



## Licenses

---

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



---

**Note** The FMC supports either a Smart License or a legacy PAK (Product Activation Keys) license for its platform license. For more information about using the PAK license, see [Configure Legacy FMC PAK-Based Licenses, on page 43](#).

---

- [About Licenses, on page 1](#)
- [Requirements and Prerequisites for Licensing, on page 17](#)
- [Create a Smart Account and Add Licenses, on page 20](#)
- [Configure Smart Licensing, on page 20](#)
- [Configure Specific License Reservation \(SLR\), on page 33](#)
- [Configure Legacy FMC PAK-Based Licenses, on page 43](#)
- [Configure Cisco Success Network Enrollment, on page 44](#)
- [Configure Cisco Support Diagnostics Enrollment, on page 45](#)
- [Additional Information about Licensing, on page 46](#)
- [History for Licenses, on page 46](#)

## 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](https://software.cisco.com)). For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](https://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.

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.

## 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 1: 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 <a href="#">Register the FMC with the Smart Software Manager On-Prem, on page 24</a>	For more information, see <a href="#">Configure Specific License Reservation (SLR), on page 33</a>

## How Licensing Works for the Management Center and Devices

The FMC 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 FMC does not require a license for its own use. The FMCv does require a platform license.

## 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 FMC with the Smart Software Manager. The Smart Software Manager issues an ID certificate for communication between the FMC 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 FMC may be removed from your account.

The FMC 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 FMC so the changes immediately take effect. You also can wait for the FMC to communicate as scheduled.

Your FMC must either have direct internet access to the Smart Software Manager, or use one of the options described in [Licensing Options for Air-Gapped Deployments, on page 2](#). In non-airgapped deployments, normal license communication occurs every 30 days, but with the grace period, your FMC will operate for up to 90 days without contacting the Smart Software Manager. Ensure that the FMC contacts the Smart Software Manager before 90 days have passed, or else the FMC will revert to an unregistered state.

## Evaluation Mode

Before the FMC registers with the Smart Software Manager, it operates for 90 days in evaluation mode. You can assign feature licenses to managed devices, and they will remain in compliance for the duration of evaluation mode. When this period ends, the FMC becomes unregistered.

If you register the FMC with the Smart Software Manager, the evaluation mode ends. If you later deregister the FMC, you cannot resume evaluation mode, even if you did not initially use all 90 days.

For more information about the unregistered state, see [Unregistered State, on page 4](#).



---

**Note** You cannot receive an evaluation license for Strong Encryption (3DES/AES); you must register with the Smart Software Manager to receive the export-compliance token that enables the Strong Encryption (3DES/AES) license.

---

## Out-of-Compliance State

The FMC can become out of compliance in the following situations:

- Over-utilization—When the managed devices or the FMCv uses unavailable licenses.
- License expiration—When a managed device term-based license expires.

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

- FMCv platform license—Operation is not affected.
- All managed device licenses—Operation is not affected.

After you resolve the licensing problem, the FMC 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 FMC can become unregistered in the following situations:

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

In an unregistered state, the FMC 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 2: Smart Licenses*

License You Assign	Subscription You Purchase	Duration	Granted Capabilities
Base	Based on license type	Perpetual or Subscription  <b>Note</b> Base subscription licenses are supported only on FTDv.	Except for Specific License Reservation and the Secure Firewall 3100, Base perpetual licenses are automatically assigned with all FTDs.  User and application control  Switching and routing  NAT  For details, see <a href="#">Base Licenses, on page 6</a> .
Threat	<ul style="list-style-type: none"> <li>• T</li> <li>• TC (Threat + URL)</li> <li>• TMC (Threat + Malware + URL)</li> </ul>	Subscription	Intrusion detection and prevention  File control  Security Intelligence filtering  For details, see <a href="#">Threat Licenses, on page 7</a>

License You Assign	Subscription You Purchase	Duration	Granted Capabilities
Malware	<ul style="list-style-type: none"> <li>• TM (Threat + Malware)</li> <li>• TMC (Threat + Malware + URL)</li> <li>• AMP</li> </ul>	Subscription	<p>Malware defense</p> <p>Secure Malware Analytics</p> <p>File storage</p> <p>For details, see <a href="#">Malware Licenses, on page 6</a> and <i>License Requirements for File and Malware Policies</i> in the <a href="#">Firepower Management Center Device Configuration Guide</a>.</p>
URL Filtering	<ul style="list-style-type: none"> <li>• TC (Threat + URL)</li> <li>• TMC (Threat + Malware + URL)</li> <li>• URL</li> </ul>	Subscription	<p>Category and reputation-based URL filtering</p> <p>For details, see <a href="#">URL Filtering Licenses, on page 8</a>.</p>
FMCv	Based on license type	<ul style="list-style-type: none"> <li>• Regular Smart Licensing—Perpetual</li> <li>• Specific License Reservation—Subscription</li> </ul>	<p>The platform license determines the number of devices the FMCv can manage.</p> <p>For details, see <a href="#">FMCv Licenses, on page 6</a>.</p>
Export-Controlled Features	No subscription required	Perpetual	<p>Features that are subject to national security, foreign policy, and anti-terrorism laws and regulations; see <a href="#">Licensing for Export-Controlled Functionality, on page 9</a>.</p>
Remote Access VPN: <ul style="list-style-type: none"> <li>• AnyConnect Apex</li> <li>• AnyConnect Plus</li> <li>• AnyConnect VPN Only</li> </ul>	Based on license type	Subscription or perpetual	<p>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 FTD can use any valid AnyConnect Client license. The available features do not differ based on license type.</p> <p>For more information, see <a href="#">AnyConnect Client Licenses, on page 8</a> and <i>VPN Licensing</i> in the <a href="#">Firepower Management Center Device Configuration Guide</a>.</p>



---

**Note** Subscription licenses are term-based licenses.

---

## FMCv Licenses

The FMCv requires a platform license that correlates with the number of devices it can manage.

