

Licensing the System

The following topics explain how to license the Firewall Threat Defense device.

- Smart Licensing for the Firewall System, on page 1
- Managing Smart Licenses, on page 6
- Applying Permanent Licenses, on page 11

Smart Licensing for the Firewall System

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 license 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.

Cisco Smart Software Manager

When you purchase one or more licenses for the Firewall Threat Defense device, you manage them in the Cisco Smart Software Manager: https://software.cisco.com/#SmartLicensing-Inventory. The Cisco Smart Software Manager lets you create a primary account for your organization.

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

Licenses and appliances are managed per virtual account; only that virtual account's appliances can use the licenses assigned to the account. If you need additional licenses, you can transfer an unused license from another virtual account. You can also transfer appliances between virtual accounts.

When you register a device with Cisco Smart Software Manager, you create a Product Instance Registration Token in the manager, and then enter it in Firewall Device Manager. A registered device becomes associated with a virtual account based on the token that is used.

For more information about the Cisco Smart Software Manager, see the online help for the manager.

Periodic Communication with the License Authority

When you use a Product Instance Registration Token to register the Firewall Threat Defense device, the device registers with the Cisco License Authority. The License Authority issues an ID certificate for communication between the device and the License Authority. This certificate is valid for one year, although it will be renewed every six months. If an ID certificate expires (usually in nine months or a year with no communication), the device reverts to a de-registered state and licensed feature usage is suspended.

The device communicates with the License Authority on a periodic basis. If you make changes in the Cisco Smart Software Manager, you can refresh the authorization on the device so the changes immediately take effect. You also can wait for the device to communicate as scheduled. Normal license communication occurs every 12 hours, but with the grace period, your device will operate for up to 90 days without calling home. You must contact the License Authority before 90 days have passed.

Smart License Types

The following table explains the licenses available for the Firewall Threat Defense device.

Your purchase of a Firewall Threat Defense device automatically includes a Essentials license. All additional licenses are optional.

Table 1: Smart License Types

License	Duration	Granted Capabilities
Essentials	Perpetual	All features not covered by the optional term licenses. The Essentials license is automatically added to your account when you register. The exception is for the Secure Firewall 3100. You obtain a Base license when you purchase the firewall, and the license is managed like other licenses in your account. For example, you need to make sure the license is in the correct virtual account when you register. You must also specify whether to **Allow export-controlled functionality on the products registered with this token**. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.

License	Duration	Granted Capabilities
IPS	Term-based	Required to use the following policies: • Intrusion • File (the Malware Defense is also required) • Security Intelligence
Malware Defense	Term-based	File policies (the IPS is also required).
URL	Term-based	URL policies—Category and reputation-based URL filtering or DNS lookup request filtering. You can perform URL filtering on individual URLs without this license.
RA VPN: • Secure Client Advantage • Secure Client Premier • Secure Client VPN Only	Term-based or perpetual based on license type.	Remote access VPN configuration. Your base license must allow export-controlled functionality to configure RA VPN. You select whether you meet export requirements when you register the device. The Firewall Device Manager can use any valid Secure Client license. The available features do not differ based on license type. If you have not already purchased one, see Licensing Requirements for Remote Access VPN. Also see *Cisco AnyConnect Ordering Guide*, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.
Carrier	Term-based	Mobile network protocol inspection. You need this license to configure GTP/GPRS, Diameter, SCTP, and M3UA inspections. Use FlexConfig to configure these inspections.

Firewall Threat Defense Virtual Licensing

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

Performance Tiers for Firewall Threat Defense Virtual Smart Licensing

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

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

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

Firewall Threat Defense Virtual Performance Tier Licensing Guidelines and Limitations

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

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



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

- The default performance tier is FTDv50 when deploying a new Firewall Threat Defense Virtual device, or when provisioning the Firewall Threat Defense Virtual using the REST API.
- Essentials licenses are subscription-based and mapped to performance tiers. Your virtual account needs to have the Essentials license entitlements for the Firewall Threat Defense Virtual devices, as well as for IPS, Malware Defense, and URL Filtering licenses.
- Each HA peer consumes one entitlement, and the entitlements on each HA peer must match, including Essentials license.

