

Licenses

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

- Licenses, on page 1
- Prerequisites for licensing, on page 14
- Create a Cisco account, on page 17
- Create a smart account and add licenses, on page 18
- Configure Smart Licensing, on page 20
- Specific License Reservation, on page 31
- Additional information about licensing, on page 42
- History for licenses, on page 42

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**: Cisco License Central 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 License Central.

For a more detailed overview on Cisco Licensing, visit the Licensing Hub.

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. For instructions, refer to Create a Cisco Account.

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

You manage licenses by virtual account. Only that virtual account's devices can use the licenses assigned to the account. If you need additional licenses, you can transfer an unused license from another virtual account. You can also transfer devices between virtual accounts.

Licensing options for air-gapped deployments

This 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, refer to Register the Firewall Management Center with the Smart Software Manager On-Prem, on page 23	For more information, refer to Specific License Reservation, on page 31

Licensing for Management Center and devices

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

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

Periodic communications with the Smart Software Manager

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

The Firewall Management Center communicates with the Smart Software Manager on a periodic basis. If you make changes in the Smart Software Manager, you can refresh the authorization on the Firewall Management

Center so the changes immediately take effect. You also can wait for the Firewall Management Center to communicate as scheduled. Your Firewall Management Center must either have direct internet access to the Smart Software Manager, 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. With the grace period, your Firewall Management Center will operate for up to 90 days without contacting the Smart Software Manager. Ensure that the Firewall Management Center contacts the Smart Software Manager within 90 days, or the Firewall Management Center will revert to an unregistered state.

If your device is unable to communicate due to network issues, it continues working for up to 90 days. Once communication resumes and the ID certificate is validated, license entitlement is restored.

Evaluation mode

Evaluation mode is a temporary license that

- operates for 90 days before the Firewall Management Center registers with the Smart Software Manager,
- allows you to assign feature licenses to managed devices while they remain in compliance for the duration of evaluation mode, and
- ends when the Firewall Management Center becomes unregistered after the 90-day period expires.

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

For more information about the unregistered state, refer to 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.



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

Out-of-compliance state

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

- Over-utilization—When the managed devices or the Firewall Management Center Virtual uses unavailable licenses.

Note Even if one license is unavailable for a device, the Firewall Management Center will be in the **Out-of-Compliance** state. Deployment of all configurations will work. For example, you have two Malware licenses and three managed devices. All three devices will be in the **Out-of-Compliance** state, and Malware feature will not work. This behavior is applicable for all licenses.

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

In an out-of-compliance state, these effects occur:

- Firewall Management Center Virtual platform license—Operation is not affected.
- All managed device licenses—Operation is not affected.

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

Unregistered state

The Firewall Management Center can become unregistered in these situations:

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

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

End-user license agreement

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

License types and restrictions

This section describes the types of licenses available for Secure Firewall.

Table 2: Smart Licenses

License You Assign	Duration	Granted Capabilities
Essentials	Perpetual or Subscription **Note** Essentials subscription licenses are supported only on Firewall Threat Defense Virtual .	Except for Specific License Reservation and the Secure Firewall 1200/ 3100 /4200 , Essentials perpetual licenses are automatically assigned with all Firewall Threat Defense s. User and application control Switching and routing NAT For details, see Essentials licenses, on page 6 .
IPS	Subscription	Intrusion detection and prevention File control Security Intelligence filtering For details, see IPS licenses, on page 8
Malware defense	Subscription	Malware defense Secure Malware Analytics File storage (IPS license is a prerequisite for a Malware defense license.) For details, see Malware Defense Licenses, on page 7 and *License Requirements for File and Malware Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide* .
Carrier	Subscription for Firepower 4100/9300, Secure Firewall 3100 /4200 , and Firewall Threat Defense Virtual	Diameter, GTP/GPRS, M3UA, and SCTP inspection For details, see Carrier license, on page 9 .
URL Filtering	Subscription	Category and reputation-based URL filtering For details, see URL Filtering licenses, on page 10 . (IPS license is a prerequisite for a URL Filtering license.)
Firewall Management Center Virtual	• Regular Smart Licensing—Perpetual • Specific License Reservation—Subscription	The platform license determines the number of devices the Firewall Management Center Virtual can manage. For details, see Firewall Management Center Virtual licenses, on page 6 .

License You Assign	Duration	Granted Capabilities
Export-Controlled Features	Perpetual	Features that are subject to national security, foreign policy, and anti-terrorism laws and regulations; see License for export-controlled functionality, on page 11 .
Remote Access VPN: • Secure Client Premier • Secure Client Advantage • Secure Client VPN Only	Subscription or perpetual	Remote access VPN configuration. Your account must allow export-controlled functionality to configure remote access VPN. You select whether you meet export requirements when you register the device. The Firewall Threat Defense can use any valid Secure Client license. The available features do not differ based on license type. For more information, see Secure Client licenses, on page 10 and *VPN Licensing* in the *Cisco Secure Firewall Management Center Device Configuration Guide* .

Note Subscription licenses are term-based licenses.

Firewall Management Center Virtual licenses

The Firewall Management Center Virtual requires a platform license that correlates with the number of devices it can manage.

The Firewall Management Center Virtual supports Smart Licensing.

In regular Smart Licensing, these licenses are perpetual.

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

Starting from Firewall Management Center version 7.3, in regular Smart Licensing and Specific License Reservation, the licenses can be perpetual or subscription licenses. The subscription term can be 3,5, or 10 years. Select the type of license based on your requirement. By default, subscription licenses are selected.