The FMCv supports Smart Licensing.

In regular Smart Licensing, these licenses are perpetual.

In Specific License Reservation (SLR), these licenses are subscription-based.



---

**Note** For the add-on license requirements of your new devices on FMCv, it is recommended to migrate to a higher FMCv model that supports additional devices.

---

## Base Licenses

The Base 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 Threat license is enabled.

### Secure Firewall 3100

You obtain a Base license when you purchase the Secure Firewall 3100.

### Other Models

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

## Malware Licenses

A Malware license lets you perform AMP for Networks 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 (AMP) service subscription as a stand-alone subscription or in combination with Threat (TM) or Threat and URL Filtering (TMC) subscriptions. Threat license is a prerequisite for a Malware license.



**Note** Managed devices with Malware 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 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 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 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 license is required only if you deploy AMP for Networks and Secure Malware Analytics. Without a Malware license, the FMC can receive AMP for Endpoints 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 [Firepower 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 AMP for Networks configurations.
- 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.

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

## 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).

When you disable this license:

- The FMC 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 FMC 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 Threat.

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

## 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 Threat (TC) or Threat and Malware (TMC) subscriptions. Threat 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 FMC will not download URL information. You cannot deploy the access control policy until you first add a URL Filtering license to the FMC, then enable it on the devices targeted by the policy.

When you disable this license:

- You may lose access to URL filtering.
- Access control rules with URL conditions immediately stop filtering URLs.
- Your FMC 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 FMC moves to the out-of-compliance state.

## AnyConnect Client Licenses

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

To enable remote access VPN, you must purchase and enable one of the following licenses: AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only. You can select AnyConnect Plus and AnyConnect Apex if you have both licenses and you want to use them both. The AnyConnect VPN Only license cannot be used



with **Apex** or **Plus**. The AnyConnect 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 AnyConnect 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 FTD requires strong encryption (which is higher than DES) for successfully establishing remote access VPN connections with AnyConnect Clients.

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

- Smart Licensing on the FMC 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.

When approved by Cisco, you can manually add a strong encryption license to your account so you can use export-controlled features. For more information, see [Enable the Export Control Feature for Accounts Without Global Permission, on page 25](#)

- 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 FMC, then you must deregister and then re-register the FMC using a new Product Instance Registration Token with export-controlled functionality enabled.

If you registered devices to the FMC in evaluation mode or before you enabled strong encryption on the FMC, 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>.

## FTDv Licenses

This section describes the performance-tiered license entitlements available for the FTDv.

Any FTDv license can be used on any supported FTDv vCPU/memory configuration. This allows FTDv 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 FTDv VM, the maximum supported number of cores (vCPUs) is 16 ; and the maximum supported memory is 32 GB RAM .

### Performance Tiers for FTDv Smart Licensing

Session limits for RA VPNs are determined by the installed FTDv 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 3: FTDv 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

### FTDv Performance Tier Licensing Guidelines and Limitations

Please keep the following guidelines and limitations in mind when licensing your FTDv device.

- The FTDv supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements.
- Any FTDv license can be used on any supported FTDv core/memory configuration. This allows the FTDv customers to run on a wide variety of VM resource footprints.

- You can select a performance tier when you deploy the FTDv, 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 FTDv to Version 7.0, you can choose **FTDv - Variable** to maintain your current license compliance. Your FTDv 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 FTDv device, or when provisioning the FTDv using the REST API.
- Base licenses are subscription-based and mapped to performance tiers. Your virtual account needs to have the Base license entitlements for the FTDv devices, as well as for Threat, Malware, and URL Filtering licenses.
- Each HA peer consumes one entitlement, and the entitlements on each HA peer must match, including Base license.
- A change in performance tier for an HA pair should be applied to the primary peer.
- 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 **Find Products and Solutions** search field on the [Cisco Commerce Workspace](#). Search for the following license Product IDs (PIDs).

**Figure 1: License Search**

### FMCv PIDs

- VMware:
  - SF-FMC-VMW-2-K9—2 devices
  - SF-FMC-VMW-10-K9—10 devices
  - SF-FMC-VMW-K9—25 devices
  - SF-FMC-VMW-300-K9—300 devices
- KVM:

- SF-FMC-KVM-2-K9—2 devices
- SF-FMC-KVM-10-K9—10 devices
- SF-FMC-KVM-K9—25 devices
- PAK-based VMware:
  - FS-VMW-2-SW-K9—2 devices
  - FS-VMW-10-SW-K9—10 devices
  - FS-VMW-SW-K9—25 devices

### FTDv PIDs

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

- Base 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
- Threat, Malware, 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
- RA VPN—See the [Cisco Secure Client Ordering Guide](#).

### Firepower 1010 PIDs

- Threat, Malware, 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
- RA VPN—See the [Cisco Secure Client Ordering Guide](#).

### Firepower 1100 PIDs

- Threat, Malware, 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
- RA VPN—See the [Cisco Secure Client Ordering Guide](#).

