利用 FMC 和 FTD 智能许可证注册及常见问题排除故障

目录

简介

先决条件

- 要求
- 使用的组件

FMC、FTD和智能许可证注册

FMC智能许可证注册

- 先决条件
- FMC智能许可证注册
- 在思科许可证中心端进行确认
- FMC智能许可证取消注册

RMA

故障排除

- 时间同步验证
- 启用名称解析并检查与tools.cisco.com的连通性（smartreceiver.cisco.com，来自FMC 7.3+）
- 验证从FMC到tools.cisco.com（smartreceiver.cisco.com从FMC 7.3+）的HTTPS(TCP 443)访问
- DNS验证
- 代理验证
  - 过期的令牌ID
  - 更改FMC网关
  - 检查FMC上的运行状况事件
  - 检查思科许可证中心端的事件日志

常见问题

- 案例研究1.无效令牌
- 案例研究2.无效的DNS
- 案例研究3.时间值无效
- 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
  - 思科许可证中心发送的电邮通知
- 从FMC获取运行状况警报通知
- 同一智能帐户上的多个FMC
- FMC必须保持Internet连接
- 部署多个FMCv

常见问题(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

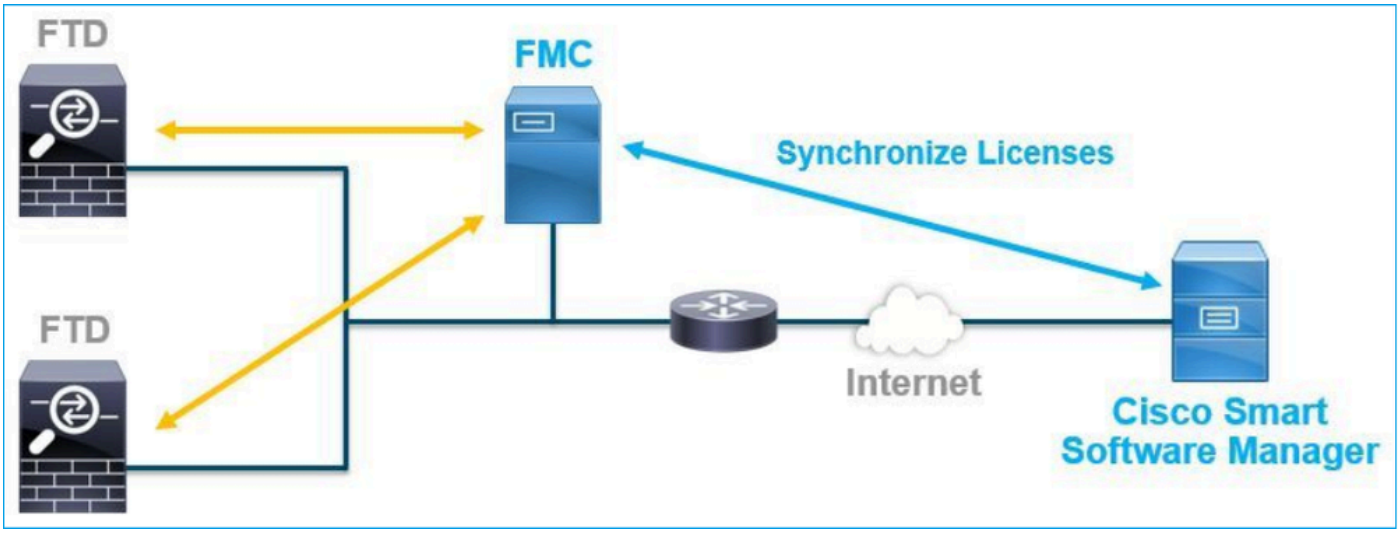
本文档没有任何特定的要求。

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。

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通过互联网与思科许可中心门户通信。在思科许可证中心，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注册到思科许可证中心时，此许可证将自动注册到您的智能帐户。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还需要思科许可证中心中的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。

