

Securing Networks with
Cisco FTD

Chapter 3

Licensing and Registration

Mohsen Kheradmand

Cisco Licensing Architecture

The Cisco Secure Firewall supports both **smart licensing** and **classic licensing** models

	classic licensing	smart licensing
Supervision	Provides a limited view. You are unable to view all of the licenses that are owned and used by your company	Provides a complete view. You can view the usages of all of your licenses and devices from a single portal in real time
Scope	Device-specific licensing. Licenses are specific to only one device.	Company-specific licensing. You can apply licenses across any applicable devices in your company.
Activation	A PAK is required to unlock and register a device.	A PAK is not required to complete registration (Product Activation Key)

You can manage the smart licenses of your company using the Cisco Smart Software Manager (SSM)
SSM : cloud-based web application at cisco.com

Cisco Licensing Architecture

Cisco Smart Software Manager
(SSM) cloud

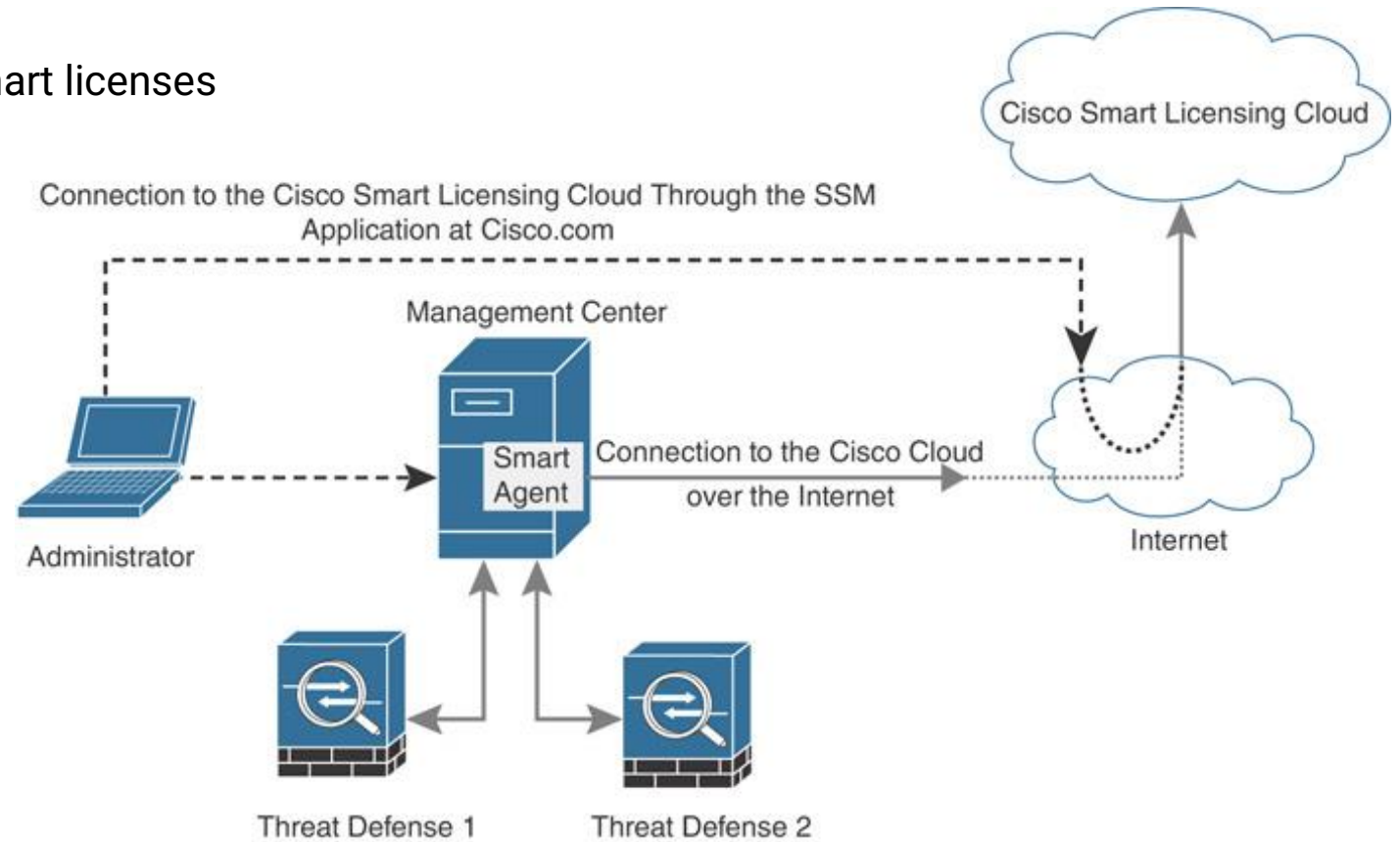
The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The top navigation bar includes the Cisco logo, a search icon, and a language selector (US/EN). The main header displays 'Cisco Software Central > Smart Software Licensing' and 'Smart Software Licensing' with links for Feedback, Support, and Help. A secondary navigation bar contains links for Alerts, Inventory, Convert to Smart Licensing, Reports, Preferences, On-Prem Accounts, and Activity. The main content area is titled 'Virtual Account: Cisco' and features four tabs: General, Licenses, Product Instances, and Event Log. The 'General' tab is active, showing the 'Virtual Account' details: Description (Cisco Secure Firewall) and Default Virtual Account (No). Below this is the 'Product Instance Registration Tokens' section, which includes a note about using registration tokens and a 'New Token...' button. A black arrow points to this button. At the bottom, a table lists the registration tokens.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
OGY1N2E4NWYL	2022-Aug-03 23:32:01...		Allowed	Cisco Secure Firewall	nrajib	Actions