### Firepower 2100 PIDs

- Threat, Malware, and URL license combination:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-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-FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y

- L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- RA VPN—See the [Cisco Secure Client Ordering Guide](#).

### Secure Firewall 3100 PIDs

- Base license:
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- Threat, Malware, 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-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
- RA VPN—See the [Cisco Secure Client Ordering Guide](#).

### Firepower 4100 PIDs

- Threat, Malware, and URL license combination:
  - L-FPR4110T-TMC=
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4120T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4140T-TMC=
  - L-FPR4145T-TMC=
  - L-FPR4150T-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-FPR4110T-TMC-1Y
- L-FPR4110T-TMC-3Y
- L-FPR4110T-TMC-5Y
- 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-FPR4120T-TMC-1Y
- L-FPR4120T-TMC-3Y
- L-FPR4120T-TMC-5Y
- L-FPR4125T-TMC-1Y

- L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4140T-TMC-1Y
  - L-FPR4140T-TMC-3Y
  - L-FPR4140T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y
  - L-FPR4150T-TMC-1Y
  - L-FPR4150T-TMC-3Y
  - L-FPR4150T-TMC-5Y
- RA VPN—See the [Cisco Secure Client Ordering Guide](#).

### Firepower 9300 PIDs

- Threat, Malware, and URL license combination:
  - L-FPR9K-24T-TMC=
  - L-FPR9K-36T-TMC=
  - L-FPR9K-40T-TMC=
  - L-FPR9K-44T-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-24T-TMC-1Y
- L-FPR9K-24T-TMC-3Y
- L-FPR9K-24T-TMC-5Y
- L-FPR9K-36T-TMC-1Y
- L-FPR9K-36T-TMC-3Y
- L-FPR9K-36T-TMC-5Y
- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y



- L-FPR9K-44T-TMC-1Y
  - L-FPR9K-44T-TMC-3Y
  - L-FPR9K-44T-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
- RA VPN—See the [Cisco AnyConnect Ordering Guide](#).

### ISA 3000 PIDs

- Threat, Malware, 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
- RA VPN—See the [Cisco AnyConnect Ordering Guide](#).

## Requirements and Prerequisites for Licensing

For Specific License Reservation requirements, see [Requirements and Prerequisites for Specific License Reservation, on page 33](#).

### General Prerequisites

- Make sure NTP is configured on the FMC 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 FMC.

### 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 High Availability (for device High Availability and also FMCv High Availability), clustering, and multi-instance deployments.

### Licensing for FMC High Availability

Each device requires the same licenses whether managed by a single FMC or by FMCs in a high availability pair (hardware or virtual).

**Example:** If you want to enable advanced malware protection for two devices managed by a FMC pair, buy two Malware licenses and two TM subscriptions, register the active FMC with the Smart Software Manager, then assign the licenses to the two devices on the active FMC.

Only the active FMC is registered with the Smart Software Manager. When failover occurs, the system communicates with Smart Software Manager to release the license entitlements from the originally-active FMC and assign them to the newly-active FMC.

In Specific License Reservation deployments, only the primary FMC requires a Specific License Reservation.

#### Hardware FMC

No special license is required for hardware FMCs in a high availability pair.

#### FMCv

You will need two identically licensed FMCvs.

**Example:** For the FMCv high availability pair managing 10 devices, you can use:

- Two (2) FMCv 10 entitlements
- 10 device licenses

If you break the high availability pair, the FMCv entitlements associated with the secondary FMCv are released. (In the example, you would then have two standalone FMCv 10s.)

### Licensing for Device High-Availability

Both FTD 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 FMC 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 Base license and a Threat license, and the standby unit has only a Base license, the FMC communicates with the Smart Software Manager to obtain an available Threat 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

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 FMC, 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 in the **Devices > Device Management > Cluster > License** area.



**Note** If you add the cluster before the FMC is licensed (and running in Evaluation mode), then when you license the FMC, 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.

## Licensing for Multi-Instance Deployments

All licenses are consumed per security engine/chassis (for the Firepower 4100) or per security module (for the Firepower 9300), and not per container instance. See the following details:

- Base licenses are automatically assigned: one per security module/engine.
- Feature licenses are manually assigned to each instance; but you only consume one license per feature per security module/engine. For example, for the Firepower 9300 with 3 security modules, you only need one URL Filtering license per module for a total of 3 licenses, regardless of the number of instances in use.

For example:

**Table 4: Sample License Usage for Container Instances on a Firepower 9300**

Firepower 9300	Instance	Licenses
Security Module 1	Instance 1	Base, URL Filtering, Malware
	Instance 2	Base, URL Filtering
	Instance 3	Base, URL Filtering
Security Module 2	Instance 4	Base, Threat
	Instance 5	Base, URL Filtering, Malware, Threat
Security Module 3	Instance 6	Base, Malware, Threat
	Instance 7	Base, Threat

**Table 5: Total Number of Licenses**

Base	URL Filtering	Malware	Threat
3	2	3	2

# 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.

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 Smart Software Manager.
- Go to <https://software.cisco.com/#module/SmartLicensing> and sign in.
- Step 5** 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 11](#).
- 

# Configure Smart Licensing

This section describes how to use Smart Licensing using the Smart Software Manager or the Smart Software Manager On-Prem. To use Specific License Reservation, see [Configure Specific License Reservation \(SLR\), on page 33](#).

