Licenses

This chapter provides in-depth information about the different license types, service subscriptions, licensing requirements and more.

Note The Firewall Management Center supports either a Smart License or a legacy PAK (Product Activation Keys) license for its platform license.

About Licenses

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure—you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Smart Software Manager and Accounts

When you purchase one or more licenses, you manage them in the Smart Software Manager: https://software.cisco.com/#module/SmartLicensing. The Smart Software Manager lets you create a primary account for your organization. If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a primary account for your organization. For instructions, see Create a Cisco Account.

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

You manage licenses by virtual account. Only that virtual account's devices 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 devices between virtual accounts.

How Licensing Works for the Management Center and Devices

The Firewall Management Center registers with the Smart Software Manager, and then assigns licenses for each managed device. Devices do not register directly with the Smart Software Manager.

A physical Firewall Management Center does not require a license for its own use.

Periodic Communication with the Smart Software Manager

In order to maintain your product license entitlement, your product must communicate periodically with the Smart Software Manager.

You use a Product Instance Registration Token to register the Firewall Management Center with the Smart Software Manager. The Smart Software Manager issues an ID certificate for communication between the Firewall Management Center and the Smart Software Manager. This certificate is valid for one year, although it will be renewed every six months. If an ID certificate expires (after a year with no communication), the Firewall Management Center may be removed from your account.

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

Your Firewall Management Center must either have direct internet access to the Smart Software Manager. In non-airgapped deployments, normal license communication occurs every 30 days, but with the grace period, your Firewall Management Center will operate for up to 90 days without contacting the Smart Software Manager. Ensure that the Firewall Management Center contacts the Smart Software Manager before 90 days have passed, or else the Firewall Management Center will revert to an unregistered state.

Cloud-Delivered Firewall Management Center and Threat Defense Licenses

You do not have to purchase a separate license to use the Cloud-Delivered Firewall Management Center in Security Cloud Control; the base subscription for a Security Cloud Control tenant includes the cost for the Cloud-Delivered Firewall Management Center.

Cloud-delivered Firewall Management Center Evaluation License

The cloud-delivered Firewall Management Center comes provisioned with a 90-day evaluation license. After the evaluation period has elapsed, you can still onboard Firewall Threat Defense devices to the cloud-delivered Firewall Management Center. However, any manually triggered or scheduled deployments are blocked, until you register your cloud-delivered Firewall Management Center with the Cisco Smart Software Manager (CSSM). As your evaluation license approaches the expiry date, Security Cloud Control notifies you through alerts on the notifications window.

We also recommend that, after registering to CSSM, you purchase the required licenses for the features you want to use. Purchasing licenses keeps the cloud-delivered Firewall Management Center from going out of compliance.

To know more about how to register the cloud-delivered Firewall Management Center with CSSM, see Register the Management Center with the Smart Software Manager.

To learn how to get a cloud-delivered Firewall Management Center provisioned on your Security Cloud Control tenant, see Request a Cloud-delivered Firewall Management Center for your Security Cloud Control Tenant.

Note The Cloud-Delivered Firewall Management Center does not support specific license reservation (SLR) for devices in air-gapped networks.

Threat Defense Licenses for Cloud-Delivered Firewall Management Center

You need individual licenses for each Secure Firewall Threat Defense device managed by the Cloud-Delivered Firewall Management Center. See Licensing in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Firewall in Security Cloud Control* for information.

To know how Security Cloud Control handles licensing for the devices migrated to the Cloud-Delivered Firewall Management Center, see Migrate Threat Defense from Management Center to Cloud.

Note The Talos certificate for Evaluation Mode in Secure Firewall version 7.6.0 is set to expire on March 31, 2025. After this date, access to Talos-hosted services in Evaluation Mode (specifically those related to web reputation / categorization lookups) will be discontinued.

Out-of-Compliance State

The Firewall Management Center can become out of compliance in the following situations:

- License expiration—When a managed device term-based license expires.

In an out-of-compliance state, see the following effects:

- All managed device licenses—Operation is not affected.

After you resolve the licensing problem, the Firewall Management Center will show that it is now in compliance after its regularly scheduled authorization with the Smart Software Manager. To force an authorization, click **Re-Authorize** on the **System** (⚙) > **Licenses** > **Smart Licenses** page.

Unregistered State

The Firewall Management Center can become unregistered in the following situations:

- Evaluation mode expiration—Evaluation mode expires after 90 days.
- Manual deregistration of the Firewall Management Center
- Lack of communication with the Smart Software Manager—The Firewall Management Center does not communicate with the Smart Software Manager for 1 year. Note: After 90 days, the Firewall Management Center authorization expires, but it can successfully resume communication within one year to automatically re-authorize. After a year, the ID certificate expires, and the Firewall Management Center is removed from your account so you will have to manually re-register the Firewall Management Center.

In an unregistered state, the Firewall Management Center cannot deploy any configuration changes to devices *for features that require licenses*.

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.

License Types and Restrictions

This section describes the types of licenses available.

