

# 使用FMC和FTD智慧授權註冊和常見問題疑難排解

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [背景資訊](#)

### [FMC 智慧型授權註冊](#)

[必要條件](#)

[FMC 智慧型授權註冊](#)

[Smart Software Manager \(SSM\) 端的確認](#)

[FMC 智慧型授權取消註冊](#)

### [RMA](#)

### [疑難排解](#)

### [常見問題](#)

[案例研究1.無效令牌](#)

[案例研究2.無效的DNS](#)

[案例研究3.時間值無效](#)

[案例研究4.無訂閱](#)

[案例研究5.不合規\(OOC\)](#)

[案例研究6.無強加密](#)

### [附加說明](#)

[設定智慧型授權狀態的通知](#)

[從FMC獲取運行狀況警報通知](#)

[相同智慧型帳戶的多個 FMC](#)

[FMC 必須維持網路連線](#)

[部署多個 FMCv](#)

### [常見問題\(FAQ\)](#)

### [相關資訊](#)

---

## 簡介

本文檔介紹Firepower威脅防禦託管裝置上的Firepower管理中心的智慧許可證註冊配置。

## 必要條件

## 需求

本文件沒有特定需求。

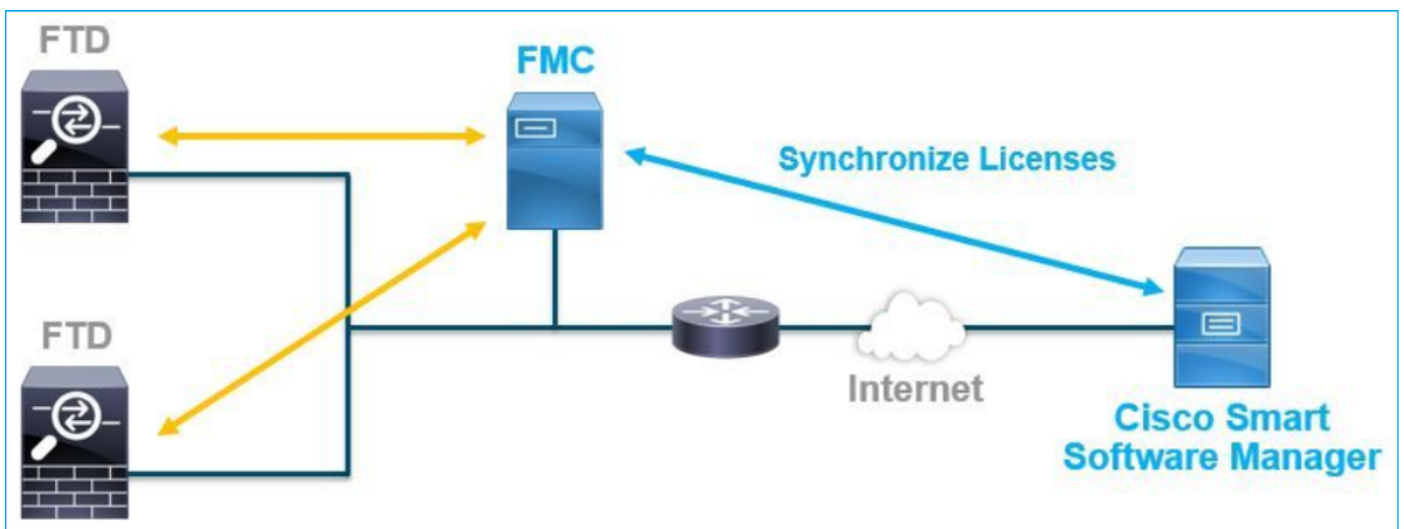
## 採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

FMC、FTD和智慧授權註冊。

在Firepower管理中心(FMC)上執行智慧許可證註冊。FMC 會透過網際網路與 Cisco Smart Software Manager (CSSM) 入口網站通訊。在CSSM中，防火牆管理員管理智慧帳戶及其許可證。FMC可以自由為託管Firepower威脅防禦(FTD)裝置分配許可證和刪除許可證。換句話說，FMC集中管理FTD裝置的許可證。



若要使用 FTD 裝置的特定功能，則必須具有額外授權。[FTD License Types and Restrictions](#)中記錄了客戶可以分配給FTD裝置的智慧許可證型別。

基本許可證包含在FTD裝置中。當FMC註冊到CSSM時，此許可證會自動註冊到您的智慧帳戶。基於期限的許可證：威脅、惡意軟體和URL過濾是可選的。若要使用與許可證相關的功能，需要將許可證分配給FTD裝置。

若要將Firepower管理中心虛擬(FMCv)用於FTD管理，FMCv還需要在CSSM中使用Firepower MCv裝置許可證。

FMCv 授權已包含於軟體中，且永久有效。

此外，本文檔還提供了一些方案，幫助對常見的許可證註冊錯誤進行故障排除。

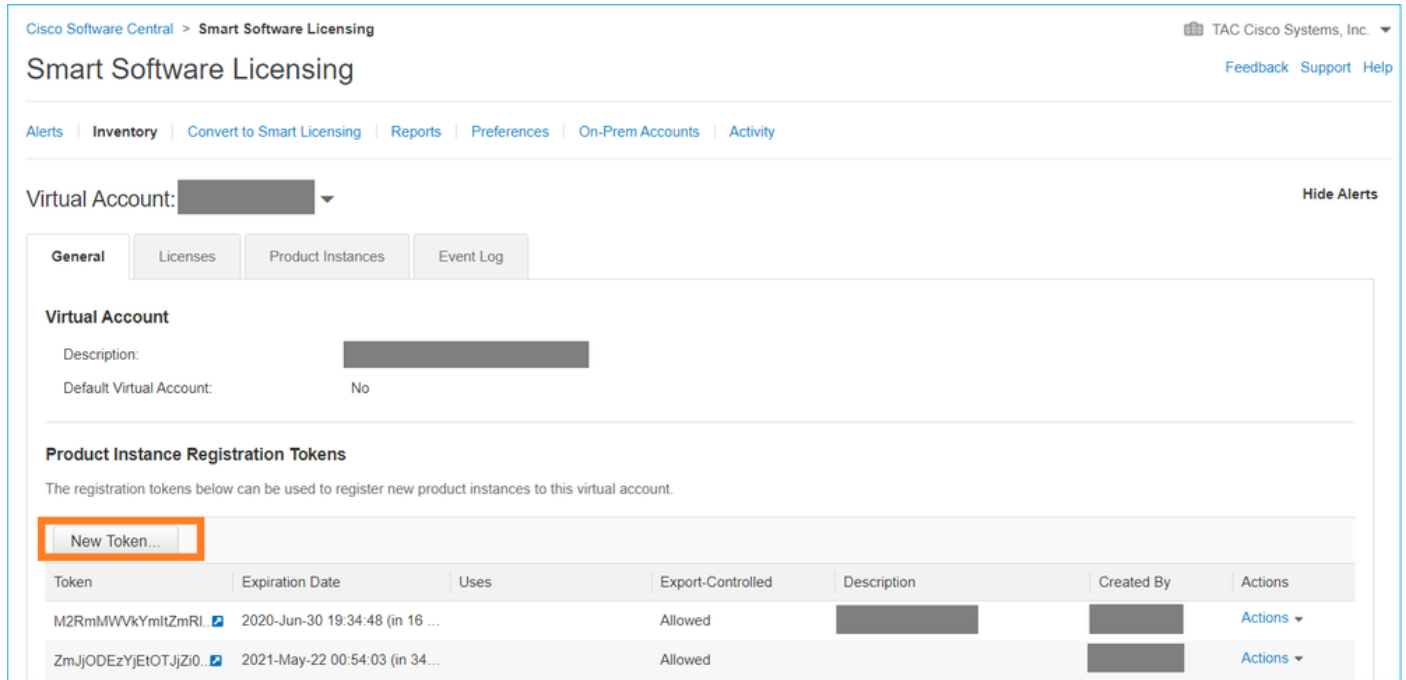
如需有關授權的詳細資料，請查看 [Cisco Firepower System 功能授權](#)和 [Firepower 授權相關常見問題 \(FAQ\)](#)。