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

Essentials licenses

The Essentials license allows you to configure and manage firewall devices with essential networking and security capabilities, including switching, routing, high availability, clustering, user control, application control, and database updates.

The Essentials license allows you to:

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

Secure Firewall 1200/3100/4200

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

Other Models

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

Malware Defense Licenses

A Malware defense license lets you perform Malware Defense and Secure Malware Analytics. With this feature, you can use devices to detect and block malware in files transmitted over your network.

To support this feature license, you can purchase the Malware defense (AMP) service subscription as a stand-alone subscription or in combination with IPS (TM) or IPS and URL Filtering (TMC) subscriptions. IPS license is a prerequisite for a Malware defense license.



Note Managed devices with Malware defense licenses enabled periodically attempt to connect to the Secure Malware Analytics Cloud even if you have not configured dynamic analysis. Because of this, the device's Interface Traffic dashboard widget shows transmitted traffic; this is expected behavior.

You configure Malware Defense as part of a file policy, which you then associate with one or more access control rules. File policies can detect your users uploading or downloading files of specific types over specific application protocols. Malware Defense allows you to use local malware analysis and file preclassification to inspect a restricted set of those file types for malware. You can also download and submit specific file types to the Secure Malware Analytics Cloud for dynamic and Spero analysis to determine whether they contain malware. For these files, you can view the network file trajectory, which details the path the file has taken through your network. The Malware Defense license also allows you to add specific files to a file list and enable the file list within a file policy, allowing those files to be automatically allowed or blocked on detection.

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

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

When you disable this license:

- The system stops querying the Secure Malware Analytics Cloud, and also stops acknowledging retrospective events sent from the Secure Malware Analytics Cloud.
- You cannot re-deploy existing access control policies if they include Malware Defense configurations.
- For a very brief time after a Malware defense license is disabled, the system can use existing cached file dispositions. After the time window expires, the system assigns a disposition of **Unavailable** to those files.

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

IPS licenses

A IPS license allows you to perform intrusion detection and prevention, file control, and Security Intelligence filtering.

License capabilities

- *Intrusion detection and prevention* allows you to analyze network traffic for intrusions and exploits and, optionally, drop offending packets.
- *File control* allows you to detect and, optionally, block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. *Malware defense*, which requires a Malware defense license, allows you to inspect and block a restricted set of those file types based on their dispositions.
- *Security Intelligence filtering* allows you to block —deny traffic to and from—specific IP addresses, URLs, and DNS domain names, before the traffic is subjected to analysis by access control rules. Dynamic feeds allow you to immediately block connections based on the latest intelligence. Optionally, you can use a "monitor-only" setting for Security Intelligence filtering.

License purchase options

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

Disabled license behavior

When you disable this license:

- The Firewall Management Center stops acknowledging intrusion and file events from the affected devices. As a consequence, correlation rules that use those events as a trigger criteria stop firing.
- The Firewall Management Center does not contact the internet for either Cisco-provided or third-party Security Intelligence information.
- You cannot re-deploy existing intrusion policies until you re-enable IPS.

Expired license behavior

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

Carrier license

The Carrier license enables the inspection of specific protocols used in next-generation mobile and telecom networks. This license supports protocol inspection for Diameter, GTP/GPRS, M3UA, and SCTP protocols across supported devices.

Enabled protocols

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



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

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

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

Supported devices

- Cisco Secure Firewall 3100 Series
  - Secure Firewall 3110
  - Secure Firewall 3120
  - Secure Firewall 3130
  - Secure Firewall 3140
- Cisco Secure Firewall 4100 Series
  - Firepower 4112
  - Firepower 4115
  - Firepower 4125

- Firepower 4145

- Cisco Secure Firewall 4200 Series
  - Secure Firewall 4215
  - Secure Firewall 4225
  - Secure Firewall 4245
- Firepower 9300
- Firewall Threat Defense Virtual

URL Filtering licenses

The URL Filtering license allows you to write access control rules that determine the traffic that can traverse your network based on URLs requested by monitored hosts, correlated with information about those URLs. To support this feature license, you can purchase the URL Filtering service subscription as a stand-alone subscription or in combination with IPS (TC) or Threat and Malware defense (TMC) subscriptions. IPS license is a prerequisite for this license.



Tip Without a URL Filtering license, you can specify individual URLs or groups of URLs to allow or block. This option gives you granular, custom control over web traffic, but does not allow you to use URL category and reputation data to filter network traffic.

Although you can add category and reputation-based URL conditions to access control rules without a URL Filtering license, the Firewall Management Center will not download URL information. You cannot deploy the access control policy until you first add a URL Filtering license to the Firewall Management Center, then enable it on the devices targeted by the policy.

When you disable this license:

- You may lose access to filtering network traffic based on the URL category and reputation ACP rules. The manual URL filtering options will continue to be supported.
- Access control rules with URL conditions immediately stop filtering URLs.
- Your Firewall Management Center can no longer download updates to URL data.
- You cannot re-deploy existing access control policies if they include rules with category and reputation-based URL conditions.

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

Secure Client licenses

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

To enable remote access VPN, you must purchase and enable one of these licenses: Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only. You can select Secure Client Advantage and Secure Client Premier if you have both licenses and you want to use them both. The Secure Client VPN Onlylicense cannot

be used with **Apex** or **Plus**. The Secure Client license must be shared with the Smart Account. For more instructions, refer to http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

You cannot deploy the remote access VPN configuration to the device if the specified device does not have the entitlement for a minimum of one of the specified Secure Client license types. If the registered license moves out of compliance or entitlements expire, the system displays licensing alerts and health events.