Table 1: Smart Licenses

License You Assign	Duration	Granted Capabilities
Essentials	Perpetual or Subscription **Note** Essentials subscription licenses are supported only on Firewall Threat Defense Virtual.	Except for Specific License Reservation and the Secure Firewall 1200/3100/4200, Essentials perpetual licenses are automatically assigned with all Firewall Threat Defenses. User and application control Switching and routing NAT For details, see Essentials Licenses, on page 6.
IPS	Subscription	Intrusion detection and prevention File control Security Intelligence filtering For details, see IPS Licenses, on page 7

License You Assign	Duration	Granted Capabilities
Malware defense	Subscription	Malware defense Secure Malware Analytics File storage (IPS license is a prerequisite for a Malware defense license.) For details, see Malware Defense Licenses, on page 6 and *License Requirements for File and Malware Policies* in the Cisco Secure Firewall Management Center Device Configuration Guide.
Carrier	Subscription for Firepower 4100/9300, Secure Firewall 3100/4200, and Firewall Threat Defense Virtual	Diameter, GTP/GPRS, M3UA, and SCTP inspection For details, see Carrier License, on page 7.
URL Filtering	Subscription	Category and reputation-based URL filtering For details, see URL Filtering Licenses, on page 9. (IPS license is a prerequisite for a URL Filtering license.)
Export-Controlled Features	Perpetual	Features that are subject to national security, foreign policy, and anti-terrorism laws and regulations; see Licensing for Export-Controlled Functionality, on page 10.
Remote Access VPN: - Secure Client Premier - Secure Client Advantage - Secure Client VPN Only	Subscription or perpetual	Remote access VPN configuration. Your account must allow export-controlled functionality to configure remote access VPN. You select whether you meet export requirements when you register the device. The Firewall Threat Defense can use any valid Secure Client license. The available features do not differ based on license type. For more information, see Secure Client Licenses, on page 9 and *VPN Licensing* in the Cisco Secure Firewall Management Center Device Configuration Guide.

Note Subscription licenses are term-based licenses.

Essentials Licenses

The Essentials license allows you to:

- Configure your devices to perform switching and routing (including DHCP relay and NAT)
- Configure devices as a high availability pair
- Configure clustering
- Implement user and application control by adding user and application conditions to access control rules
- Update the Vulnerability database (VDB) and geolocation database (GeoDB).
- Download intrusion rules such as SRU/LSP. However, you cannot deploy access control policy or rules that have intrusion policy to the device unless IPS license is enabled.

Secure Firewall 1200/3100/4200

You obtain a Essentials license when you purchase the Secure Firewall 1200/3100/4200.

Other Models

Except in deployments using Specific License Reservation, a Essentials license is automatically added to your account when you register a device to the Firewall Management Center. For Specific License Reservation, you need to add the Essentials license to your account.

Malware Defense Licenses

A Malware defense license lets you perform Malware Defense and Secure Malware Analytics. With this feature, you can use devices to detect and block malware in files transmitted over your network. To support this feature license, you can purchase the Malware defense (AMP) service subscription as a stand-alone subscription or in combination with IPS (TM) or IPS and URL Filtering (TMC) subscriptions. IPS license is a prerequisite for a Malware defense license.

Note Managed devices with Malware defense licenses enabled periodically attempt to connect to the Secure Malware Analytics 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 Malware Defense 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. Malware Defense 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 Secure Malware Analytics 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 Defense 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.

Note that a Malware defense license is required only if you deploy Malware Defense and Secure Malware Analytics. Without a Malware defense license, the Firewall Management Center can receive Secure Endpoint malware events and indications of compromise (IOC) from the Secure Malware Analytics Cloud.

See also important information at *License Requirements for File and Malware Policies* in the Cisco Secure Firewall Management Center Device Configuration Guide.

When you disable this license:

- The system stops querying the Secure Malware Analytics Cloud, and also stops acknowledging retrospective events sent from the Secure Malware Analytics Cloud.
- You cannot re-deploy existing access control policies if they include Malware Defense configurations.
- For a very brief time after a Malware defense 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.

If the license expires, your entitlement for the above capabilities ceases and the Firewall Management Center moves to the out-of-compliance state.

IPS Licenses

A IPS 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. *Malware defense*, which requires a Malware defense 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 IPS license as a stand-alone subscription (T) or in combination with URL Filtering (TC), Malware defense (TM), or both (TMC).

When you disable this license:

- The Firewall 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.
- The Firewall Management Center does 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 IPS.

If the license expires, your entitlement for the above capabilities ceases and the Firewall Management Center moves to the out-of-compliance state.

Carrier License

The Carrier license enables the inspection of the following protocols:

- Diameter—Diameter is an Authentication, Authorization, and Accounting (AAA) protocol used in next-generation mobile and fixed telecom networks such as EPS (Evolved Packet System) for LTE (Long

Term Evolution) and IMS (IP Multimedia Subsystem). It replaces RADIUS and TACACS in these networks.