# FMC 智慧型授權註冊

## 必要條件

1.對於智慧許可證註冊，FMC必須訪問Internet。由於憑證是在FMC和使用HTTPS的智慧授權雲之間交換，因此請確保路徑中不存在可影響/修改通訊的裝置。（例如，防火牆、代理、SSL解密裝置等）。

2.訪問CSSM並從庫存>常規>新建令牌按鈕發出令牌ID，如下圖所示。



Cisco Software Central > Smart Software Licensing TAC Cisco Systems, Inc. Feedback Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: [Redacted] Hide Alerts

General Licenses Product Instances Event Log

**Virtual Account**

Description: [Redacted]

Default Virtual Account: No

**Product Instance Registration Tokens**

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
M2RmMWVkymltZmRI. [lock]	2020-Jun-30 19:34:48 (in 16 ...)		Allowed	[Redacted]	[Redacted]	Actions
ZmJjODEzYjEtOTJjZi0. [lock]	2021-May-22 00:54:03 (in 34...)		Allowed		[Redacted]	Actions

要使用強加密，請在使用此令牌註冊的產品上啟用Allow export-controlled功能。啟用時，覈取方塊中顯示一個複選標籤。

3.選擇建立令牌。

## Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:

\* Expire After:  Days  
*Between 1 - 365, 30 days recommended*

Max. Number of Uses:

*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 ?

## FMC 智慧型授權註冊

導覽至FMC上的System > Licenses > Smart Licenses，然後選擇Register按鈕，如下圖所示。

Firepower Management Center  
 System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects AMP Intelligence

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register

Smart License Status

Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--
Cisco Success Network:	--
Cisco Support Diagnostics:	--

在「Smart Licensing Product Registration」視窗中輸入令牌ID，然後選擇Apply Changes，如下圖所示。

## Smart Licensing Product Registration

Product Instance Registration Token:

OWI4Mzc5MTAtNzQwYi00YTVILTkyNTktMGMxNGJIYmRmNDUwLTE1OTQ3OTQ5%  
0ANzc3ODB8SnVXc2tPaks4SE5Jc25xTDkySnFYempTZnJEWVdVQU1SU1NiOWFM

If you do not have your ID token, you may copy it from your Smart Software manager The under the assigned virtual account. [Cisco Smart Software Manager](#)

Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.

### Cisco Success Network

The Cisco Success Network provides usage information and statistics to Cisco. This information allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [sample data](#) that will be sent to Cisco.

Enable Cisco Success Network

### Cisco Support Diagnostics

The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration and operational health data from your devices and process that data through our automated problem detection system, and proactively notify you of issues detected. To view a sample

Internet connection is required.

Cancel

Apply Changes

如果智慧許可證註冊成功，則「產品註冊」狀態顯示Registered，如下圖所示。

The screenshot shows the Cisco Smart Software Manager (SSM) interface. At the top, there is a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The main content area is divided into two sections:

- Smart License Status:** A table showing the status of various license components:
 

Usage Authorization:	Authorized (Last Synchronized On Jun 15 2020)
Product Registration:	Registered (Last Renewed On Jun 15 2020)
Assigned Virtual Account:	[Redacted]
Export-Controlled Features:	Enabled
Cisco Success Network:	Enabled ⓘ
Cisco Support Diagnostics:	Disabled ⓘ
- Smart Licenses:** A table showing the status of different license types:
 

License Type/Device Name	License Status	Device Type	Domain	Group
> Base (5)	✓			
Malware (0)				
Threat (0)				
URL Filtering (0)				

若要將期限型授權指派至 FTD 裝置，請選取「編輯」授權。接著，選取並將託管裝置新增至「使用授權的裝置」區段。最後，選擇Apply按鈕，如下圖所示。

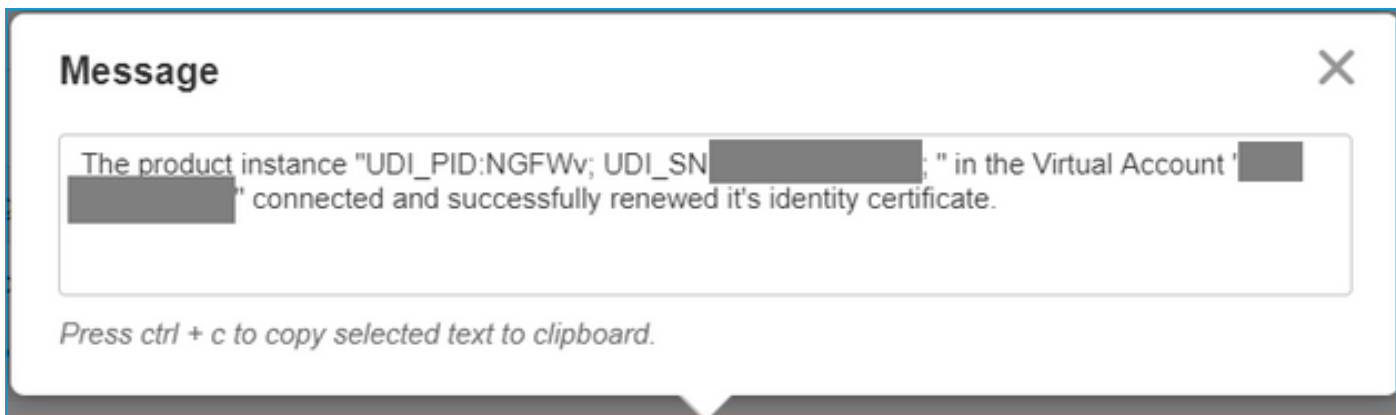
The screenshot shows the 'Edit Licenses' interface. At the top, there are tabs for Malware, Threat, URL Filtering, AnyConnect Apex, AnyConnect Plus, and AnyConnect VPN Only. The main content area is divided into two sections:

- Devices without license:** A search bar and a list of devices. One device, 'FTD', is highlighted with an orange box and labeled '1'.
- Devices with license (1):** A list of devices. One device, 'FTD', is highlighted with an orange box and labeled '2'.

At the bottom right, there are two buttons: 'Cancel' and 'Apply'. The 'Apply' button is highlighted with an orange box and labeled '3'.

## Smart Software Manager (SSM) 端的確認

FMC智慧許可證註冊成功與否可在CSSM中的清單>事件日誌中確認，如下圖所示。

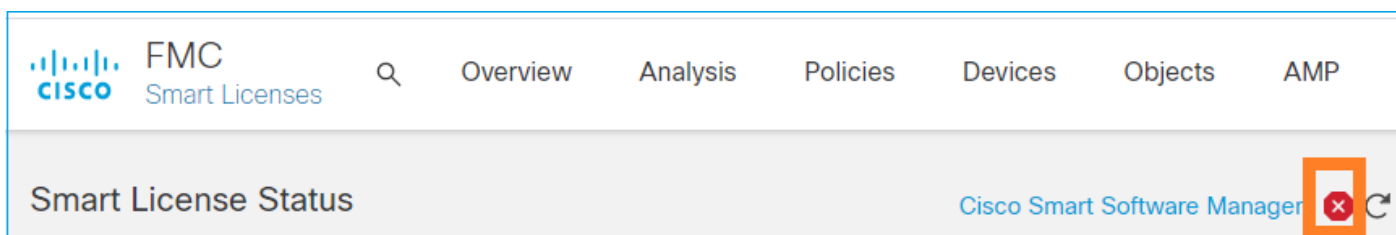


FMC的註冊狀態可以通過庫存>產品例項確認。從Event Log (事件日誌) 頁籤檢查事件日誌。可從Inventory > Licenses頁籤檢查智慧許可證註冊和使用狀態(Smart License registration and use status)。驗證購買的基於期限的許可證是否正確使用，以及沒有表示許可證不足的警報。

