Frequently Asked Questions (FAQ) about Cisco Secure Firewall Licensing

First Published: 2018-01-18

Last Modified: 2025-03-05

Frequently Asked Questions (FAQ) about Licensing

The Frequently Asked Questions (FAQ) about Licensing provides answers to common questions about smart and classic licensing, feature license service subscriptions, expired subscriptions, license requirements for high availability and clustered deployments, and more.

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

This Document Does Not Replace the Official Ordering Guide or Your License Agreement

Information in this document is intended to provide general information, but it is subject to change and cannot capture the full complexity of the licensing options.

Work with your Cisco representative to ensure that you purchase the correct licenses for your products and deployment.

For information about expired or out-of-compliance licenses, your license or purchase agreement supersedes any information in this document or the configuration guide for your product.

General License Management

Q. What licenses do I need?

A. The licenses you need depend on the software you will run on your hardware.

If you will run software:

- Start with this document and the documents mentioned in More Information, on page 16.
- Secure Firewall Management Center hardware does not require licensing.

  Management Center Virtual appliances require licensing.

  For details, see the "Management Center Virtual Licenses" topic in the Licensing chapter of the Cisco Secure Firewall Management Center Administration Guide for your version.
- Secure Firewall Threat Defense devices use Smart licensing. For more information, see Smart Licensing for Threat Defense Features, on page 4.
- All other devices use Classic licensing. For more information, see Classic Licensing for Threat Defense Features, on page 7.

If you will run other software, such as Secure Firewall ASA:

- See the documentation for your software product.
- The same hardware may have different licensing requirements depending on the software it runs.

Q. Does the management center require a license?

A. In Version 6.0 and later, the management center manages feature licenses for your devices, but you do not need licenses to use the management center hardware. Management Center Virtual appliances require licenses. For details, see the Licensing chapter of the Cisco Secure Firewall Management Center Administration Guide for your version.

In Version 5.4.x and earlier, a FireSIGHT license is required to use a FireSIGHT Defense Center. You must add this license to the Defense Center during initial setup.

Q. Does my device need Classic or Smart Licenses?

A. The software, not the hardware, determines the required license type for your products.

- Devices running Threat Defense software require Smart Licenses.
- All other devices ASA with FirePOWER Services, 7000 or 8000 Series, and NGIPSv require Classic licenses.
- For hardware that is not running Threat Defense software, see the documentation for your software product.

  For example, for hardware running Cisco Adaptive Security Appliance (ASA) software *without* FirePOWER Services, see https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/licenseroadmap.html.

Q. What is the difference between a Smart License and a Classic license?

A. Some products require one or the other type of license (see above.)

The details and processes for deploying each type of license differ.

- For more information about Smart licenses, see Smart Licensing for Threat Defense Features, on page 4.
- For more information about Classic licenses, also called "traditional" licenses, see Classic Licensing for Threat Defense Features, on page 7

Additional information about deploying each type of license is available in the Licensing chapter of the Cisco Secure Firewall Management Center Administration Guide.

Q. Can a management center manage devices that use different license types (Smart and Classic)?

A. Yes. However, the steps you take on the management center to manage the license types differ slightly. For more information, see the Licensing chapter in the Cisco Secure Firewall Management Center Administration Guide.

Q. Can I convert my Classic license to a Smart License entitlement?

A. Generally, if your hardware can run either a software product that uses a Classic license or a software product that uses a Smart License, you can convert the license.

You can look in your account to see which PAKs can be converted:

- In the Product License Registration Portal (LRP), after the PAK is in the Smart Account, click the **PAKs or Tokens** tab, mouse over a PAK to see the blue arrow, then click the blue arrow. If the

license can be converted, you will see a **Convert to Smart Licensing** option. (The LRP shows the product associated with the PAK, but lists all PAKs whether or not they can be converted.)

- In Cisco Smart Software Manager (CSSM), click the **Convert to Smart Licensing** tab to view your convertible PAKs. To see which product is associated with each PAK in the list, click the PAK to view details. (CSSM only lists PAKs that can be converted, but you must click each PAK to determine what product the PAK is associated with.)

Convertibility may change over time; if a PAK becomes eligible for conversion, its status in the LRP and CSSM will update automatically.

