与FMC集成的Threat Grid设备故障排除

目录

简介

本文档详细介绍与Firepower管理中心(FMC)的线程网格设备(TGA)集成。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower管理FMC
- Threat Grid设备基本配置
- 创建授权证书(CA)
- Linux/Unix

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FMC版本6.6.1
- Threat Grid 2.12.2
- CentOS 8

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。

问题

在此使用的案例场景中，您可以看到2个问题和2个错误代码。

场景 1

集成失败，但出现错误：

```
Sandbox registration failed: Peer certificate cannot be authenticated with given CA certificates
(code = 60)
```

在此问题中，问题与未作为完整链上传到FMC的证书有关。由于使用了CA签名的证书，因此需要将整个证书链合并到一个PEM文件中。换句话说，您以根CA **>中间证书**（如果适用）**> Clean Int开头**。请参阅官方指南中介绍要求和程序的本文。

如果存在多级CA签名链，则所有必需的中间证书和根证书必须包含在上传到FMC的单个文件中。

所有证书都必须采用PEM编码。

文件的新行必须是UNIX，而不是DOS。

如果Threat Grid设备提供自签名证书，请上传您从该设备下载的证书。

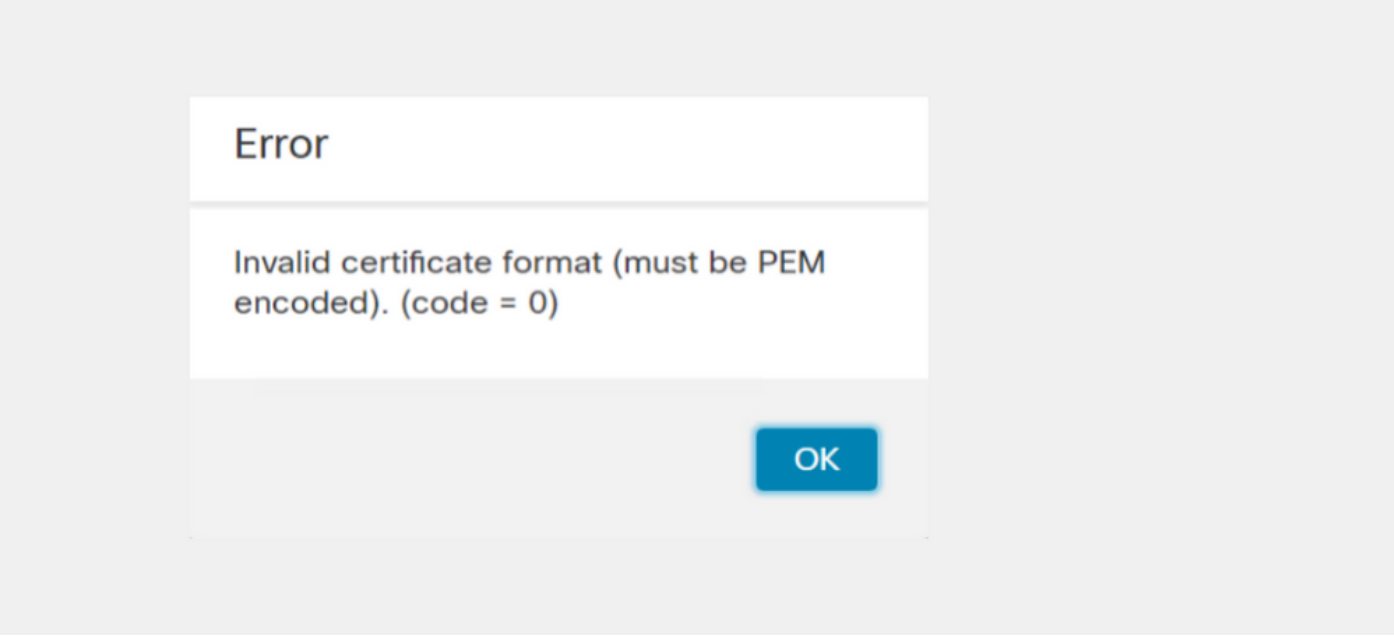
如果Threat Grid设备提供CA签名的证书，请上传包含证书签名链的文件。

场景 2

证书格式错误无效

```
Invalid Certificate format (must be PEM encoded) (code=0)
```

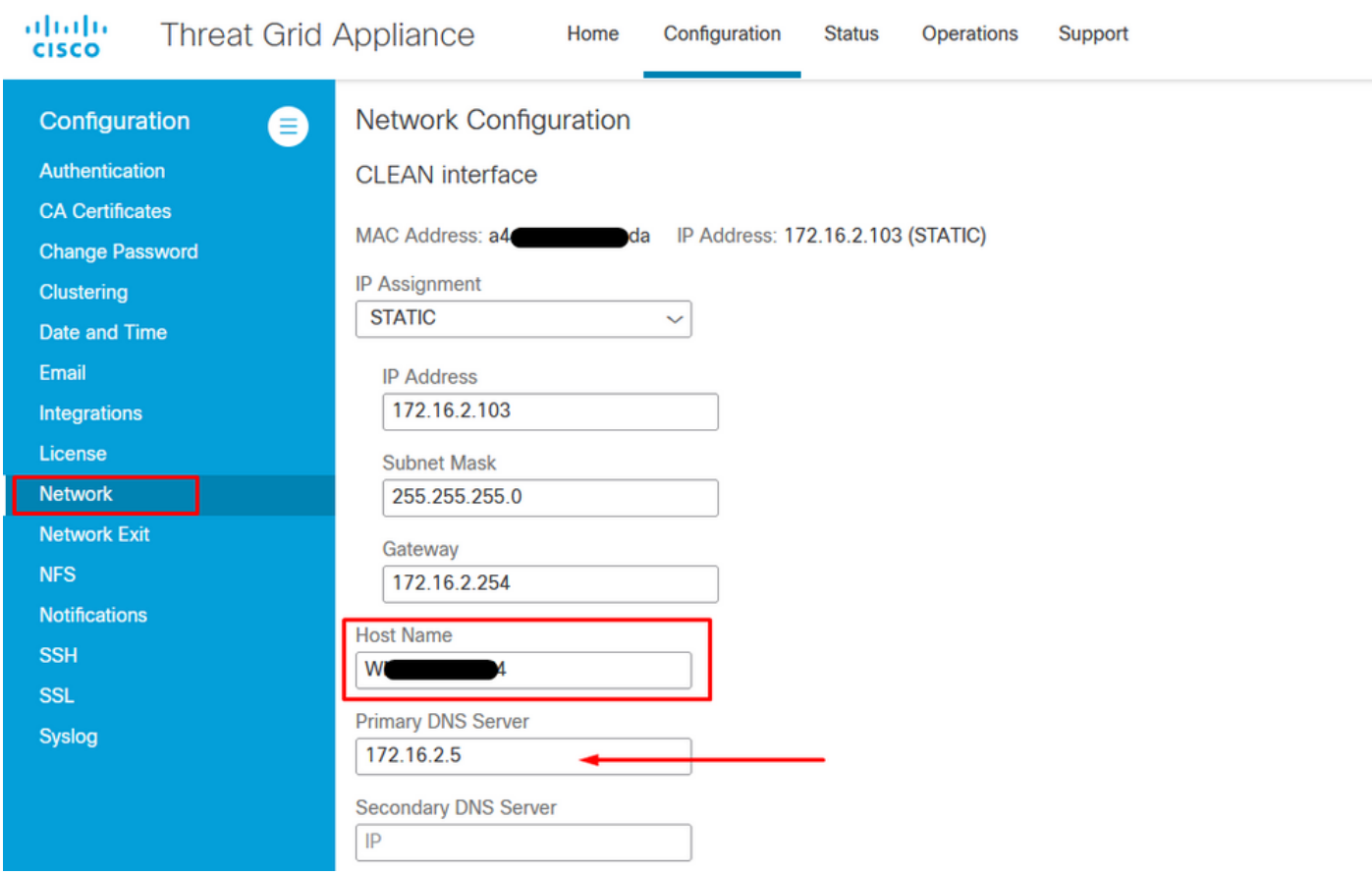
证书格式错误，如图所示。



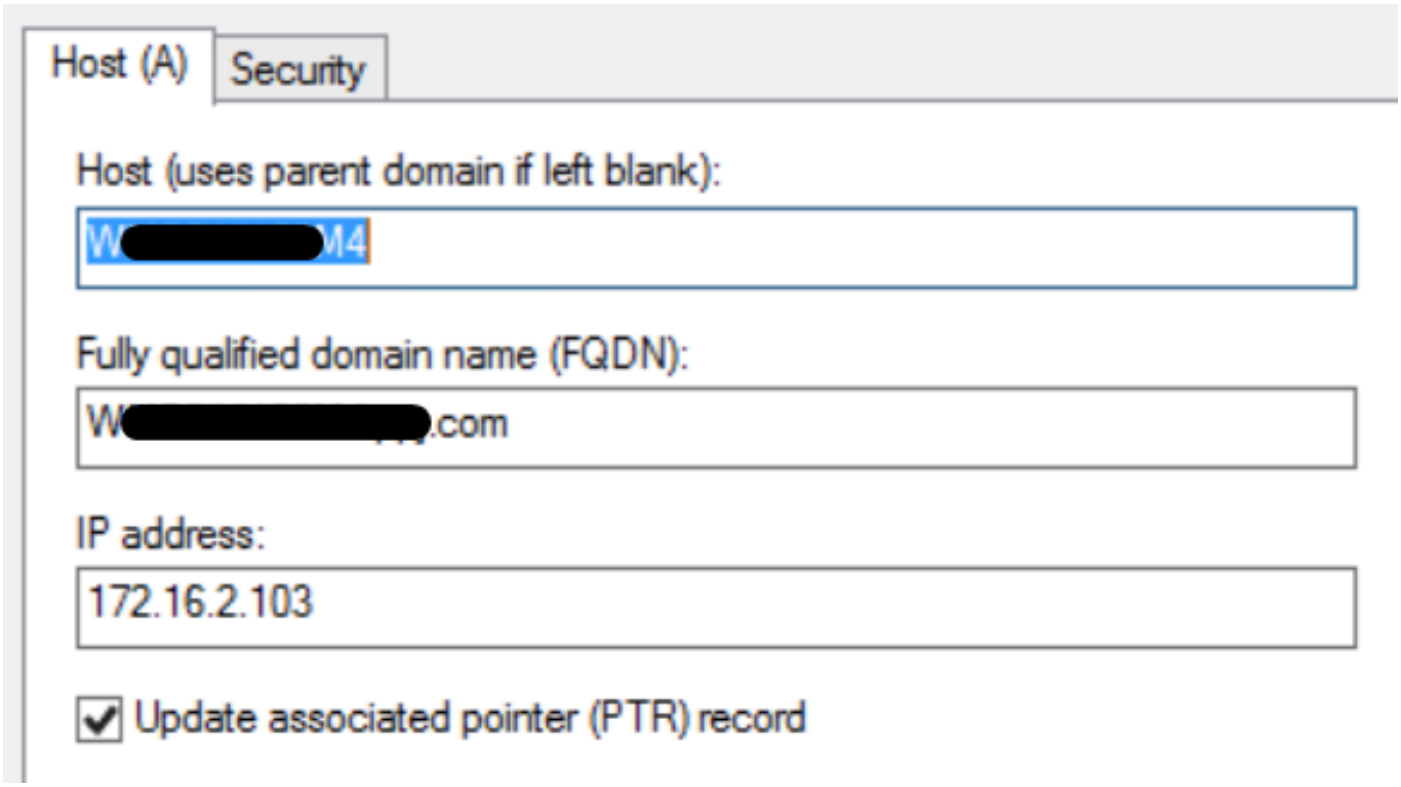
此错误是由于在使用OpenSSL的Windows计算机上创建的组合PEM证书的格式错误所致。强烈建议使用Linux计算机创建此证书。