## FMC 智慧型授權取消註冊

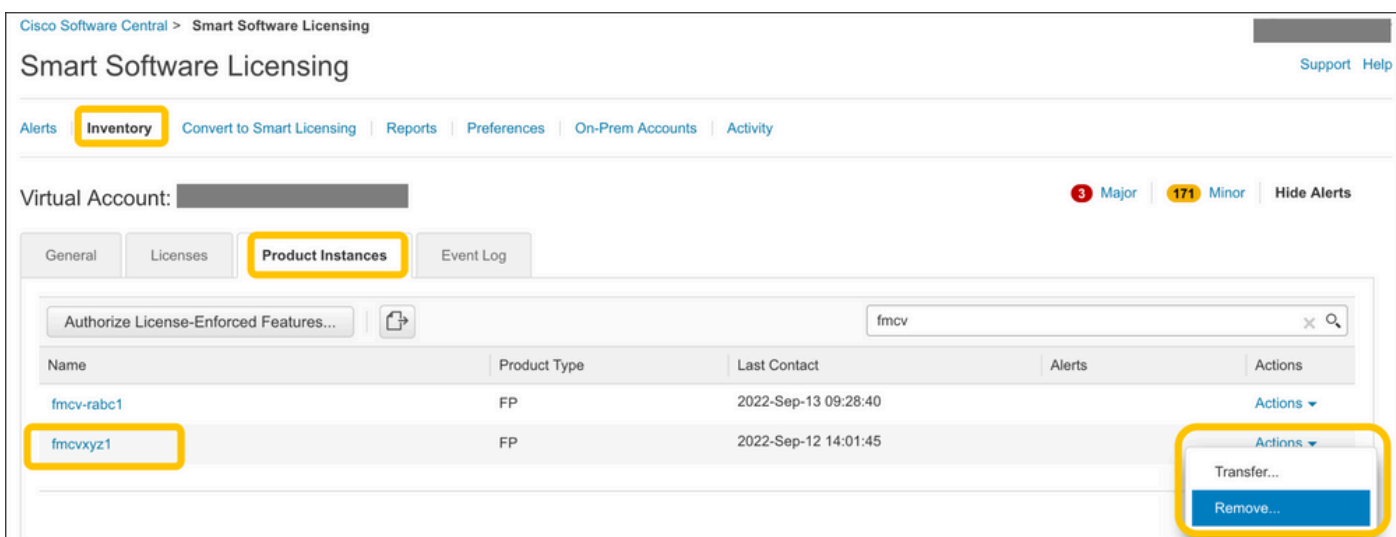
從Cisco SSM註銷FMC

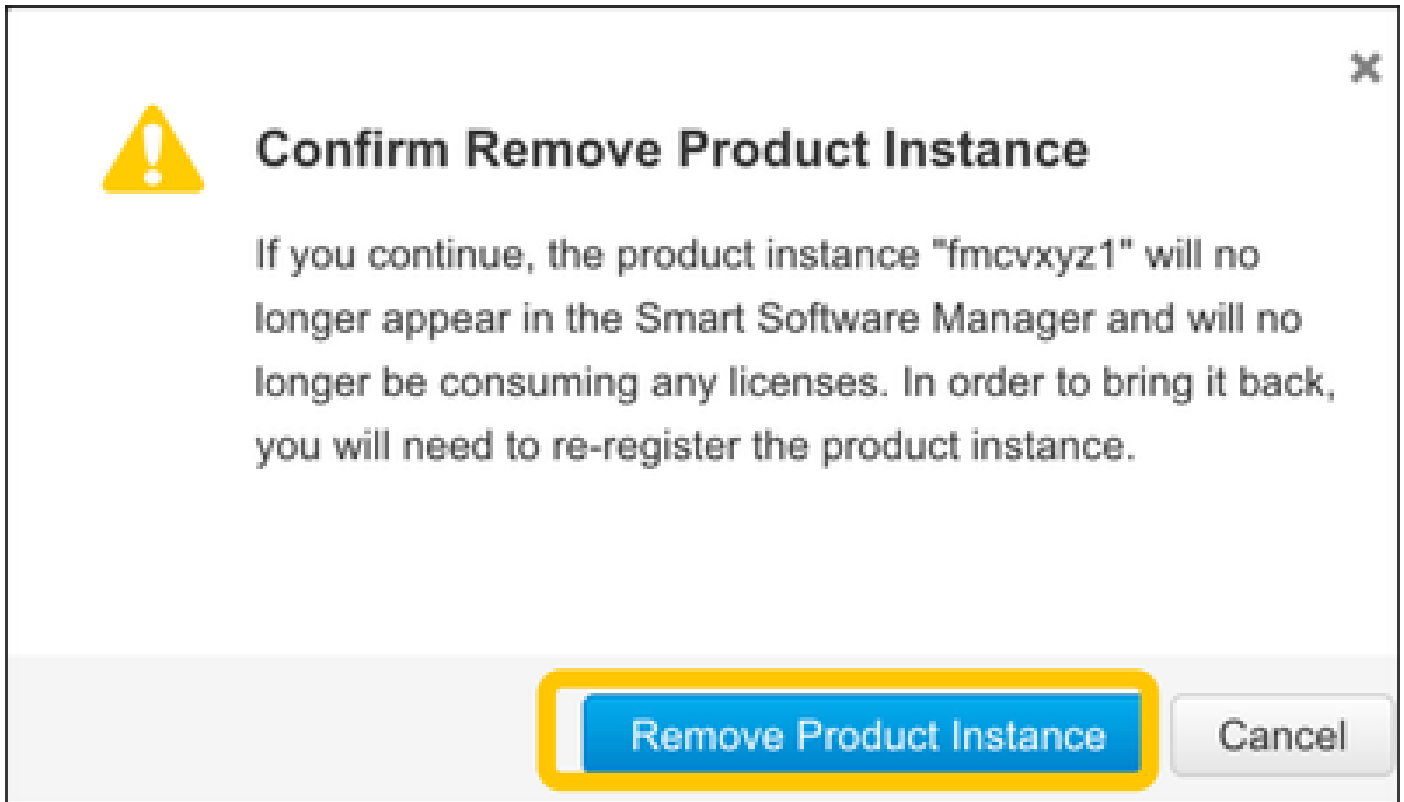
若要由於某種原因釋放許可證或使用其他令牌，請導航到System > Licenses > Smart Licenses，然後選擇de-register按鈕，如下圖所示。



從 SSM 端移除註冊

訪問智慧軟體管理器([Cisco Smart Software Manager](#))，並從清單>產品例項中選擇目標FMC上的刪除。然後選擇Remove Product Instance以刪除FMC並釋放分配的許可證，如下圖所示。





## RMA

如果FMC是RMA'd，請使用FMC智慧許可證取消註冊>從SSM端刪除註冊部分中的步驟從Cisco Smart Software Manager(CSSM)中註銷FMC，然後使用FMC智慧許可證註冊部分中的步驟向CSSM重新註冊FMC。

## 疑難排解

### 時間同步驗證

訪問FMC CLI ( 例如SSH )，並確保時間正確且與受信任的NTP伺服器同步。由於證書用於智慧許可證身份驗證，因此FMC具有正確的時間資訊非常重要：

```
<#root>
```

```
admin@FMC:~$
```

```
date
```

```
Thu
```

```
Jun 14 09:18:47 UTC 2020
```

```
admin@FMC:~$
```

```
admin@FMC:~$
```

```
ntpq -pn
```

```
remote          refid          st t when poll reach  delay  offset  jitter
```

```
=====
```



```
*10.0.0.2      171.68.xx.xx    2 u  387 1024 377    0.977    0.469    0.916
127.127.1.1   .SFCL.          13 l   -   64    0    0.000    0.000    0.000
```