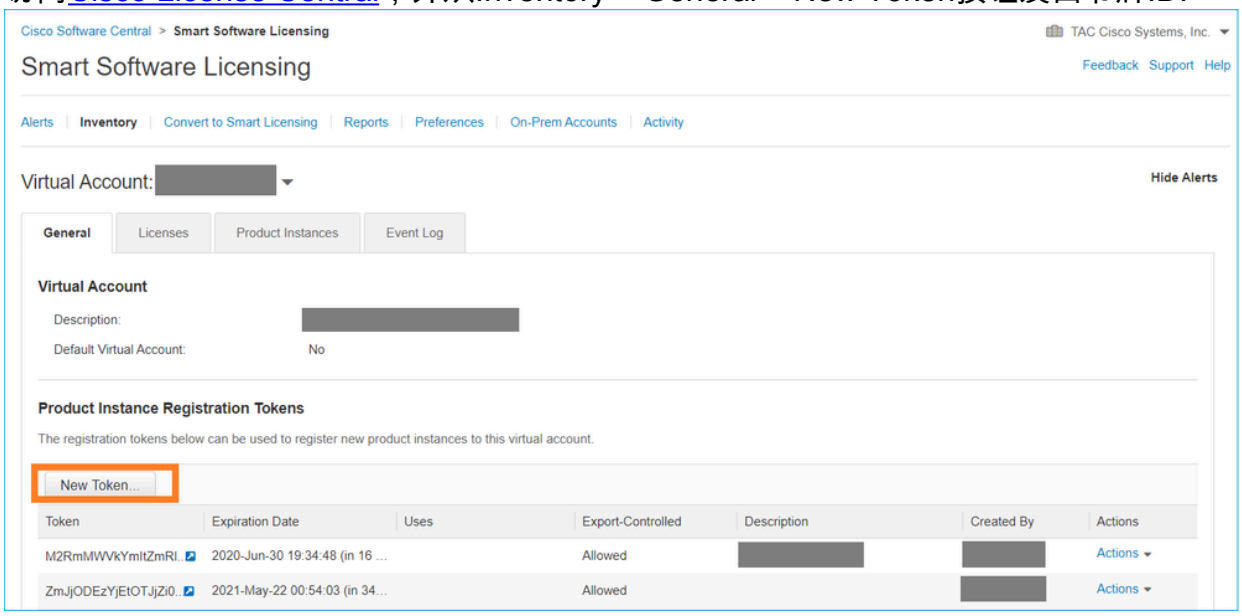
此外，本文档中的场景有助于排除潜在的常见许可证注册错误。

有关许可证的详细信息，请查看Cisco Firepower系统功能许可证和有关Firepower许可的常见问题(FAQ)。

FMC智能许可证注册

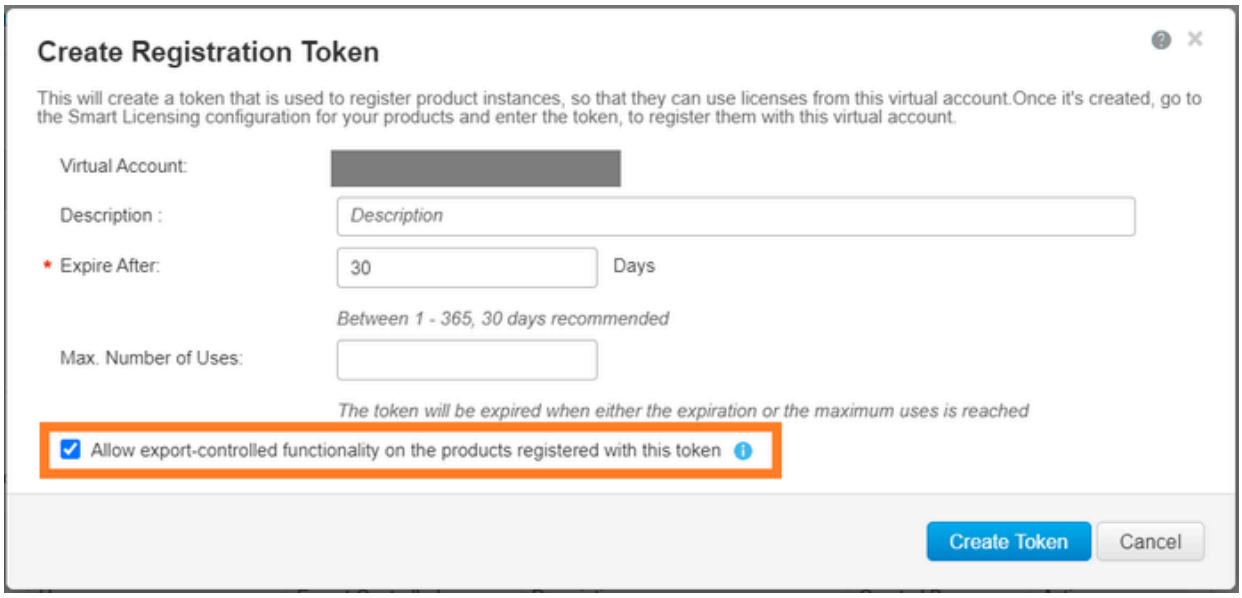
先决条件

1. 对于智能许可证注册，FMC必须访问互联网。由于证书在FMC和使用HTTPS的智能许可证云之间交换，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Cisco License Central，并从Inventory > General > New Token按钮发出令牌ID:



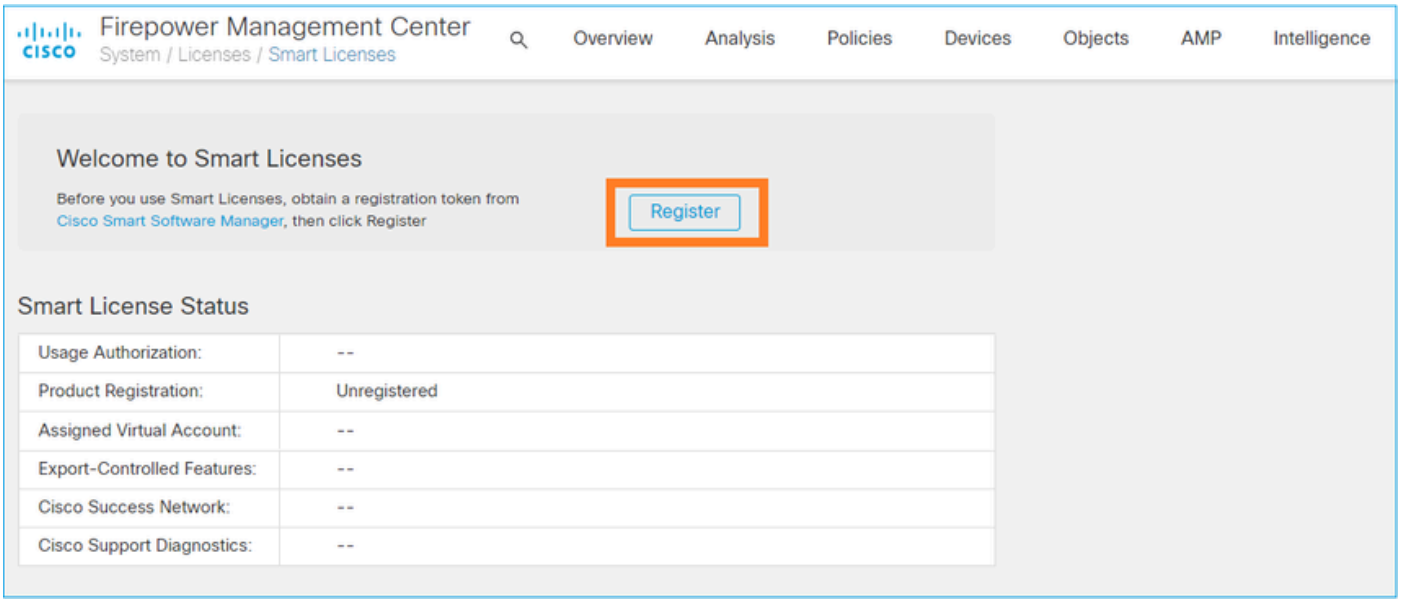
要使用强加密，请在使用此令牌注册的产品上启用Allow export-controlled（允许导出控制）功能。启用后，复选框中显示一个复选标记。