Information about converting licenses is in the Licensing chapter of the Cisco Secure Firewall Management Center Administration Guide.

See also "Convert PAK License SKU's in LRP to Smart License Entitlements in Smart Software Manager (SSM)" in the Cisco License Registration Portal (LRP) User Guide.

Q. Can I convert my Smart License entitlement to a Classic license?

A. No. If you accidentally use a Smart License entitlement instead of a Classic license, contact Cisco TAC.

Q. What is the difference between a license and a service subscription?

A. A feature license is a *right-to-use* license. The license is perpetual; you can continue to use the features and functionality present in the version of the feature you initially install, regardless of whether you purchase a service subscription to support the license.

A service subscription is the *entitlement* to download updates related to the feature. For example, if you buy a Threat (T) subscription to support your Threat license, you can download intrusion rule updates. This entitlement is term-based; that is, it expires periodically. For more information, see License Expiration, on page 13.

When you purchase a feature license, you specify a subscription period, such as 3 years.

Q. When does the term for a service subscription start and end? Is the start date tied to the purchase date or the initial activation date?

A. The start and end date of each service subscription is specified on the sales order. The subscription start date is not tied to the initial activation date.

Q. Can I register my management center to more than one Smart Account? Can I register it to multiple virtual accounts within the same Smart Account?

A. No.

Note Smart Accounts can manage both Smart Licenses and Classic licenses, so this answer applies to both types of licenses.

If you need to move your registration, you must first un-register the management center from the original account. Licenses assigned to devices managed by that management center instance are automatically released.

Q. I have threat defense and ASA running on the same chassis. How do I license them?

A. Your hardware model must support this configuration. License each software product as if it were not sharing a chassis.

Q. Where can I find documentation to help me with Cisco's license-management tools?

A. https://community.cisco.com/t5/licensing-enterprise-agreements/software-on-demand-training-resources-for-customers/ta-p/3639797

Q. What if I have a question about or problem with a license that the account administrator at my company cannot answer?

A. Contact licensing@cisco.com.

Smart Licensing for Threat Defense Features

Q. What is a Smart License?

A. Cisco Smart Licensing is the newer form of license at Cisco. It allows you to manage a pool of licenses centrally. Unlike Classic licenses, Smart Licenses are not tied to a specific serial number or PAK. You activate a Smart License from the Secure Firewall Management Center or the Secure Firewall device manager.

Q. What devices use Smart Licenses for threat defense features?

A. Products that are running threat defense software use Smart Licensing. For a full list of these devices, see the Compatability Guide.

Q. What is a Smart Account and how do I get one?

A. Your Smart Account holds the licenses that your company has purchased (both Smart and Classic.) Smart Licenses must be in your Smart Account before you can see them in the Smart Software Manager (CSSM) and consume them.

Your Cisco account representative or authorized reseller deposits your purchased licenses to your Smart Account, and may create your Smart Account for you.

If you need to create a Smart Account, go to https://software.cisco.com/smartaccounts/setup#accountcreation-account. For information about setting up your Smart Account, see https://www.cisco.com/c/en/us/buy/smart-accounts.html.

Q. What if Smart Licenses that I have purchased do not appear in my Smart Account?

A. Check the following, in order:

- Make sure the licenses are not in a different virtual account within your organization's Smart Account. Because the licenses may be in a virtual account that you cannot access, you will need to contact the Smart Account administrator at your organization.
- Contact the person or organization who sold you the licenses.

- Contact Licensing@cisco.com.

Q. How do I give other people at my company access to a Smart Account that I set up?

A. See https://community.cisco.com/t5/licensing-enterprise-agreements/request-access-to-an-existing-smart-account-quick-reference/ta-p/3628587?attachment-id=144211.

Q. What is a Product Instance Registration Token?

A. The Product Instance Registration Token allows you to register your management center or device manager with the Cisco Smart Software Manager. You create the token in the Cisco Smart Software Manager. For more information, see https://www.cisco.com/web/fw/softwareworkspace/smartlicensing/SSMCompiledHelps/c_Creating_a_Product_Instance_Registration_Token.html.