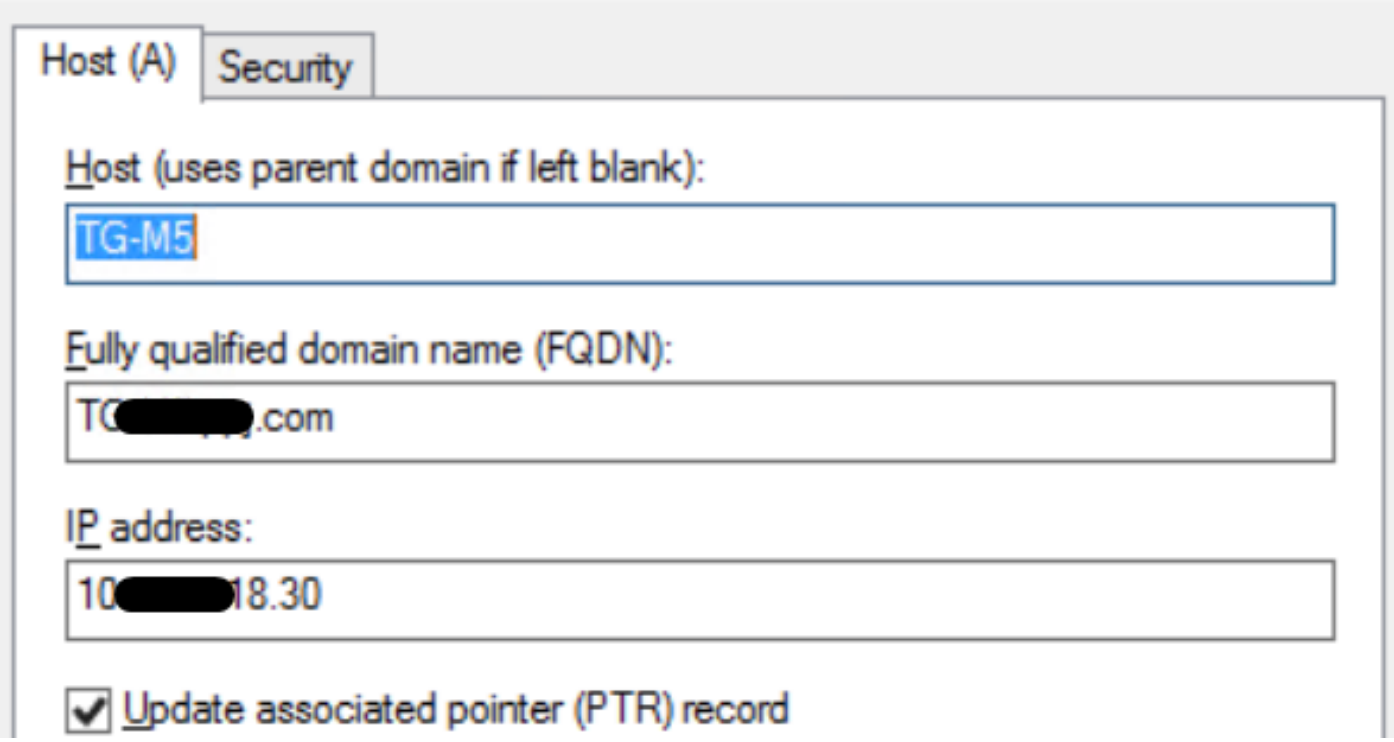
集成

步骤1.配置TGA，如图所示。




ADMIN interface
MAC Address: 40:[redacted]30
IP Address: 10
8.30 (STATIC)
IP Assignment
STATIC
IP Address
10[redacted]30
Subnet Mask
255.255.255.192
Gateway
10[redacted]1
Host Name
TG-M5
Save
Activate


Host (A)
Security
Host (uses parent domain if left blank):
W[redacted]M4
Fully qualified domain name (FQDN):
W[redacted].com
IP address:
172.16.2.103
Update associated pointer (PTR) record



Clean Admin接口的内部CA签名证书

步骤1.生成用于管理界面和干净界面的私钥。

```
openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem
```