## Register the FMC for Smart Licensing

You can register the FMC 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 FMC with the Smart Software Manager

Register the FMC 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 11](#).

- Ensure that the FMC can reach the Smart Software Manager at `tools.cisco.com:443`.
- 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 FMC.

- If your organization has multiple FMCs, make sure each FMC has a unique name that clearly identifies and distinguishes it from other FMCs 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**.



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

The screenshot shows a web interface with tabs for 'General', 'Licenses', 'Product Instances', and 'Event Log'. Under 'Product Instances', there is a section for 'Virtual Account' with fields for 'Description' and 'Default Virtual Account' (set to 'No'). Below this is the 'Product Instance Registration Tokens' section, which includes a 'New Token...' button circled in red. A table below the button lists existing tokens with columns for 'Token', 'Expiration Date', and 'Description'. One token is visible: 'NWU1MzY1MzEtZjNmOS00MjF..' with an expiration date of '2018-Jul-06 14:20:13 (in 354 days)' and a description of 'FTD-5506'.

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

The 'Create Registration Token' dialog box contains the following fields and options: 'Virtual Account' (pre-filled), 'Description' (empty text box), 'Expire After' (set to '30' days), and a checked checkbox for 'Allow export-controlled functionality on the products registered with this token'. A note below the checkbox states: 'Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.' At the bottom right, there are 'Create Token' and 'Cancel' buttons.

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

Figure 2: View Token

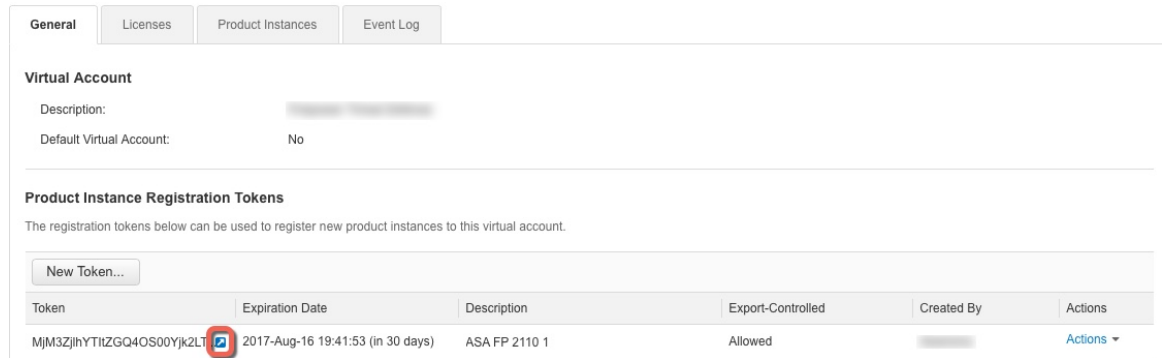
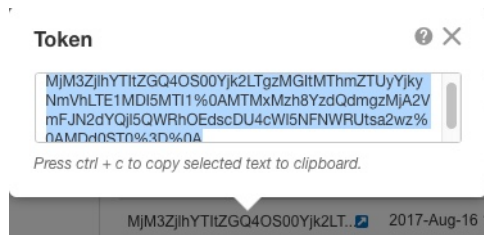


Figure 3: Copy Token



**Step 2** In the FMC, 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** 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. For more information, see [Configure Cisco Success Network Enrollment, on page 44](#).
- **Enable Cisco Support Diagnostics** is disabled by default. You can review the kind of data Cisco collects in the link provided above the check box. For more information, see [Configure Cisco Support Diagnostics Enrollment, on page 45](#).

- Note**
- When enabled, Cisco Support Diagnostics is enabled in the devices in the next sync cycle. The FMC sync with the device runs once every 30 minutes.
  - When enabled, Cisco Support Diagnostics is enabled automatically on any new device registered in this FMC.

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

**What to do next**

- Add a Device to the FMC; see *Add a Device to the FMC* in the [Firepower Management Center Device Configuration Guide](#).
- Assign licenses to your devices; see [Assign Licenses to Multiple Managed Devices](#), on page 27.

**Register the FMC with the Smart Software Manager On-Prem**

As described in [Periodic Communication with the Smart Software Manager](#), on page 3, the FMC 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 (formerly known as "Smart Software Satellite Server") as a proxy for connections to the Smart Software Manager:

- Your FMC 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 2.)
- Your FMC has permanent connectivity, but you want to manage your Smart Licenses via a single connection from your network.

The 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 the Smart Software Manager On-Prem, see <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem>

**Procedure****Step 1**

Deploy and set up Smart Software Manager On-Prem.

- See the documentation for the Smart Software Manager On-Prem, available from <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem>.
- Make a note of the CN of the TLS/SSL certificate on your Smart Software Manager On-Prem.
- 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.

**Step 2**

Register the FMC with the Smart Software Manager On-Prem.

- Choose **System** (⚙) > **Integration**.
- Click **Smart Software Satellite**.
- Select **Connect to Cisco Smart Software Satellite Server**.
- 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 Smart Software Manager On-Prem.



- e) Add a new **SSL Certificate** and paste the certificate text that you copied earlier.
- f) Click **Apply**.
- g) Select **System > Licenses > Smart Licenses** and click **Register**.
- h) Create a new token on Smart Software Manager On-Prem.
- i) Copy the token.
- j) Paste the token into the form on the management center page.
- k) Click **Apply Changes**.

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

**Step 3** After you assign licenses to devices, synchronize Smart Software Manager On-Prem to the Smart Software Manager.