- A change in performance tier for an HA pair should be applied to the primary peer.
- 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.

Impact of Export Control Setting on Encryption Features

When you register a device, you must also specify whether to **Allow export-controlled functionality on the products registered with this token**. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.

Evaluation mode is treated the same as registering using a non-export-compliant account. That means that you cannot configure remote access VPN, or use advanced encryption algorithms, when running in evaluation mode.

Most particularly, the DES standard is available only in evaluation or non-export-compliant mode.

Thus, if you configure encrypted features, such as site-to-site VPN, or encrypt the failover connection in a high availability group, you might end up with connection problems after registering in an export-compliant account. If the feature was using DES in evaluation mode, that configuration will be broken after you register the account.

Consider the following recommendations for avoiding encryption-related problems:

- Avoid configuring encrypted features, such as site-to-site VPN and encrypted failover connections, until after you register the device.
- After registering the device using an export-compliant account, edit all encrypted features that you configured in evaluation mode and select more secure encryption algorithms. Test and verify each of these features to ensure they are functioning correctly.



Note If you configured HA failover encryption in evaluation mode, you will also need to reboot both devices in the HA group to start using stronger encryption. We recommend you remove the encryption first to avoid a split-brain situation, where both devices consider themselves the active unit.

Impact of Expired or Disabled Optional Licenses

If one of the following optional licenses expires, you can continue using features that require the license. However, the license is marked out of compliance and you need to purchase the license and add it to your account to bring the license back into compliance.

If you disable an optional license, the system reacts as follows:

- Malware Defense—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 file policies. Note that 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.

- IPS—The system no longer applies intrusion or file policies. For Security Intelligence policies, the system no longer applies the policy and stops downloading feed updates. You cannot re-deploy existing policies that require the license.
- URL—Access control rules with URL category conditions immediately stop filtering URLs or DNS lookup requests, and the system no longer downloads updates to URL data. You cannot re-deploy existing access control policies if they include rules with category and reputation-based URL conditions.
- RA VPN—You cannot edit the remote access VPN configuration, but you can remove it. Users can still connect using the RA VPN configuration. However, if you change the device registration so that the system is no longer export compliant, the remote access VPN configuration stops immediately and no remote users can connect through the VPN.

Managing Smart Licenses

Use the Smart License page to view the current license status for the system. The system must be licensed.

The page shows you whether you are using the 90-day evaluation license, or if you have registered with the Cisco Smart Software Manager. Once registered, you can see the status of the connection to the Cisco Smart Software Manager as well as the status for each type of license.

Usage Authorization identifies the Smart License Agent status:

- Authorized ("Connected," "Sufficient Licenses")—The device has contacted and registered successfully with the License Authority, which has authorized the license entitlements for the appliance. The device is now In-Compliance.
- Out-of-Compliance—There is no available license entitlement for the device. Licensed features continue to work. However, you must either purchase or free up additional entitlements to become In-Compliance.
- Authorization Expired—The device has not communicated with the Licensing Authority in 90 or more days. Licensed features continue to work. In this state, the Smart License Agent retries its authorization requests. If a retry succeeds, the agent enters either an Out-of-Compliance or Authorized state, and begins a new Authorization Period. Try manually synchronizing the device.



Note Click the **i** button next to the Smart License status to view the virtual account, export-controlled features, and get a link to open the Cisco Smart Software Manager. Export-Controlled Features control software that is subject to national security, foreign policy, and anti-terrorism laws and regulations.

The following procedure provides an overview of how to manage licenses for the system.

Before you begin

If you do not have a path to the internet for the system, you cannot use Smart Licensing. Instead, switch to Permanent License Reservation (PLR) mode. For detailed information, see Applying Permanent Licenses, on page 11.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Register the device.

You must register with the Cisco Smart Software Manager before you can assign the optional licenses. Register before the end of the evaluation period.

See Registering the Device, on page 7.