在FMC UI中，從System > Configuration > Time Synchronization驗證NTP伺服器值。

啟用 tools.cisco.com 的「名稱解析」與「檢查連線能力」

確保FMC可以解析FQDN並且可以訪問tools.cisco.com:

```
<#root>
```

```
>
```

```
expert
admin@FMC2000-2:~$
```

```
sudo su
```

```
Password:
root@FMC2000-2:/Volume/home/admin# ping tools.cisco.com
PING tools.cisco.com (173.37.145.8) 56(84) bytes of data.
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=1 ttl=237 time=163 ms
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=2 ttl=237 time=163 ms
```

在FMC UI中，從System > Configuration > Management Interfaces驗證管理IP和DNS伺服器IP。

驗證從 FMC 連線至 tools.cisco.com 的 HTTPS (TCP 443) 存取權

使用Telnet或curl命令確保FMC對tools.cisco.com具有HTTPS訪問許可權。如果TCP 443通訊中斷，請驗證它未被防火牆阻止，並且路徑中沒有SSL解密裝置。

```
<#root>
```

```
root@FMC2000-2:/Volume/home/admin#
```

```
telnet tools.cisco.com 443
```

```
Trying 72.163.4.38...
```

```
Connected to tools.cisco.com.
```

```
Escape character is '^['.
```

```
^CConnection closed by foreign host.
```

```
<--- Press Ctrl+C
```

Curl 測試：

```
<#root>
```

```
root@FMC2000-2:/Volume/home/admin#
```

```
curl -vvk https://tools.cisco.com
```

```
*
```

```
Trying 72.163.4.38...
```

```
* TCP_NODELAY set
```

```
* Connected to tools.cisco.com (72.163.4.38) port 443 (#0)
```

```
* ALPN, offering http/1.1
```

```
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
```

```
* successfully set certificate verify locations:
```

```
* CAfile: /etc/ssl/certs/ca-certificates.crt
```

```
CApath: none
```

```
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
```

```
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
```

```
* TLSv1.2 (IN), TLS handshake, Server hello (2):
```

```
* TLSv1.2 (IN), TLS handshake, Certificate (11):
```

```
* TLSv1.2 (IN), TLS handshake, Server finished (14):
```

```
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
```

```
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
```

```
* TLSv1.2 (OUT), TLS handshake, Finished (20):
```

```
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
```

```
* TLSv1.2 (IN), TLS handshake, Finished (20):
```

```
* SSL connection using TLSv1.2 / AES128-GCM-SHA256
```

```
* ALPN, server accepted to use http/1.1
```

```
* Server certificate:
```

```
* subject: C=US; ST=CA; L=San Jose; O=Cisco Systems, Inc.; CN=tools.cisco.com
```

```
* start date: Sep 17 04:00:58 2018 GMT
```

```
* expire date: Sep 17 04:10:00 2020 GMT
```

```
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
```

```
* SSL certificate verify ok.
```

```
> GET / HTTP/1.1
```

```
> Host: tools.cisco.com
```

```
> User-Agent: curl/7.62.0
```

```
> Accept: */*
```

```
>
```

```
< HTTP/1.1 200 OK
```

```
< Date: Wed, 17 Jun 2020 10:28:31 GMT
```

```
< Last-Modified: Thu, 20 Dec 2012 23:46:09 GMT
```

```
< ETag: "39b01e46-151-4d15155dd459d"
```

```
< Accept-Ranges: bytes
```

```
< Content-Length: 337
```

```
< Access-Control-Allow-Credentials: true
```

```
< Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
```

```
< Access-Control-Allow-Headers: Content-type, fromPartyID, inputFormat, outputFormat, Authorization, Co
```

```
< Content-Type: text/html
```

```
< Set-Cookie: CP_GUTC=10.163.4.54.1592389711389899; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain
```

```
< Set-Cookie: CP_GUTC=10.163.44.92.1592389711391532; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain
```

```
< Cache-Control: max-age=0
```

```
< Expires: Wed, 17 Jun 2020 10:28:31 GMT
```

```
<
```

```
<html>
```

```
<head>
```

```
<script language="JavaScript">
```

```
var input = document.URL.indexOf('intellishield');
```

```
if(input != -1) {
```

```
    window.location="https://intellishield.cisco.com/security/alertmanager/";
```

```
}
```

```
else {
```

```
window.location="http://www.cisco.com";
};

</script>
</head>

<body>
<a href="http://www.cisco.com">www.cisco.com</a>
</body>
</html>
* Connection #0 to host tools.cisco.com left intact
root@FMC2000-2:/Volume/home/admin#
```

## DNS 驗證

驗證是否成功解析到tools.cisco.com:

```
<#root>

root@FMC2000-2:/Volume/home/admin#

nslookup tools.cisco.com

Server:          192.0.2.100
Address:         192.0.2.100#53

Non-authoritative answer:

Name:   tools.cisco.com
Address: 72.163.4.38
```

## Proxy 驗證

如果使用apProxy，請檢查FMC和代理伺服器端上的值。在FMC上，檢查FMC是否使用正確的代理伺服器IP和埠。

```
<#root>

root@FMC2000-2:/Volume/home/admin#

cat /etc/sf/smart_callhome.conf

KEEP_SYNC_ACTIVE:1
PROXY_DST_URL:https://tools.cisco.com/its/service/oddce/services/DDCEService

PROXY_SRV:192.0.xx.xx

PROXY_PORT:80
```

在FMC UI中，代理值可從System > Configuration > Management Interfaces確認。

如果FMC端值正確，請檢查代理伺服器端值(例如，如果代理伺服器允許從FMC和tools.cisco.com進行存取)。此外，允許流量和憑證透過 Proxy 交換。FMC 會使用憑證進行智慧型授權註冊。)

## 到期權杖 ID

驗證頒發的令牌ID是否未過期。如已到期，請要求 Smart Software Manager 管理員發行新的權杖，然後向智慧型授權重新註冊新的權杖 ID。

## 變更 FMC 閘道

在某些情況下，由於中繼代理或SSL解密裝置的影響，智慧許可證身份驗證無法正確執行。如果可能，請更改FMC Internet訪問的路由以避免這些裝置，並重試智慧許可證註冊。

## 檢查 FMC 的健康狀況事件

在FMC上，導航到System > Health > Events，然後檢查智慧許可證監視器模組的狀態是否有錯誤。例如，如果連線由於證書過期而失敗，則會生成一個錯誤，如id certificated expired，如下圖所示。

Module Name	Test Name	Time	Description	Value	Units	Status	Domain	Device
Smart License Monitor	Smart License Monitor	2020-06-17 13:48:55	Smart License usage is out of compliance.	0	Licensess	!	Global	FMC2000-2
Appliance Heartbeat	Appliance Heartbeat	2020-06-17 13:48:55	Appliance mzafeiro_FP2110-2 is not sending heartbe...	0		!	Global	FMC2000-2

## 檢查SSM端上的事件日誌

如果FMC可以連線到CSSM，請在清單>事件日誌中檢查連線的事件日誌。檢查CSSM中是否存在此類事件日誌或錯誤日誌。如果FMC站點的值/操作沒有問題，並且CSSM端沒有事件日誌，則可能存在FMC和CSSM之間的路由問題。

## 常見問題

註冊和授權狀態摘要:

產品註冊狀態	使用授權狀態	意見
未註冊	—	FMC既未處於註冊模式，也未處於評估模式。這是FMC安裝後或90天評估許可證到期後的初始狀態。
已註冊	已獲授權的	FMC已向思科智慧軟體管理員(CSSM)註冊，且有已註冊的有效訂閱的FTD裝置。
已註冊	授權已過期	FMC與思科許可證後端通訊超過90天失敗。

