC
Managed Device Model	Cisco Firepower 2130 NGFW Appliance Cisco Firepower Threat Defense VMware
Managed Device Serial Number	9AMDESQP6UN
Managed Device PID	FPR2130-NGFW-K9 NGFWv
Is URL Filtering License Used for Device?	True
AC Rules with URL Filtering Per Device	10
Number of AC Rules with URL Filtering That Use URL Filtering License	3

Data Point	Example Value
Number of AC Rules with URL Filtering That Use Threat License	3
Is Threat License Used for Device?	True
Does AC Policy Have Intrusion Rule Attached?	True
Number of AC Rules with Intrusion Policies	10
Is Malware License Used for Device?	True
Number of AC Rules with Malware Policy	10
Number of AC Rules with Malware Policy That Use Malware License	5
Is Threat Intelligence Director (TID) Used for Device?	True

Deployment Information

After you configure your deployment, and any time you change that configuration, you must deploy the changes to the affected devices. The following table describes the collected and monitored data about configuration deployment, such as the number of devices affected and the status of deployments, including success and failure information.

Table 10: Deployment Information

Data Point	Example Value
Job ID	8589936079
Number of Devices Selected for Deployment	3
Number of Devices with Deployment Failure	1
Number of Devices with Deployment Success	2
End Time	1523993913001
Start Time	1523993840445
Status	SUCCEEDED
Target Device UUID	4f14f644-41e0 -11e8-9354- cf32315d7095
Policy Types Deployed	NetworkDiscovery NGFWPolicy DeviceConfiguration
Last Deployment Job ID Collected in Current Run	8589936079

TLS/SSL Inspection Event Data

By default, the Firepower System cannot inspect traffic encrypted with the Secure Socket Layer (SSL) protocol or its successor, the Transport Layer Security (TLS) protocol. *TLS/SSL inspection* enables you to either block encrypted traffic without inspecting it, or inspect encrypted or decrypted traffic with access control. The following tables describe statistics.shared with Cisco Success Network about encrypted traffic.

Handshake Process

When the system detects a TLS/SSL handshake over a TCP connection, it determines whether it can decrypt the detected traffic. As the system handles encrypted sessions, it logs details about the traffic.

Table 11: TLS/SSL Inspection - Handshake Telemetry Data

Data Point	Example Value
The system reports the following applied actions when the traffic **cannot be decrypted** and is: • Blocked • Blocked with a TCP reset • Not decrypted	An integer value of 0 or greater
The system reports the following applied actions when the traffic **can be decrypted**: • With a known private key • With a replacement key only • By resigning a self-signed certificate • By resigning the server certificate	An integer value of 0 or greater

Cache Data

After a TLS/SSL handshake completes, the managed device caches encrypted session data, which allows session resumption without requiring the full handshake. The managed device also caches server certificate data, which allows faster handshake processing in subsequent sessions.

Table 12: TLS/SSL Inspection - Cache Telemetry Data

Data Point	Example Value
The system caches encrypted session data and server certificate data, and reports on the **cache** per SSL connections, specifically: • The number of times SSL session information was cached • The number of times the SSL certificate validation cache was hit • The number of times the SSL certificate validation cache lookup missed • The number of times the SSL original certificate cache was hit • The number of times the SSL original certificate cache lookup missed • The number of times the SSL resigned certificate cache was hit • The number of times the SSL resigned certificate cache lookup missed	An integer value of 0 or greater

Certificate Status

The system evaluates encrypted traffic and reports the certificate status of the encrypting server.

Table 13: TLS/SSL Inspection - Certificate Status Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic based on the **certificate status** of the encrypting server, and reports the number of connections where the SSL Certificate: • Is valid • Is expired • Has an invalid issuer • Has an invalid signature • Is not checked • Is not yet valid • Is revoked • Is self signed • Is unknown	An integer value of 0 or greater

Failure Reason

The system evaluates encrypted traffic and reports the failure reason when the system fails to decrypt traffic.