While using remote access VPN, your Smart Account must have the export controlled features (strong encryption) enabled. The Firewall Threat Defense requires strong encryption (which is higher than DES) for successfully establishing remote access VPN connections with Secure Clients.

You cannot deploy remote access VPN if these conditions are true:

- Smart Licensing on the Firewall Management Center is running in evaluation mode.
- Your Smart Account is not configured to use export-controlled features (strong encryption).

License for export-controlled functionality

This topic provides information about software features that are subject to export control laws and regulations, and describes how to determine and enable export-controlled functionality for your system.

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
- SD-WAN VPN
- SSH platform policy with strong encryption
- SSL policy with strong encryption
- Functionality such as SNMPv3 with strong encryption

Verify export-controlled functionality in your system

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

Enable 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 24

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

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

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

The entitlement is perpetual and does not require a subscription.

More information

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

Firewall Threat Defense Virtual Licenses

Learn about the performance-tiered license entitlements for Firewall Threat Defense Virtual, including supported vCPU and memory configurations, compatible VM resource footprints, and RA VPN session limits by entitlement tier.

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

Performance Tiers for Firewall Threat Defense Virtual Smart Licensing

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

Table 3: Firewall Threat Defense Virtual Licensed Feature Limits Based on Entitlement

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250
FTDv20, 3Gbps	4 core/8 GB	3Gbps	250
FTDv30, 5Gbps	8 core/16 GB	5Gbps	250

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv50, 10Gbps	12 core/24 GB	10Gbps	750
FTDv100, 16Gbps	16 core/32 GB	16Gbps	10,000

Firewall Threat Defense Virtual Performance Tier Licensing Guidelines and Limitations

Review and follow these guidelines and limitations when licensing your Firewall Threat Defense Virtual device.

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



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

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

Edit performance tier of Firewall Threat Defense Virtual

The Firewall Threat Defense Virtual supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements. You can edit the performance tier using this procedure.

Before you begin

Ensure that you review Firewall Threat Defense Virtual Performance Tier Licensing Guidelines and Limitations , on page 13.

Procedure

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

Step 2 Click **Edit Performance Tier**.

Step 3 Choose a tier from the **Target Performance Tier** drop-down list.

Step 4 From the **Available Devices** list, select the required devices and click **Add**.

Step 5 Click **Apply**.

Prerequisites for licensing

This topic lists the prerequisites, supported domains, and user roles required for licensing.

General prerequisites

- Make sure NTP is configured on the Firewall Management Center and managed devices. Time must be synchronized for registration to succeed.
- For a Firepower 4100/9300, you must configure NTP on the chassis using the same NTP server for the chassis as for the Firewall Management Center.

  For Specific License Reservation requirements, see Prerequisites for Specific License Reservation, on page 31.

Supported domains

Global, except where indicated.

User roles

Admin

Prerequisites for licensing in high availability, clustering, and multi-instance

This section describes the licensing requirements for High Availability (for device High Availability and also Firewall Management Center Virtual High Availability), clustering, and multi-instance deployments.

Licensing for Firewall Management Center high availability

Ensure proper licensing is configured before implementing Firewall Management Center high availability.

License assignment examples for high availability configurations

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

Hardware management center license requirements

No special license is required for hardware Firewall Management Centers in a high availability pair.

Virtual management center license requirements

You need two identically licensed Firewall Management Center Virtuals. Firewall Management Center Virtual requires an individual license for each device it manages.

Each registered device in a Firewall Management Center Virtual high availability pair must have its own license. Although only the active FMC registers with Smart Software Manager at any time, entitlement usage accounts for both Firewall Management Center Virtuals in the high availability pair.

Entitlement calculation for Firewall Management Center Virtual high availability pairs is as follows:

Firewall Management Center Virtual entitlement = Number of Firewall Management Center Virtual peers in the high availability pair x Number of managed devices

In Specific License Reservation deployments, only the primary Firewall Management Center requires a Specific License Reservation.

Example: For the Firewall Management Center Virtual high availability pair managing 2 devices, you can use:

- Two (2) Firewall Management Center Virtual entitlements
- 2 device licenses

Note Firepower MCv Device Licenses seen on Smart Software Manager is 4

Example: For two Firewall Management Center Virtual high availability pair managing 2 devices each, you can use:

- Four (4) Firewall Management Center Virtual entitlements
- 4 device licenses

Note Firepower MCv Device Licenses seen on Smart Software Manager is 8

If you break the high availability pair, the Firewall Management Center Virtual entitlements associated with the secondary Firewall Management Center Virtual are released. (In the example, you would then have two standalone Firewall Management Center Virtual devices.)

License requirements for Firewall Threat Defense device high availability

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

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

Before high availability is established, it does not matter which licenses are assigned to the secondary/standby device. During high availability configuration, the Firewall Management Center releases any unnecessary licenses assigned to the standby unit and replaces them with identical licenses assigned to the primary/active unit.

For example, if the active unit has a Essentials license and a IPS license, and the standby unit has only a Essentials license, the Firewall Management Center communicates with the Smart Software Manager to obtain an available IPS license from your account for the standby unit. If your license account does not include enough purchased entitlements, your account becomes Out-of-Compliance until you purchase the correct number of licenses.