Note
When you register, you elect whether to send usage data to Cisco. You can change your election by clicking the **Go To Cisco Success Network** link next to the gear icon.

Step 3 Request and manage the optional feature licenses.

You must register the optional licenses to use the features controlled by the license. See Enabling or Disabling Optional Licenses, on page 9.

Step 4 Maintain system licensing.

You can do the following tasks:

- Synchronizing with the Cisco Smart Software Manager, on page 10
- Unregistering the Device, on page 10

Registering the Device

Your purchase of the Firewall Threat Defense device automatically includes the Essentials license. The Essentials license covers all features not covered by the optional licenses. It is a perpetual license.

During initial system setup, you are prompted to register the device with Cisco Smart Software Manager. If you instead elected to use the 90-day evaluation license, you must register the device before the end of the evaluation period.

When you register the device, your virtual account allocates the license to the device. Registering the device also registers any optional licenses that you have enabled.

Before you begin

When you register a device, only that device is registered. If the device is configured for high availability, you must log into the other unit in the high availability pair to register that unit.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Click **Register Device** and follow the instructions.

a) Click the link to open the Cisco Smart Software Manager and log into your account, or create a new one if necessary.
b) Generate a new token.

   When you create the token, you specify the amount of time the token is valid for use. The recommended expiration period is 30 days. This period defines the expiration date of the token itself, and has no impact on the device that you register using the token. If the token expires before you can use it, you can simply generate a new token.

   You must also specify whether to **Allow export-controlled functionality on the products registered with this token**. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.

c) Copy and paste the token into the edit box on the Smart License Registration dialog box.
d) (**Firewall Threat Defense Virtual only**) Select a performance tier for your Firewall Threat Defense Virtual device, or leave the default selection.

   When no performance tier is selected, your Firewall Threat Defense Virtual device runs in legacy mode with default settings of 4 cores/8 GB; see Changing the Firewall Threat Defense Virtual Performance Tier, on page 8 for more information.

e) Select your region for Cisco Cloud Services registration.

   After registration, if you need to change this region, you must unregister the device, then register it again and select the new region.

f) Decide whether to send usage data to Cisco.

   Read the information in the Cisco Success Network step, click the **Sample Data** link to view the actual data that is collected, then decide whether to leave the **Enable Cisco Success Network** option selected.

g) Click **Register Device**.

Changing the Firewall Threat Defense Virtual Performance Tier

The Firewall Threat Defense Virtual supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements. Any license can be used on any supported core/memory configuration. This allows the Firewall Threat Defense Virtual customers to run on a wide variety of VM resource footprints; see Performance Tiers for Firewall Threat Defense Virtual Smart Licensing, on page 3.

When you upgrade the Firewall Threat Defense Virtual to version 7.0+, the device is automatically moved to the “FTDv Variable” tier state and continues to consume non-tiered entitlements until you choose the entitlement level.

Keep the following in mind:

- You can change the performance tier to meet your deployment needs based on throughput or RA VPN requirements. Keep in mind that the Firewall Threat Defense Virtual deploys with adjustable core and memory resources. Your selected performance tier should not exceed your device specifications.
- Changing the performance tier is not supported for AWS.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select the desired option from the **Performance Tier** drop-down list.

- FTDv5 (4 core/8 GB)
- FTDv10 (8 core/8 GB)
- FTDv20 (8 core/8 GB)
- FTDv30 (8 core/16 GB)
- FTDv50 (12 core/24 GB)
- FTDv100 (16 core/24 GB)
- FTDvU (unlimited)

Note
The system highlights the optimal tier based on the current device specifications.

Step 3 Review your selection and device specifications.

Note
When configuring the Firewall Threat Defense Virtual VM, the maximum supported number of cores (vCPUs) is 12 (16 for FTDv100 on VMware and KVM); and the maximum supported memory is 24 GB RAM. Your selected performance tier should not exceed your device specifications.

Step 4 Click **YES** to change the performance tier.

Enabling or Disabling Optional Licenses

You can enable (register) or disable (release) optional licenses. You must enable a license to use the features controlled by the license.

