

使用FMC和FTD智能许可证注册和常见问题进行故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[FMC智能许可证注册](#)

[先决条件](#)

[FMC智能许可证注册](#)

[在智能软件管理器\(SSM\)端确认](#)

[FMC智能许可证取消注册](#)

[RMA](#)

[故障排除](#)

[常见问题](#)

[案例研究1.无效令牌](#)

[案例分析2.无效的DNS](#)

[案例分析3.无效的时间值](#)

[案例研究4.无订用](#)

[案例研究5.不合规\(OOC\)](#)

[案例研究6.无强加密](#)

[其他说明](#)

[设置智能许可证状态的通知](#)

[从FMC获取运行状况警报通知](#)

[同一智能帐户上的多个FMC](#)

[FMC必须维护Internet连接](#)

[部署多个FMCv](#)

[常见问题解答\(FAQ\)](#)

[相关信息](#)

简介

本文档介绍Firepower威胁防御受管设备上Firepower管理中心的智能许可证注册配置。

先决条件

要求

本文档没有任何特定的要求。

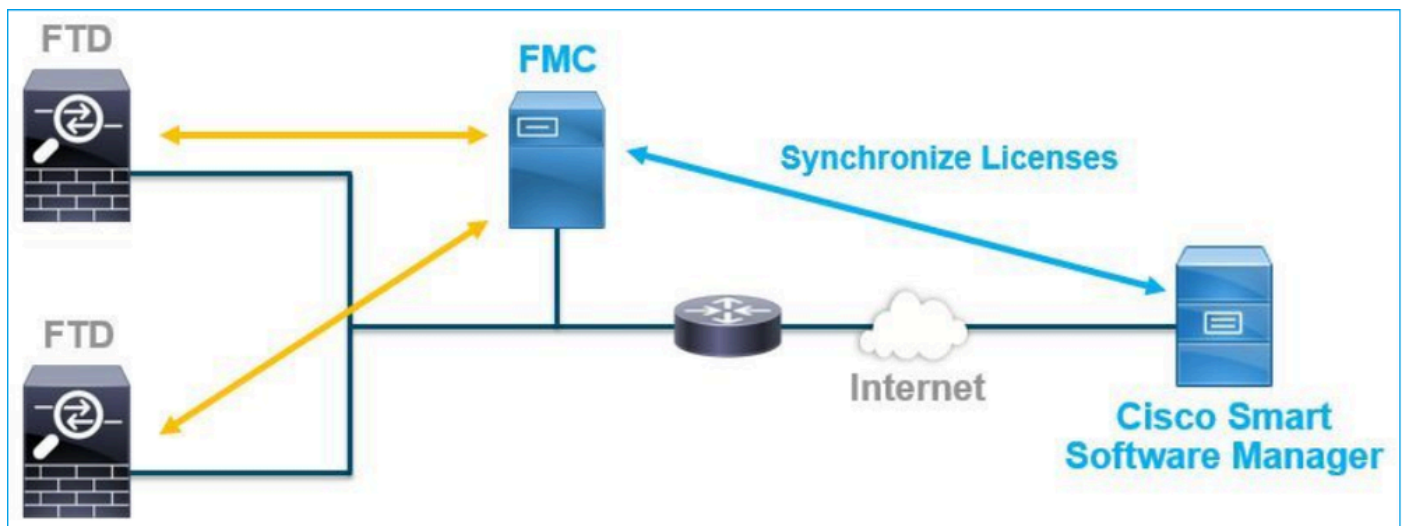
使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FMC、FTD和智能许可证注册。

智能许可证注册在Firepower管理中心(FMC)上执行。FMC通过互联网与思科智能软件管理器(CSSM)门户通信。在CSSM中，防火墙管理员管理智能帐户及其许可证。FMC可以自由地将许可证分配和删除到托管Firepower威胁防御(FTD)设备。换句话说，FMC集中管理FTD设备的许可证。



使用FTD设备的某些功能需要额外的许可证。客户可以分配给FTD设备的智能许可证类型记录在[FTD许可证类型和限制](#)中。

基本许可证包含在FTD设备中。当FMC注册到CSSM时，此许可证将自动在您的智能帐户中注册。基于期限的许可证：威胁、恶意软件和URL过滤是可选的。要使用与许可证相关的功能，需要向FTD设备分配许可证。