已註冊	未註冊	FMC已向思科智慧軟體管理員(CSSM)註冊，但FMC上未註冊FTD裝置。
已註冊	不符合規定	FMC已向思科智慧軟體管理員(CSSM)註冊，但存在向無效訂閱註冊的FTD裝置。 例如，FTD(FP4112)裝置使用THREAT訂用，但是對於思科智慧軟體管理器(CSSM)，沒有可用於FP4112的THREAT訂用。
評估 ( 90 天 )	不適用	評估期正在使用中，但FMC上沒有註冊的FTD裝置。

## 案例研究1.無效令牌

症狀：由於無效令牌，註冊到CSSM將很快失敗（~10秒），如下圖所示。

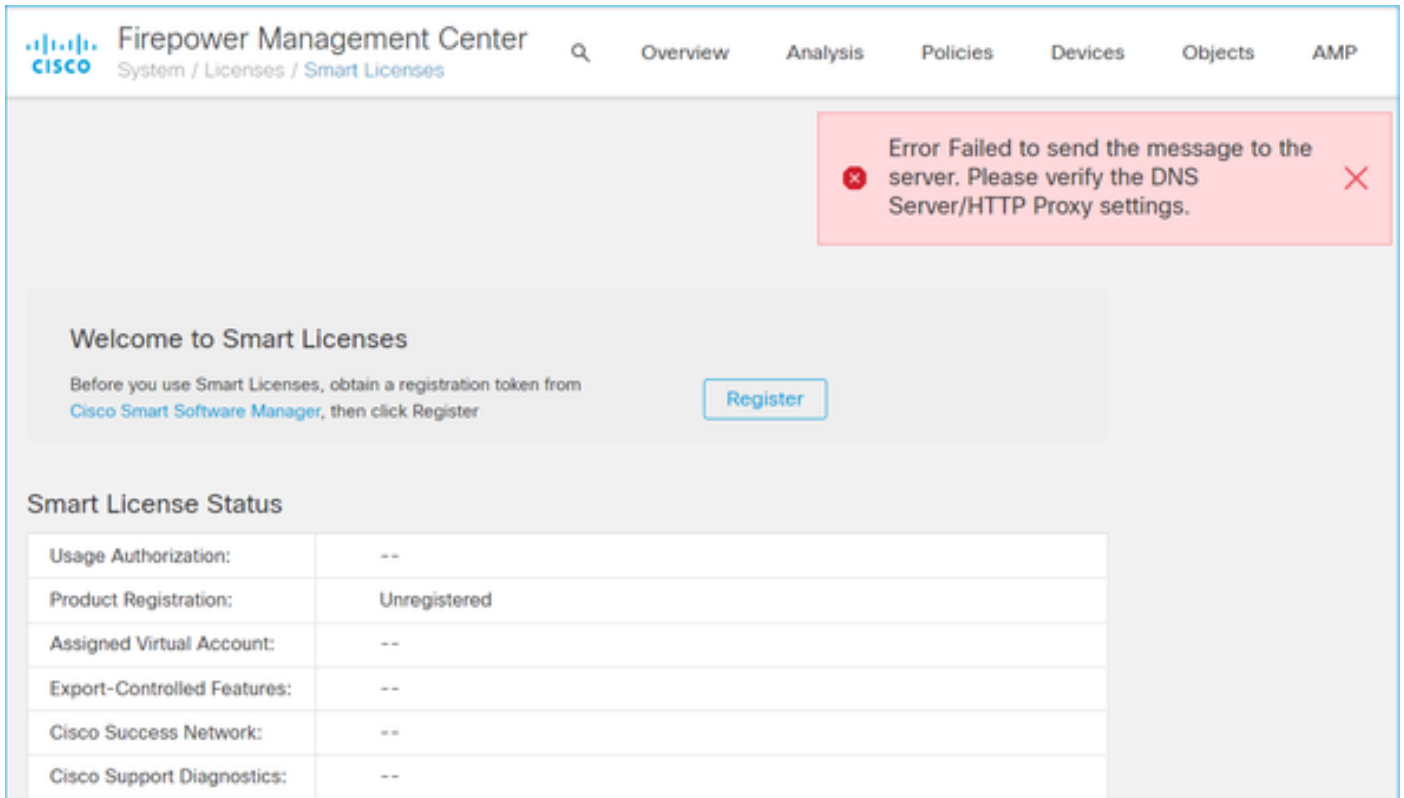
The screenshot shows the Cisco FMC Smart Licenses interface. At the top, there is a navigation bar with the Cisco logo and the text 'FMC Smart Licenses'. Below the navigation bar, there is a search icon and several menu items: Overview, Analysis, Policies, Devices, Objects, AMP, and Intellig. A prominent red error message box is displayed in the center, stating 'Error The token you have entered is invalid.' Below the error message, there is a 'Welcome to Smart Licenses' section with the text 'Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register' and a 'Register' button. At the bottom, there is a 'Smart License Status' table with the following data:

Smart License Status	Status
Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--
Cisco Success Network:	--
Cisco Support Diagnostics:	--

解決方法：使用有效的令牌。

## 案例研究2.無效的DNS

症狀：註冊到CSSM在一段時間（~25秒）後失敗，如下圖所示。



檢查 /var/log/process\_stdout.log 檔案。出現DNS問題：

```
<#root>
```

```
root@FMC2000-2:/Volume/home/admin#
```

```
cat /var/log/process_stdout.log
```

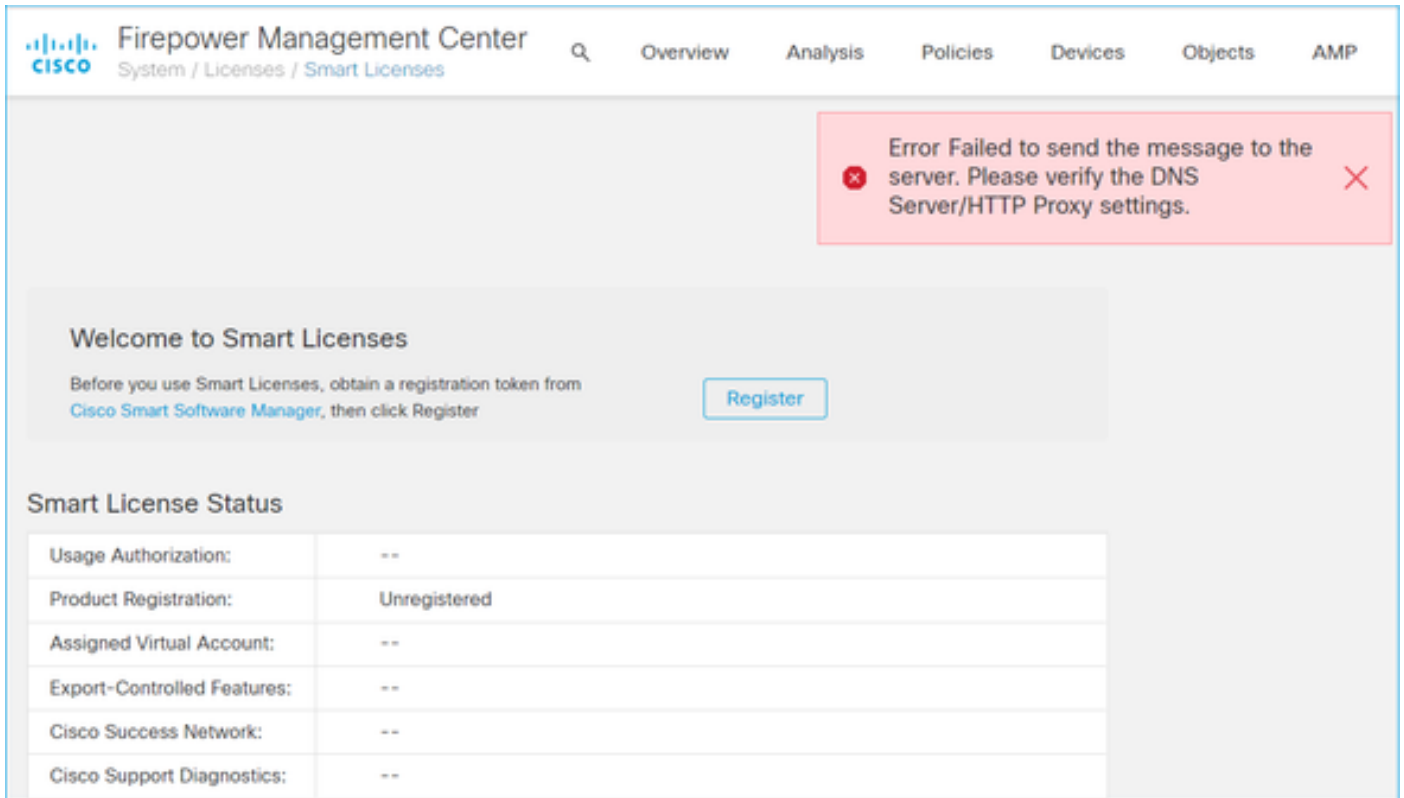
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_cur1_send_msg[494], failed to perform, err code 6, err string
```