- GTP/GPRS—GPRS Tunneling Protocol (GTP) is used in GSM, UMTS, and LTE networks for general packet radio service (GPRS) traffic. GTP provides a tunnel control and management protocol to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP also uses a tunneling mechanism for carrying user data packets.
- M3UA—MTP3 User Adaptation (M3UA) is a client/server protocol that provides a gateway to the Signaling System 7 (SS7) network for IP-based applications that interface with the SS7 Message Transfer Part 3 (MTP3) layer. M3UA makes it possible to run the SS7 User Parts (such as ISUP) over an IP network.
- SCTP—Stream Control Transmission Protocol (SCTP) is a transport-layer protocol that supports the SS7 protocol over IP networks. It supports the 4G LTE mobile network architecture. SCTP can handle multiple simultaneous streams, multiplexed streams, and provides more security features.

Note After you enable this license on a device, use a FlexConfig policy to enable the protocol inspection.

The Carrier license PIDs are available per family and not per device model. You can enable this license for each device either in the evaluation mode or with a Smart License.

The Carrier license for Firepower 4100/9300, Secure Firewall 3100/4200, and Firewall Threat Defense Virtual is term-based. This license also supports Specific License Reservation.

Supported Devices

The devices that support the Carrier License are:

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140
- Firepower 4112
- Firepower 4115
- Firepower 4125
- Firepower 4145
- Secure Firewall 4215
- Secure Firewall 4225
- Secure Firewall 4245
- Firepower 9300
- Firewall Threat Defense Virtual

URL Filtering Licenses

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 service subscription as a stand-alone subscription or in combination with IPS (TC) or Threat and Malware defense (TMC) subscriptions. IPS license is a prerequisite for this license.

Tip Without a URL Filtering license, you can specify individual URLs or groups of URLs to allow or block. This option 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 Firewall Management Center will not download URL information. You cannot deploy the access control policy until you first add a URL Filtering license to the Firewall Management Center, then enable it on the devices targeted by the policy.

When you disable this license:

- You may lose access to filtering network traffic based on the URL category and reputation ACP rules. The manual URL filtering options will continue to be supported.
- Access control rules with URL conditions immediately stop filtering URLs.
- Your Firewall 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.

If the license expires, your entitlement for the above capabilities ceases and the Firewall Management Center moves to the out-of-compliance state.

Secure Client Licenses

You can configure remote access VPN using the Secure Client and standards-based IPSec/IKEv2.

To enable remote access VPN, you must purchase and enable one of the following licenses: Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only. You can select Secure Client Advantage and Secure Client Premier if you have both licenses and you want to use them both. The Secure Client VPN Onlylicense cannot be used with **Apex** or **Plus**. The Secure Client license must be shared with the Smart Account. For more instructions, see http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

You cannot deploy the remote access VPN configuration to the device if the specified device does not have the entitlement for a minimum of one of the specified Secure Client 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 Account must have the export controlled features (strong encryption) enabled. The Firewall Threat Defense requires strong encryption (which is higher than DES) for successfully establishing remote access VPN connections with Secure Clients.

You cannot deploy remote access VPN if the following are true:

- Smart Licensing on the Firewall Management Center is running in evaluation mode.

- Your Smart Account is not configured to use export-controlled features (strong encryption).

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
- 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 the Smart Software Manager, contact your account representative.
- If the option “Allow export-controlled functionality on the products registered with this token” appears when you generate a new Product Instance Registration Token in the Smart Software Manager, make sure you check it before generating the token.

  If you did not enable export-controlled functionality for the Product Instance Registration Token that you used to register the Firewall Management Center, then you must deregister and then re-register the Firewall Management Center using a new Product Instance Registration Token with export-controlled functionality enabled.

If you registered devices to the Firewall Management Center in evaluation mode or before you enabled strong encryption on the Firewall Management Center, reboot each managed device to make strong encryption available. In a high availability deployment, the active and standby devices must be rebooted together to avoid an Active-Active condition.

The entitlement is perpetual and does not require a subscription.

More Information

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

Firewall Threat Defense Virtual Licenses

This section describes the performance-tiered license entitlements available for the Firewall Threat Defense Virtual.

Any Firewall Threat Defense Virtual license can be used on any supported Firewall Threat Defense Virtual vCPU/memory configuration. This allows Firewall Threat Defense Virtual customers to run on a wide variety of VM resource footprints. This also increases the number of supported AWS and Azure instances types. When configuring the Firewall Threat Defense Virtual VM, the maximum supported number of cores (vCPUs) is 16 ; and the maximum supported memory is 32 GB RAM .

Performance Tiers for Firewall Threat Defense Virtual Smart Licensing

Session limits for RA VPNs are determined by the installed Firewall Threat Defense Virtual platform entitlement tier, and enforced via a rate limiter. The following table summarizes the session limits based on the entitlement tier and rate limiter.

Table 2: Firewall Threat Defense Virtual Licensed Feature Limits Based on Entitlement

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250
FTDv20, 3Gbps	4 core/8 GB	3Gbps	250
FTDv30, 5Gbps	8 core/16 GB	5Gbps	250
FTDv50, 10Gbps	12 core/24 GB	10Gbps	750
FTDv100, 16Gbps	16 core/32 GB	16Gbps	10,000
FTDvU	32 core/64 GB	Not limited	20,000
FTDvU	64 core/128 GB	Not limited	32,000

Firewall Threat Defense Virtual Performance Tier Licensing Guidelines and Limitations

Please keep the following guidelines and limitations in mind when licensing your Firewall Threat Defense Virtual device.