Table 14: TLS/SSL Inspection - Failure Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic and reports the **failure reason** when the system fails to decrypt traffic due to: • A decryption error • Making a policy verdict during the handshake • Making a policy verdict before the handshake • Compression being negotiated • An uncached session • An interface in passive mode • An unknown cipher suite • An unsupported cipher suite	An integer value of 0 or greater

Version

The system evaluates encrypted traffic and reports the negotiated TLS/SSL version per connection.

Table 15: TLS/SSL Inspection - Version Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic and reports the negotiated **version** per SSL connections where: • SSLv2 was negotiated • SSLv3 was negotiated • An unknown version was negotiated • TLSv1.0 was negotiated • TLSv1.1 was negotiated • TLSv1.2 was negotiated • TLSv1.3 was negotiated	An integer value of 0 or greater

Snort Restart Data

When the traffic inspection engine referred to as the Snort process on a managed device restarts, inspection is interrupted until the process resumes. Creating or deleting a user-defined application, or activating or

deactivating a system or custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing restarts the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains.

Table 16: Snort Restart Telemetry Data

Data Point	Example Value
Count of snort restarts when you enable or disable a custom application detector	An integer value of 0 or greater
Count of snort restarts when you create or modify a custom application detector	An integer value of 0 or greater

Contextual Cross-Launch Data

The contextual cross-launch feature allows you to quickly find more information about potential threats in web-based resources outside of the Firepower Management Center. You can click directly from an event in the event viewer or dashboard in the FMC to the relevant information in an external resource. This lets you quickly gather context around a specific event based on its IP addresses, ports, protocol, domain, and/or SHA 256 hash.

Table 17: Contextual Cross-Launch Telemetry Data

Data Point	Example Value
The count of the Contextual Cross-Launch resources configured on the FMC	An integer value of 0 or greater
The count of the Contextual Cross-Launch resources enabled on the FMC	An integer value of 0 or greater
The count of Contextual Cross-Launch instances containing a domain variable	An integer value of 0 or greater
The count of Contextual Cross-Launch instances containing an IP variable	An integer value of 0 or greater
The count of Contextual Cross-Launch instances containing a SHA 256 variable	An integer value of 0 or greater