License for device clusters

Device clusters require specific licensing considerations for proper operation and feature functionality.

Performance tier license requirements

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

Feature license assignment

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

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

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

Note APEX, PLUS, and VPN-Only licenses are not supported for clustering. Before you create a cluster, remove unsupported license assignments from the devices that will become cluster nodes.

Licensing for multi-instance deployments

This topic provides licensing information specific to multi-instance deployments where multiple container instances require appropriate license allocation and management.

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 details:

- Essentials 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	Essentials, URL Filtering, Malware Defense
	Instance 2	Essentials, URL Filtering
	Instance 3	Essentials, URL Filtering
Security Module 2	Instance 4	Essentials, IPS
	Instance 5	Essentials, URL Filtering, Malware Defense, IPS
Security Module 3	Instance 6	Essentials, Malware Defense, IPS
	Instance 7	Essentials, IPS

Table 5: Total number of licenses

Essentials	URL Filtering	Malware Defense	IPS
3	2	3	2

Create a Cisco account

You need a Cisco account to access Smart Account functionality and license any Cisco products.

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

Procedure

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

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

Step 3 Click **Register**.

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

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

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

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

What to do next

Enter the newly created account details on the login page to request a Smart Account. Refer to Create a smart account and add licenses, on page 18.

Create a smart account and add licenses

Create a Smart Account to centrally manage and track your Cisco software licenses across your organization.

You should set up this account before you purchase licenses. 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.

Before you begin

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

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

Procedure

Step 1 Go to the Create a Smart Account page.

You are prompted to log in with your Cisco account. In the **Create a Smart Account** page, your basic account information is displayed.

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



Step 3 Click **Personal** and configure these parameters:

a) In the **Your Company Details** section, click **Edit**.

b) In the **Company or organization** field, type your organization name.

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

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

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

1. In the **Address** drop-down list, click the drop-down arrow and click **Add New Address**.
2. You can select one of the following **Address Type** options:
   - **Company/Organization**: To provide your organization's address. Cisco verifies this address. If the address and company name cannot be validated with the country, you may not be able to proceed. Therefore, you must ensure that the correct address is provided.
   - **Personal**: To provide your personal address.

e) Enter all the mandatory fields associated with your company and click **Update**.

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

A success message appears if your company details are validated.

Step 4 Click **Update**.

A success message appears if your company details are validated.

Step 5 Open the **Create a Smart Account** page, which was opened in the previous tab. Refresh the page if changes are not reflecting.

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

Step 6 Click **Create Account**.

The **Account Summary** page displays your account details.

Step 7 Click **Done**.

Step 8 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 9 Make sure your Smart Licensing account contains the available licenses you need.

What to do next

To configure Smart License using the Smart Software Manager, refer to Configure Smart Licensing, on page 20.

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 Specific License Reservation, on page 31.

Register the Firewall Management Center for Smart Licensing

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

Register the Firewall Management Center with the Smart Software Manager

Register the Firewall Management Center with the Smart Software Manager to enable Smart Licensing functionality and proper license management.

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.

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

- 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.

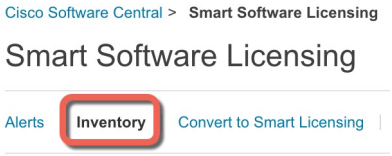
  For the Firepower 4100/9300, configure NTP on the chassis using the same NTP server as the Firewall Management Center.

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

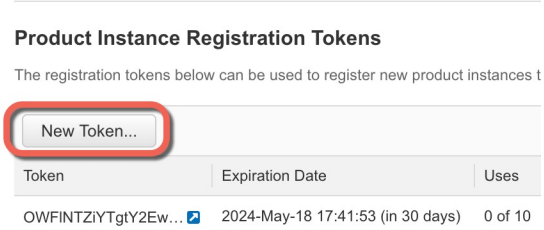
Procedure

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.

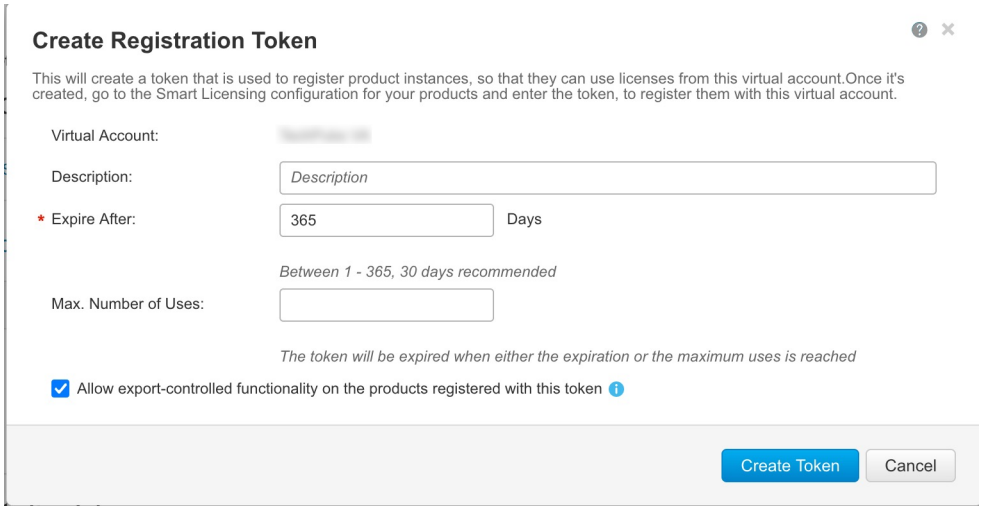
a) Click **Inventory**.