If you no longer want to use the features covered by an optional term license, you can disable the license. Disabling the license releases it in your Cisco Smart Software Manager account, so that you can apply it to another device.

You can also enable evaluation versions of these licenses when running in evaluation mode. In evaluation mode, the licenses are not registered with Cisco Smart Software Manager until you register the device. However, you cannot enable the RA VPN or Carrier license in evaluation mode.

Before you begin

Before disabling a license, ensure that you are not using it. Rewrite or delete any policies that require the license.

For units operating in a high availability configuration, you enable or disable licenses on the active unit only. The change is reflected on the standby unit the next time you deploy the configuration, when the standby unit requests (or frees) the necessary licenses. When enabling licenses, you must ensure that your Cisco Smart Software Manager account has sufficient licenses available, or you could have one unit compliant while the other unit is non-compliant.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Click the **Enable/Disable** control for each optional license as desired.

- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.
- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.

Step 3 If you enabled the **RA VPN** license, select the type of license you have available in your account.

Synchronizing with the Cisco Smart Software Manager

The system periodically synchronizes license information with Cisco Smart Software Manager. Normal license communication occurs every 30 days, but with the grace period, your appliance will operate for up to 90 days without calling home.

However, if you make changes in the Cisco Smart Software Manager, you can refresh the authorization on the device so the changes immediately take effect.

Synchronization gets the current status of licenses, and renews authorization and the ID certificate.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select **Resync Connection** from the gear drop-down list.

Unregistering the Device

If you no longer want to use the device, you can unregister it from the Cisco Smart Software Manager. When you unregister, the Essentials license and all optional licenses associated with the device are freed in your virtual account. Optional licenses are available to be assigned to other devices. In addition, the device is unregistered from the cloud and cloud services.

After unregistering the device, the current configuration and policies on the device continue to work as-is, but you cannot make or deploy any changes.

Caution You must use this procedure to unregister the device. If you instead unregister from your Cisco Smart Software Manager account, there will be an inconsistency between the license state on the device and the one in Cisco Smart Software Manager. This will cause errors when you try to license the device again, such as when you form an HA pair. Messages symptomatic of this failure are "Failed to generate token to enroll with Cisco Cloud using Smart License" and "Could not return the certificate for the given sn (*serial_number*) since it is REVOKED." If this happens, unregister the units using this procedure and try again.

Before you begin

When you unregister a device, only that device is unregistered. If the device is configured for high availability, you must log into the other unit in the high availability pair to unregister that unit.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select **Unregister Device** from the gear drop-down list.

Step 3 Read the warning and click **Unregister** if you really want to unregister the device.

Applying Permanent Licenses

You can apply permanent licenses in both non-air-gapped and air-gapped networks. An air-gapped network is one in which there is no path to the Internet. These are high-security networks where you want to prevent any possibility of external entry and attack. Because there is no path to the Internet, you cannot register the device directly with the Cisco Smart Software Manager. Instead, you can use Permanent License Reservation (PLR) mode to obtain a license you can apply to the device.

If you need to use PLR mode, please keep the following in mind:

- Features that require access to the internet, such as file policies, URL Lookups, or contextual cross-launch to public web sites, will not work.
- Even if you enable Web Analytics and Cisco Success Network, Cisco does not collect the associated data due to the lack of internet access.
- You will need to manually upload updates to the Geolocation Database, Intrusion Rules, and Vulnerability Database (VDB). For example, you can download the updates to a flash drive, then take the drive into your secured building and upload them from a secured workstation.

Note Cisco Smart Software Manager uses the device's serial number to assign the permanent license. If you need to unregister the device, and the normal unregistration or cancellation processes fail to remove the license assignment, you will need to contact Cisco Technical Support to remove the registration from Cisco Smart Software Manager. Reimaging the device will not remove the license registration.

The following topics explain more about the different types of permanent license, how to apply them, and how to cancel registration or unregister the device.