要将Firepower管理中心虚拟(FMCv)用于FTD管理，FMCv还需要在CSSM中使用Firepower MCv设备许可证。

FMCv许可证包含在软件中，并且是永久许可证。

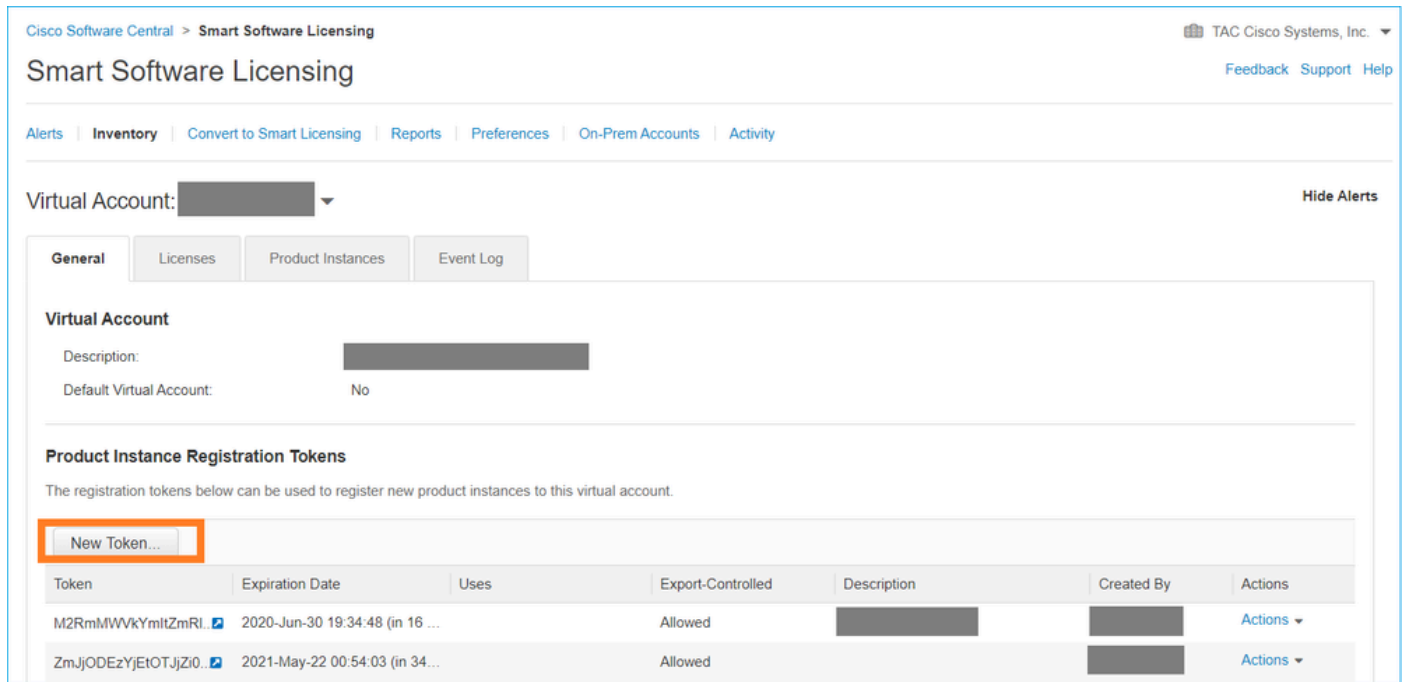
此外，本文档还提供了一些可帮助排除可能出现的常见许可证注册错误的方案。

有关许可证的更多详细信息，请查看[思科Firepower系统功能许可证](#)和[Firepower许可常见问题\(FAQ\)](#)。

FMC智能许可证注册

先决条件

1. 对于智能许可证注册，FMC必须访问互联网。由于证书是通过HTTPS在FMC和智能许可证云之间交换的，请确保路径中没有可影响/修改通信的设备。（例如，防火墙、代理、SSL解密设备等）。
2. 访问CSSM并从资产>常规>新建令牌按钮发出令牌ID，如下图所示。



要使用强加密，请启用在使用此令牌注册的产品上允许导出控制功能选项。启用后，复选框中将出现一个复选标记。

3. 选择创建令牌。

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 ?

[Create Token](#) [Cancel](#)

FMC智能许可证注册

导航到FMC上的System > Licenses > Smart Licenses，然后选择Register按钮，如下图所示。

Firepower Management Center
System / Licenses / Smart Licenses

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from [Cisco Smart Software Manager](#), then click Register

[Register](#)

Smart License Status

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

在智能许可产品注册窗口中输入令牌ID，然后选择应用更改，如下图所示。

Smart Licensing Product Registration

Product Instance Registration Token:

OWI4Mzc5MTAtNzQwYi00YTVILTkyNTktMGMxNGJlYmRmNDUwLTE1OTQ3OTQ5%
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

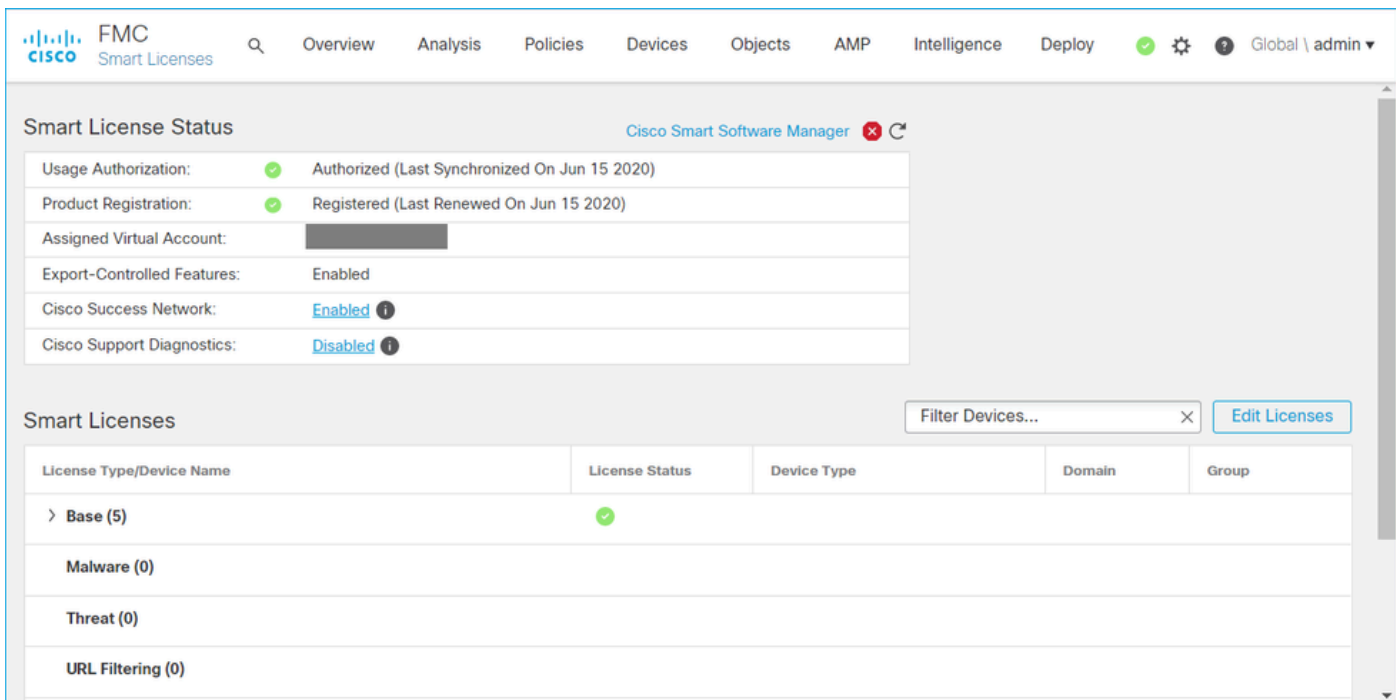
The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration and operational health data from 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.