- The Firewall Threat Defense Virtual supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements.
- Any Firewall Threat Defense Virtual license can be used on any supported Firewall Threat Defense Virtual core/memory configuration. This allows the Firewall Threat Defense Virtual customers to run on a wide variety of VM resource footprints.
- You can select a performance tier when you deploy the Firewall Threat Defense Virtual, whether your device is in evaluation mode or is already registered with Cisco Smart Software Manager.

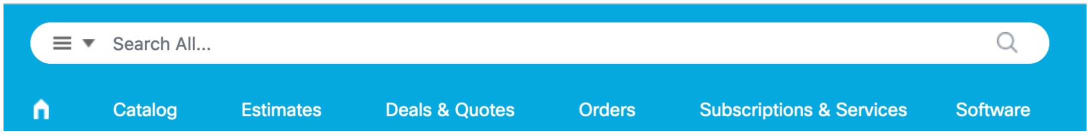
Note Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. If you are upgrading your Firewall Threat Defense Virtual to Version 7.0, you can choose **FTDv - Variable** to maintain your current license compliance. Your Firewall Threat Defense Virtual continues to perform with session limits based on your device capabilities (number of cores/RAM).

- The default performance tier is FTDv50 when deploying a new Firewall Threat Defense Virtual device, or when provisioning the Firewall Threat Defense Virtual using the REST API.
- Essentials licenses are subscription-based and mapped to performance tiers. Your virtual account needs to have the Essentials license entitlements for the Firewall Threat Defense Virtual devices, as well as for IPS, Malware Defense, and URL Filtering licenses.
- Each HA peer consumes one entitlement, and the entitlements on each HA peer must match, including Essentials license.
- A change in performance tier for an HA pair should be applied to the primary peer.
- You assign feature licenses to the cluster as a whole, not to individual nodes. However, each node of the cluster consumes a separate license for each feature. The clustering feature itself does not require any licenses.
- Universal PLR licensing is applied to each device in an HA pair separately. The secondary device will not automatically mirror the performance tier of the primary device. It must be updated manually.

License PIDs

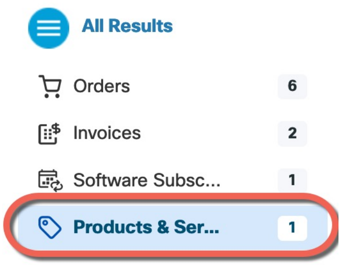
When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Search All** field on the Cisco Commerce Workspace.

Figure 1: License Search



Choose **Products & Services** from the results.

Figure 2: Results



Firewall Threat Defense Virtual PIDs

When you order FTDV-SEC-SUB, you must choose a Essentials license and optional feature licenses (12 month term):

- Essentials license:
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- IPS, Malware defense, and URL license combination:
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC
  - FTD-V-50S-TMC
  - FTD-V-100S-TMC
- Carrier—FTDV_CARRIER
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Firepower 1010 PIDs

- IPS, Malware defense, and URL license combination:
  - L-FPR1010T-TMC=

  When you add the above PID to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Firepower 1100 PIDs

- IPS, Malware defense, and URL license combination:
  - L-FPR1120T-TMC=

    - L-FPR1140T-TMC=
    - L-FPR1150T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

    - L-FPR1120T-TMC-1Y
    - L-FPR1120T-TMC-3Y
    - L-FPR1120T-TMC-5Y
    - L-FPR1140T-TMC-1Y
    - L-FPR1140T-TMC-3Y
    - L-FPR1140T-TMC-5Y
    - L-FPR1150T-TMC-1Y
    - L-FPR1150T-TMC-3Y
    - L-FPR1150T-TMC-5Y

- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Secure Firewall 1210/1220 PIDs

- Essentials license:
    - *Included automatically*
- IPS, Malware defense, and URL license combination:
    - L-CSF1210CET-TMC=
    - L-CSF1210CPT-TMC=
    - L-CSF1220CXT-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

    - L-CSF1210CE-TMC-1Y
    - L-CSF1210CE-TMC-3Y
    - L-CSF1210CE-TMC-5Y
    - L-CSF1210CP-TMC-1Y
    - L-CSF1210CP-TMC-3Y
    - L-CSF1210CP-TMC-5Y
    - L-CSF1220CX-TMC-1Y
    - L-CSF1220CX-TMC-3Y

    - L-CSF1220CX-TMC-5Y

- Strong Encryption (3DES/AES):
    - L-CSF1200TD-ENCK9=. Only required if your account is not authorized for strong encryption.
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Secure Firewall 1230/1240/1250 PIDs

- Essentials license:
    - *Included automatically*
- IPS, Malware defense, and URL license combination:
    - L-CSF1230T-TMC=
    - L-CSF1240T-TMC=
    - L-CSF1250T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