Cisco Licensing Architecture

Cisco offers different architectures to enable smart licenses

- Direct cloud access
- On-premises server
- Offline access

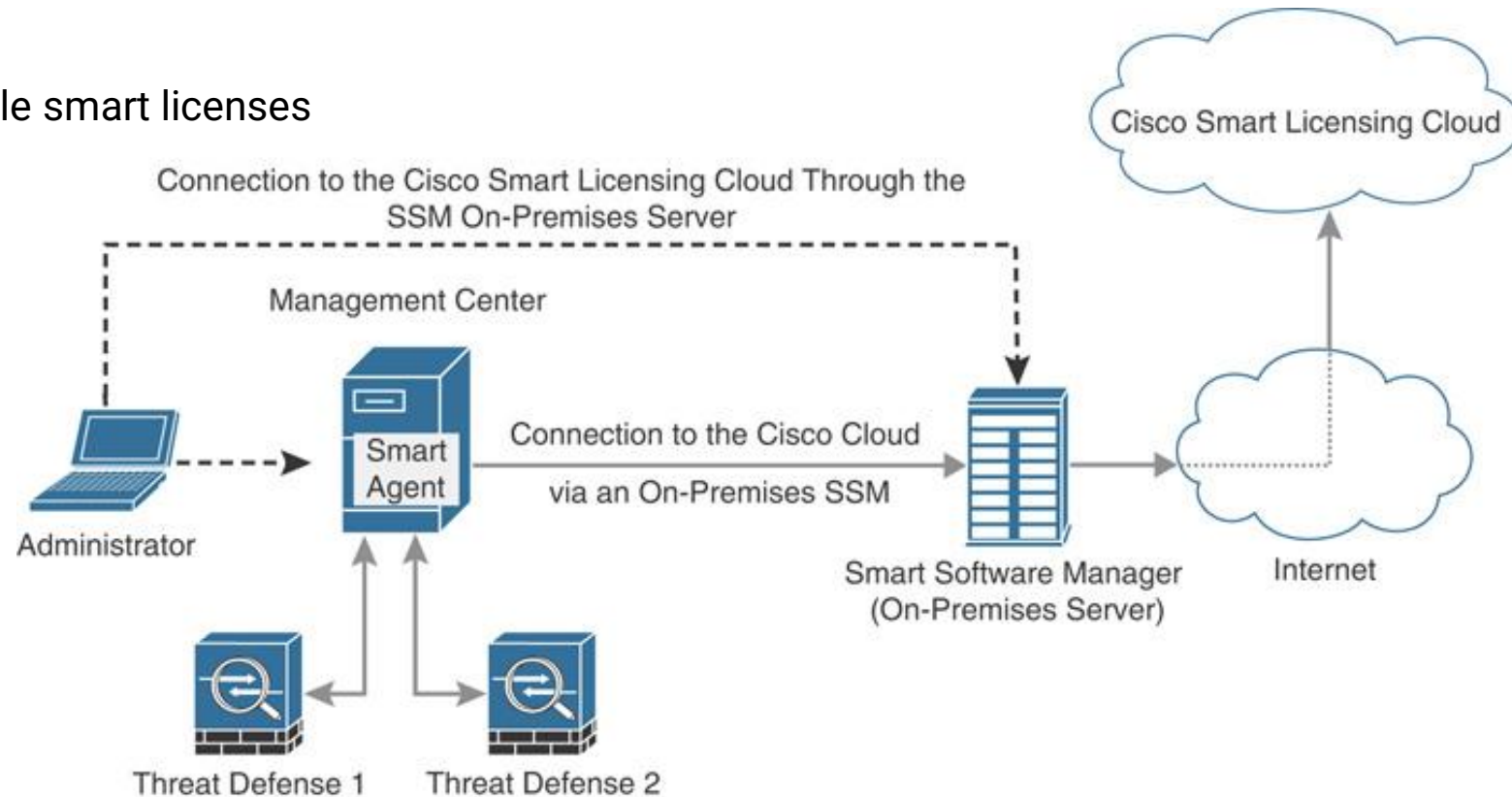


- 1) Manager connects to the cloud directly over the Internet or via a proxy server.
- 2) After a successful registration, the Cisco cloud issues an ID certificate
- 3) The Smart Agent process uses this certificate to communicate with the Cisco cloud

Cisco Licensing Architecture

Cisco offers different architectures to enable smart licenses

- Direct cloud access
- On-premises server
- Offline access



Smart Software Manager On-Prem Configuration

☐ Connect directly to Cisco Smart Software Manager

☒ Connect to Cisco Smart Software Manager On-Prem Server

URL

SSL Certificate

+

Apply

- No direct access to internet via FMC
- An on-premises version of the Cisco SSM server deployed from an OVA image
- This server is registered to the Cisco Smart Licensing Cloud through the Internet

Cisco Licensing Architecture

Cisco offers different architectures to enable smart licenses

- Direct cloud access
- On-premises server
- Offline access :

This is known as **Permanent License Reservation (PLR)**.

- ✓ No need to connect to the Cisco SSM cloud application
- ✓ You can manually copy and paste licensing information between the management center and cisco.com

The PLR model offers two options for license reservation:

- **SLR: Specific License Reservation** (for a specific limited period)
- **UPLR : Universal Permanent License Reservation** (for an unlimited term)

Universal Permanent License Reservation

[?](#) [×](#)

i If you have **Cloud Services enabled** you might want to disable them.

- 1 Save Request Code for this Device.
↓
Request Code