You can create tokens with or without enabling export-controlled functionality. However, some important Threat Defense features require that you enable export-controlled functionality. If your account qualifies for export-controlled functionality, this functionality must be must be authorized before you generate the token and you must select the option when you generate the token. Cisco recommends that you understand your needs before generating these tokens. (Starting in Release 6.3, accounts that do not qualify for export-controlled functionality may be able to obtain it on a per-management center basis. Contact your reseller or account representative for more information. The mechanism for this solution does not involve the Product Instance Registration Token.)

After you create the token, you add it to the managing device to register that device with the Cisco Smart Software Manager. After the managing device is registered, you can assign Smart Licenses to managed devices. For more information, see the Cisco Secure Firewall Management Center Administration Guide.

Q. Where do I find the Product Instance Registration Token for my management center or device manager?

A. You can create and copy the token from your virtual account in the Cisco Smart Software Manager. For more information, see https://www.cisco.com/web/fw/softwareworkspace/smartlicensing/SSMCompiledHelps/c_Managing_Product_Instance_Registration_Tokens.html.

Q. How do I access the Cisco Smart Software Manager (CSSM)?

A. On the management center, choose **System** > **Licenses** > **Smart Licenses**, and click **Cisco Smart Software Manager**.

You can also access the Cisco Smart Software Manager directly in a browser:

https://software.cisco.com/#module/SmartLicensing

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

Q. How many licenses do I need for a multi-instance deployment?

A. 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 device.
- Feature licenses are manually assigned to each instance; but you only consume one license per feature per device. 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.

Q. What happens if my products are not able to communicate with the smart licensing server?

A. Each product communicates with the License Authority every 30 days. If you make changes in the Smart Software Manager, you can refresh the authorization on your product so the change takes place immediately. Or you can wait for the device to communicate as scheduled. Optionally, you can configure an HTTP proxy.

Device Manager: The product must have Internet access either directly or through an HTTP proxy at least every 90 days. Normal license communication occurs every 30 days, but with the grace period, your device will operate for up to 90 days without calling home. After the grace period, the device must contact the Licensing Authority, or you will not be able to make configuration changes to features requiring special licenses; operation is otherwise unaffected.

Management Center: If the management center does not communicate with the Smart Software Manager for 1 year, it will become unregistered and the management center cannot deploy any configuration changes to devices for features that require licenses. Note: After 90 days, the 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 management center is removed from your account so you will have to manually re-register the management center.

For a comparison of options for air-gapped environments, or to deploy Smart Software Manager On-Prem (formerly known as a Cisco Smart Satellite Server) to communicate with the License Authority, see the Licensing chapter in the Cisco Secure Firewall Management Center Administration Guide.

Q. Is Permanent License Reservation (PLR) available for my devices?

A.

- Secure Firewall Threat Defense managed by Secure Firewall Management Center:

  Specific License Reservation was introduced in release 6.3. For details, see the Licensing chapter in the Cisco Secure Firewall Management Center Administration Guide.

- Secure Firewall Threat Defense managed bySecure Firewall device manager

  PLR was introduced in release 6.6 and is also available in release 6.4.0.10 (but not in 6.5.x). For more information, see "Licensing the System" chapter in the Cisco Secure Firewall Device Manager Configuration Guide.

Q. What does it mean when my product is in an out-of-compliance state and how do I know if this happens?

A. The license can become out of compliance in the following situations:

- Over-utilization—When the product uses unavailable licenses.
- License expiration—When a time-based license expires.

To verify whether your account is in, or approaching, an Out-of-Compliance state, look at the Smart Licensing page in your management center or in your Smart Account.

Classic Licensing for Threat Defense Features

Q. What is a Classic license?

A. This is the older form of license at Cisco. Classic licenses require a product authorization key (PAK) to activate and are non-transferrable between devices. Classic licensing is also referred to as "traditional licensing."

Q. What devices use Classic licenses for features?

A. 7000 and 8000 Series devices, ASA FirePOWER modules, and NGIPSv.

Q. Are Classic licenses transferrable between devices?

A. No.

Q. What is a product authorization key (PAK)?

A. The product authorization key (PAK) enables you to activate a Classic license. The PAK is included in the Software Claim Certificate that Cisco provides when you purchase a license.