3. 选择Create Token。

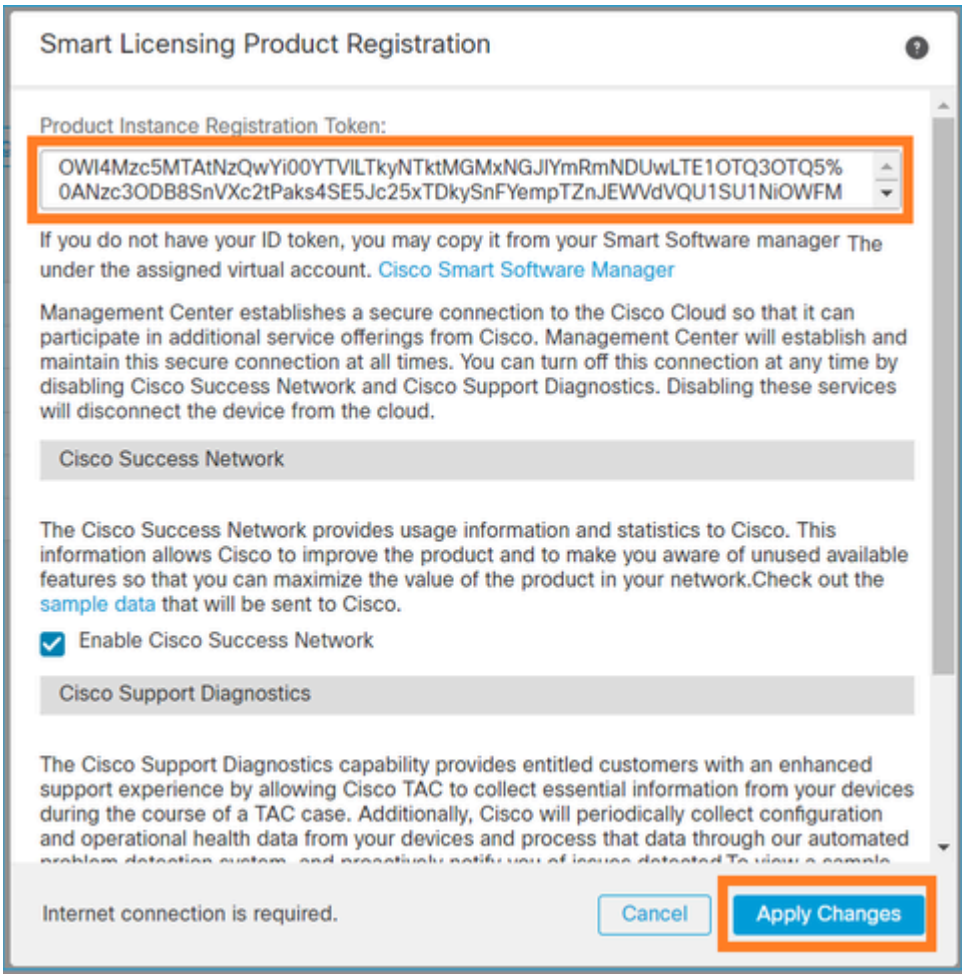


FMC智能许可证注册

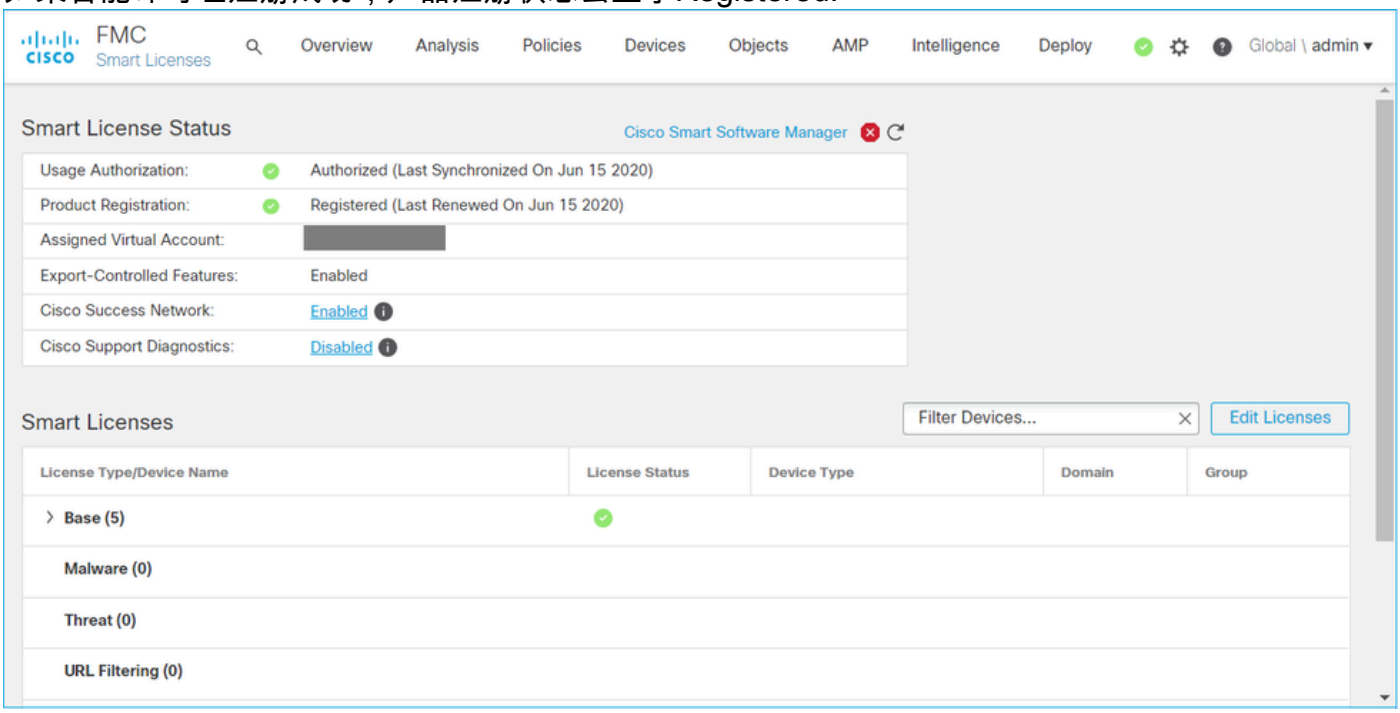
导航到FMC上的System > Licenses > Smart Licenses，然后选择Register按钮：



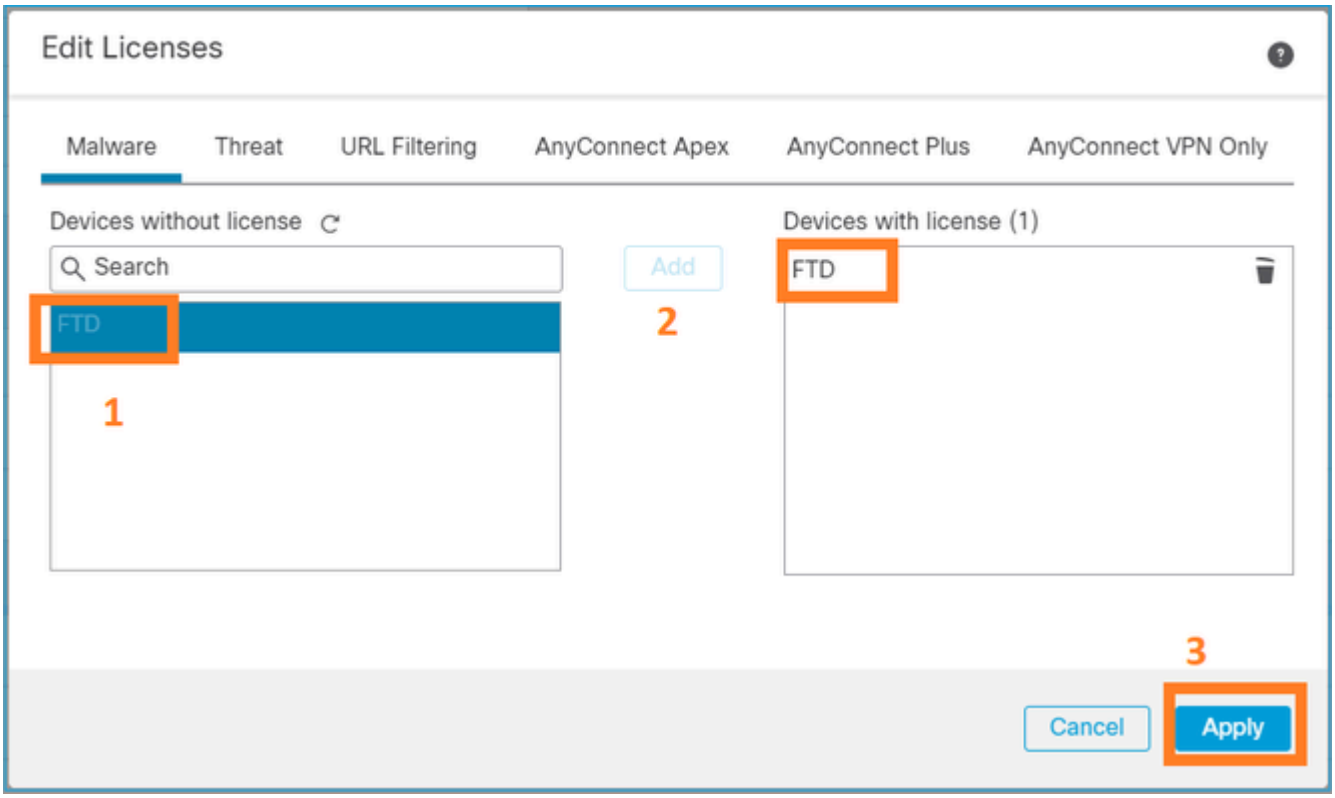
在Smart Licensing Product Registration窗口中输入令牌ID，然后选择Apply Changes:



如果智能许可证注册成功，产品注册状态会显示Registered:

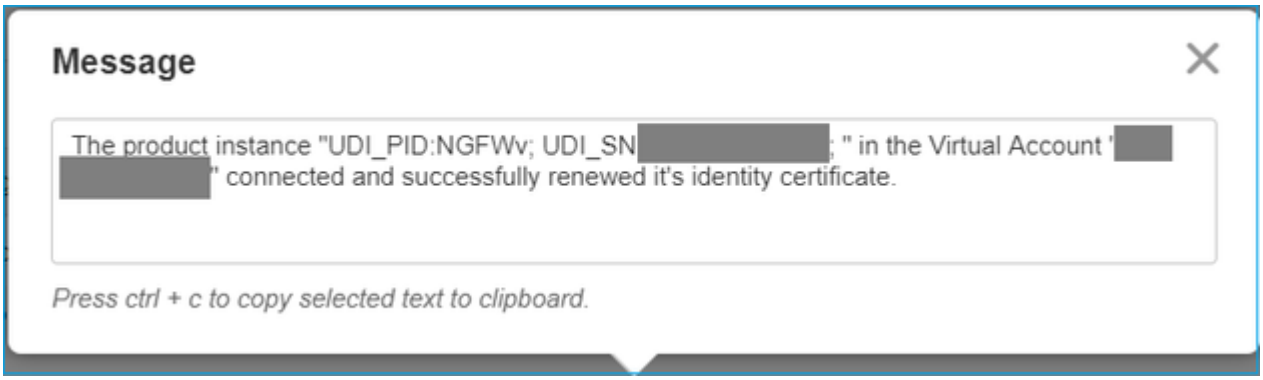


要将基于期限的许可证分配到FTD设备，请选择Edit Licenses。然后，选择受管设备并将其添加到Devices with license部分。最后，选择Apply按钮：