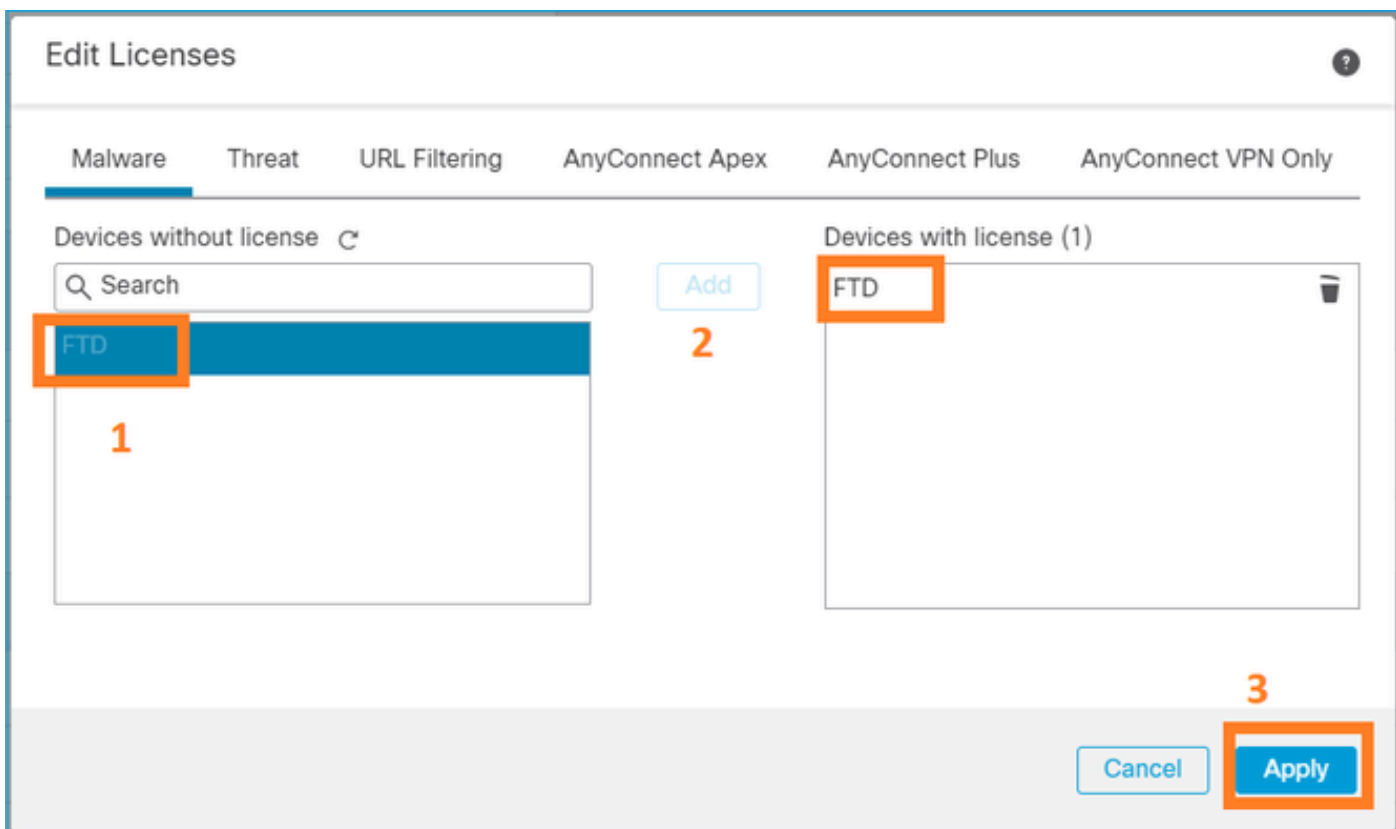
Cancel

Apply Changes

如果智能许可证注册成功，则产品注册状态将显示已注册，如下图所示。

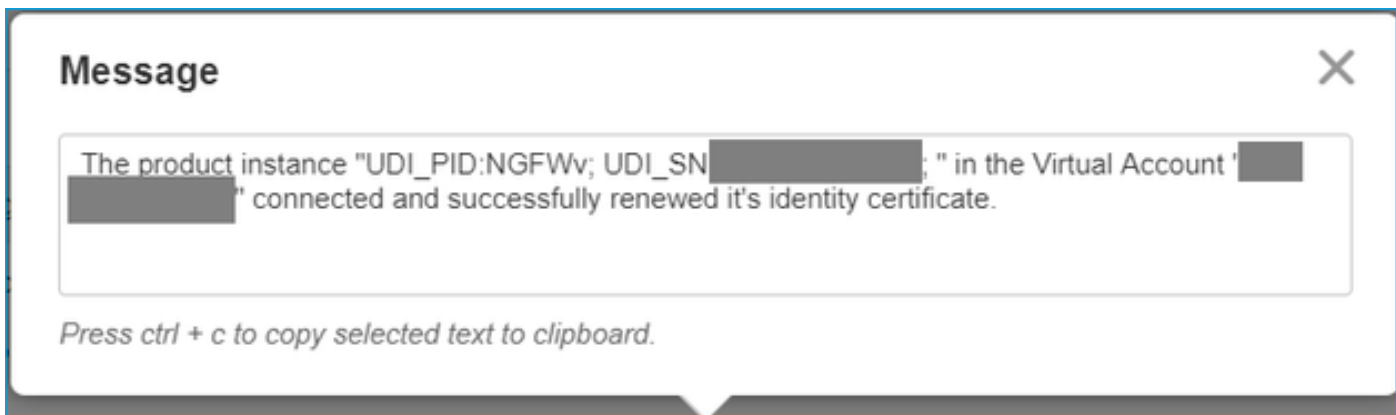


要将基于期限的许可证分配到FTD设备，请选择Edit Licenses。然后选择受管设备并将其添加到Devices with license部分。最后，请选择Apply按钮，如下图所示。



在智能软件管理器(SSM)端确认

可以通过CSSM中的资产>事件日志确认FMC智能许可证注册成功，如下图所示。

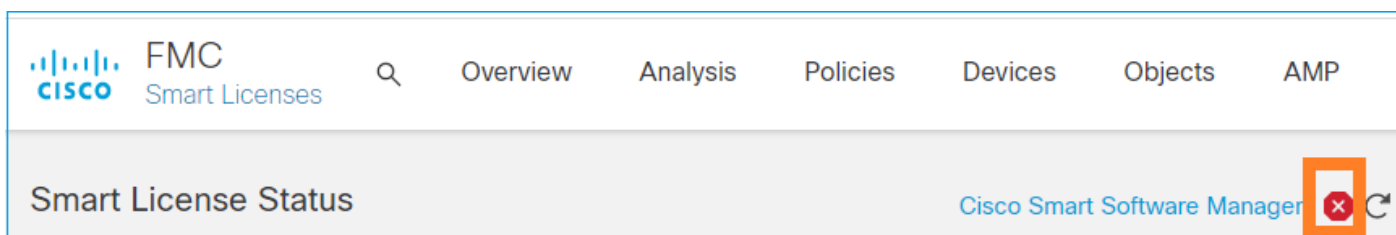


FMC的注册状态可以通过资产>产品实例进行确认。从Event Log选项卡检查事件日志。智能许可证注册和使用状态可以通过资产>许可证选项卡进行检查。确认已正确使用购买的基于期限的许可证，并且没有表明许可证不足的警报。