    - L-CSF1230-TMC-1Y
    - L-CSF1230-TMC-3Y
    - L-CSF1230-TMC-5Y
    - L-CSF1240-TMC-1Y
    - L-CSF1240-TMC-3Y
    - L-CSF1240-TMC-5Y
    - L-CSF1250-TMC-1Y
    - L-CSF1250-TMC-3Y
    - L-CSF1250-TMC-5Y
- Strong Encryption (3DES/AES):
    - L-CSF1200TD-ENCK9=. Only required if your account is not authorized for strong encryption.
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Secure Firewall 3100 PIDs

- Essentials license:
    - *Included automatically*
- IPS, Malware defense, and URL license combination:

    - L-FPR3110T-TMC=
    - L-FPR3120T-TMC=
    - L-FPR3130T-TMC=
    - L-FPR3140T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

    - L-FPR3105T-TMC-1Y
    - L-FPR3105T-TMC-3Y
    - L-FPR3105T-TMC-5Y
    - L-FPR3110T-TMC-1Y
    - L-FPR3110T-TMC-3Y
    - L-FPR3110T-TMC-5Y
    - L-FPR3120T-TMC-1Y
    - L-FPR3120T-TMC-3Y
    - L-FPR3120T-TMC-5Y
    - L-FPR3130T-TMC-1Y
    - L-FPR3130T-TMC-3Y
    - L-FPR3130T-TMC-5Y
    - L-FPR3140T-TMC-1Y
    - L-FPR3140T-TMC-3Y
    - L-FPR3140T-TMC-5Y

- Carrier—L-FPR3K-FTD-CAR=
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Firepower 4100 PIDs

- IPS, Malware defense, and URL license combination:

    - L-FPR4112T-TMC=
    - L-FPR4115T-TMC=
    - L-FPR4125T-TMC=
    - L-FPR4145T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y

- Carrier—L-FPR4K-FTD-CAR=
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Secure Firewall 4200 PIDs

- Essentials license:
  - *Included automatically*
- IPS, Malware defense, and URL license combination:
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

  - L-FPR4215T-TMC-1Y
  - L-FPR4215T-TMC-3Y
  - L-FPR4215T-TMC-5Y
  - L-FPR4225T-TMC-1Y
  - L-FPR4225T-TMC-3Y
  - L-FPR4225T-TMC-5Y
  - L-FPR4245T-TMC-1Y
  - L-FPR4245T-TMC-3Y

  - L-FPR4245T-TMC-5Y

- Carrier—L-FPR4200-FTD-CAR=
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Firepower 9300 PIDs

- IPS, Malware defense, and URL license combination:
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y
  - L-FPR9K-56T-TMC-5Y

- Carrier—L-FPR9K-FTD-CAR=
- Cisco Secure Client—See the Cisco AnyConnect Ordering Guide.

ISA 3000 PIDs

- IPS, Malware defense, and URL license combination:
  - L-ISA3000T-TMC=

  When you add the above PID to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

  - L-ISA3000T-TMC-1Y
  - L-ISA3000T-TMC-3Y
  - L-ISA3000T-TMC-5Y

- Cisco Secure Client—See the Cisco AnyConnect Ordering Guide.

Requirements and Prerequisites for Licensing

General Prerequisites

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

  For a Firepower 4100/9300, you must configure NTP on the chassis using the same NTP server for the chassis as for the Firewall Management Center.

Supported Domains

Global, except where indicated.

User Roles

- Admin

Requirements and Prerequisites for Licensing for High Availability, Clustering, and Multi-Instance

This section describes the licensing requirements for device High Availability.

FTD Services does not support clustering or multi-instance deployments.

Licensing for Device High-Availability

Both Firewall Threat Defense units in a high availability configuration must have the same licenses.

High availability configurations require two license entitlements: one for each device in the pair.

Before high availability is established, it does not matter which licenses are assigned to the secondary/standby device. During high availability configuration, the Firewall Management Center releases any unnecessary licenses assigned to the standby unit and replaces them with identical licenses assigned to the primary/active unit. For example, if the active unit has a Essentials license and a IPS license, and the standby unit has only a Essentials license, the Firewall Management Center communicates with the Smart Software Manager to obtain an available IPS license from your account for the standby unit. If your license account does not include enough purchased entitlements, your account becomes Out-of-Compliance until you purchase the correct number of licenses.

Licensing for Device Clusters

Each Firewall Threat Defense Virtual cluster node requires the same performance tier license. We recommend using the same number of CPUs and memory for all members, or else performance will be limited on all nodes to match the least capable member. The throughput level will be replicated from the control node to each data node so they match.

You assign feature licenses to the cluster as a whole, not to individual nodes. However, each node of the cluster consumes a separate license for each feature. The clustering feature itself does not require any licenses.

When you add the control node to the Firewall Management Center, you can specify the feature licenses you want to use for the cluster. Before you create the cluster, it doesn't matter which licenses are assigned to the data nodes; the license settings for the control node are replicated to each of the data nodes. You can modify licenses for the cluster by clicking **Edit Licenses** in **System** (⚙) > **Licenses** > **Smart Licenses** or choosing**Devices** > **Device Management**, clicking **Edit** (✎) for the cluster, and then in the **Cluster** > **License** area, clicking **Edit** (✎).