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



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



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Max. Number of Uses**
- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

The token is added to your inventory.

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

Figure 1: View token

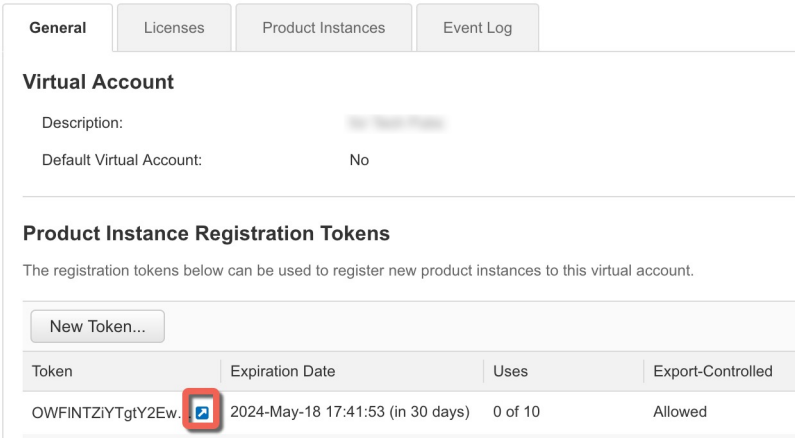
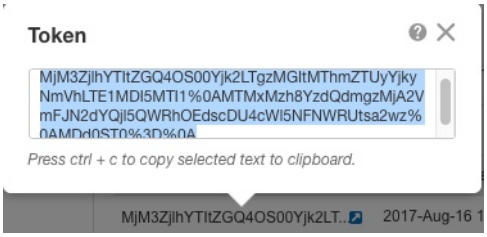


Figure 2: Copy token



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

Step 3 Click **Register**.

Step 4 Paste the token you generated from Smart Software Manager into the **Product Instance Registration Token** field.

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

Step 5 If the Firewall Management Center instance is already registered with Smart Licensing, you can check the **Override Existing Registered Management Center Instance** check box to override the existing registered instance.

Step 6 Decide whether to send usage data to Cisco.

- The Cisco Success Network capability allows Cisco to collect customer usage metrics and statistics to analyze product usage and enhance customer experience of Cisco products. This feature is enabled by default. To opt out of sending Cisco Success Network telemetry data to Cisco, see Configure Firewall Management Center to share usage metrics and statistics with Cisco. For more information about the telemetry data that Cisco collects, click **sample data**.
- The Cisco Support Diagnostics capability allows Cisco to collect essential information from your devices to provide you with an enhanced support experience. This feature is enabled by default. To opt out of sending Cisco Support Diagnostics metrics to Cisco, see Configure Firewall Management Center to share device health data with Cisco.

Note

- When Cisco Support Diagnostics is enabled, it gets applied to the devices in the next sync cycle. The Firewall Management Center sync with the device runs once every 30 minutes.

- When Cisco Support Diagnostics is enabled, it gets applied automatically on any new device registered in this Firewall Management Center.

Step 7 Click **Apply Changes**.

What to do next

- Add a device to the Firewall Management Center; see *Add a Device to the Firewall Management Center* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- Assign licenses to your devices; see Assign licenses to multiple managed devices, on page 26.

Register the Firewall Management Center with the Smart Software Manager On-Prem

As described in Periodic communications with the Smart Software Manager, on page 2, the Firewall Management Center 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 Firewall Management Center is offline or otherwise has limited or no connectivity (in other words, is deployed in an air-gapped network.)

  (For an alternate solution for air-gapped networks, see Licensing options for air-gapped deployments, on page 2.)

- Your Firewall Management Center 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, refer to 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 Firewall Management Center with the Smart Software Manager On-Prem.

a) Choose **Integration** > **Other Integrations** and click **Smart Software Manager On-Prem**.

b) Select **Connect to Cisco Smart Software Manager On-Prem Server**.
c) 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/SmartTransport`

The FQDN or hostname must match the CN value of the CERTIFICATE presented by your Smart Software Manager On-Prem.

d) Add a new **SSL CERTIFICATE** and paste the CERTIFICATE text that you copied earlier, and click **Apply**.
e) Choose **System** (⚙) > **Licenses** > **Smart Licenses** and click **Register**.
f) Create a new token on Smart Software Manager On-Prem and copy the token.
g) Paste the token into the form in the Firewall Management Center page.
h) Click **Apply Changes**.

The Firewall 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.

Refer to 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, refer to 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, in the **Inventory** > **Licenses** page, verify that you have the license that corresponds to your Firewall Management Center:

Export Control License	Firewall Management Center Model
Cisco Virtual FMC Series Strong Encryption (3DES/AES)	All Firewall Management Center Virtuals
Cisco FMC 1K Series Strong Encryption (3DES/AES)	1000, 1600
Cisco FMC 2K Series Strong Encryption (3DES/AES)	2500, 2600

Export Control License	Firewall Management Center Model
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**

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

What to do next

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

In High Availability deployments both the Firewall Threat Defense 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 Firewall Management Center. You can also assign licenses per device, or for multiple devices.

Assign licenses to a single device

This task allows you to enable or disable specific licensed features on a managed device by assigning or removing licenses as needed.