Downloading Threat Intelligence with Permanent 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

If you are using regular Smart Licensing, registering with Cisco Smart Software Manager sets up SSE integration. But if you are using Permanent License Reservation in a non-air-gapped deployment, you must instead enable Security Cloud Control. For more information on how to enable Cisco Security Cloud Control, see Enabling or Disabling Security Cloud Control (Legacy Device Manager Mode) or Configuring Cloud Services.

If you have concerns with data sharing, disable all sharing options. But, the Firewall Device Manager must still be able to reach the regional cloud listed in Internet Resources Accessed by the Device.

Note that in air-gapped deployments, you update threat intelligence manually.

Universal Permanent vs. Specific License Reservation

There are two separate types of license reservation:

- Universal Permanent License Reservation (Universal PLR or UPLR)—The Universal Permanent License permits perpetual, unlimited use of supported firewall products, including all optional licenses. Once you purchase and apply a Universal Permanent License, any applied feature licenses, which are normally time-based, are permanently applicable. However, you are still responsible for purchasing replacement licenses as they expire in your Smart License account.
- Specific License Reservation—Specific License Reservation requires the same number and types of licenses as standard Smart Licensing. When you obtain this license, you select which optional feature licenses you want in addition to the base license. You must periodically update your licenses as they expire.

Firewall Device Manager supports Universal PLR only.

You must work with your Cisco representative to enable Universal Permanent License Reservation (PLR) mode in your Cisco Smart Software Manager (CSSM) account.

Verify That Your Smart Account Can Provide a Universal License

To verify that you can obtain and apply a permanent license, log into your CSSM account and go to the **Smart Software Licensing** > **Inventory** page, then click the **Licenses** tab. If you can see the **License Reservation** button, then you are authorized to obtain permanent license reservations.

However, this button starts a wizard that works for both Universal and Specific Permanent Licenses.

You must also look through your list of available licenses to verify that there is a Universal License for the device. This license will appear as a selectable item in step 2 of the wizard launched by the **License Reservation** button.

If you can see the **License Reservation** button and you can get a Universal License, then you can proceed with converting the system to use a permanent license. If the button does not appear, or you can reserve Specific licenses only, call your Cisco representative and request that Universal PLR mode be enabled for your account.

Switch to PLR Mode and Apply a Universal License

Once you verify that you can obtain a permanent license, as explained in Verify That Your Smart Account Can Provide a Universal License, on page 12, and you have purchased the required Universal License, you can switch to Permanent License Reservation (PLR) mode and apply the license.

Caution If you are currently in evaluation mode, once you switch to PLR mode, you cannot switch back to evaluation mode.

Before you begin

If the device is configured for High Availability, you must complete this task separately for both devices in the HA group.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 If you have already registered the device using Smart Licensing, select **Unregister Device** from the gear drop-down list and then confirm unregistration. Wait for the unregistration task to complete before proceeding.

Step 3 Select **Switch to Universal PLR** from the gear drop-down list to switch to Universal Permanent License Reservation (PLR) mode.

Read the warning and click **Yes** to confirm the switch.

The system converts to PLR mode and then starts the PLR registration process.

Step 4 Complete the PLR registration.

a) When the system opens the Universal Permanent License Reservation dialog box, the first step includes the request code you will need. You can click **Save As TXT** to save it in a text file, or **Print** to print it out. You can also highlight the string and press Ctrl+C to copy it to the clipboard.

If you canceled out of the process after switching modes, you can restart at this point by clicking the **Continue Reservation** button on the Licensing page.

b) Log into your CSSM account, go to the **Smart Software Licensing** > **Inventory** page, and click the **Licenses** tab.

c) Click the **License Reservation** button and follow the instructions in the wizard. You will be prompted to enter the request code you generated, and in return, you will get an authorization code.