在思科许可证中心端进行确认

FMC智能许可证注册成功与否可在思科许可证中心的资产>事件日志中确认：

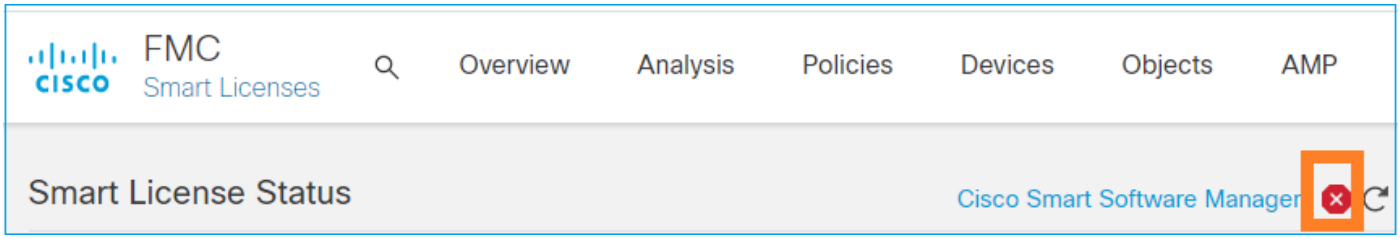


FMC的注册状态可以通过资产>产品实例确认。从Event Log（事件日志）选项卡中检查事件日志。智能许可证注册和使用状态可以从Inventory > Licenses选项卡进行检查。验证所购买的基于期限的许可证是否正确使用，以及是否有任何警报表明许可证不足。

FMC智能许可证取消注册

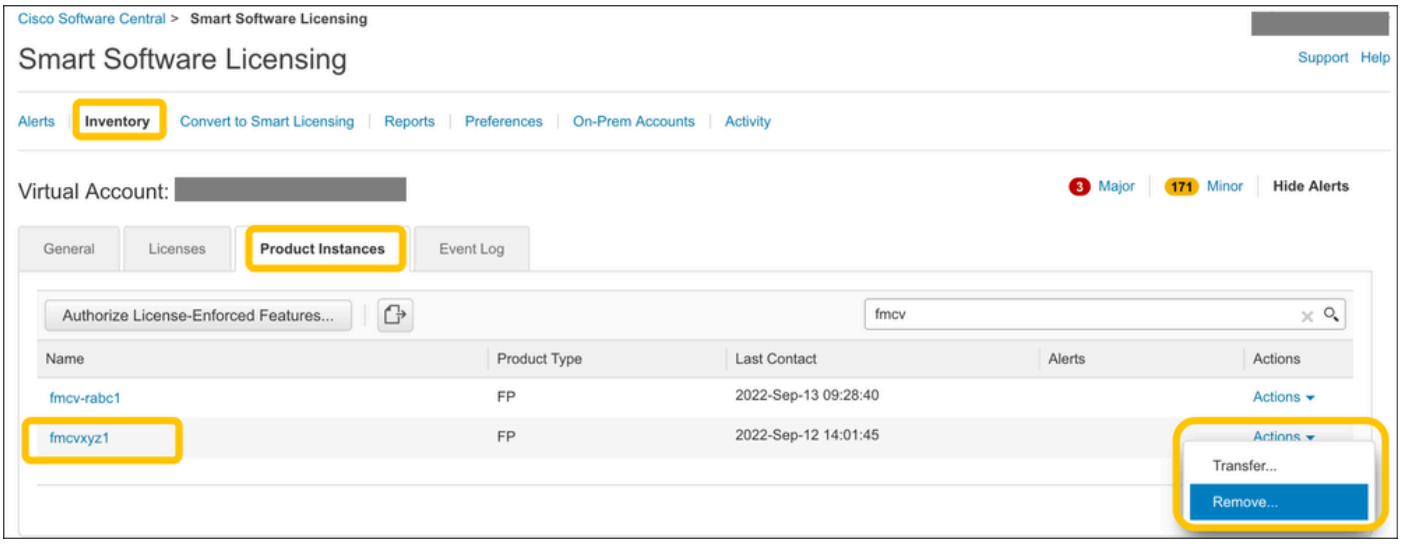
从思科许可证中心注销FMC

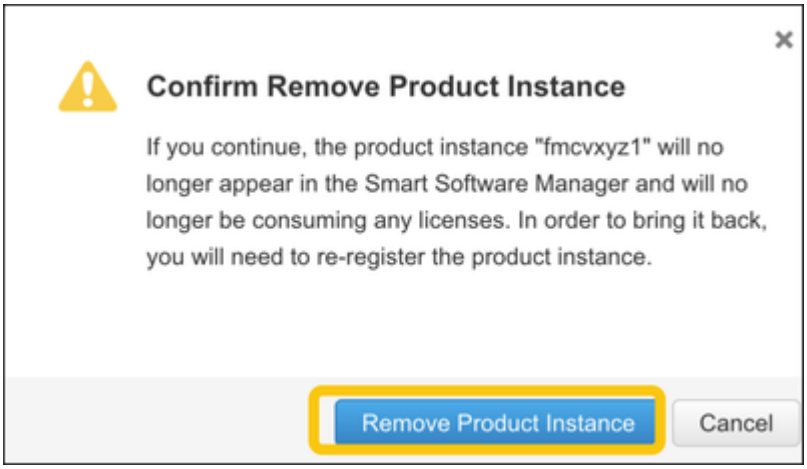
要因某种原因释放许可证或使用其他令牌，请导航到System > Licenses > Smart Licenses，然后选择“取消注册”按钮：



从思科许可证中心端删除注册

访问Cisco License Central，从Inventory > Product Instances中选择目标FMC上的Remove。然后选择Remove Product Instance以删除FMC并释放分配的许可证：





RMA

如果返回FMC，请按照FMC智能许可证撤销注册>从思科许可证中心端删除注册部分中的步骤从思科许可证中心注销FMC，然后按照FMC智能许可证注册部分中的步骤向思科许可证中心重新注册FMC。

故障排除

时间同步验证

访问FMC CLI（例如，SSH），并确保时间正确且与受信任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的连通性（smartreceiver.cisco.com，来自FMC 7.3+）

确保FMC可以解析FQDN并能根据Cisco Bug ID CSCwj95397从FMC 7.3开始访问tools.cisco.com(smartreceiver.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，从System > Configuration > Management Interfaces验证管理IP和DNS服务器IP。

验证从FMC到tools.cisco.com（smartreceiver.cisco.com从FMC 7.3+）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（来自FMC 7.3+的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
  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; 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

如果使用代理，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@FMC:/Volume/home/admin#

cat /etc/sf/iprep_proxy.conf


iprep_proxy {
PROXY_HOST proxy.example.com;
PROXY_PORT 80;
}
```

在较早的FMC版本中，使用：

<#root>

```
root@FMC:/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，可以从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tools.cisco.com。此外，允许通过代理交换流量和证书。FMC使用证书进行智能许可证注册)。