You can enable or disable specific licensed features on a managed device by assigning or removing licenses as needed. Although there are some exceptions, you cannot use the features associated with a license if you disable it on a managed device.

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

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

Before you begin

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

Procedure

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

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

Step 3 Click **Device**.

Step 4 Next to the **License** section, click **Edit** ( ).

Step 5 Check or clear the appropriate check boxes to assign or disable licenses for the device.

Step 6 Click **Save**.

Step 7 Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

What to do next

Verify license status:

1. Choose **System** ( ) > **Licenses** > **Smart Licenses**.
2. Enter the hostname or IP address of the device into the filter at the top of the Smart Licenses table
3. Verify that only a green circle with a **Check Mark** ( ) appears for each device, for each license type.

   If you see any other icon, hover over the icon for more information.

Assign licenses to multiple managed devices

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

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

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

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

Procedure

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

Step 2 Click **Edit Licenses**.

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

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

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

e) Repeat this subprocedure for each type of license you want to add.
f) To remove a license, click the **Delete** ( ) next to the device.
g) Click **Apply**.

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

What to do next

Verify that your licenses are correctly installed. Follow the procedure in Monitor Smart Licensing, on page 29.

Manage Smart Licensing

This section describes how to manage Smart Licensing.

Deregister the Firewall Management Center

Deregister your Firewall Management Center from the Smart Software Manager to release all of the license entitlements back to your Smart Account so they can be used for other devices.

Deregister if you need to decommission the Firewall Management Center or reimage it.

Refer to 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 Firewall Management Center

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**.

Monitor Smart License status

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

Usage authorization

Possible status values are:

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

Product registration

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

Assigned virtual account

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

Export-Controlled features

If this option is enabled, you can deploy restricted features. For details, see License for export-controlled functionality, on page 11.

Cisco success network

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

Monitor Smart Licensing

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

For each type of license in your deployment, the page lists the total number of licenses consumed, whether the license is in compliance or out of compliance, the device type, and the domain and group where the device is deployed. You can also view the Firewall Management Center's Smart License Status. Container instances on the same security module/engine only consume one license per security module/engine. Therefore, even though the Firewall Management Center lists each container instance separately under each license type, the number of licenses consumed for feature license types will only be one.

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

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

  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 Firewall Management Center Virtual licenses, each represents one managed device.

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

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

What to do next

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

Troubleshoot Smart Licensing

This topic lists some common Smart Licensing issues and provides troubleshooting steps.

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 Licensing server

Check the obvious causes first. For example, make sure your Firewall Management Center has outside connectivity. See Communication Ports and Internet Access.

Unexpected out-of-compliance notification or other error

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

Troubleshoot other issues

For solutions to other common issues, see Use FMC and FTD Smart License Registration and Common Issues to Troubleshoot.

Specific License Reservation

If you cannot have or do not want direct communications between the Firewall Management Center and the Smart Software Manager or the Smart Software Manager On-Prem, use Specific License Reservation. Specific License Reservation uses the same licenses as regular Smart Licensing.

Configuration process

To configure Specific License Reservation, you will generate a request code on the Firewall Management Center, access the Smart Software Manager with your browser, enter the request code to obtain an authorization code, then return the authorization code to the Firewall Management Center.

Note Various names are used at Cisco for Specific License Reservation. These include 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.

Prerequisites for Specific License Reservation

This topic lists the prerequisites for configuring Specific License Reservation.

Switching to Specific License Reservation

If you are currently using regular Smart Licensing, de-register the Firewall Management Center from Smart Software Manager before you implement Specific License Reservation; refer to Deregister the Firewall Management Center, on page 27.

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

Specific License Reservation and high availability

Configure high availability before you assign licenses. If you already assigned licenses to devices on the secondary Firewall Management Center, be sure to unassign them.

If an SLR license is assigned to a primary Firewall Management Center, when the secondary Firewall Management Center becomes active after a failover, you cannot add the SLR license to the secondary Firewall Management Center.

- Perform a failover to make the primary Firewall Management Center active.
- Unassign and re-assign the license to the secondary Firewall Management Center.

Downloading threat intelligence with Specific License Reservation

Security Services Exchange (SSE) integration is required for a secure connection to Talos Cloud Services, where the system gets:

- Intrusion rule updates

- URL filtering data and lookups
- Event enrichment data

The Talos Connectivity Status health module monitors connectivity with Talos Cloud Services.

If you are using regular Smart Licensing, registering with Smart Software Manager sets up SSE integration. But if you are using Specific License Reservation in a non-airgapped deployment, you must instead enable Security Cloud Control : Enable Cisco Security Cloud integration.

If you have concerns with data sharing, disable all sharing options including event storage, Cisco Success Network, and Cisco Support Diagnostics. But the Firewall Management Center still must be able to reach the regional cloud listed in Communication Ports and Internet Access. Note that in airgapped deployments, you update threat intelligence manually, with the exception of event enrichment, which is not supported.

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 Firewall Management Center.

Before you begin

- Ensure that you have met the requirements described in Prerequisites for Specific License Reservation, on page 31.
- 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 Firewall Management Center Virtual entitlements for your devices, if applicable.

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

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 Firewall Management Center.

Procedure

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

Step 2 Log into the Firewall Management Center 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 Firewall Management Center 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 Firewall Management Center

Use specific license reservation when you need to reserve and use licenses offline or in environments where direct communication with Smart Software Manager is not available.