The wizard includes these steps:

1. Enter the license request code, or upload the text file that contains the code, and click **Next**.

2. In step 2, you are presented with the product details for the system you are licensing, and a bullet list of the available licenses. Select the Universal License for a locally-managed the Firewall Threat Defense device, and click **Next**.
3. In step 3, verify you have the correct license selected, and click **Generate Authorization Code**.
4. In step 4, you are presented with the authorization code. Either click **Download as File** or **Copy to Clipboard**, as appropriate, to save the code.
5. Click **Close** to exit the wizard.

d) Back in the Firewall Device Manager, paste the authorization code into the appropriate field.

A valid authorization code for a Universal License has the following format: XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX, where X is an alpha-numeric character. If your authorization code is instead an XML file, you have a Specific License and you cannot use it on this system. Please cancel the registration as described in Cancel PLR Registration, on page 14, ensuring that you release the reserved licenses in CSSM. Then, work with your Cisco representative to get your Smart Account converted to Universal PLR.

e) Click **Register**.

The system will start the registration process. Refresh the Licensing page to check the registration status.

Step 5 Enable the optional feature licenses as required.

The Universal License registers the device for the Essentials license only. You can now click **Enable** for each of the feature licenses you need.

Cancel PLR Registration

You can cancel a Universal Permanent License Reservation (PLR) request before it is completed. For example, if you start the PLR registration process, and discover that your Smart Software Manager account is not set up for PLR, you can cancel the process while you get the authorization for PLR mode and your Smart License account is set up appropriately.

If you have completed the PLR registration process, you cannot cancel it. Instead, see Unregister the Device in PLR Mode, on page 15.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select **Cancel PLR** from the gear drop-down list to start the cancellation process.

Step 3 Select the option that fits your situation:

- **I have a license in CSSM**—Use this option if you have gone through the License Registration wizard in the Cisco Smart Software Manager (CSSM) and you have obtained an authorization code. At this point, there are licenses reserved in CSSM, and you need to release them.

- **I do not have a license in CSSM**—Use this option if you have not completed the CSSM wizard to the point where you obtained an authorization code. For example, if you started PLR registration in Firewall Device Manager but then discovered the **License Reservation** button was not available in your Smart Account.

Step 4 (If you selected **I have a license in CSSM**.) You need to obtain a release code from CSSM to ensure that your licenses are no longer marked as in-use. Otherwise, those licenses will not be usable by other devices.

a) Paste the authorization code you obtained from CSSM (when registering) into the cancellation dialog box and click **Generate Release Code**.
b) When there is a code in the **Release License Code** field, click **Save As TXT** to save it to a text file, or **Print** to print it. You can also select the code and press Ctrl+C to copy it to the clipboard.
c) In CSSM, find the device in the **Smart Software Licensing** > **Inventory** page (the Name is the device serial number), click **Action** > **Remove**, and enter the release code.

   Wait for CSSM to indicate that the product was successfully removed.

Step 5 Click **OK** to complete the cancellation process.

The system returns to Smart License mode. However, the device will be unregistered, and you cannot restart evaluation mode. At this point, you must register the device using a Smart License, or switch back to PLR mode and register again, to use it.

Unregister the Device in PLR Mode

If you no longer need to license the device, for example, because you are decommissioning it or moving it to a different facility, where you will license it separately, you can unregister the device.

Unregistering the device returns the license to an unused state. If you do not unregister the device, the license remains marked as in-use and you cannot use it for other purposes.

Procedure

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select **Unregister Universal PLR** from the gear drop-down list, read the warning, and click **Yes** to start the process.

Step 3 When the Unregister Universal Permanent License Reservation dialog box opens, the **Release License Code** field is populated with the code you need to release the licenses currently assigned in your CSSM account. Click **Save as TXT** or **Print** to retain a copy of this code. You can also select it and use Ctrl+C to copy it to the clipboard.

Step 4 Go to your CSSM account, find the device in the **Smart Software Licensing** > **Inventory** page (the Name is the device serial number), click **Action** > **Remove**, and enter the release code.

Wait for CSSM to indicate that the product was successfully removed.

Step 5 Back in the Firewall Device Manager, click **Unregister** in the Unregister Device dialog box.

This completes the process. At this point, the licenses in CSSM are free to assign to another device, and the Firewall Threat Defense device is unlicensed.