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

**Step 4** Schedule ongoing synchronization times.

## Enable the Export Control Feature for Accounts Without Global Permission

If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

### Before you begin

- Make sure that your deployment does **not** already support the export-controlled functionality.  
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 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 the [Smart Software Manager](#), on the **Inventory > Licenses** page, verify that you have the license that corresponds to your FMC:

Export Control License	FMC Model
Cisco Virtual FMC Series Strong Encryption (3DES/AES)	All FMCvs
Cisco FMC 1K Series Strong Encryption (3DES/AES)	1000, 1600
Cisco FMC 2K Series Strong Encryption (3DES/AES)	2500, 2600
Cisco FMC 4K Series Strong Encryption (3DES/AES)	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.

Disable the export control license by clicking **Return Export Key**

---

## 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 FTD 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 FTD devices need to be rebooted simultaneously, to avoid an Active-Active condition.

---

## Assign Licenses to Devices

You can assign most licenses when you register a device to the FMC. 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 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

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

### Procedure

---

- Step 1** Choose **Devices > Device Management**.
  - Step 2** Next to the device where you want to assign or disable a license, click **Edit** (✎).  
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
  - Step 3** Click **Device**.
  - Step 4** Next to the **License** section, click **Edit** (✎).
  - Step 5** Check or clear the appropriate check boxes to assign or disable licenses for the device.
  - Step 6** Click **Save**.
  - Step 7** Deploy configuration changes; see the [Firepower Management Center Device Configuration Guide](#).
- 

### 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 FMC obtain their licenses via the FMC, 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 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.

---

### 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**.
- 

#### What to do next

Verify that your licenses are correctly installed. Follow the procedure in [Monitoring Smart Licenses, on page 29](#).

## Manage Smart Licensing

This section describes how to manage Smart Licensing.

### Deregister the FMC

Deregister your FMC 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 FMC 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** (  ).


---

### Synchronize or Reauthorize the FMC

By default, the ID certificate is automatically renewed every 6 months, and the license entitlement is renewed every 30 days. You might want to manually renew the registration for either of these items if you have a limited window for internet access, or if you make any licensing changes in the Smart Software Manager, for example.

#### Procedure

---

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

- Step 2** To renew the ID certificate, click **Synchronize** (🔄).
- Step 3** To renew the license entitlements, click **Re-Authorize**.

---

## Monitoring Smart License Status

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

### Usage Authorization

Possible status values are:

- **In-compliance** (🟢) — All licenses assigned to managed devices are in compliance and the FMC 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 FMC 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 FMC has not communicated with the Smart Software Manager in more than 90 days.

### Product Registration

Specifies the last date when the FMC 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 FMC. If this deployment is not associated with a particular virtual account within your Smart Account, this information is not displayed.

### Export-Controlled Features

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

### Cisco Success Network

Specifies whether you have enabled Cisco Success Network for the FMC. 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 [Configure Cisco Success Network Enrollment, on page 44](#) for more information.

## Monitoring Smart Licenses

To view the license status for the FMC 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 FMC'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 FMCv 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.

## 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 FMC 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 the FMC, on page 28](#).

### 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>

## Convert a Classic License for Use on the FTD

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



---

**Note** 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 FTD. 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 and Add Licenses, on page 20](#).
- 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 Smart Software Manager, you must have your Smart Account credentials in order to initiate the conversion process.

### Procedure

---

**Step 1** The conversion process you 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 License Registration Portal:
    - 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/mds3ab3fctk6pzonq5meukvcpjzt7wu>.

There are three conversion procedures. Choose the conversion procedure applicable to your situation.
  - Sign in to the License Registration Portal at <https://tools.cisco.com/SWIFT/LicensingUI/Home> and follow the instructions in the documentation above.
  - To convert PAKs or licenses using the Smart Software Manager:
    - *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 the Smart Software Manager 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 FTD 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 the FDM to manage this device as a standalone device:
- See information about licensing the device in the FDM configuration guide 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 FMC:
- a) Set up Smart Licensing on your new FTD.  
See [Assign Licenses to Multiple Managed Devices, on page 27](#).
  - b) Verify that the new Smart License has been successfully applied to the device.  
See [Monitoring Smart Licenses, on page 29](#).
- Step 6** If you have not yet deployed Smart Licensing on your FMC:
- See [Configure Smart Licensing, on page 20](#). (Skip any steps that do not apply or that you have already completed.)
-



# Configure 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 FMC reserves licenses from your virtual account for a specified duration without accessing the Smart Software Manager or using Smart Software Manager On-Prem.

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.

## Requirements and Prerequisites for Specific License Reservation

- If you are currently using regular Smart Licensing, de-register the FMC before you implement Specific License Reservation. For information, see [Deregister the FMC, on page 28](#).

All Smart Licenses that are currently deployed to the FMC 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 uses the same licenses as regular Smart Licensing.
- (Recommended) If you deploy the FMC pair in a high availability configuration, configure high availability before you assign licenses. If you already assigned licenses to devices on the secondary FMC, be sure to unassign them.

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

To prevent problems when deploying your Specific License Reservation, complete this procedure before you make any changes in your FMC.

### Before you begin

- Ensure that you have met the requirements described in [Requirements and Prerequisites for Specific License Reservation, on page 33](#).
- Make sure you have your Smart Software Manager credentials.

### Procedure

---

- Step 1** Sign in to the 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 FMCv 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.
- Note** 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 the FMC.