CB-ZNGFWv:9APHW9AFG29-BxbkYu4wT-53

SAVE AS TXT

PRINT
- 2 Log into your [Cisco Smart Software Manager](#) account, go to the Inventory > Licenses page, and start the License Reservation process. Use the request code to generate an Authorization Code. Note that you must work with your Cisco representative to enable Universal Permanent License Reservation mode in your account. If you cannot start the License Reservation process (that is, the button does not appear on the Inventory > License page), please contact your Cisco representative.
- 3 Paste or type in the Authorization Code:
Authorization Code

Paste code from clipboard here

CANCEL

REGISTER

Cisco Licensing Architecture

Activate **SLR** or **PLR**

- Connect to the FMC CLI (directly or via SSH)
 - Enter to the **Expert** mode
 - Type **Sudo MANAGE_PLR.PL**
 - Select **2** to enable PLR mode
-
- You can do this steps for **SLR license**

Permanent License Reservation

Permanent License Reservation or PLR allows us to reserve and install licenses in a network that has no path to inbound or outbound internet traffic at all

1

Generate a request code

3331-11f0-8373-cb54791dcb2e-AssRatmKa-DD

Generate

Cancel Code

2

Create or login into your **Cisco Smart Software Manager** account to generate an authorization code against the request code you have just created

3

Put the authorization code and Install

Install

Cisco Licensing Architecture

Feature License

Base :

- ✓ Update the system
- ✓ Control applications and users
- ✓ Perform switching, routing, and NAT

No separate purchase; included automatically during a device purchase

Expiry : Permanent

Threat :

- ✓ Detect and prevent intrusion attempts
- ✓ Blacklist traffic based on intelligence
- ✓ Block transfer of certain types of files