FMC智能许可证取消注册

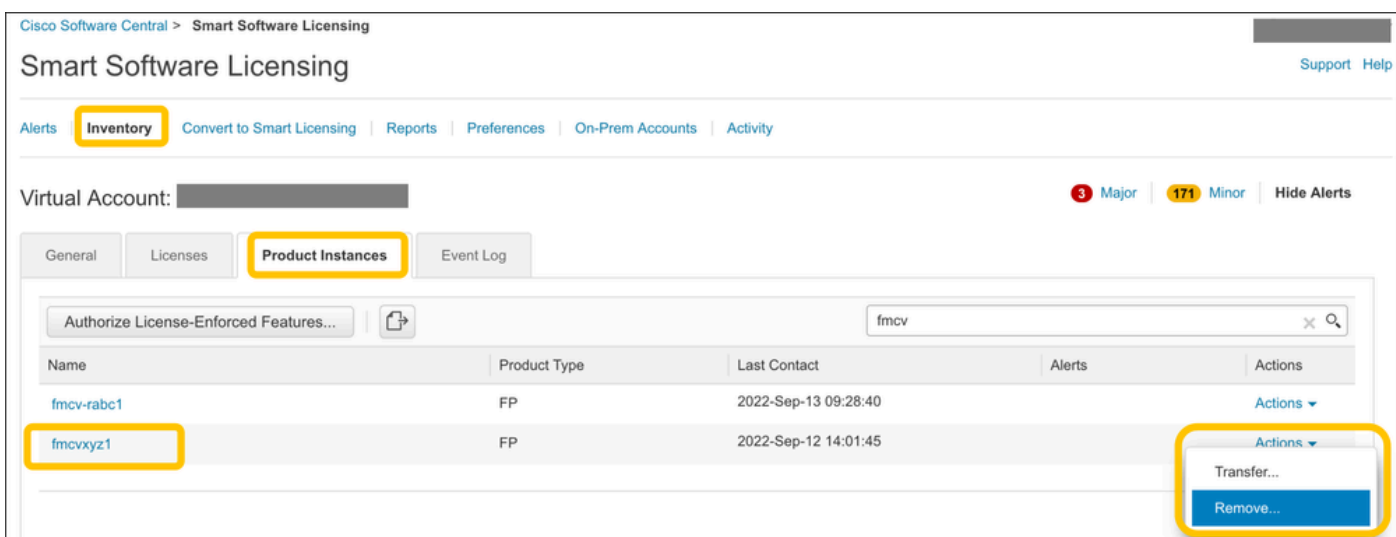
从Cisco SSM注销FMC

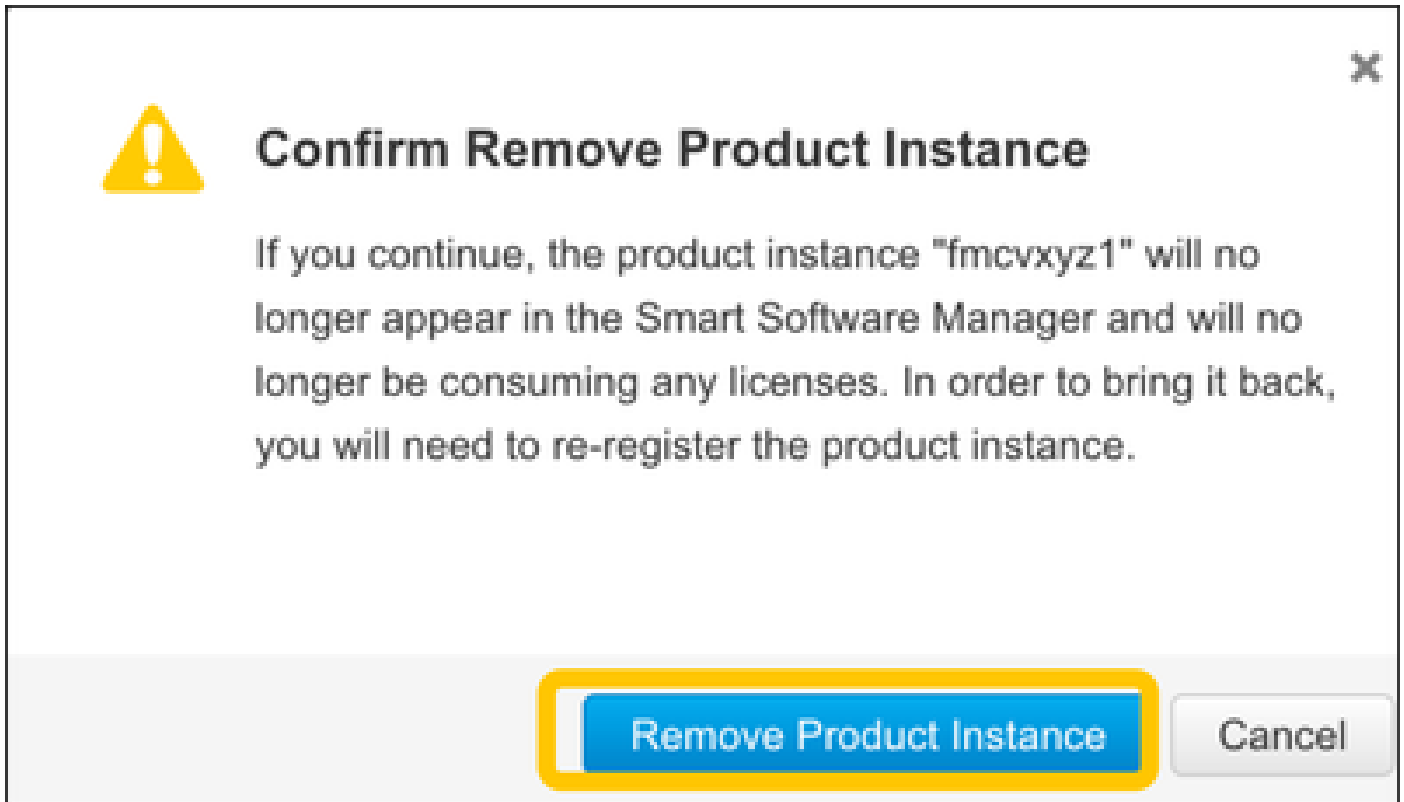
要为某些原因发布许可证或使用其他令牌，请导航到System > Licenses > Smart Licenses，然后选择de-register按钮，如下图所示。



从SSM端删除注册

访问智能软件管理器(思科智能软件管理器)，然后从资产>产品实例中，选择目标FMC上的删除。然后选择删除产品实例以删除FMC并释放分配的许可证，如下图所示。





RMA

如果返回FMC，请按照FMC智能许可证取消注册>从SSM端删除注册部分中的步骤从思科智能软件管理器(CSSM)取消注册FMC，然后按照FMC智能许可证注册部分中的步骤将FMC重新注册到CSSM。

故障排除

时间同步验证

访问FMC CLI（例如，SSH），确保时间正确且与受信任的NTP服务器同步。由于证书用于智能许可证身份验证，因此FMC具有正确的时间信息非常重要：

```
<#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，从System > Configuration > Time Synchronization验证NTP服务器值。

启用名称解析并检查与tools.cisco.com的可达性(smartreceiver.cisco.com from FMC 7.3+)

确保FMC可以解析FQDN并能根据[思科漏洞ID CSCwj](#)从FMC 7.3开始访问tools.cisco.com(smartreceiver.cisco.com[95397](#))

```
<#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，从System > Configuration > Management Interfaces验证管理IP和DNS服务器IP。

验证从FMC到tools.cisco.com(从FMC 7.3+到smartreceiver.cisco.com)的HTTPS (TCP 443)访问

使用Telnet或curl命令确保FMC可以通过HTTPS访问tools.cisco.com(从FMC 7.3+访问smartreceiver.cisco.com)。如果TCP 443通信中断，请验证它未被防火墙阻止，并且路径中没有SSL解密设备。

```
<#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
```

卷曲测试：

<#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

Cpath: 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; domai

< 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验证

验证是否成功解析到tools.cisco.com(来自FMC 7.3+的smartreceiver.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
```

代理验证

如果使用了apProxy，请检查FMC和代理服务器端的值。在FMC上，检查FMC是否使用正确的代理服务器IP和端口。

```
<#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，可以通过System > Configuration > Management Interfaces确认代理值。

如果FMC端值正确，请检查代理服务器端的值(例如，如果代理服务器允许从FMC访问和tools.cisco.com。此外，允许通过代理的流量和证书交换。FMC使用证书进行智能许可证注册)。