Telemetry Example File

The following is an example of a Cisco Success Network telemetry file for streaming policy and deployment information about a Firepower Management Center and its managed devices:

```
{
  "version": "1.0",
  "metadata": {
    "topic": "fmc.telemetry",
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_FMC",
```

```
"recordVersion": "6.3.0",
"recordedAt": 1509133291334,
"fmc": {
  "deviceInfo": {
    "deviceModel": "Cisco Firepower Management Center",
    "deviceName": "FMC",
    "deviceUuid": "c40d793c-bb33-11e7-804d-6f32258941f8",
    "serialNumber": "615-10110800010110",
    "smartLicenseProductInstanceIdentifier": "0fa56138-5211-442a-846c-97b6431146fd",
    "smartLicenseVirtualAccountName": "Firepower Threat Defense",
    "systemUptime": 11658000,
    "udiProductIdentifier": "FMC4500-K9T"
  },
  "versions": {
    "items": [{
      "type": "SOFTWARE",
      "version": "6.3.0-10222"
    }, {
      "lastUpdated": 0,
      "type": "SNORT_RULES_DB",
      "version": "2018-02-13-001-vrt"
    }, {
      "lastUpdated": 0,
      "type": "VULNERABILITY_DB",
      "version": "290"
    }, {
      "type": "GEOLOCATION_DB",
      "version": "None"
    }]
  }
},
"managedDevices": {
"items": [{
  "deviceInfo": {
    "deviceManager": "FMC",
    "deviceModel": "Cisco Firepower 2130 NGFW Appliance",
    "deviceName": "10.2.4.107",
    "deviceVersion": "6.3.0-10222",
    "serialNumber": "515-10110800100010"
  },
  "urlFiltering" : {
      "urlFilteringLicenseUsed" : True,
      "acRulesWithURLFiltering" : 10
  }
},
{
  "deviceInfo": {
    "deviceManager": "FMC",
    "deviceModel": "Cisco Firepower 2140 NGFW Appliance",
    "deviceName": "192.168.0.119",
    "deviceVersion": "6.3.0-10222",
    "serialNumber": "725-10010900101020"
  },
  "urlFiltering" : {
      "urlFilteringLicenseUsed" : True,
      "acRulesWithURLFiltering" : 10
  }
}, {
  "deviceInfo": {
    "deviceManager": "FMC",
    "deviceModel": "Cisco Firepower Threat Defense for VMWare",
    "deviceName": "192.168.0.117",
    "deviceVersion": "6.3.0-10222",
    "serialNumber": "None"
```

```
      },
      "urlFiltering" : {
          "urlFilteringLicenseUsed" : False,
          "acRulesWithURLFiltering" : 0
      }
    }]
  },
    "deploymentData": {
    "deployJobInfoList": [{
       "jobDeviceList": [{
          "deployEndTime": "1523959960957",
          "deployStartTime": "1523959863411",
          "deployStatus": "SUCCEEDED",
          "deviceUuid": "4f14f644-41e0-11e8-9354-cf32315d7095",
          "pgTypes": "[PG.FIREWALL.NGFWAccessControlPolicy, PG.FIREWALL.PrefilterPolicy,
PG.PLATFORM.NgfwInlineSetPage]"
      }],
           "jobId": "8589935776",
           "numberOfDevices": 1,
           "numberOfFailedDevices": 0,
           "numberOfSuccessDevices": 1
      },{
        "jobDeviceList": [{
           "deployEndTime": "1523993913001",
           "deployStartTime": "1523993840445",
           "deployStatus": "SUCCEEDED",
           "deviceUuid": "4f14f644-41e0-11e8-9354-cf32315d7095",
           "pgTypes": "[PG.FIREWALL.NGFWAccessControlPolicy, PG.FIREWALL.PrefilterPolicy,
PG.PLATFORM.NgfwInlineSetPage]"
       }],
            "jobId": "8589936079",
            "numberOfDevices": 1,
            "numberOfFailedDevices": 0,
            "numberOfSuccessDevices": 1
       }],
            "lastJobId": "8589936079"
       }
    }
  }
```


Changing Cisco Success Network Enrollment

You enable Cisco Success Network when you register the Firepower Management Center with the Cisco Smart Software Manager. After that, use the following procedure to view or change enrollment status.

Note Cisco Success Network does not work in evaluation mode.

Procedure

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

Step 2 Under Smart License Status, next to Cisco Success Network, click **Enabled/Disabled** control for the Cisco Success Network feature to change the setting as appropriate.

Step 3 Read the information provided by Cisco, choose whether you want to **Enable Cisco Success Network**, and click **Apply Changes**.

What to do next

(Optional) See (Optional) Opt Out of Web Analytics Tracking.

End-User License Agreement

The Cisco end-user license agreement (EULA) and any applicable supplemental agreement (SEULA) that governs your use of this product are available from http://www.cisco.com/go/softwareterms.

History for Licensing

Feature	Version	Details
Licensing for multi-instance capability for the FTD on the Firepower 4100/9300	6.3	You can now deploy multiple FTD container instances on a Firepower 4100/9300. You only need a single license per feature per security module/engine. The base license is automatically assigned to each instance. New/Modified screens: **System** > **Licenses** > **Smart Licenses** Supported platforms: FTD on the Firepower 4100/9300
Specific License Reservation for air-gapped deployments	6.3	Customers whose deployments cannot connect to the internet to communicate with the Cisco License Authority can use a Specific License Reservation. For details, see: Specific License Reservation (SLR), on page 23. New/Modified screens: **System** > **Licenses** > **Specific Licenses** (This option is not available by default.) Supported platforms: FMC, FTD
Export-controlled functionality for restricted customers	6.3	Certain customers whose Smart Accounts are not otherwise eligible to use restricted functionality can purchase term-based licenses, with approval. For details, see: Enabling the Export Control Feature (for Accounts Without Global Permission), on page 19. Supported platforms: FMC, FTD