T: Threat license only

Expiry : term based

Malware :

- ✓ Protect the network from malware, and enable malware defense feature (formerly AMP for networks and AMP Threat Grid)

M: Threat and malware licenses in a bundle

AMP: Malware license only

Expiry : term based

URL filtering :

- ✓ Filter URLs based on reputation and category

TMC: Threat, Malware, & URL filtering licenses in a bundle

URL: URL filtering license only

Expiry : term based

Note : a Threat license is a prerequisite for Malware and URL Filtering

Cisco Licensing Architecture

Export-Controlled License

- The export-controlled functionalities utilize strong encryption
- A popular application of encryption is Remote Access Virtual Private Network (RAVPN)
- To establish RAVPN you also need AnyConnect license

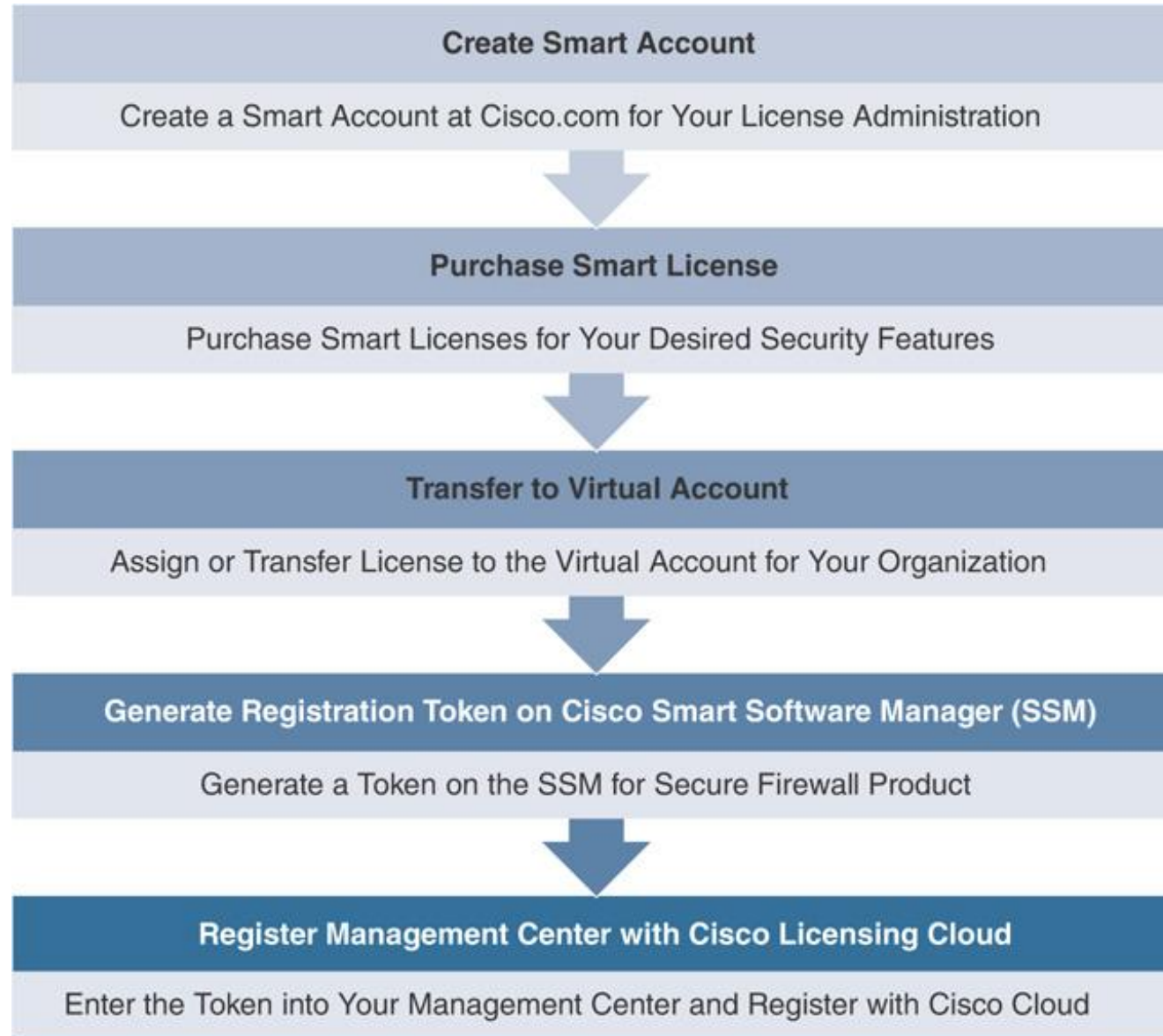
The screenshot displays the 'Create Registration Token' dialog within the Cisco Software Central interface. The dialog includes the following fields and options:

- Virtual Account:** Cisco
- Description:** A text input field with the placeholder 'Description'.
- Expire After:** 30 Days. A note below indicates 'Between 1 - 365, 30 days recommended'.
- Max. Number of Uses:** An empty text input field. A note below states 'The token will be expired when either the expiration or the maximum uses is reached'.
- Allow export-controlled functionality on the products registered with this token:** This checkbox is checked, and a black arrow points to it from the left.

At the bottom right of the dialog are two buttons: 'Create Token' (in blue) and 'Cancel' (in gray).

Cisco Licensing Architecture

General Workflow of Smart License



Device Registration

In FTD

You can change management IP address of FTD via CLI (in case you need)

`“ configure network ipv4 manual <mgmt0 IP> <netmask> <gateway> management0 ”`

For example : Configure network IPv4 manual 192.168.1.200 255.255.255.0 192.168.1.1 management0

- Specify the manager in the FTD
 - Enter the IP address of FMC and registration key (password)
`“ configure manager add <FMC IP > <registration key> ”`
For example : configure manager add 192.168.1.250 P@ssw0rd

Note : as you configure manager IP , FDM will be disabled

To configure FTD locally via FDM , enter this commands:

- ✓ Configure manager delete
- ✓ Configure manager local

Device Registration

Log Into FMC

 Firepower Management Center

Devices / Device Management

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligence

Deploy 🔍 ✓ ⚙️ ? Kheradmand ▼

View By:

Group ▼

[Deployment History](#)

All (0) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (0) ● Deployment Pending (0) ● Upgrade (0)

🔍 Search Device

Add ▼

[Collapse All](#)

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy
☐	Ungrouped (0)					

Device

High Availability

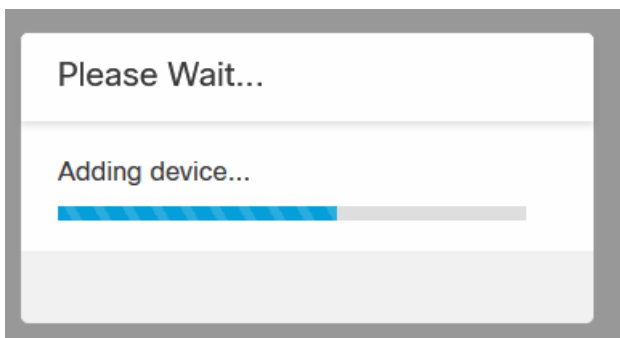
Stack

Group

- Under Device
- Click Add / Device

Device Registration

- Enter the IP address of the FTD
- Type a name for that FTD
- Enter registration key (you entered in last stage)
- Group (optional)
- Access control policy : create a new one
- Select Tier : if you are registering virtual FTD
- Enable Malware , Threat , URL Filtering (license based)
- NAT ID (optional) : if there is NAT between FMC & FTD
- Click register



Add Device

Host: +
172.16.1.201

Display Name:
FTD1

Registration Key: *
.....

Group:
EVE

Access Control Policy: *
Default policy

Smart Licensing

Note: All virtual FTDs require a performance tier license. 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. Click [here](#) for information about the FTD performance-tiered licensing. Until you choose a tier, your FTDv defaults to the FTDv50 selection.

Performance Tier (only for FTDv 7.0 and above):
FTDv10 - Tiered (Core 4 / 8 GB)

☒ Malware
☒ Threat
☒ URL Filtering

Advanced

Unique NAT ID: +

☒ Transfer Packets

Cancel Register

New Policy

Name:
Default

Description:
Default policy , All denied

Select Base Policy:
None

Default Action:
☒ Block all traffic
☐ Intrusion Prevention
☐ Network Discovery

Cancel Save

Device Registration

NAT ID (optional) : if there is NAT between FMC & FTD

- Specify a unique NAT ID on both sides
- But just specify FMC ip address on FTD (you don't need to enter FTD ip address to into FMC)