过期的令牌ID

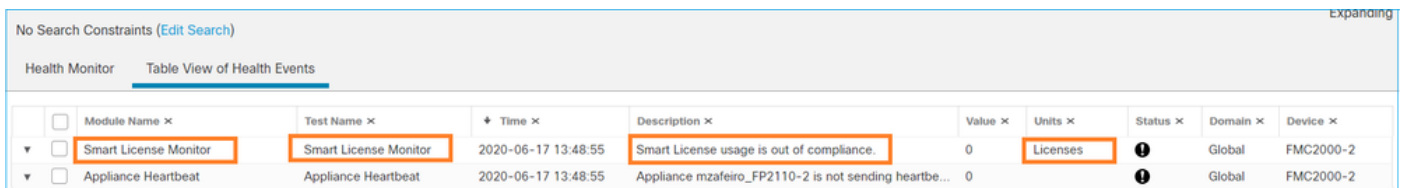
验证颁发的令牌ID是否未过期。如果到期，请要求智能软件管理器管理员颁发新令牌，并使用新令牌ID重新注册智能许可证。

更改FMC网关

在某些情况下，由于中继代理或SSL解密设备的影响，智能许可证身份验证无法正确执行。如有可能，请更改FMC互联网访问的路由以避免这些设备，并重试智能许可证注册。

检查FMC上的运行状况事件

在FMC上，导航到系统>运行状况>事件，检查智能许可证监控模块的状态是否有错误。例如，如果连接由于证书过期而失败；则将生成一个错误，例如id certificated expired，如下图所示。



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	Licenses	!	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

检查SSM端的事件日志

如果FMC可以连接到CSSM，请在资产>事件日志中检查连接的事件日志。检查CSSM中是否存在此类事件日志或错误日志。如果FMC站点的值/操作没有问题，并且CSSM端没有事件日志，则可能是FMC和CSSM之间的路由有问题。

常见问题

注册和授权状态摘要：

产品注册状态	使用授权状态	备注
未注册	—	FMC既不处于“已注册”模式，也不处于“评估”模式。这是FMC安装后或90天评估许可证到期后的初始状态。
已注册	已授权	FMC已向思科智能软件管理器(CSSM)注册，并且存在使用有效订用注册的FTD设备。
已注册	授权已过期	FMC与思科许可证后端通信超过90天。

已注册	未注册	FMC向思科智能软件管理器(CSSM)注册，但FMC上未注册FTD设备。
已注册	不合规	FMC已向思科智能软件管理器(CSSM)注册，但存在使用无效订用注册的FTD设备。 例如，FTD (FP4112)设备使用THREAT订用，但是对于思科智能软件管理器(CSSM)，没有可用于FP4112的THREAT订用。
评估 (90天)	不适用	评估期正在使用中，但是在FMC上没有注册FTD设备。

案例研究1.无效令牌

症状：由于令牌无效，注册到CSSM会快速失败（约10秒），如下图所示。

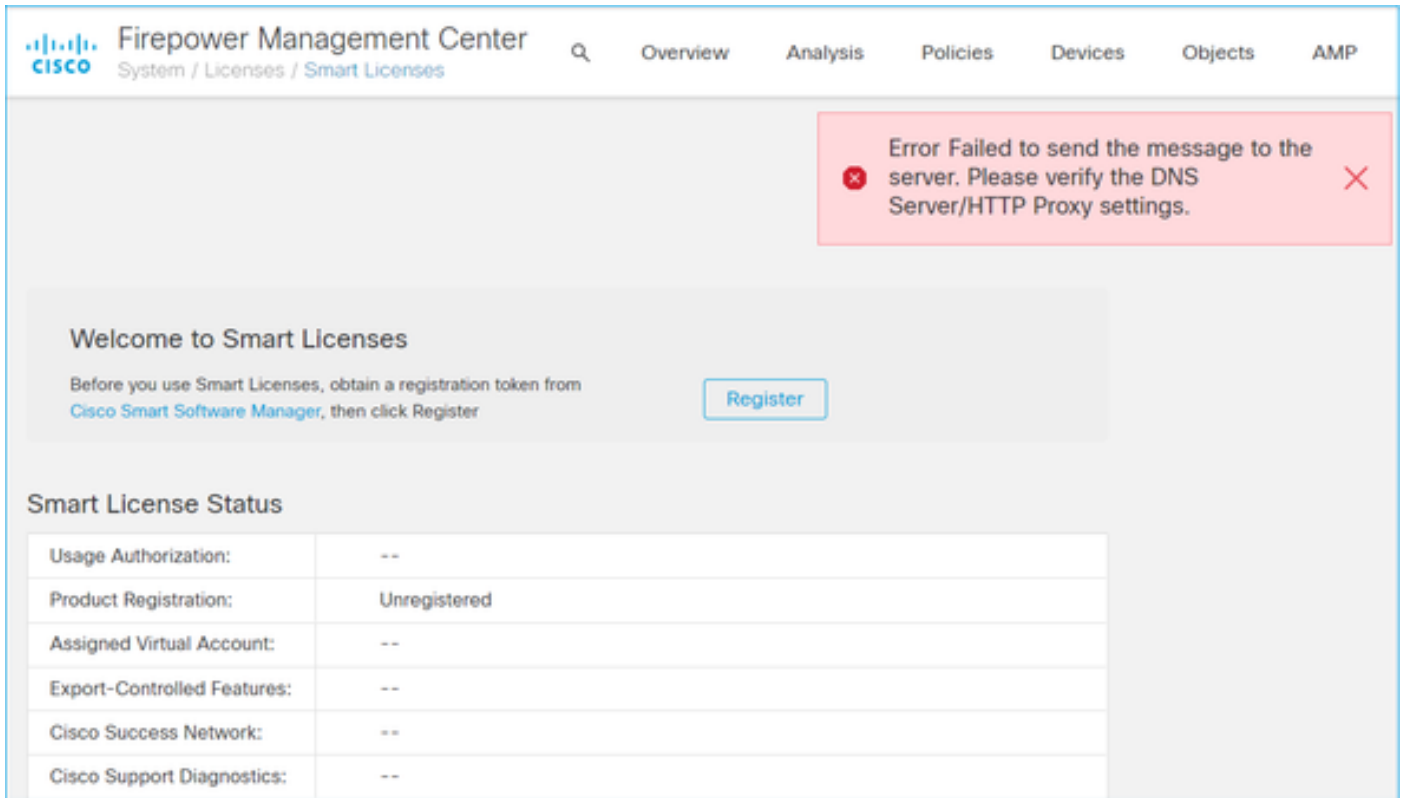
The screenshot shows the Cisco FMC Smart Licenses management page. At the top, there is a navigation bar with 'FMC Smart Licenses' and various menu items like Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. A prominent red error message box states: 'Error The token you have entered is invalid.' Below this, a 'Welcome to Smart Licenses' section provides instructions to obtain a registration token from Cisco Smart Software Manager and includes a 'Register' button. At the bottom, a 'Smart License Status' table shows the following information:

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

解决方法：使用有效令牌。

案例分析2.无效的DNS

症状：注册到CSSM在一段时间（-25秒）后失败，如下图所示。



检查/var/log/process_stdout.log文件。发现DNS问题：

```
<#root>
```

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

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

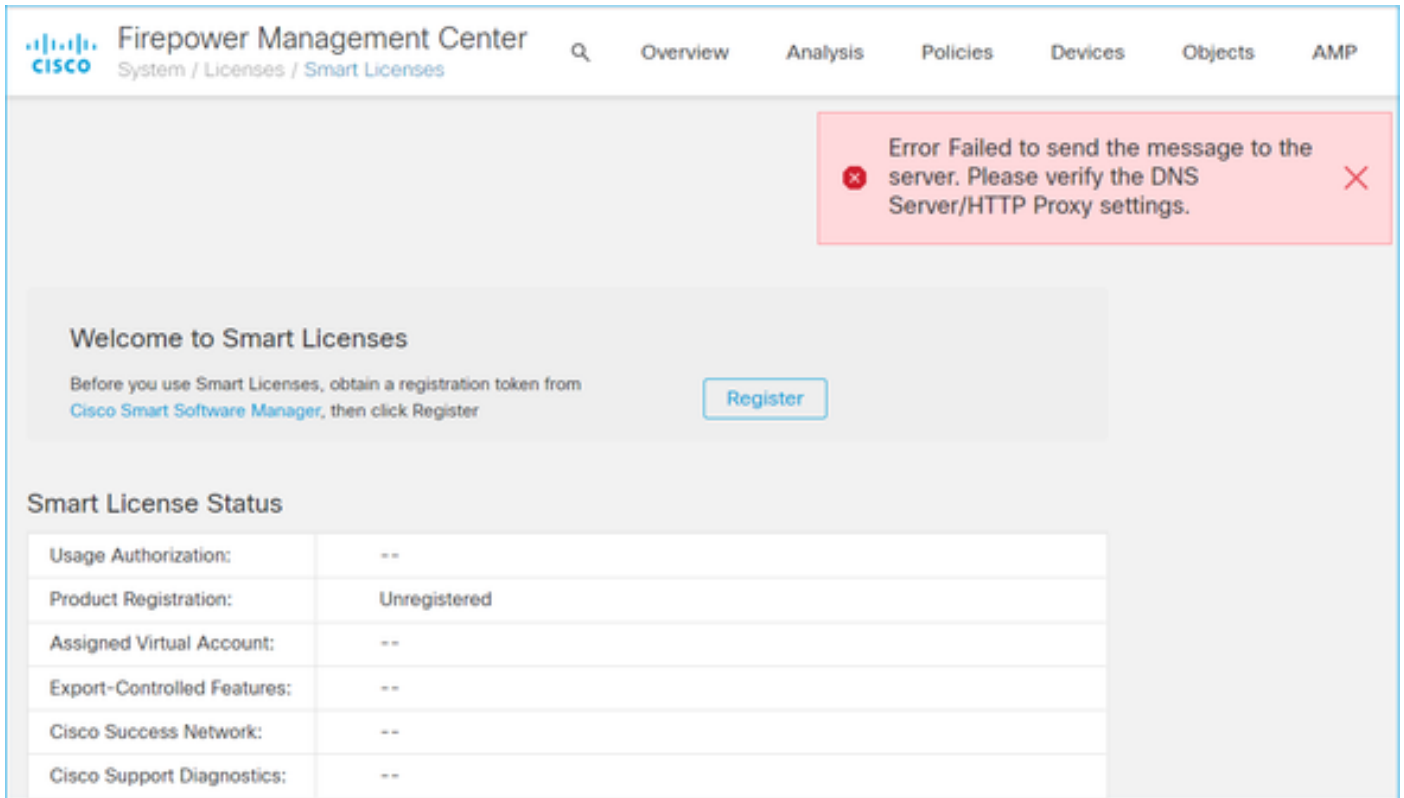
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_cur1_send_msg[494], failed to perform, err code 6, err string
```

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

解决方法：CSSM主机名解析失败。解决方法是配置DNS（如果未配置），或者修复DNS问题。

案例分析3.无效的时间值

症状：注册到CSSM在一段时间（-25秒）后失败，如下图所示。



检查/var/log/process_stdout.log文件。发现证书问题：

<#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
```