```
"Couldn't resolve host name"
```

解決方法：CSSM主機名解析失敗。解決方法是配置DNS（如果未配置），或修復DNS問題。

### 案例研究3.時間值無效

症狀：註冊到CSSM在一段時間（~25秒）後失敗，如下圖所示。



檢查 /var/log/process\_stdout.log 檔案。出現憑證問題：

<#root>

```

2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_request_init[59]
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[299]
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[302]
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_head_init[110],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_http_unlock[330], unl
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_send_http[365], send
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_issue[51
cert issue checking, ret 60, url https://tools.cisco.com/its/service/odce/services/DDCEService

```

檢查FMC時間值：

<#root>

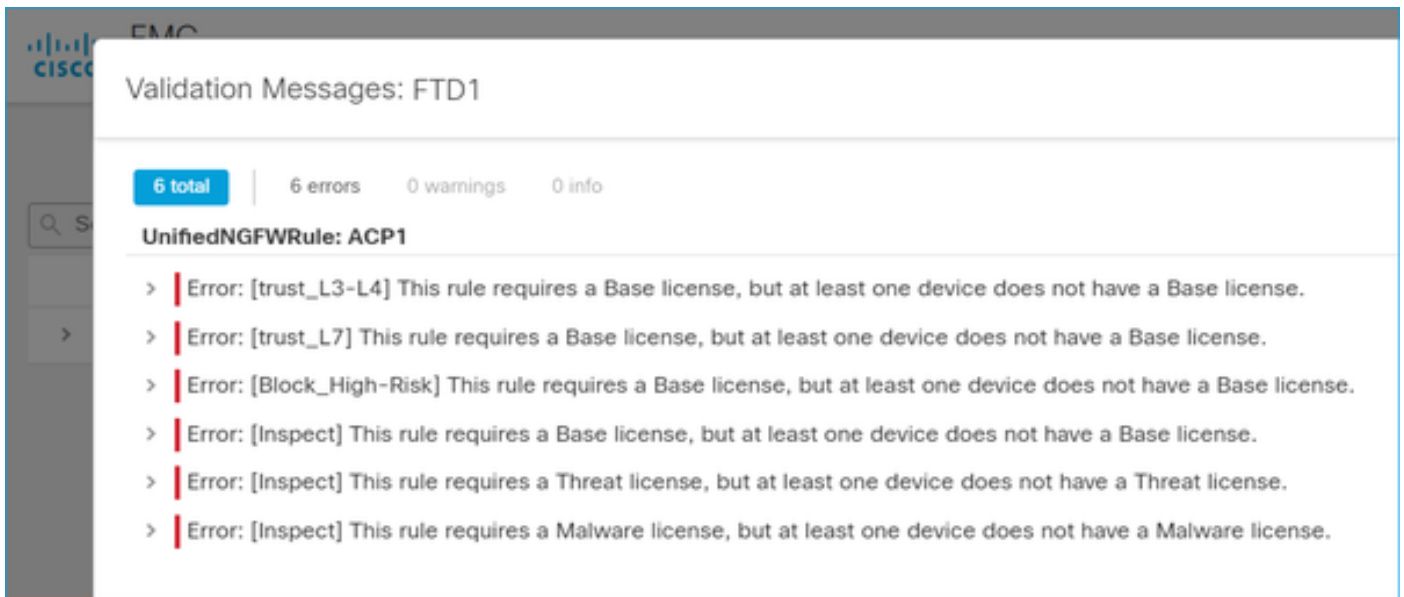
```