### Procedure

- Step 1** Access the FMC console using a USB keyboard and VGA monitor, or use SSH to access the management interface.
- Step 2** Log into the FMC CLI **admin** account.
- Step 3** 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** Enter **exit** to exit the command line interface.

- Step 9** Verify that you can access the **Specific License Reservation** page in the FMC web interface:
- If the **System > Licenses > Smart Licenses** page is currently displayed, refresh the page.
  - Otherwise, choose **System > Licenses > Specific Licenses**.
- 

## Enter the Specific License Reservation Authorization Code into the FMC

### Procedure

---

- Step 1** Generate the reservation request code.
- a) In the FMC, choose **System > Licenses > Specific Licenses**.
  - b) Click **Generate**.
  - c) Make a note of the **Reservation Request Code**.
- Step 2** Generate the reservation authorization code.
- a) Go to the Cisco Smart Software Manager: <https://software.cisco.com/#SmartLicensing-Inventory>
  - b) If necessary, select the correct account from the top right of the page.
  - c) If necessary, click **Inventory**.
  - d) Click **Licenses**.
  - e) Click **License Reservation**.
  - f) Enter the code that you generated from FMC into the **Reservation Request Code** box.
  - g) Click **Next**.
  - h) Select **Reserve a specific license**.
  - i) Scroll down to display the entire License grid.
  - j) Under **Quantity To Reserve**, enter the number of each platform and feature license needed for your deployment.
- Note**
- You must explicitly include a Base license for each managed device, or, for multi-instance deployments, for each container.
  - If you are using the FMCv, you must include a platform entitlement for each container (in multi-instance deployments) or each managed device (all other deployments).
  - If you use strong encryption 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-FMC, you must select the appropriate license.
- For the correct license name to choose for your FMC, see the prerequisites in [Enable the Export Control Feature for Accounts Without Global Permission, on page 25](#).
- k) Click **Next**.
  - l) Click **Generate Authorization Code**.

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

m) Download the Authorization Code in preparation for entering it into the FMC.

**Step 3**

Enter the authorization code in the FMC.

- a) In the FMC, click **Browse** to upload the text file with the authorization code that you generated from the Smart Software Manager.
- b) Click **Install**.
- c) Verify that the **Specific License Reservation** page shows the **Usage Authorization** status as authorized.
- d)

**Step 4**

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 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.
- Step 6** Deploy configuration changes; see the [Firepower Management Center Device Configuration Guide](#).

## Manage Specific License Reservation

This section describes how to manage Specific License Reservation.

### Important! Maintain Your Specific License Reservation 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). If any of the licenses expire, the FMC will be in the Out of Compliance state if the usage count is greater than the available count.

## Update a Specific License Reservation

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

Use this procedure if you need to renew your licenses after they expire. If you do not have the required licenses, the following actions are restricted:

- Device registration
- Policy deployment

### Procedure

---

- Step 1** In the FMC, obtain the unique product instance identifier of this FMC:
- 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 the Smart Software Manager, identify the FMC to update:
- a) Go to the Smart Software Manager:  
<https://software.cisco.com/#SmartLicensing-Inventory>
  - b) If necessary, click **Inventory**.
  - 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 FMC is the correct FMC. Click the name.
  - e) Look at the **UUID** and see if it is the UUID of the FMC that you are trying to modify.
- If not, you must repeat these steps until you find the correct FMC.
- Step 3** When you have located the correct FMC in the 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.

**Note**

- You must explicitly include a Base license for each managed device, or, for multi-instance deployments, for each container.
- If you are using the FMCv, you must include a platform entitlement for each container (in multi-instance deployments) or each managed device (all other deployments).
- If you use strong encryption 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-FMC, you must select the appropriate license.

For the correct license name to choose for your FMC, see the prerequisites in [Enable the Export Control Feature for Accounts Without Global Permission](#), on page 25.

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

**Step 4**

Update the Specific Licenses in the FMC.

- 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 FMC, matches with the licenses that you have reserved in the Smart Software Manager.

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

**Step 5**

Enter the confirmation code in the Smart Software Manager:

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

UDI\_PID:FS-VMW-SW-K9; UDI\_SN:3;

Overview Event Log

**Description**  
Firepower Threat Defense

**General**

Name: UDI\_PID:FS-VMW-SW-K9; UDI\_SN:3;  
 Product: Firepower Threat Defense  
 Host Identifier: -  
 MAC Address: -  
 PID: FS-VMW-SW-K9  
 Serial Number: 3  
 UUID: 8c048120-c048-11e8-ba04-0421c0eb6149  
 Virtual Account: FTD-ENG-AST  
 Registration Date: 2018-Oct-11 17:03:24  
 Last Contact: 2018-Oct-16 09:47:49 (Reserved Licenses) - Download Reservation Authorization Code

**License Usage** These licenses are reserved on this product instance [Update reservation](#)

License	Billing	Expires	Required
Threat Defense Virtual URL Filtering	Prepaid	2018-Dec-08	1
Threat Defense Virtual URL Filtering	Prepaid	2018-Dec-04	10
Threat Defense Virtual URL Filtering	Prepaid	-	11

Showing all 8 Rows

Transfer...  
 Update Reserved Licenses...  
**Enter Confirmation Code...**  
 Remove...  
 Actions

c) Enter the confirmation code that you generated from the FMC.

**Step 6** In the FMC, 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 [Monitoring Specific License Reservation Status, on page 41](#) for more information.