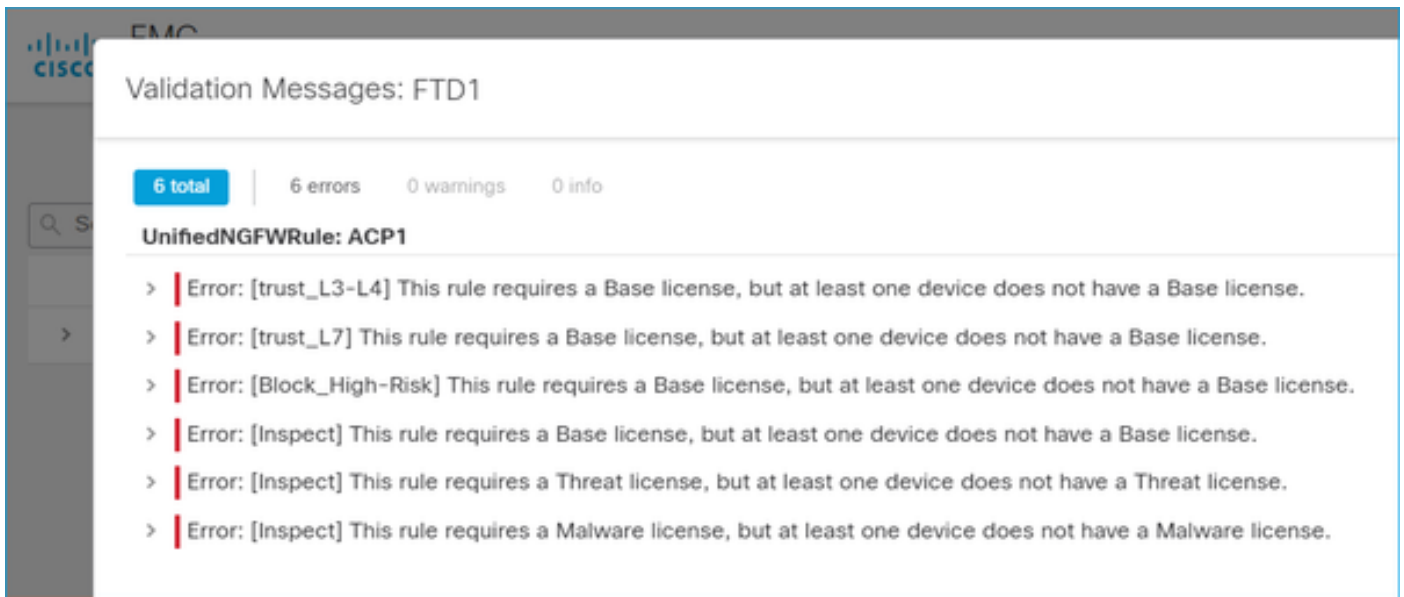
检查FMC时间值：

<#root>

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

案例研究4.无订用

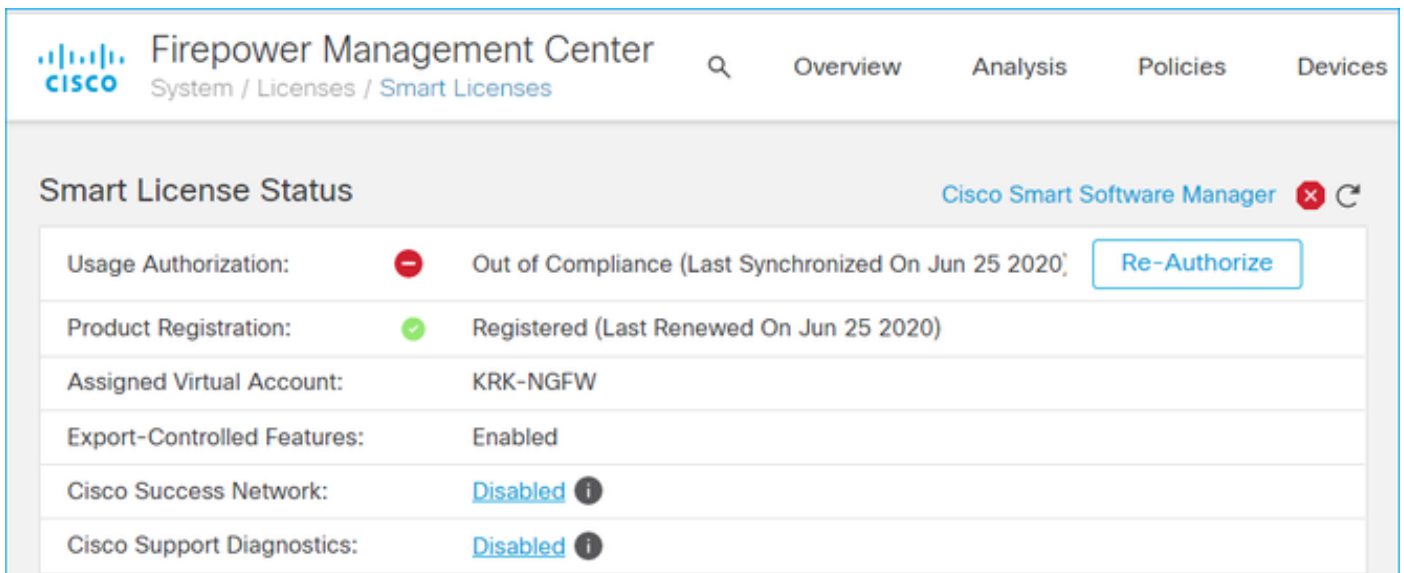
如果没有特定功能的许可证订用，则无法进行FMC部署：



解决方案：需要购买所需订用并将其应用到设备。

案例研究5.不合规(OOC)