root@FMC2000-2:/Volume/home/admin#
date
Fri Jun 25 09:27:22 UTC 2021

```

## 案例研究4.無訂閱

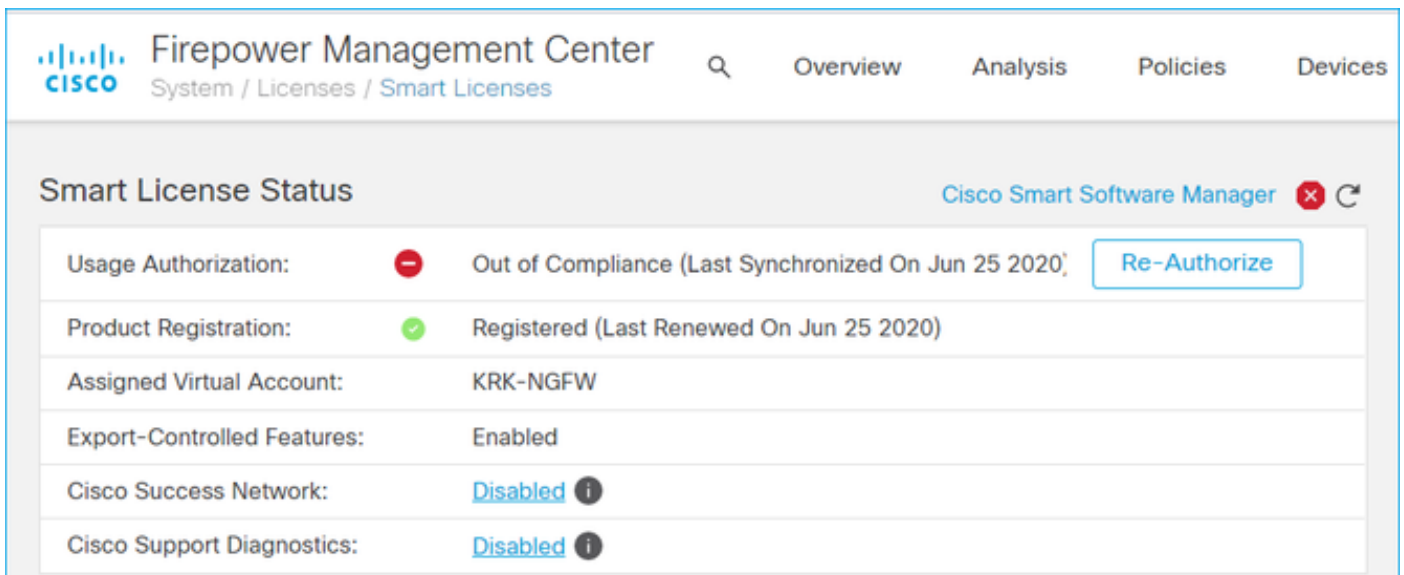
如果沒有特定功能的許可證訂用，則無法進行FMC部署：



解決方案：需要購買裝置並將所需的訂閱應用於裝置。

## 案例研究5.不合規(OOC)

如果沒有針對FTD訂閱的許可權，則FMC智慧許可證將進入不合規(OOC)狀態：



在CSSM中，檢查警報中的錯誤：



License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> FPR4110 Threat Defense Threat Protection	Prepaid	75	2	+ 73		Actions
<input type="checkbox"/> FPR4110 Threat Defense URL Filtering	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/> FPR4115 Threat Defense Malware Protection	Prepaid	0	1	-1	Insufficient Licenses	Actions
<input type="checkbox"/> FPR4115 Threat Defense Threat Protection	Prepaid	0	1	-1	Insufficient Licenses	Actions
<input type="checkbox"/> FPR4115 Threat Defense URL Filtering	Prepaid	0	1	-1	Insufficient Licenses	Actions
<input type="checkbox"/> FPR4120 Threat Defense Malware Protection	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/> FPR4120 Threat Defense Threat Protection	Prepaid	75	0	+ 75		Actions

## 案例研究6.無強加密

如果僅使用基本授權，則會在FTD LINA引擎中啟用資料加密標準(DES)加密。在這種情況下，諸如L2L虛擬專用網路(VPN)等具有較強演算法的部署會失敗：

Validation Messages

Device: FTD1

2 total | 1 error | 1 warning | 0 info

Site To Site VPN: FTD\_VPN

Error: Strong crypto (i.e encryption algorithm greater than DES ) for VPN topology FTD\_VPN is not supported. This can be because FMC is running in evaluation mode or smart license account is not entitled for strong crypto.  
MSG\_SEPARATOR IKEv2 PolicyTITLE\_SEPARATORAES-GCM-NULL-SHA MSG\_SEPARATORMSG\_SEPARATOR

Firepower Management Center

System / Licenses / Smart Licenses

Smart License Status

Usage Authorization: ✔ Authorized (Last Synchronized On Jun 25 2020)

Product Registration: ✔ Registered (Last Renewed On Jun 25 2020)

Assigned Virtual Account: KRK-NGFW

**Export-Controlled Features: Disabled** [Request Export Key](#)

Cisco Success Network: Enabled ⓘ

Cisco Support Diagnostics: Disabled ⓘ

解決方案：向CSSM註冊FMC並啟用強加密屬性。

## 附加說明

設定智慧型授權狀態的通知

SSM 的電子郵件通知

在SSM端，SSM電子郵件通知允許接收各種事件的摘要電子郵件。例如，缺少許可證或許可證即將到期的通知。可以接收產品例項連線或更新失敗的通知。

此函式對於通知和防止由於許可證到期而出現的功能限制非常有用。

## Smart Software Licensing

[Alerts](#) | [Inventory](#) | [License Conversion](#) | [Reports](#) | [Email Notification](#) | [Satellites](#) | [Activity](#)

### Email Notification

#### Daily Event Summary

Receive a daily email summary containing the events selected below

Email Address:

Alert Events:

- Insufficient Licenses - Usage in account exceeds available licenses
- Licenses Expiring - Warning that term-limited licenses will be expiring. Sent 90, 60, 30, 14, 7, 3 and 1 day prior to expiration.
- Licenses Expired - Term-limited licenses have expired. Only displayed if Licenses Expiring warning have not been dismissed.
- Product Instance Failed to Connect - Product has not successfully connected during its renewal period
- Product Instance Failed to Renew - Product did not successfully connect within its maximum allowed renewal period.
- Satellite Synchronization Overdue - Satellite has not synchronized within the expected time period.
- Satellite Unregistered and Removed - Satellite failed to synchronize in 90 days and has been removed.
- Licenses Not Converted - One or more traditional licenses were not automatically converted to Smart during Product Instance Registration.

Informational Events:

- New Licenses - An order has been processed and new licenses have been added to the account
- New Product Instance - A new product instance has successfully registered with the account
- Licenses Reserved - A product instance has reserved licenses in the account

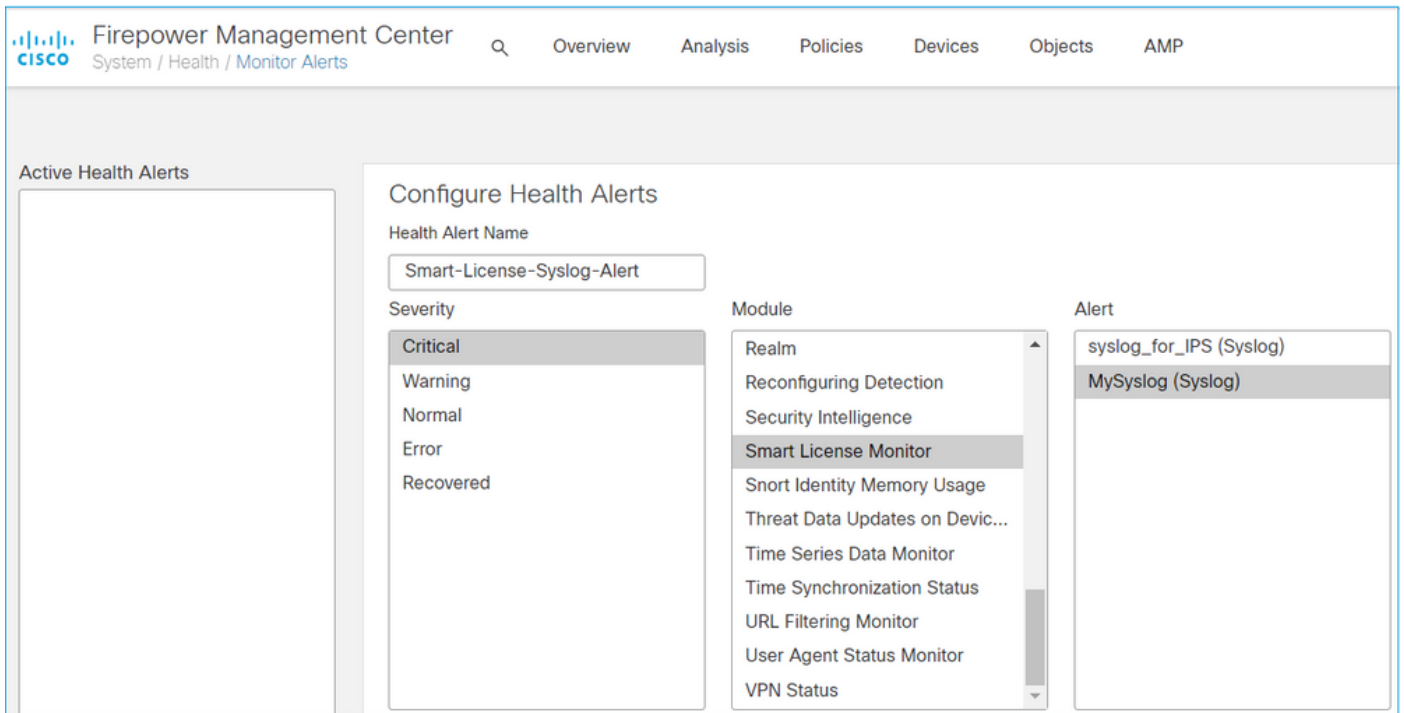
#### Status Notification

Receive an email when a Satellite synchronization file has finished processing by Smart Software Manager

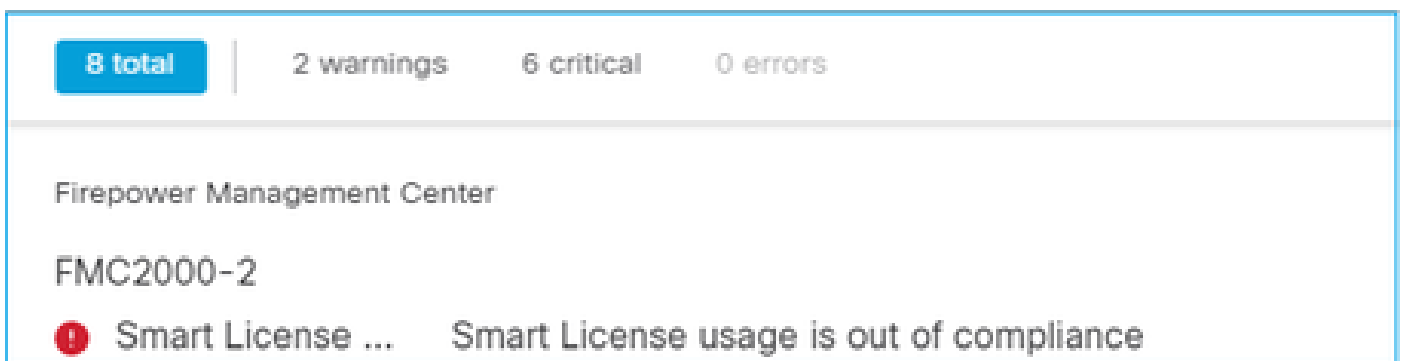
## 從FMC獲取運行狀況警報通知

在 FMC 端中，您可設定健康狀況監控警示，並接收健康狀況事件的警示通知。Smart License Monitor 模組可檢查智慧型授權狀態。該監控警示支援系統日誌、電子郵件及 SNMP 設陷。

此為智慧型授權監控事件發生時取得系統日誌訊息的組態範例：



以下為健康狀況警示的範例：



FMC生成的系統日誌消息為：