In the Cisco Product License Registration Portal, use the PAK in combination with the license key to generate the license text required to add licenses to the management center.

Q. How do I access the Cisco License Registration Portal (LRP)?

A. On the management center, choose **System** > **Licenses** > **Classic Licenses**, click **Add New License**, and click **Get License**.

You can also access the License Registration Portal directly in a browser:

https://www.cisco.com/go/license

For more information on using this portal, see *Product License Registration Tools & Resources* (https://www.cisco.com/web/fw/tools/swift/xui/html/help.html).

Q. How are Software Claim Certificates (SCCs) delivered?

A. If you buy a physical device (for example, a Firepower 8250), you receive a paper copy of the Software Claim Certificate for the related Control license in the box with the physical device.

If you deploy a virtual device (for example, management center virtual), you receive the Software Claim Certificate for the related Control license as an email attachment.

If you buy feature licenses for either physical or virtual devices (for example, URL Filtering), you receive the Software Claim Certificate as an email attachment.

Q. What happens if I lose or misplace my Software Claim Certificate before I register my PAK in the Cisco Product Licensing Registration Portal?

A. Contact Cisco TAC.

Q. What is a license key?

A. The license key uniquely identifies a managing device in the Cisco Product License Registration Portal. Managing devices include ASDM locally managing ASA FirePOWER modules, and management centers.

This license key has the following format:

product_code:*address*

The *product_code* element varies depending on the type of managing device, and the *address* element is the MAC address of the managing device. On management center, this is the MAC address of the management interface (Eth0).

For example, a possible licensing key for a management center is "66:00:00:77:FF:CC:88".

In the Cisco Product License Registration Portal, use the license key in combination with the PAK to generate the license text required to add Classic feature licenses to the managing device.

Q. Where do I find the license key?

A.
- On the management center, choose **System** > **Licenses** > **Classic Licenses** > **Add New License**. The License Key appears in the resulting dialog.
- In ASDM, obtain the License Key for your chassis by choosing **Configuration > ASA FirePOWER Configuration > Licenses** and clicking **Add New License**. The License Key is near the top; for example, 72:78:DA:6E:D9:93:35.

Q. Where do I find the license text I need to add a Classic license to the management center?

A. Generate the license text in the Cisco Product License Registration Portal. After you generate the license text, either copy the text from the License Registration Portal display or from 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. Make sure that you copy and paste only one license at a time. Each license begins with a BEGIN LICENSE line and ends with an END LICENSE line. (Include these lines when you copy and paste each license.)

Q. How soon after purchasing a feature license in the Cisco Commerce Workspace (CCW) can I generate license text in the Cisco License Registration Portal (LRP)?

A. Typically, you receive the electronic Software Claim Certificate immediately. However, you may encounter a delay of up to 24 hours between purchasing the feature license in Cisco Commerce Workspace and being able to register the PAK and generate license text in the License Registration Portal .

Q. Can I delete a license from one management center and then reuse it on a different management center?

A. Not directly. The generated license is specific to each management center. However, you can re-use the PAK in the Cisco Product License Registration Portal to generate a new license that uses the unique identifier of the other management center.

Q. I bought a Classic license for a device, but did not register it in the Cisco License Registration Portal (LRP) or assign it to the device. Can I repurpose this license for another device?

A. You can only repurpose an unused license if the original device and new device are the same model. For example, if you buy a Protection license for an ASA FirePOWER module on an ASA 5508-X, you can assign it to any ASA 5508-X, but you cannot assign it to an ASA 5516-X.

You cannot repurpose the service subscription that you bought at the same time as the original license. The timer on that subscription starts the day it is issued, even if you do not assign it to a device. Contact Sales to inquire about a possible credit for the remaining portion of the service subscription.

Licensing in High Availability Configurations

- Management Center (Hardware) High Availability

- Management Center (Virtual) High Availability
- Threat Defense High Availability
- Firepower 7000 & 8000 Series Device High Availability

Management Center (Hardware) High Availability

Q. Do I need any special licensing to configure two hardware management center appliances as a high-availability pair?

A. A hardware management center requires no special licensing, whether it is standalone or part of a high-availability pair.