过期的令牌ID

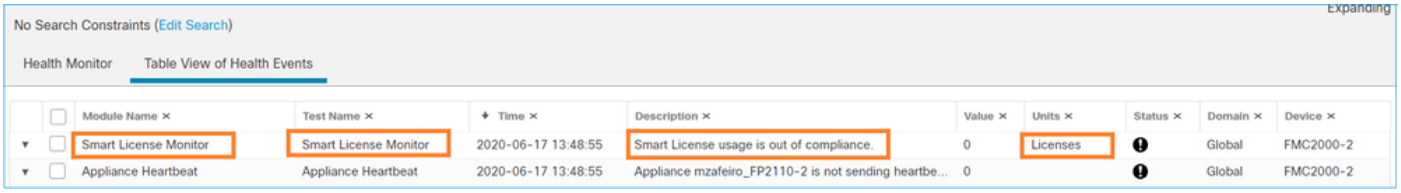
验证颁发的令牌ID未过期。如果该令牌已过期，请要求思科许可证中心管理员颁发新令牌，并使用新令牌ID重新注册智能许可证。

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。如果可能，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System > Health > Events，并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；生成错误，例如id certificated expired:



检查思科许可证中心端的事件日志

如果FMC可以连接到思科许可证中心，请在资产 > 事件日志中检查连接的事件日志。检查思科许可证中心是否有此类事件日志或错误日志。如果FMC站点的值/操作没有问题，并且思科许可证中心端没有事件日志，则可能是FMC和思科许可证中心之间的路由有问题。

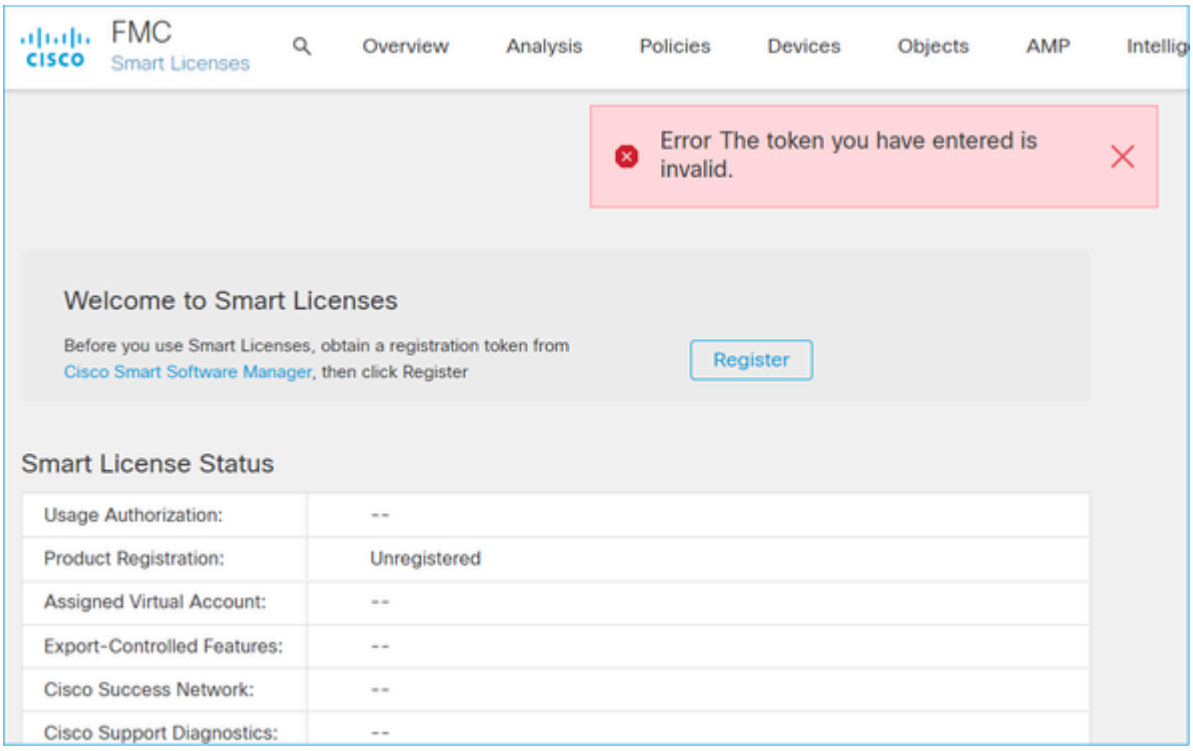
常见问题

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。
Registered	已授权	FMC已在思科许可证中心注册，并且存在使用有效订用注册的FTD设备。
Registered	授权已过期	FMC与思科许可证后端通信超过90天失败。
Registered	未注册	FMC已向思科许可证中心注册，但FMC上未注册FTD设备。
Registered	不合规	FMC已向思科许可证中心注册，但存在向无效订用注册的FTD设备。 例如，FTD(FP4112)设备使用THREAT订用，但是对于思科许可证中心，FP4112没有可用的THREAT订用。
评价（90天）	不适用	评估期正在使用中，但是在FMC上未注册FTD设备。