**Step 7** Deploy configuration changes; see the [Firepower Management Center Device Configuration Guide](#).

## Deactivate and Return the Specific License Reservation

If you no longer need a specific license, you must return it to your Smart Account. If you want to register your Smart Licensing account, you must disable the Specific License Reservation (Step 6 of the procedure below).



**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 FMC back to your virtual account. After you de-register, no updates or changes on licensed features are allowed.

## Procedure

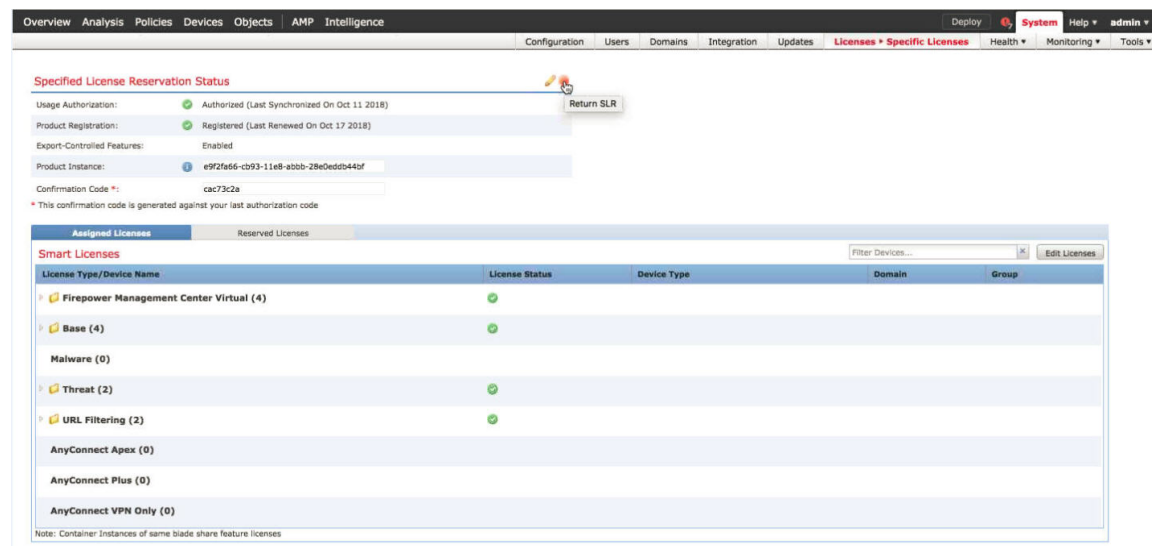
**Step 1** In the FMC Web interface, select **System > Licenses > Specific Licenses**.

**Step 2** Make a note of the **Product Instance** identifier for this FMC.

**Step 3** Generate a return code from the FMC.

a) Click **Return SLR**.

The following figure shows Return SLR.



Devices become unlicensed and the FMC moves to the de-registered state.

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

**Step 4** In the Smart Software Manager, identify the FMC to deregister:

a) Go to the Smart Software Manager:

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

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

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 FMC is the correct FMC. Click the name.

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

If not, you must repeat these steps until you find the correct FMC.

**Step 5** When you have identified the correct FMC, 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 FMC 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 FMC is removed from the Smart Software Manager Product Instances list.

**Step 6** Disable the Specific License in the FMC Linux shell:

- a) Access the FMC console using a USB keyboard and VGA monitor, or use SSH to access the management interface.
- b) Log in to the FMC CLI **admin** account. This gives you access to the command line interface.
- c) Enter the **expert** command to access the Linux shell.
- 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) Enter **exit** to exit the command line interface.

## Monitoring Specific License Reservation Status

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

### Usage Authorization

Possible status values are:

- **Authorized** — The FMC 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 FMC 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 FMC.

### Export-Controlled Features

Specifies whether you have enabled export-controlled functionality for the FMC.

For more information about Export-Controlled Features, see [Licensing for Export-Controlled Functionality, on page 9](#).

### Product Instance

The Universally Unique Identifier (UUID) of this FMC. This value identifies this device in the 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.

## Troubleshoot Specific License Reservation

### How do I identify a particular FMC in the Product Instance list in Smart Software Manager?

On the Product Instances page in 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 FMC.

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

### I do not see a License Reservation button in the 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 FMC web interface, cancel the request code.
2. Disable Specific License Reservation in the FMC Linux shell as described within the section [Deactivate and Return the Specific License Reservation, on page 39](#).
3. Register the FMC with the 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 the Smart Software Manager, you can go to the **Product Instance** page in the Smart Software Manager, click the product instance, then click **Download Reservation Authorization Code**.

**I am unable to register devices to the FMCv**

Make sure you have enough FMCv 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 37](#).

**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 39](#).

**What if I do not see a Specific License page in the FMCv?**

You need to enable Specific License to view the Specific License page. For more information see, [Enable the Specific Licensing Menu Option, on page 34](#).

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

The **Return Code** is saved in the FMCv. You must re-enable the Specific License from the Linux shell (see [Enable the Specific Licensing Menu Option, on page 34](#)), then refresh the FMCv web interface. Your **Return Code** will be displayed.

## Configure Legacy FMC PAK-Based Licenses

The FMC 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.

**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 FMC 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 FMC; 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 FMC.

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 '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**.