Q. If I want to enable a licensed feature for a device managed by a hardware Secure Firewall Management Center high availability pair, how many licenses must I buy?

A. A device managed with management center instances in a high availability configuration requires the same number of feature licenses and related subscriptions as a device managed by a single management center.

The system automatically replicates all managed devices' feature licenses from active to standby management center, so the licenses are available to managed devices on failover.

Management Center (Virtual) High Availability

Q. What are the licensing requirements for management center virtual in a high availability pair?

A.

- **Starting in release 6.7:**

  Management Center Virtual running on VMWare with entitlement for 10, 25, or 300 managed devices can be configured in a high availability pair.

  You will need two identically licensed management center virtual's to form an management center virtual-HA pair.

  All managed devices (threat defense and Classic) also require their own licenses, as described above for hardware management center in a high availability configuration.

  For example, to manage 10 threat defense devices and 3 NGIPS devices with an management center virtual high availability pair, you need two (2) FMCv25 entitlements, 10 threat defense entitlements, and 3 Classic entitlements.

  For details, see the licensing requirements topic in the "Management Center High Availability" chapter of the Cisco Secure Firewall Management Center Administration Guide for your version.

- **Management Center Virtual releases earlier than 6.7:**

A Secure Firewall Management Center Virtual appliance cannot be a member of a high-availability pair.

Threat Defense High Availability

Q. What are the license requirements for threat defense devices in a high-availability configuration?

A. There is no specific license required to configure threat defense devices in a high-availability pair. However, each device should have a license for each feature your deployment will use.

Q. If a management center virtual appliance manages threat defense devices that are configured in a high availability pair, do I need one entitlement for each device or one entitlement for each pair?

A. You need one entitlement for each device.

Q. If I want to enable a licensed feature for threat defense devices in a high-availability configuration, how many licenses must I buy?

A. Each device should be licensed for every feature it will use, whether or not the device is a member of a high-availability pair.

Therefore, for each feature, you should buy two Smart License entitlements for that feature—an entitlement for each device in the high-availability pair. Contact Sales to discuss possible discounting for licenses used in this configuration.

When you configure threat defense devices in a high-availability pair, the management center communicates with the Cisco Smart Software Manager and obtains the necessary licenses from your account so that the standby device has the same feature licenses as the active device. If your Smart Licenses account does not include enough purchased entitlements, your account becomes out of compliance

(OOC) until you purchase the necessary licenses. Licenses for features on the standby device that were not present on the active device are released back into the pool of available licenses.

Q. Are there limitations on changing licenses for threat defense devices in a high-availability configuration?
A. After you pair the devices on the management center, you cannot change the license options for individual devices in the pair, but you can change the license for the entire high-availability pair.

Q. How many licenses do I need for a high-availability pair in a multi-instance deployment
A. High availability pairs are formed between instances on two different chassis and thus will consume two feature licenses.

Firepower 7000 & 8000 Series Device High Availability

Q. If I want to enable a licensed feature for Firepower 7000 & 8000 Series devices in a high-availability configuration, how many licenses must I buy?
A. You must buy two licenses for that feature—one for each device in the high-availability pair. Contact Sales to discuss possible discounting for licenses used in this configuration.

Q. What are the license requirements for Firepower 7000 & 8000 Series devices in a high-availability configuration?
A. There is no additional license required to configure 7000 & 8000 Series devices in a high-availability pair. However, before you can configure 7000 & 8000 Series devices in a high-availability pair, you must assign the same feature licenses to both devices on the management center.

Q. Are there limitations on changing licenses for Firepower 7000 & 8000 Series devices in a high-availability configuration?
A. After you pair the devices on the management center, you cannot change the license options for individual devices in the pair, but you can change the license for the entire high-availability pair.

Licensing in Threat Defense Device Clusters

- Intra-Chassis Clustering
- Inter-Chassis Clustering

Intra-Chassis Clustering

Note Intra-chassis clustering is only supported for threat defense modules on Firepower 9300 devices.

Q. If I want to enable a licensed feature for threat defense modules in an intra-chassis cluster, how many licenses must I buy?
A. You must buy a Smart license for that feature for each module in the cluster. For example, if you want your cluster to include three modules that use URL filtering, you must buy three URL Filtering licenses and related subscriptions.