案例研究1.无效令牌

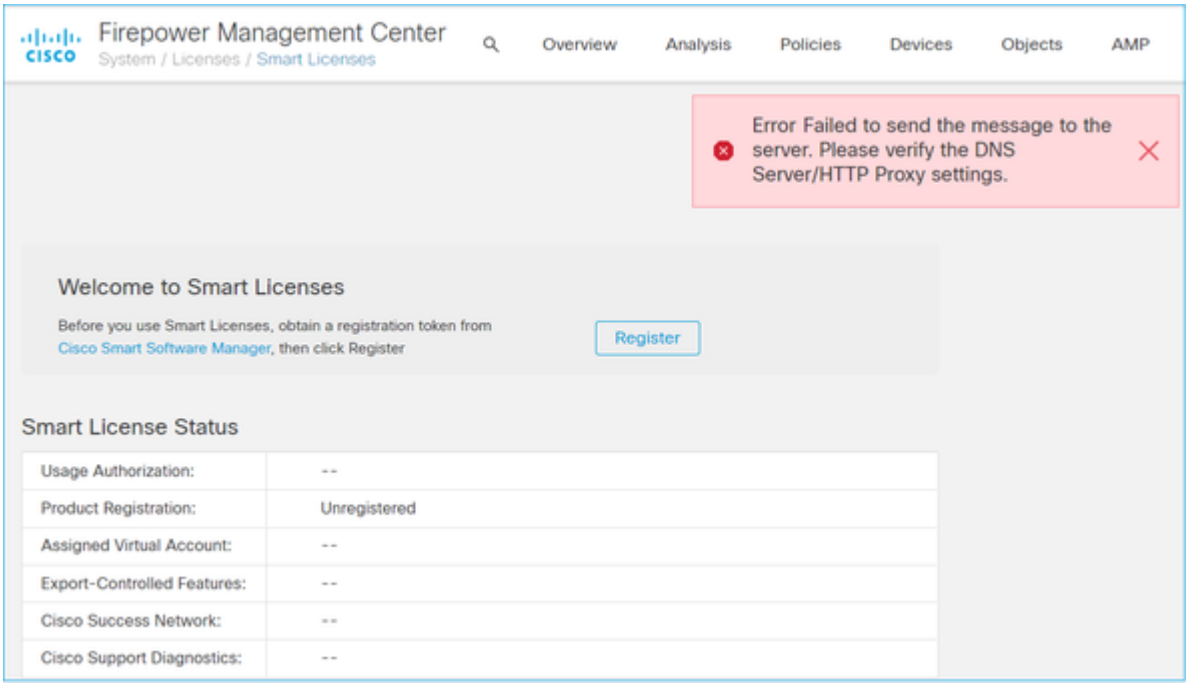
症状：由于令牌无效，向思科许可证中心注册快速（约10秒）失败：



分辨率：使用有效令牌。

案例研究2.无效的DNS

症状：向思科许可证中心注册在一段时间（约25秒）后失败：



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

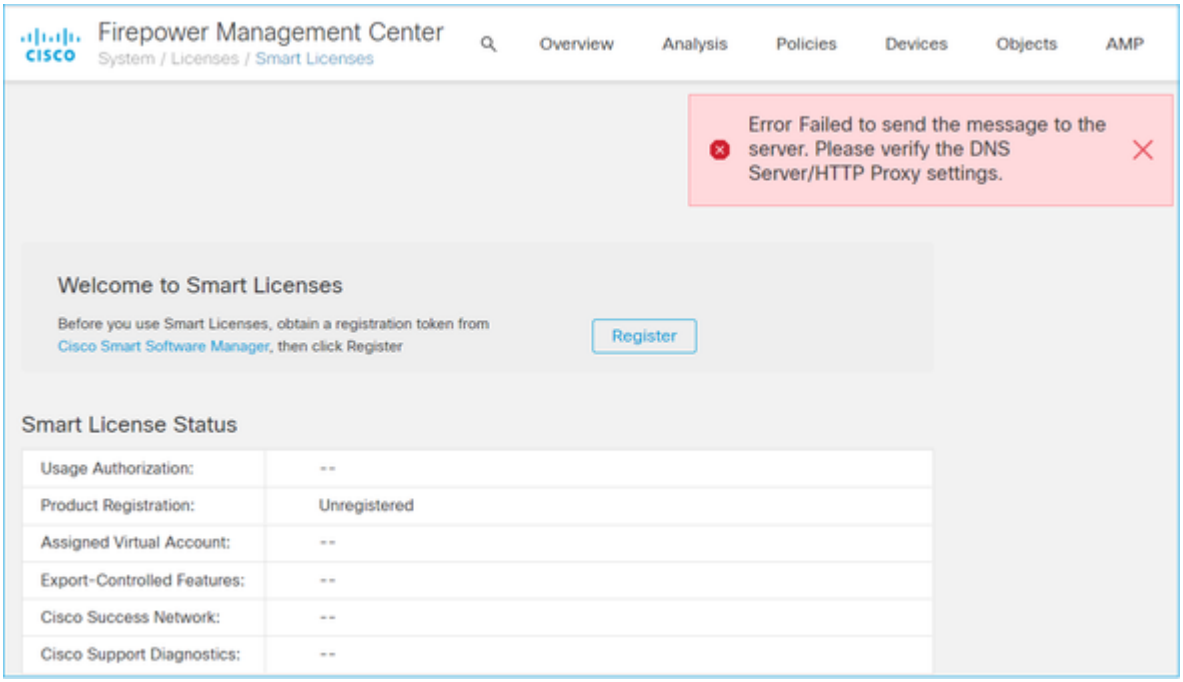
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494], failed to perform, err code 6, err string

"Couldn't resolve host name"

分辨率：思科许可证中心主机名解析失败。解决方法是配置DNS（如果未配置），或者修复DNS问题。

案例研究3.时间值无效

症状：向思科许可证中心注册一段时间后（大约25秒）失败：



检查/var/log/process_stdout.log文件。证书问题可见：

<#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/oddce/services/DDCEService
```

检查FMC时间值：