```
<#root>
```

```
Mar 13 18:47:10 xx.xx.xx.xx Mar 13 09:47:10 FMC :
```

```
HMNOTIFY: Smart License Monitor (Sensor FMC)
```

```
: Severity: critical: Smart License usage is out of compliance
```

如需有關健康狀況監控警示相關的其他詳細資料，請參閱[健康狀況監控](#)。

## 相同智慧型帳戶的多個 FMC

在同一智慧帳戶上使用多個FMC時，每個FMC主機名必須是唯一的。在CSSM中管理多個FMC時，要區分每個FMC，每個FMC的主機名必須是唯一的。若要進行 FMC 智慧型授權維護，此規則相

當實用。

## FMC 必須維持網路連線

註冊後，FMC每30天檢查一次智慧許可證雲和許可證狀態。如果 FMC 在 90 天內無法通訊，則表示授權功能正在維護，但其仍處於授權到期狀態。即使在此狀態下，FMC仍會不斷嘗試連線到智慧許可證雲。

## 部署多個 FMCv

在虛擬環境中使用Firepower系統時，克隆（熱或冷）不受正式支援。每個 Firepower Management Center Virtual (FMCv) 皆是獨立的，因此其內部具有驗證資訊。要部署多個FMCv，必須從開放式虛擬化格式(OVF)檔案逐一建立FMCv。如需有關此限制的詳細資訊，請參閱[適用於 VMware 部署的 Cisco Firepower Management Center Virtual 快速入門指南](#)。

## 常見問題(FAQ)

在 FTD HA 中，需要使用多少個裝置授權？

在高可用性中使用兩個FTD時，每台裝置都需要一個許可證。例如，如果在FTD HA配對上使用入侵防禦系統(IPS)和進階惡意軟體防護(AMP)功能，則需要兩個威脅及惡意軟體授權。

FTD為什麼沒有使用AnyConnect許可證？

將FMC註冊到智慧帳戶後，確保AnyConnect許可證已啟用。要啟用許可證，請導航至FMC > Devices，選擇您的裝置，然後選擇License。選擇鉛筆圖示，選擇存放在「智慧帳戶」中的許可證，然後選擇「儲存」。

為什麼當連線100個使用者時，智慧帳戶中只有一個AnyConnect許可證「正在使用」？

這是預期行為，因為智慧帳戶會跟蹤啟用此許可證的裝置數量，而不是連線的活動使用者。

為什麼會有錯誤 Device does not have the AnyConnect License 在FMC配置和部署遠端訪問VPN之後？

確保FMC已註冊到智慧許可證雲。預期行為是當FMC未註冊或處於評估模式時，無法部署遠端訪問配置。如果FMC已註冊，請確保您的智慧帳戶中存在AnyConnect許可證，並且已將其分配給裝置。

要分配許可證，導覽 成長至FMC設備，選擇您的裝置，許可證（鉛筆圖示）。在智慧帳戶中選擇許可證，然後選擇 儲存。

為什麼會有錯誤 Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled 何時部署遠端訪問VPN配置？

部署於 FTD 的遠端存取 VPN 需要啟用強式加密授權。Zt確保在FMC上啟用了強加密許可證。要檢查強加密許可證的狀態，導覽 到 FMC系統>許可證>智慧許可並驗證是否已啟用匯出控制功能。

如果出現以下情況，如何啟用強加密許可證 `Export-Controlled Features` 是否禁用？

如果FMC註冊到智慧帳戶雲期間使用的令牌具有選項`Allow export-controlled functionality on the products registered with this token enabled`，則會自動啟用此功能。如果權杖未啟用此選項，則請取消註冊 FMC，並在啟用此選項的情況下再次註冊。

生成令牌時，如果選項「允許使用此令牌註冊的產品上的匯出控制功能」不可用，該怎麼辦？

請聯絡您的思科客戶團隊。

為什麼收到「Strong crypto ( 即，加密演算法大於DES ) for VPN topology s2s is not supported ( 不支援VPN拓撲s2的強加密 )」錯誤？

當FMC使用評估模式或智慧許可證帳戶無權獲得強加密許可證時，將顯示此錯誤。五驗證FMC是否已向許可證頒發機構註冊，並啟用使用此令牌註冊的產品上的「允許匯出控制」功能。如果不允許智慧帳戶使用強加密許可證，則不允許部署密碼比DES更強的VPN站點到站點配置。

為什麼收到FMC上的「不合規」狀態？

如果其中一個託管裝置使用不可用的授權，則該裝置會變為「不符合規定」狀態。

如何更正「不合規」狀態？

請按照《Firepower 組態指南》說明的步驟操作：

1. 請查看頁面底部的「智慧型授權」一節，判斷所需要的授權。
2. 透過常用的管道購買需要的授權。
3. 在Cisco Smart Software Manager(<https://software.cisco.com/#SmartLicensing-Inventory>)，驗證許可證是否出現在您的虛擬帳戶中。
4. 在FMC中，選擇System > Licenses > Smart Licenses。
5. 選取「重新授權」。

完整過程可在[Licensing the Firepower System](#)中找到。

什麼是 Firepower Threat Defense 基礎功能？

基本許可證允許：

- 將FTD裝置設定為交換機和路由 ( 包括DHCP中繼和NAT )。
- 在高可用性(HA)模式下設定FTD裝置。
- 將安全模組配置為Firepower 9300機箱 ( 機箱內群集 ) 內的群集。
- 將Firepower 9300或Firepower 4100系列裝置(FTD)配置為群集 ( 機箱間群集 )。
- 配置使用者和應用程式控制以及將使用者和應用程式條件新增到訪問控制規則。

如何獲得Firepower威脅防禦基礎功能許可證？

每次購買 Firepower Threat Defense 或 Firepower Threat Defense Virtual 裝置即自動隨附基本授權。當FTD註冊到FMC時，系統會自動將其新增到您的智慧帳戶中。

在FMC和智慧許可證雲之間的路徑中必須允許哪些IP地址？

FMC使用IP地址 埠443，用於與智慧許可證雲通訊。

該IP地址(<https://tools.cisco.com>)解析為以下IP地址：

- 72.163.4.38
- 173.37.145.8

## 相關資訊

- [Firepower Management Center 組態設定指南](#)
- [思科Live Smart許可概述：BRKARC-2034](#)
- [Cisco Secure Firewall Management Center功能許可證](#)
- [Cisco Smart Software Licensing 常見問題 \(FAQs\)](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。