Note If you add the cluster before the Firewall Management Center is licensed (and running in Evaluation mode), then when you license the Firewall Management Center, you can experience traffic disruption when you deploy policy changes to the cluster. Changing to licensed mode causes all data units to leave the cluster and then rejoin.

Create a Cisco Account

You must have a Cisco account to request a Smart Account and license any Cisco products.

Procedure

Step 1 Open the URL https://id.cisco.com/signin/register to create a new account.

Step 2 Enter all the required fields to create an account.

The following figure shows an example.

Step 3 Click **Register**.

An email with an activation code is sent to verify your email address.

Note
If you haven't received an email yet, send an email to the registration support team at web-help@cisco.com.

Step 4 In the **Verify with your email** page, enter the activation code to complete the registration process and click **Verify**.

After successful registration, you will be redirected to the login page.

What to do next

Enter the newly created account details on the login page to request a Smart Account. See Create a Smart Account and Add Licenses, on page 20.

Create a Smart Account and Add Licenses

You should set up this account before you purchase 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.

You must create a new Cisco account if you don't already have one. For instructions, see Create a Cisco Account.

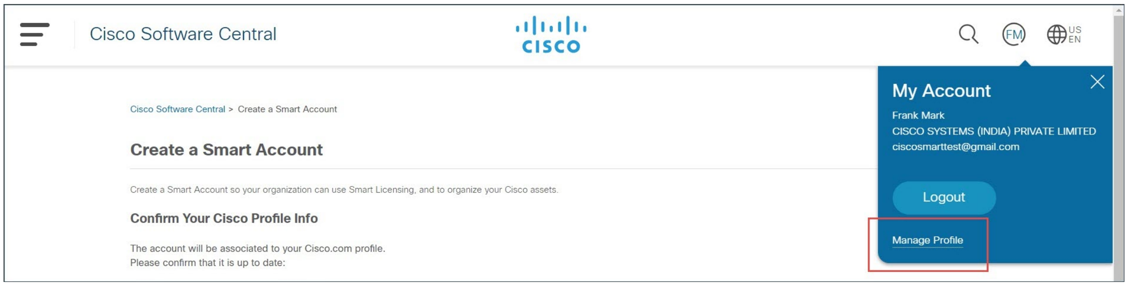
For general information about Smart Accounts, see http://www.cisco.com/go/smartaccounts.

Procedure

Step 1 Go to the Create a Smart Account page. You are prompted to log in with your Cisco account.

In the **Create a Smart Account** page, your basic account information is displayed.

Step 2 Click the **My Account** icon appearing in the top right corner and click **Manage Profile**.



Create a Smart Account so your organization can use Smart Licensing, and to organize your Cisco assets.

Confirm Your Cisco Profile Info

The account will be associated to your Cisco.com profile.
Please confirm that it is up to date:

Frank Mark
CISCO SYSTEMS (INDIA) PRIVATE LIMITED
ciscosmarttest@gmail.com

Step 3 Click **Personal**.

Step 4 In the **Your Company Details** section, click **Edit**.

Step 5 In the **Company or organization** field, type your organization name.

Step 6 If your company information is already present in our database, it will appear in the list. You can select your company.

In the **Address** drop-down list, select the address of your company.

Step 7 If your company is not listed in our database, you can continue to enter your company information in the **Company or organization** field.

a) In the **Address** drop-down list, click the drop-down arrow and click **Add New Address**.

b) You can select one of the following **Address Type** options:

- **Company/Organization**: To provide your organization's address. Cisco verifies this address. If the address and company name cannot be validated with the country, you may not be able to proceed. Therefore, you must ensure that the correct address is provided.
- **Personal**: To provide your personal address.

Step 8 Enter all the mandatory fields associated with your company and click **Update**.

The **Your Company Details** section displays the company details you entered.

A success message appears if your company details are validated.

Step 9 Click **Update**.

A success message appears if your company details are validated.

Step 10 Open the **Create a Smart Account** page, which was opened in the previous tab. Refresh the page if changes are not reflecting.

Alternatively, you can open this page using the https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation URL and login using your credentials.

Step 11 Click **Create Account**.

The Account Summary page displays your account details.

Step 12 Click **Done**.

Step 13 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 14 Make sure your Smart Licensing account contains the available licenses you need.

For license PIDs, see License PIDs, on page 12.

What to do next

To configure Smart License using the Smart Software Manager, see Configure Smart Licensing, on page 22.

Configure Smart Licensing

This section describes how to use Smart Licensing using the Smart Software Manager or the Smart Software Manager On-Prem.

Register the Firewall Management Center for Smart Licensing

You can register the Firewall Management Center directly to the Smart Software Manager over the internet, or when using an air-gapped network, with the Smart Software Manager On-Prem.

Register the Firewall Management Center with the Smart Software Manager

Register the Firewall Management Center with the Smart Software Manager.

Before you begin

- Make sure your Smart Licensing account contains the available licenses you need.

  When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Account. However, if you need to add licenses yourself, see Cisco Commerce Workspace. For license PIDs, see License PIDs, on page 12.

- Ensure that the Firewall Management Center can reach the Smart Software Manager at smartreceiver.cisco.com.