```
<#root>

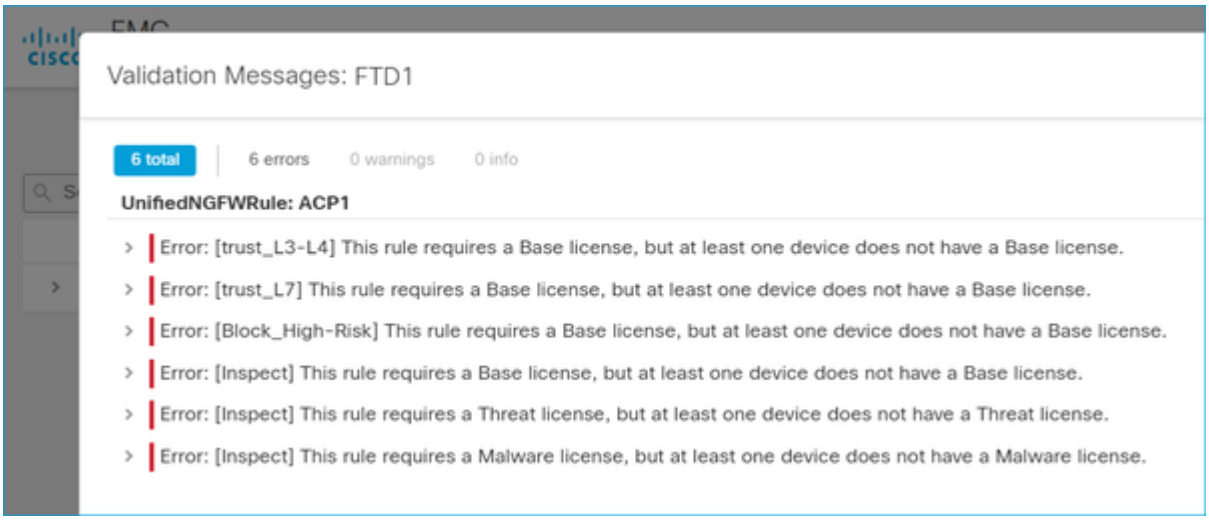
root@FMC2000-2:/Volume/home/admin#

date

Fri Jun 25 09:27:22 UTC 2021
```

案例研究4.无订用

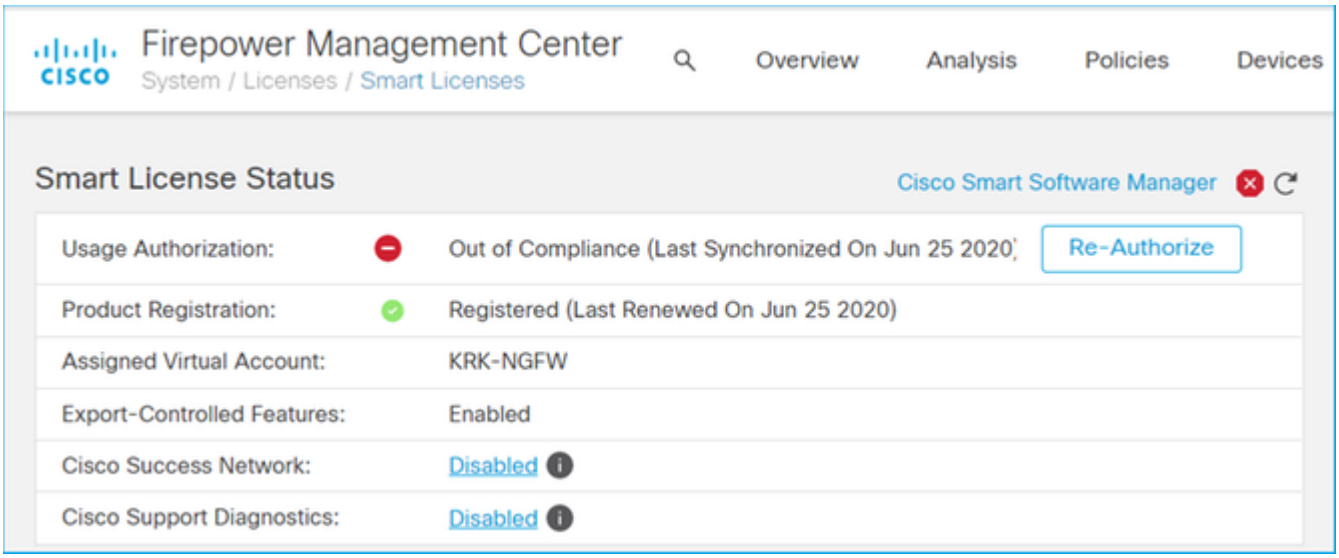
如果没有特定功能的许可证订用，则无法进行FMC部署：



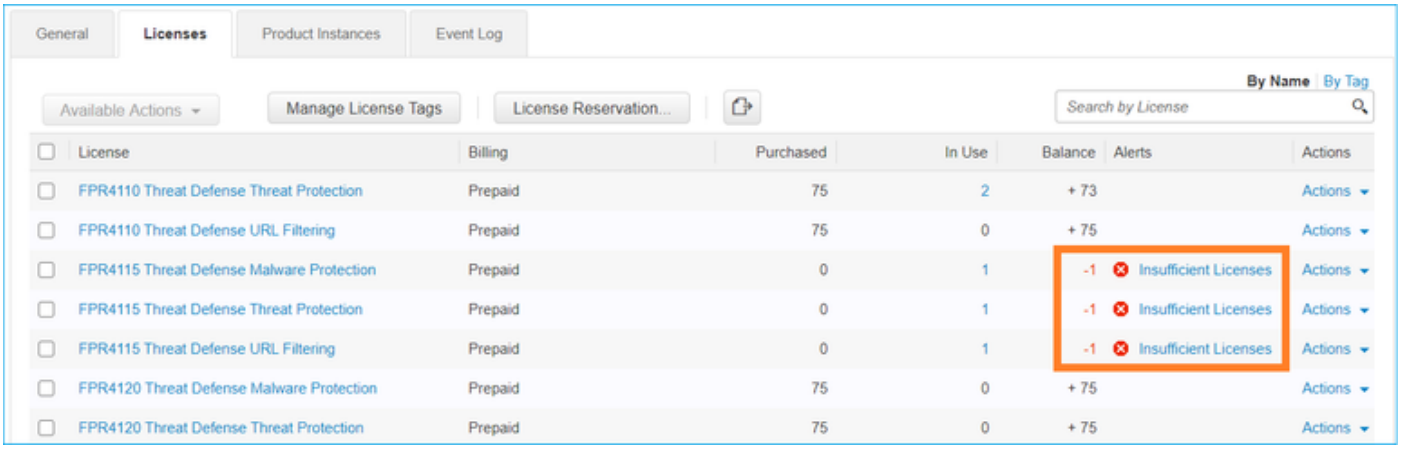
分辨率：需要购买所需订用并将其应用到设备。

案例研究5.不合规(OOC)

如果没有FTD订用的授权，则FMC智能许可证将进入不合规(OOC)状态：



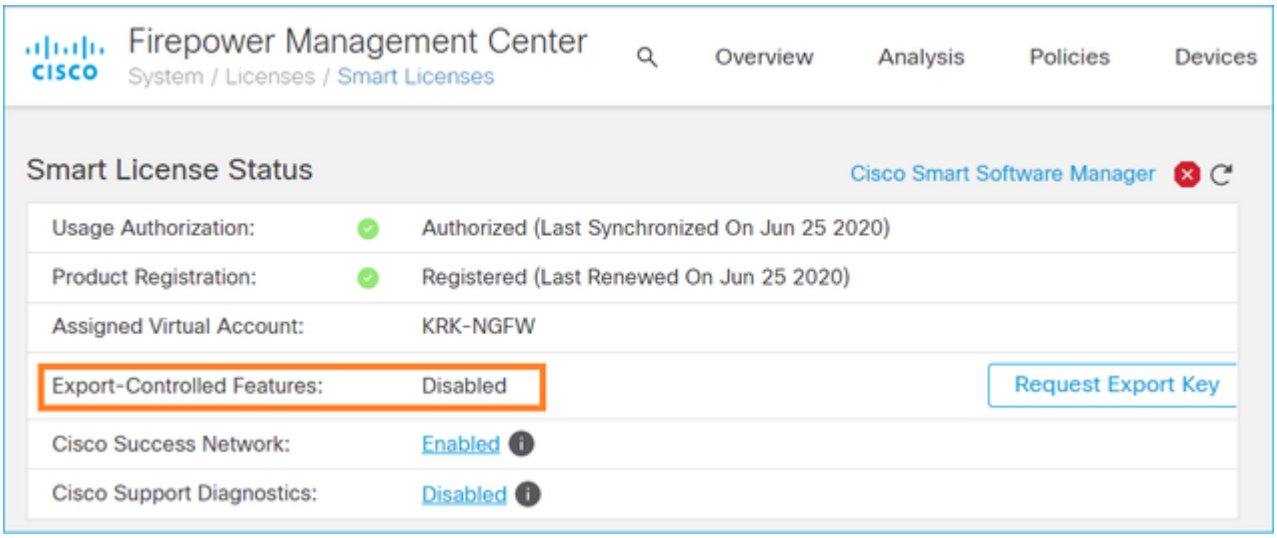
在思科许可证中心，检查警报中的错误：



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，采用更强算法的L2L虚拟专用网络(VPN)等部署会失败：





分辨率：将FMC注册到思科许可证中心，并启用强加密属性。

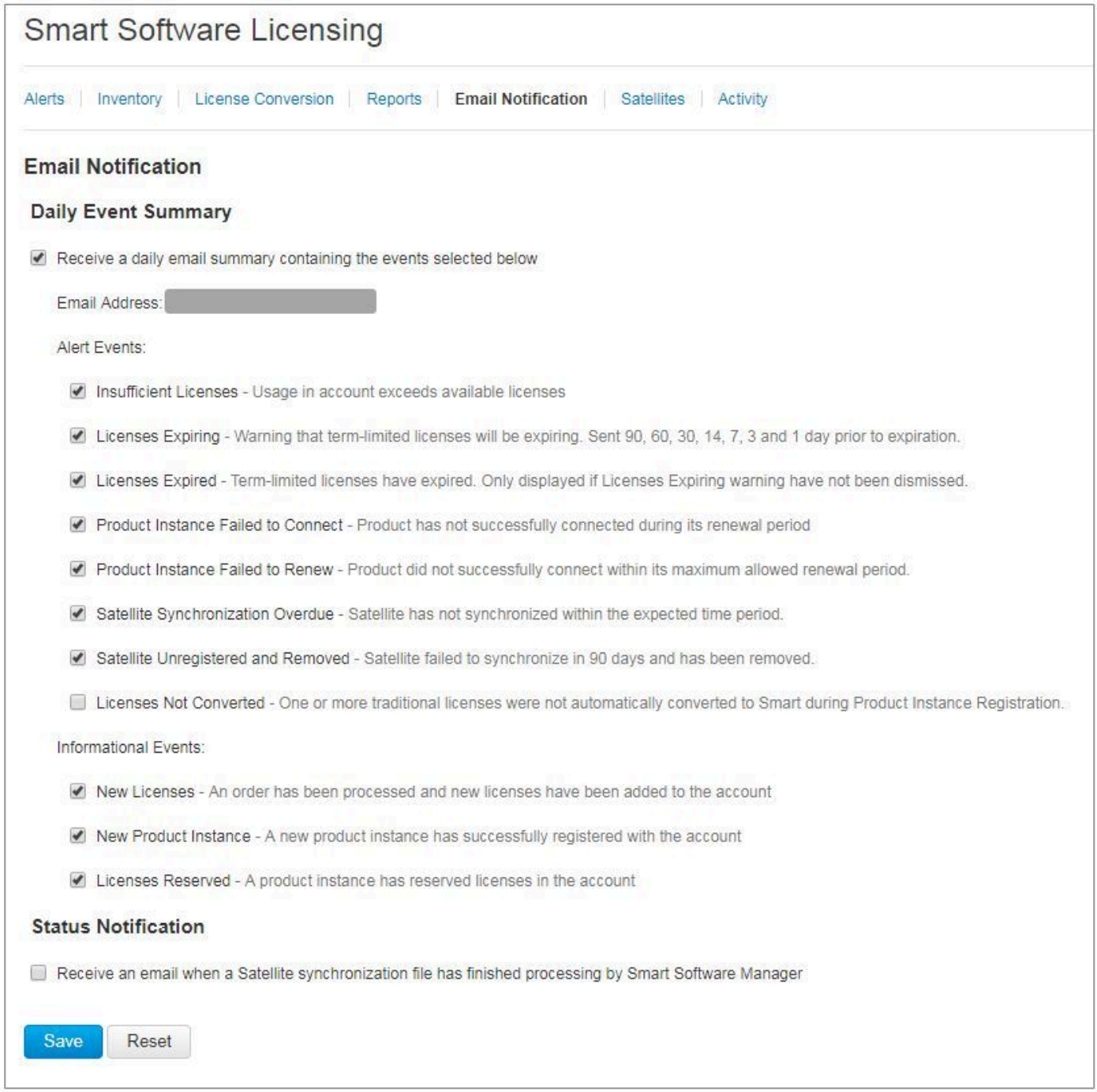
其他说明

设置智能许可证状态的通知

思科许可证中心发送的电邮通知

在思科许可证中心端，思科许可证中心电邮通知允许接收各种事件的摘要电邮。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。

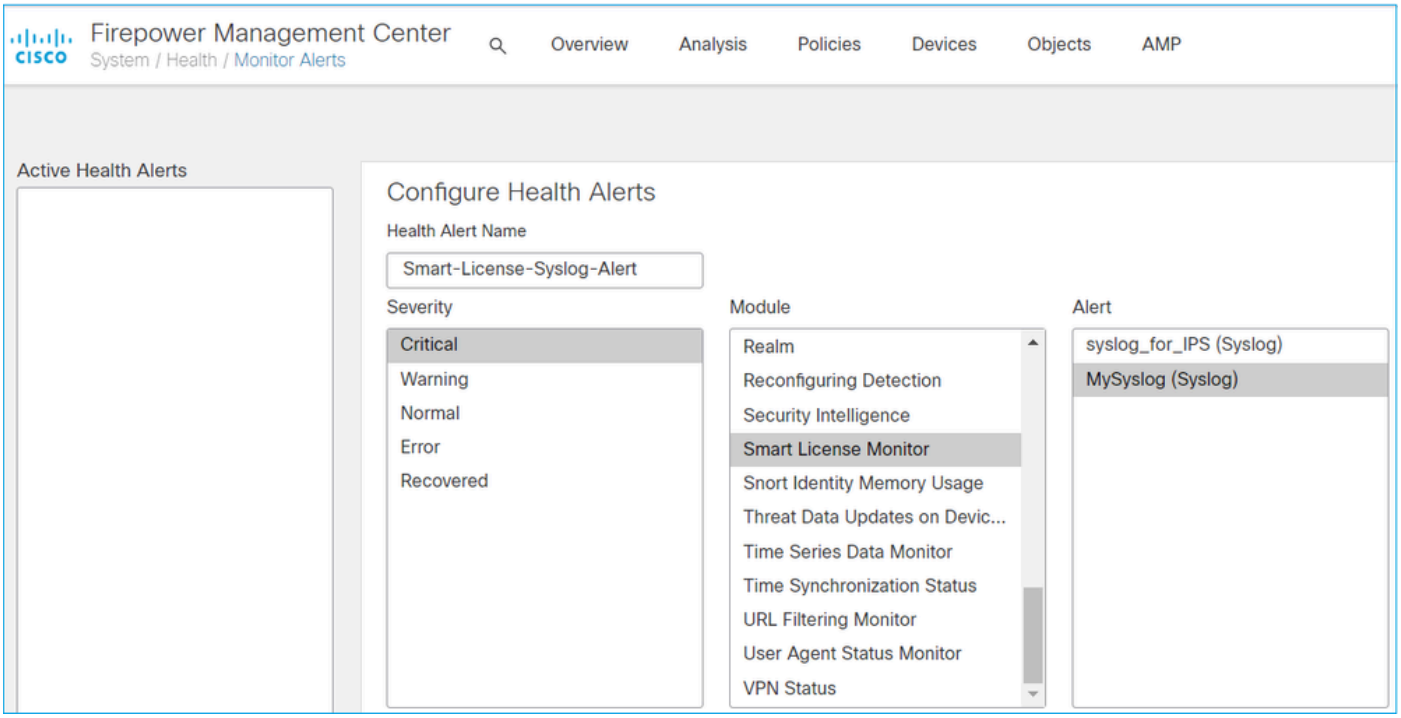
此功能非常有助于通知和防止出现由于许可证到期而导致的功能限制。



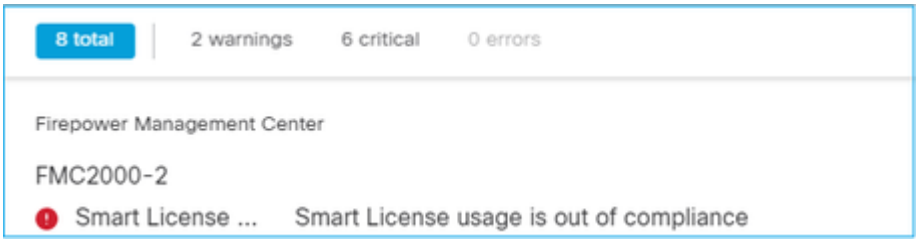
从FMC获取运行状况警报通知

在FMC端，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。模块智能许可证监视器可用于检查智能许可证状态。监控器警报支持Syslog、Email和SNMP陷阱。

以下是在发生智能许可证监控器事件时获取系统日志消息的配置示例：



下面是运行状况警报的示例：



FMC生成的系统日志消息为：

<#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主机名必须唯一。当管理思科许可证中心中的多个

FMC时，要区分每个FMC，每个FMC的主机名必须是唯一的。这对于正在运行的FMC智能许可证维护非常有用。

FMC必须保持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，则许可功能会保留，但会保留在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)文件逐个创建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(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，每台设备都需要一个许可证。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。

为什么FTD不使用AnyConnect许可证？

将FMC注册到智能帐户后，确保已启用AnyConnect许可证。要启用许可证，请导航到FMC > Devices，选择您的设备，然后选择License。选择铅笔图标，选择存放在“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“使用中”？