Procedure

Step 1 Generate the reservation request code.

a. In the Firewall Management Center, 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** and click **License Reservation**.

e. Enter the code that you generated from Firewall Management Center into the **Reservation Request Code** box and click **Next**.

f. Select **Reserve a specific license** and scroll down to display the entire License grid.

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

Note

- You must explicitly include a Essentials license for each managed device, or, for multi-instance deployments, for each container.
- If you are using the Firewall Management Center Virtual, 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-Firewall Management Center, you must select the appropriate license.

    For the correct license name to choose for your Firewall Management Center, see the prerequisites in Enable the export control feature for accounts without global permission, on page 24.

Note

-
- You must explicitly include a Essentials license for each managed device, or, for multi-instance deployments, for each container.
- If you are using the Firewall Management Center Virtual, 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-Firewall Management Center, you must select the appropriate license.

    For the correct license name to choose for your Firewall Management Center, see the prerequisites in Enable the export control feature for accounts without global permission, on page 24.

h. Click **Next** and click **Generate Authorization Code**.

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

i. Download the Authorization Code in preparation for entering it into the Firewall Management Center.

Step 3 Enter the authorization code in the Firewall Management Center.

a. In the Firewall Management Center, 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.

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, refer to Update the Specific Licenses for Firepower Management Center.

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 *Cisco Secure Firewall Management Center Device Configuration Guide*.

Manage specific license reservation

This section describes how to manage Specific License Reservation.

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 (in the **Reserved Licenses** tab). If any of the licenses expire, the Firewall Management Center 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 Firewall Management Center, 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, these actions are restricted:

- Device registration
- Policy deployment

Procedure

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

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

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

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

a) On the page that shows the correct UUID, from the **Actions** drop-down list, choose **Update Reserved Licenses**.

b) Update the reserved licenses as needed.

Note

- You must explicitly include a Essentials license for each managed device, or, for multi-instance deployments, for each container.
- If you are using the Firewall Management Center Virtual, 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-Firewall Management Center, you must select the appropriate license.

    For the correct license name to choose for your Firewall Management Center, see the prerequisites in Enable the export control feature for accounts without global permission, on page 24.

c) Click **Next** and verify the details.

d) Click **Generate Authorization Code**.

e) Download the Authorization Code in preparation for entering it into the Firewall Management Center.

f) Leave the **Update Reservation** page open. You will return to it later in this procedure.

Step 4 Update the Specific Licenses in the Firewall Management Center.

a) Choose **System** (⚙) > **Licenses** > **Specific Licenses**.

b) Click **Edit SLR**.

c) Click **Browse** to upload the newly generated authorization code.

d) Click **Install** to update the licenses.

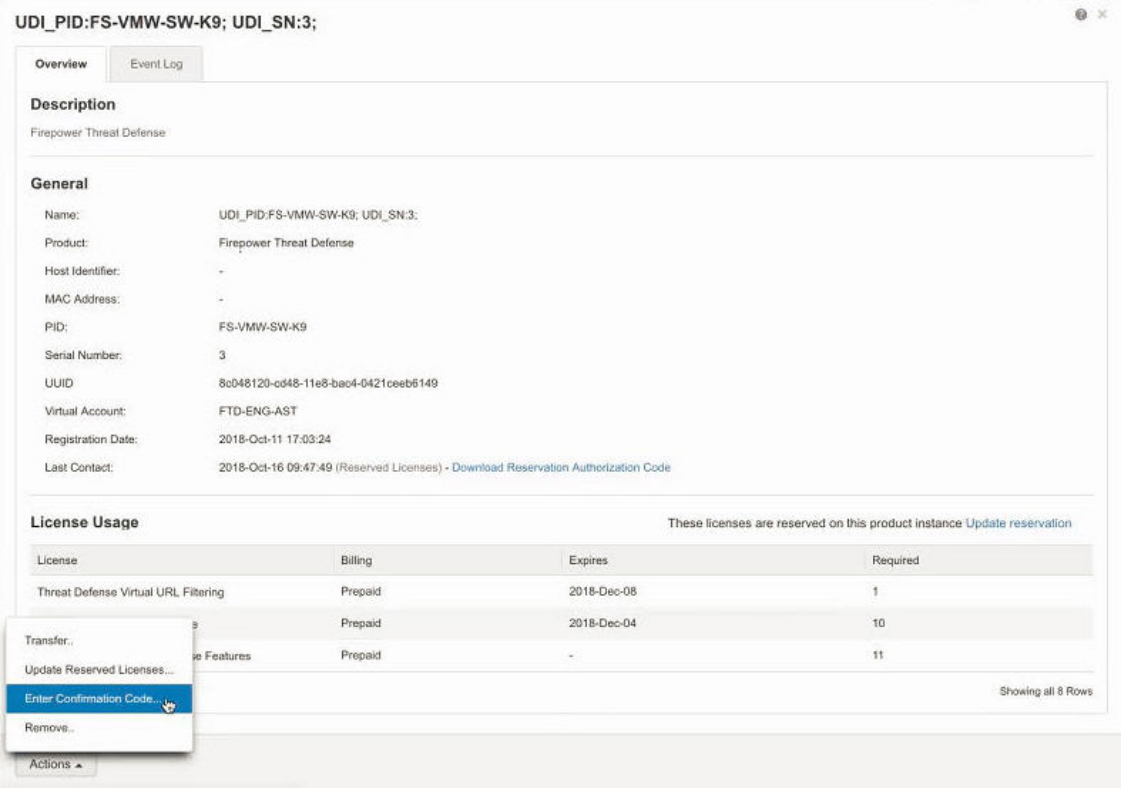
After successful installation of the authorization code, ensure that the licenses shown in the **Reserved** column of Firewall Management Center, matches with the licenses that you have reserved in the Smart Software Manager.