- Make sure you configure NTP. During registration, a key exchange occurs between the Smart Agent and the Smart Software Manager, so time must be in sync for proper registration.

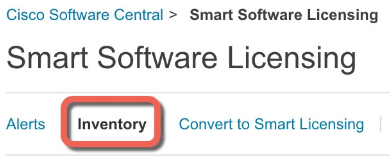
For the Firepower 4100/9300, you must configure NTP on the chassis using the same NTP server for the chassis as for the Firewall Management Center.

- If your organization has multiple Firewall Management Centers, make sure each Firewall Management Center has a unique name that clearly identifies and distinguishes it from other Firewall Management Centers 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.

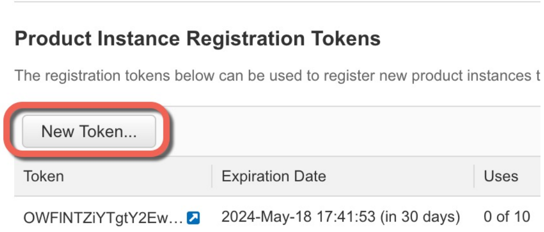
Procedure

Step 1 In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

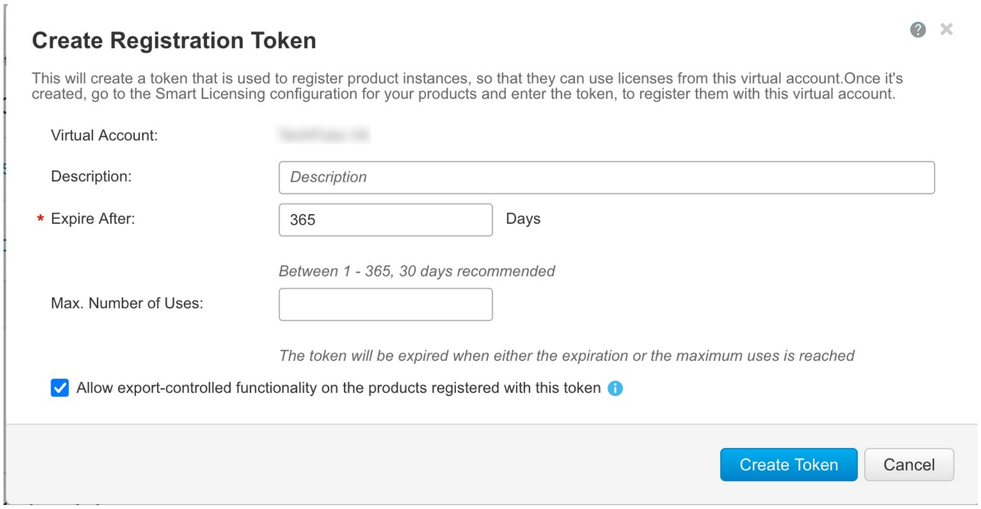

Cisco Software Central > Smart Software Licensing
Smart Software Licensing
Alerts
Inventory
Convert to Smart Licensing

b) On the **General** tab, click **New Token**.


Product Instance Registration Tokens
The registration tokens below can be used to register new product instances t
New Token...

Token	Expiration Date	Uses
OWFINTZiYTgtY2Ew...	2024-May-18 17:41:53 (in 30 days)	0 of 10

c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:



This will create a token that is used to register product instances, so that they can use licenses from this virtual account.Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: [redacted]

Description: Description

* Expire After: 365 Days

Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

☑ Allow export-controlled functionality on the products registered with this token

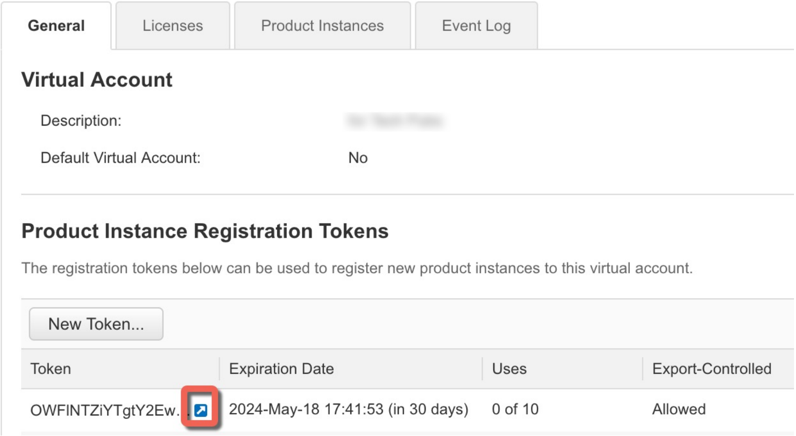
- **Description**
- **Expire After**—Cisco recommends 30 days.

- **Max. Number of Uses**
- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the Firewall Threat Defense.