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。

在FMC配置和部署远程接入VPN后，没有AnyConnect许可证的设备意味着什么？

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，请确保您的智能帐户中存在AnyConnect许可证，并且已将其分配给设备。

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

禁用导出控制功能（强加密）后，当部署远程访问VPN配置时，无法部署带SSL的远程访问VPN意味着什么？

在FTD上部署的远程访问VPN需要启用强加密许可证。确保在FMC上启用了强加密许可证。要检查强加密许可证的状态，请导航到FMC System > Licenses > Smart Licensing，并验证是否启用了导出控制功能。

如果禁用了导出控制功能，如何启用强加密许可证？

如果FMC注册到智能帐户云期间使用的令牌具有选项Allow export-controlled functionality on the products registered with this token enabled，则此功能将自动启用。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再次注册。

如果生成令牌时，使用此令牌注册的产品上的允许导出控制功能选项不可用，该怎么办？

请与您的思科客户团队联系。

对于VPN拓扑s2s，不支持强加密（即加密算法大于DES）意味着什么？

当FMC使用评估模式或智能许可证帐户无权使用强加密许可证时，会显示此错误。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的产品上的导出控制功能。如果智能帐户不允许使用强加密许可证，则不允许使用比DES更强的密码部署VPN站点到站点配置。

我为什么会在FMC上收到“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。

如何更正“不合规”状态？

执行《Firepower配置指南》中的以下步骤：

1. 查看页面底部的Smart Licenses部分，确定需要哪些许可证。
2. 通过常规渠道购买所需的许可证。
3. 在思科许可证中心中，验证许可证是否显示在虚拟帐户中。
4. 在FMC中，选择System > Licenses > Smart Licenses。
5. 选择重新授权。

在许可Firepower系统中查找完整过程。

Firepower威胁防御基础功能是什么？

基础许可证允许：

- 配置交换机和路由的FTD设备（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（机箱内集群）内的集群。
- 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，并将用户和应用条件添加至访问控制规则。

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，系统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使用端口443上的IP地址与智能许可证云通信。

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https://smartreceiver.cisco.com，解析为此IP地址：

- 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）。