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) From the **Actions** drop-down list, choose **Enter Confirmation Code**:



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

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

If necessary, refer to Monitor Specific License Reservation status, on page 40 for more information.

Step 7 Deploy configuration changes; see the *Cisco Secure Firewall 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).

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

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.

Procedure

Step 1 In the Firewall Management Center Web interface, select **System** (⚙) > **Licenses** > **Specific Licenses**.

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

Step 3 Generate a return code from the Firewall Management Center.

a) Click **Return SLR**.

Devices become unlicensed and the Firewall Management Center moves to the de-registered state. It generates a return code and allows you to re-register the Firewall Management Center with SLR.

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

Step 4 In the Smart Software Manager, identify the Firewall Management Center 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 Firewall Management Center is the correct Firewall Management Center. Click the name.

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

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

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

a) On the page that shows the correct UUID, from the **Actions** drop-down list, choose **Remove**.

b) Enter the reservation return code that you generated from the Firewall Management Center into the **Remove Product Instance** dialog box.

c) Click **Remove Product Instance**.

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

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

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

b) Log in to the Firewall Management Center CLI **admin** account. This gives you access to the command line interface.

c) Enter the **expert** command to access the Linux shell.

d) Execute this 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.

Monitor Specific License Reservation status

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

Usage authorization

Possible status values are:

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

Product registration

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

Export-Controlled features

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

For more information about Export-Controlled Features, see License for export-controlled functionality, on page 11.

Product instance

The Universally Unique Identifier (UUID) of this Firewall Management Center. 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

This topic provides troubleshooting guidance for resolving Specific License Reservation issues.

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

In 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 management center.

In the Firewall Management Center web interface, the UUID for the management center is the **Product Instance** value displayed in 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 these steps:

1. If you have already generated a **Request Code** in the management center web interface, cancel the request code.
2. Disable Specific License Reservation in the management center Linux shell as described within the section Deactivate and return the Specific License Reservation, on page 38.
3. Register the management center 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 Firewall Management Center Virtual

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

Refer to Update a Specific License Reservation, on page 36.

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 refer to, Deactivate and return the Specific License Reservation, on page 38.

What if I do not see a Specific License page in the Firewall Management Center Virtual?

You need to enable Specific License to view the Specific License page. For more information see, Enable the Specific Licensing menu option, on page 33.

I have disabled specific licensing, but forgot to copy the return code. what should I do?

The **Return Code** is saved in the Firewall Management Center Virtual. You must re-enable the Specific License from the Linux shell (see Enable the Specific Licensing menu option, on page 33), then refresh the Firewall Management Center Virtual web interface. Your **Return Code** will be displayed.

Additional information about licensing

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

- Licensing FAQ
- License Roadmap

History for licenses

This topic provides a chronological history of license-related features, enhancements, and changes implemented across different software versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Secure Firewall Threat Defense usage metric collection improvements	7.6.0	Any	The Cisco Success Network and Cisco Support Diagnostic capabilities are now enabled by default. With this enhancement, Cisco now collects telemetry data from the Secure Firewall Threat Defense deployments more efficiently. Deprecated screens: The **Enable Cisco Success Network** and the **Enable Cisco Support Diagnostics** check boxes under the **Smart Licensing Product Registration** page (**System** > **Licenses** > **Smart Licenses** > **Register**) are deprecated.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Smart Licensing Standardization	7.3	Any	We changed the license names in the Firewall Management Center GUI: • Base is now Essentials • Threat is now IPS • Malware is now Malware Defense • RA VPN/AnyConnect License is now Cisco Secure Client • AnyConnect Plus is now Secure Client Advantage • AnyConnect Apex is now Secure Client Premier • AnyConnect Apex and Plus is now Secure Client Premier and Advantage • AnyConnect VPN Only is now Secure Client VPN Only
Support for Carrier license	7.3	Any	The Carrier license enables inspection of Diameter, GTP/GPRS, SCTP, and M3UA protocols. New/Modified screens: **System** > **Smart Licenses**.
Performance tier licensing for the Firewall Threat Defense Virtual	7.0	Any	Performance-tiered licensing provides different throughput levels and VPN connection limits based on deployment requirements. License tiers map to new Firewall Threat Defense Virtual models.
Licensing for multi-instance capability for the Firewall Threat Defense on the Firepower 4100/9300	6.3	Any	You can now deploy multiple Firewall Threat Defense container instances on a Firepower 4100/9300. You only need a single license per feature per security module/engine. The base license is automatically assigned to each instance. New/Modified screens: **System** > **Licenses** > **Smart Licenses**. Supported platforms: Firewall Threat Defense on the Firepower 4100/9300
Specific License Reservation for air-gapped deployments	6.3	Any	Customers whose deployments cannot connect to the internet to communicate with the Cisco License Authority can use a Specific License Reservation. New/Modified screens: **System** > **Licenses** > **Specific Licenses** (This option is not available by default.) Supported platforms: Firewall Management Center, Firewall Threat Defense
Export-controlled functionality for restricted customers	6.3	Any	Certain customers whose Smart Accounts are not otherwise eligible to use restricted functionality can purchase term-based licenses, with approval. Supported platforms: Firewall Management Center, Firewall Threat Defense