如果没有FTD订用授权，则FMC智能许可证将进入不合规(OOC)状态：



在CSSM中，检查警报中的错误：

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.无强加密

如果仅使用基础许可证，则在FTD LINA引擎中启用数据加密标准(DES)加密。在这种情况下，诸如L2L虚拟专用网络(VPN)等具有更强算法的部署会失败：

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 ⓘ

解决方法：将FMC注册到CSSM并启用强加密属性。

其他说明

设置智能许可证状态的通知

通过SSM发送电子邮件通知

在SSM端，SSM电子邮件通知允许接收各种事件的摘要电子邮件。例如，缺少许可证或许可证即将到期的通知。可以接收产品实例连接或更新失败的通知。

此功能非常有助于注意和防止由于许可证到期而出现功能限制。

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

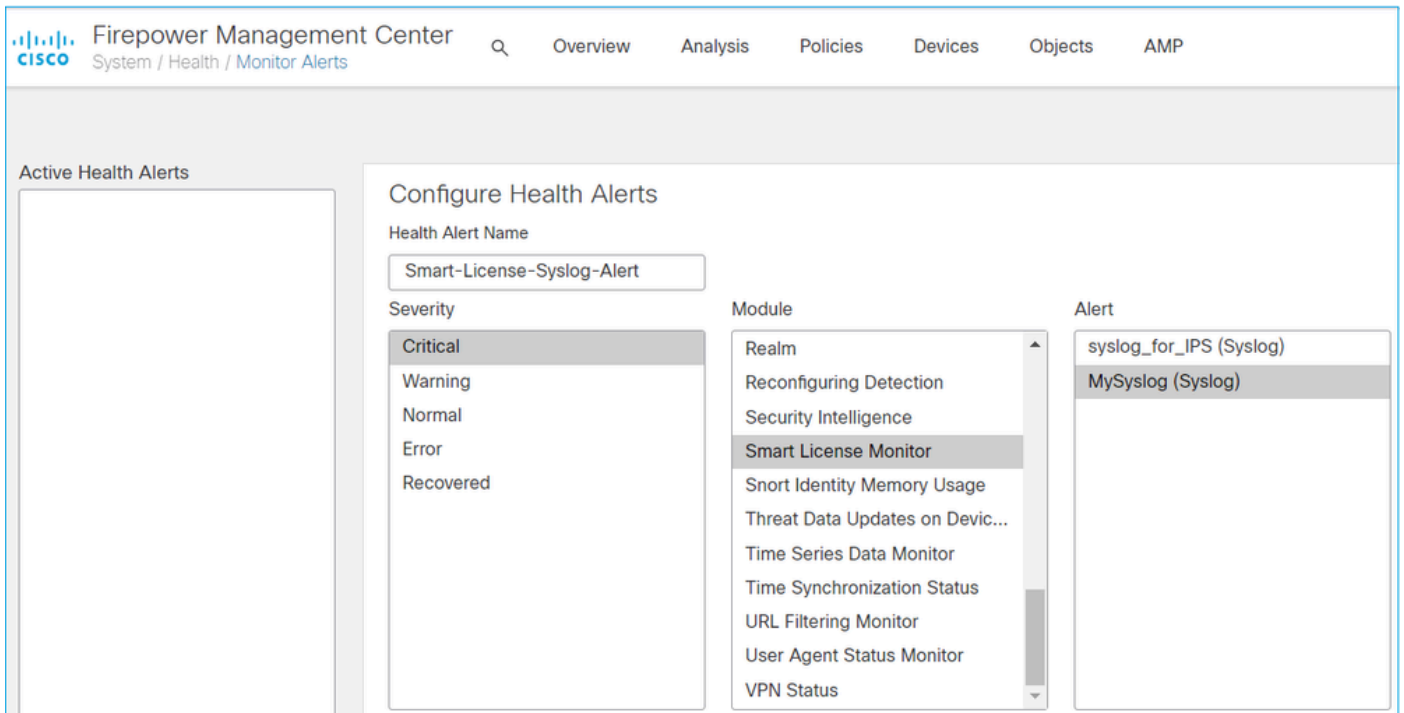
Status Notification

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

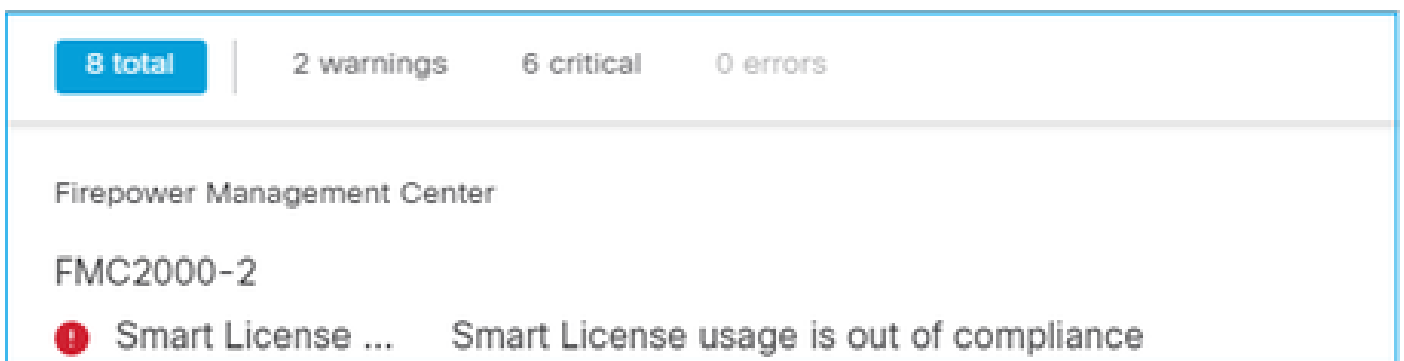
从FMC获取运行状况警报通知

在FMC侧，可以配置运行状况监视器警报并接收运行状况事件的警报通知。模块智能许可证监控器可用于检查智能许可证状态。监控器警报支持系统日志、邮件和SNMP陷阱。

以下是发生智能许可证监控事件时获取系统日志消息的配置示例：



以下是Health Alert的示例：



FMC生成的系统日志消息是：

<#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

有关运行状况监视器警报的其他详细信息，请参阅[运行状况监控](#)。

同一智能帐户上的多个FMC

在同一智能帐户上使用多个FMC时，每个FMC主机名必须是唯一的。在CSSM中管理多个FMC时，要区分每个FMC，每个FMC的主机名必须是唯一的。这对于运行中的FMC智能许可证维护非常有

用。

FMC必须维护Internet连接

注册后，FMC每30天检查一次智能许可证云和许可证状态。如果FMC在90天内无法通信，许可功能将得以保留，但是其将保持为Authorization Expired状态。即使在此状态下，FMC也会不断尝试连接到智能许可证云。

部署多个FMCv

在虚拟环境中使用Firepower系统时，克隆（热或冷）不受正式支持。每个Firepower管理中心虚拟（FMCv）都是唯一的，因为它内部具有身份验证信息。要部署多个FMCv，必须从开放式虚拟化格式（OVF）文件逐一创建FMCv。有关此限制的详细信息，请参阅[《适用于VMware的Cisco Firepower管理中心虚拟部署快速入门指南》](#)。

常见问题解答(FAQ)

在FTD HA中，需要多少设备许可证？

在高可用性中使用两个FTD时，每台设备都需要许可证。例如，如果在FTD HA对上使用入侵防御系统(IPS)和高级恶意软件防护(AMP)功能，则需要两个威胁和恶意软件许可证。

FTD为何不使用AnyConnect许可证？

将FMC注册到智能帐户后，确保AnyConnect许可证已启用。要启用许可证，请导航至FMC > Devices，选择您的设备，然后选择License。选择铅笔图标，选择存放于智能帐户中的许可证，然后选择保存。

当连接100个用户时，为什么智能帐户中只有一个AnyConnect许可证“正在使用”？

这是预期行为，因为智能帐户会跟踪启用此许可证的设备数量，而不是连接的活动用户数量。

FMC配置和部署远程接入VPN后为什么会出现Device does not have the AnyConnect License错误？

确保FMC已注册到智能许可证云。预期行为是当FMC未注册或处于评估模式时，无法部署远程访问配置。如果FMC已注册，请确保AnyConnect许可证存在于您的智能帐户中，并且已将其分配给设备。

要分配许可证，导航到FMC设备，选择您的设备，许可证（铅笔图标）。在智能帐户中选择许可证，然后选择保存。

部署远程访问VPN配置时，为什么会出现Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled错误？

在FTD上部署的远程访问VPN需要启用强加密许可证。En确定FMC上启用了强加密许可证。要检查强加密许可证的状态，导航到FMC系统>许可证>智能许可并验证是否启用了导出控制功能。

如果Export-Controlled Features被禁用，如何启用强加密许可证？

如果在FMC注册到智能帐户云期间使用的令牌已启用选项Allow export-controlled functions on the products registered with this token，则会自动启用此功能。如果令牌未启用此选项，请取消注册FMC并在启用此选项的情况下重新注册。

如果生成令牌时“允许使用此令牌注册的产品上的导出控制功能”选项不可用，可以执行什么操作？

请与您的思科客户团队联系。

为什么会收到“Strong crypto (is , encryption algorithm greater than DES) for VPN topology s s2 is not supported”错误？

当FMC使用评估模式或智能许可证帐户无权获得强加密许可证时，显示此错误。V验证FMC是否已注册到许可证颁发机构，并启用允许使用此令牌注册产品的导出控制功能。如果智能帐户不允许使用强加密许可证，则不允许部署密码强度高于DES的VPN站点到站点配置。

为什么收到FMC上的“不合规”状态？

当其中一个受管设备使用不可用的许可证时，设备可能会变得不合规。

如何纠正“不合规”状态？

按照《Firepower配置指南》中描述的步骤进行操作：

1. 查看页面底部的“智能许可证”部分，确定需要哪些许可证。
2. 通过常用渠道购买所需许可证。
3. 在思科智能软件管理器(<https://software.cisco.com/#SmartLicensing-Inventory>)，验证许可证是否出现在您的虚拟帐户中。
4. 在FMC中，选择系统>许可证>智能许可证。
5. 选择重新授权。

完整过程可在[Firepower系统许可](#)中找到。

Firepower威胁防御基础功能是什么？

基础许可证允许：

- 配置FTD设备以进行交换和路由（包括DHCP中继和NAT）。
- 在高可用性(HA)模式下配置FTD设备。
- 将安全模块配置为Firepower 9300机箱内的集群（机箱内集群）。

- 将Firepower 9300或Firepower 4100系列设备(FTD)配置为群集 (机箱间群集)。
- 配置用户和应用控制，向访问控制规则添加用户和应用条件。

如何获取Firepower威胁防御基础功能许可证？

每次购买Firepower威胁防御或Firepower威胁防御虚拟设备时，都会自动随附基本许可证。当FTD注册到FMC时，会自动将其添加到您的智能帐户。

在FMC和智能许可证云之间的路径中必须允许哪些IP地址？

FMC使用IP 端口443上，用于与智能许可证云进行通信。

该IP地址(<https://tools.cisco.com>)解析为以下IP地址：

- 72.163.4.38
- 173.37.145.8

对于高于7.3的FMC版本，它会连接到解析为以下IP地址的<https://smartreceiver.cisco.com>：

- 146.112. 59. 81

相关信息

- [Firepower管理中心配置指南](#)
- [Cisco Live智能许可概述：BRKARC-2034](#)
- [Cisco Secure Firewall Management Center功能许可证](#)
- [思科智能软件许可常见问题\(FAQ\)](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。