Q. What are the license requirements for intra-chassis clustering of threat defense modules?
A. The Base license allows you to cluster security modules within an FXOS chassis. There is no additional license required. However, if you want to use license-based features in the cluster (for example, URL

filtering), you must assign equivalent licenses to all threat defense modules before configuring them as a cluster.

Q. Are there limitations on changing licenses for threat defense modules configured in an intra-chassis cluster?

A. After you cluster the devices, you cannot change the license options for individual modules in the cluster, but you can change the license options for the entire cluster.

Inter-Chassis Clustering

Note Inter-chassis clustering is only supported for threat defense on Firepower 9300 and Firepower 4100 series devices.

Q. If I want to enable a licensed feature for threat defense devices in an inter-chassis cluster, how many licenses must I buy?

A. You must buy a Smart license for that feature for each device in the cluster. For example, if you want your cluster to include four devices that use URL filtering, you must buy four URL Filtering licenses and related subscriptions.

Q. What are the license requirements for inter-chassis clustering of threat defense devices?

A. The Base license allows you to cluster threat defense devices running on the FXOS chassis. There is no additional license required. However, if you want to use license-based features in the cluster (for example,

URL filtering), you must assign equivalent licenses to all threat defense devices before configuring them as a cluster.

Q. Are there limitations on changing licenses for threat defense devices in an inter-chassis cluster?
A. After you cluster the devices, you cannot change the license options for individual devices in the cluster, but you can change the license options for the entire cluster.

Licensing in 8000 Series Device Stacks

Q. If I want to enable a licensed feature for an 8000 Series device stack, how many licenses must I buy?
A. You must buy a Classic license for that feature for each device in the stack. For example, if you want your stack to include four devices that use URL filtering, you must buy four URL Filtering licenses and related subscriptions.

Q. What are the license requirements for an 8000 Series device stack?
A. There is no additional license required to configure an 8000 Series device stack. However, to configure 8000 Series devices in a stack, you must assign the same feature licenses to all devices before including them in the stack.

Q. Are there limitations on changing licenses for devices configured in an 8000 Series stack?
A. After you stack the devices, you cannot change the license options for individual devices in the stack, but you can change the license options for the entire stack.

License Expiration

- License Expiration vs. Service Subscription Expiration
- Smart Licensing
- Specific License Reservation
- Classic Licensing
- Subscription Renewals

License Expiration vs. Service Subscription Expiration

Q. Do feature licenses expire?
A. Strictly speaking, feature licenses do not expire. Instead, the service subscriptions that support those licenses expire.

Smart Licensing

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

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

Token expiration dates do not affect subscription expiration dates.

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

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

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

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

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

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

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

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

Specific License Reservation

Q. What happens if my Specific License Reservation expires?

A. SLR licenses are term-based.

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

- Device registration
- Policy deployment

Classic Licensing

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

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

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

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

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

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

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

A. This message merely informs you that Protect and Control functionality requires not only a right-to-use license (which never expires), but also one or more associated service subscriptions, which must be

renewed periodically. If the service subscriptions you want to use are current and will not expire soon, no action is required.

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

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

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

Table 1: Expiration Impact for Classic Licenses/Subscriptions

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

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

Subscription Renewals

Q. How do I renew an expiring Classic license?

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

Q. Can I renew a service subscription from the management center?

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

More Information

For additional information about licensing, see the following documents:

- The Cisco Secure Firewall Management Center Feature Licenses document at:

  https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

- If your deployment includes an management center, the licensing chapter in the Cisco Secure Firewall Management Center Administration Guide.

  Some features, for example Threat Intelligence Director, may have additional details in the chapter about that feature in the Cisco Secure Firewall Management Center Device Configuration Guide. Be sure to use the guide for your product version.

- If your deployment is a standalone threat defense device, the licensing chapter in the Cisco Secure Firewall Management Center Administration Guide.

- If your deployment is a standalone ASA with FirePOWER Services device, the "Licensing the ASA FirePOWER Module" chapter in the *Cisco ASA with FirePOWER Services Local Management Configuration Guide* for your version, available from https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

© 2018–2025 Cisco Systems, Inc. All rights reserved.