---

## Configure Cisco Success Network Enrollment

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the FMC and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism to select data of interest from the FMC 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 FMC establishes and maintains the secure connection between the FMC and the Cisco cloud at all times, after you have enabled either Cisco Support Diagnostics or Cisco Success Network. You can turn off this

connection at any time by disabling both Cisco Success Network and Cisco Support Diagnostics, which disconnects FMC from the Cisco cloud. However, when Cisco Support Diagnostics is enabled, a secure connection is established and maintained between the FTD and the Cisco cloud along with the FMC and Cisco cloud. Therefore, when the Cisco Support Diagnostics is disabled, both these secure connections are turned off.

You enable Cisco Success Network when you register the FMC with the Smart Software Manager. See [Register the FMC with the Smart Software Manager, on page 21](#). After that, use the following procedure to view or change enrollment status.



---

**Note** Cisco Success Network does not work in evaluation mode.

---



---

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

---

### 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 [Web Analytics](#).

## Configure Cisco Support Diagnostics Enrollment

Cisco Support Diagnostics is a user-enabled cloud-based TAC support service. When enabled, a secure connection is established between the FMC, and FTD on one side and the Cisco cloud on the other side, to stream system health related information.

Cisco Support Diagnostics provides an enhanced user experience during troubleshooting by allowing Cisco TAC to securely collect essential data from your device during a TAC case. Moreover, operational health data is periodically collected and processed through Cisco's automated problem detection system to proactively notify you of any issues. While the data collection service during a TAC case is available for all users with support contracts, the proactive notification service is only available to users with specific service contracts.

The FMC establishes and maintains the secure connection between the FMC and the Cisco cloud at all times, after you have enabled either Cisco Support Diagnostics or Cisco Success Network. You can turn off this connection at any time by disabling both Cisco Success Network and Cisco Support Diagnostics, which disconnects these features from the Cisco cloud. However, when Cisco Support Diagnostics is enabled, a secure connection is established and maintained between the FTD and the Cisco cloud along with the FMC

and Cisco cloud. Therefore, when the Cisco Support Diagnostics is disabled both these secure connections are turned off.

Administrators can view a sample data set which is collected from the FMC by following the steps in [Producing Troubleshooting Files for Specific System Functions](#) to generate a troubleshooting file, and then by opening the file to view it.

The FMC sends the collected data to the regional cloud specified on the **System > Integration > Cloud Services** page. Note that this setting is also used for Cisco Support Network, described at [Configure Cisco Success Network Enrollment, on page 44](#), and the Cisco Threat Response integration described at [Event Analysis with Cisco Threat Response](#).

You enable Cisco Support Diagnostics when you register the FMC with the Smart Software Manager. After that, use the following procedure to view or change enrollment status.

### Procedure

- 
- Step 1** Click **System > Licenses > Smart Licenses**.
- Step 2** Under Smart License Status, next to Cisco Support Diagnostics, click **Enabled/Disabled** control to change the setting as appropriate.
- Note** Read the information provided next to the **Enabled/Disabled** control before you proceed.
- Step 3** Click **Apply Changes**.
- 

### What to do next

If you have enabled Cisco Support Diagnostics, verify the regional cloud setting at **System > Integration > Cloud Services > Cisco Cloud Region** to establish where the system data is sent.

## Additional Information about Licensing

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

- FAQ—<https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html>
- License Roadmap—<https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html>

## History for Licenses

Feature	Version	Details
Performance tier licensing for the FTDv	7.0	Performance-tiered licensing provides different throughput levels and VPN connection limits based on deployment requirements. License tiers map to new FTDv models.

Feature	Version	Details
Cisco Support Diagnostics on additional FTD platforms	6.6	<p>Cisco Support Diagnostics is now fully supported on all FMCs and FTD devices. Previously, support was limited to FMCs, Firepower 4100/9300 with FTD, and FTDv for Azure.</p> <p>Supported platforms: FMC, FTD</p>
Cisco Support Diagnostics	6.5	<p><i>Cisco Support Diagnostics</i> (sometimes called <i>Cisco Proactive Support</i>) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.</p> <p>During upgrades and reimages, you may be asked to enroll. You can also change your enrollment at any time.</p> <p>In Version 6.5.0, Cisco Support Diagnostics support is limited to select platforms.</p> <p>New/Modified screens: <b>System &gt; Licenses &gt; Smart Licenses</b></p> <p>Supported platforms: FMC, Firepower 4100/9300, FTDv for Azure</p>
Enabling Cisco Success Network allows SecureX to display appliance and device status information	6.4	<p>For general information about the SecureX integration, see <a href="#">Integrate with Cisco SecureX</a> and the information linked from that topic.</p>
Licensing for multi-instance capability for the FTD on the Firepower 4100/9300	6.3	<p>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.</p> <p>New/Modified screens: <b>System &gt; Licenses &gt; Smart Licenses</b></p> <p>Supported platforms: FTD on the Firepower 4100/9300</p>
Specific License Reservation for air-gapped deployments	6.3	<p>Customers whose deployments cannot connect to the internet to communicate with the Cisco License Authority can use a Specific License Reservation.</p> <p>New/Modified screens: <b>System &gt; Licenses &gt; Specific Licenses</b> (This option is not available by default.)</p> <p>Supported platforms: FMC, FTD</p>
Export-controlled functionality for restricted customers	6.3	<p>Certain customers whose Smart Accounts are not otherwise eligible to use restricted functionality can purchase term-based licenses, with approval.</p> <p>Supported platforms: FMC, FTD</p>