Figure 3: View Token



Virtual Account

Description: [redacted]

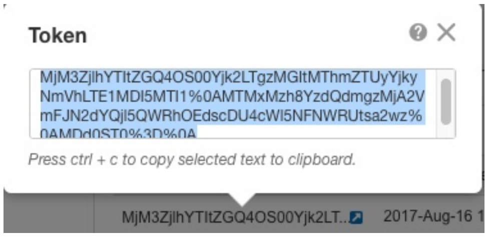
Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

Token	Expiration Date	Uses	Export-Controlled
OWFINTZiYTgtY2Ew...	2024-May-18 17:41:53 (in 30 days)	0 of 10	Allowed

Figure 4: Copy Token



Token

MjM3ZjlhYTItZGQ4OS00Yjk2LTgzMGItMThmZTUyYjky
NmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2V
mFJN2dYQjl5QWRhOEdscDU4cWI5NFNWRUtsa2wz%
0AMDd0ST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjlhYTItZGQ4OS00Yjk2LT.. 2017-Aug-16 1

Step 2 In the Firewall Management Center, choose **System** (⚙) > **Licenses** > **Smart Licenses**.

Step 3 Click **Register**.

Step 4 Paste the token you generated from 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 5 Click **Apply Changes**.

What to do next

- Add a Device to the Firewall Management Center; see *Add a Device to the Firewall Management Center* in the Cisco Secure Firewall Management Center Device Configuration Guide.

Assign Licenses to Devices

You can assign most licenses when you register a device to the Firewall Management Center. You can also assign licenses per device, or for multiple devices.

Assign Licenses to a Single Device

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

Before you begin

You must have Admin or Network Admin privileges to perform this task. When operating with multiple domains, you must do this task in leaf domains.

Procedure

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

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

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**.

Step 7 Deploy configuration changes.

What to do next

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.

Assign Licenses to Multiple Managed Devices

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

Use this procedure to enable licensing on multiple 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 the Firewall Threat Defense cluster, you apply the licenses to the cluster as a whole; note that each unit in the cluster consumes a separate license per feature.

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) To remove a license, click the **Delete** (🗑) next to the device.
g) Click **Apply**.

You can select a cluster and assign any license to all nodes of a cluster.

What to do next

Verify that your licenses are correctly installed. Follow the procedure in Monitoring Smart Licenses, on page 28.

Manage Smart Licensing

This section describes how to manage Smart Licensing.

Deregister the Firewall Management Center

Deregister your Firewall Management Center from the Smart Software Manager to release all of the license entitlements back to your Smart Account so they can be used for other devices. For example, deregister if you need to decommission the Firewall Management Center or reimage it.

See Unregistered State, on page 4 for more information about license enforcement in an unregistered state.

Procedure

Step 1 Choose **System** (⚙) > **Licenses** > **Smart Licenses**.

Step 2 Click **Deregister** (✖).

Monitoring Smart License Status

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

Usage Authorization

Possible status values are:

- **In-compliance** (🟢) — All licenses assigned to managed devices are in compliance and the Firewall Management Center is communicating successfully with the Smart Software Manager.
- **License is in compliance but communication with licensing authority has failed**— Device licenses are in compliance, but the Firewall 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 Firewall Management Center has not communicated with the Smart Software Manager in more than 90 days.

Product Registration

Specifies the last date when the Firewall Management Center contacted the Smart Software Manager 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 Firewall 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 10.

Cisco Success Network

Specifies whether you have enabled Cisco Success Network for the Firewall 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.

Monitoring Smart Licenses

To view the license status for the Firewall Management Center and its managed devices, use the Smart Licenses page.

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 Firewall 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 Firewall Management Center 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.
- 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.

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.

Troubleshooting Smart 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 Firewall Management Center has outside connectivity. See Internet Resources Accessed by Managed Devices.

Unexpected Out-of-Compliance Notification or Other Error

- If a device is already registered to a different Firewall Management Center, you need to deregister the original Firewall Management Center before you can license the device under a new Firewall Management Center. See Deregister the Firewall Management Center, on page 27.
- Check if the term of the subscription license has expired.

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

Configure Legacy Firewall Management Center PAK-Based Licenses

The Firewall Management Center supports either a Smart License or a legacy PAK (Product Activation Key) license for its platform license. This procedure describes how to apply a PAK-based license.

After re-registration of your Smart Account, you must manually add the classic licenses for all classic devices.

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.

Procedure

Step 1 The license key uniquely identifies the Firewall Management Center in the Smart Software Manager. It is composed of a product code (for example, 66) and the MAC address of the management port (eth0) of the Firewall Management Center; for example, 66:00:00:77:FF:CC:88.

a) Choose **System** (⚙) > **Licenses** > **Classic Licenses**.
b) Click **Add New License**.
c) Note the value in the **License Key** field at the top of the **Add Feature License** dialog.

Step 2 Choose **System** (⚙) > **Licenses** > **Classic Licenses**.

Step 3 Click **Add New License**.

Step 4 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 5 Click **Get License** to open the 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 6 Generate a license from the PAK in the License Registration Portal: https://cisco.com/go/license.

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

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.

Step 7 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 8 Return to the **Add Feature License** page in the management center virtual's web interface.

Step 9 Paste the license text into the **License** field.

Step 10 Click **Verify License**.

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

Step 11 Click **Submit License**.

Additional Information about Licensing

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

- FAQ—Licensing FAQ
- License Roadmap