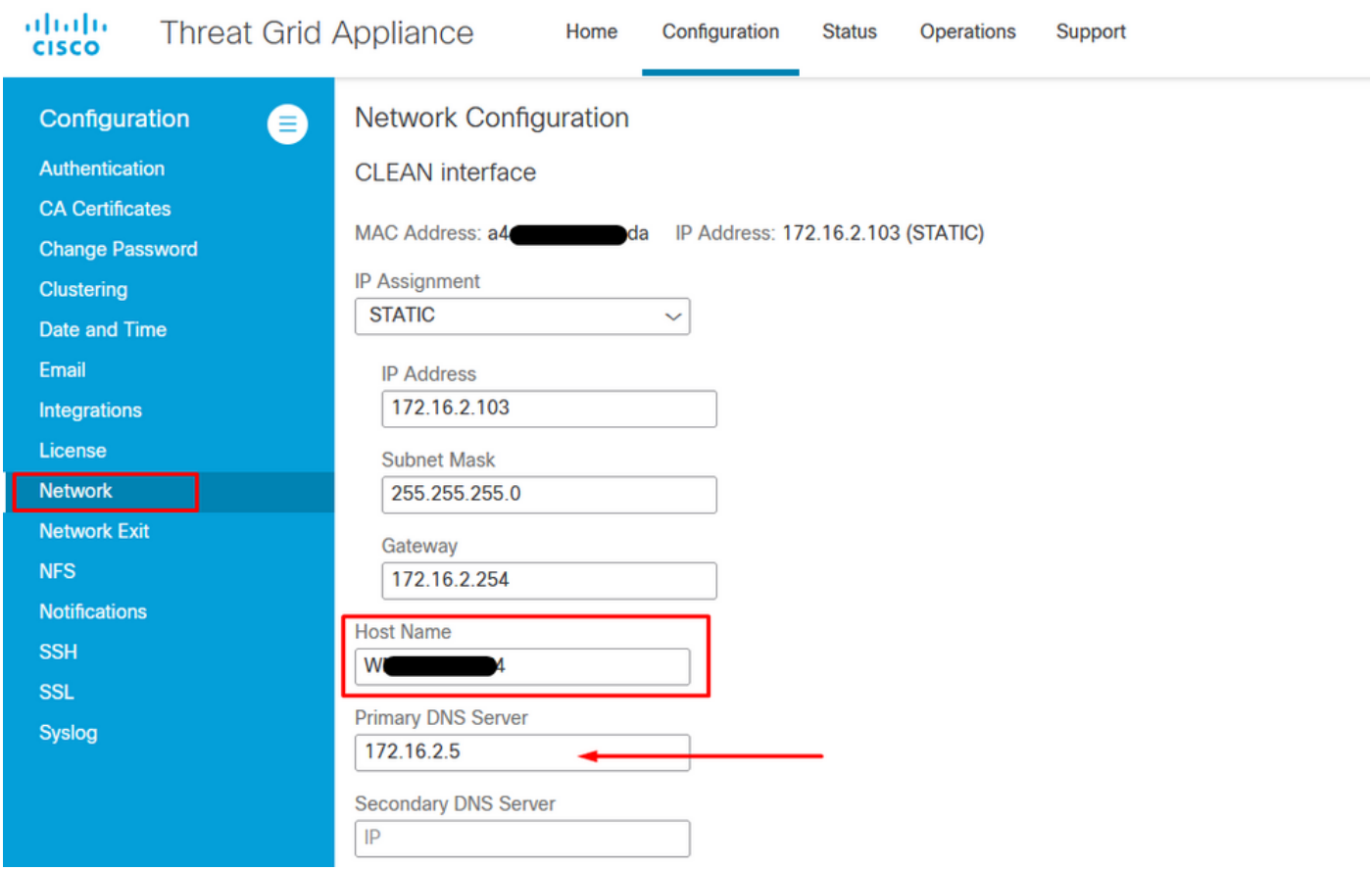
步骤2.生成CSR。

干净的接口

步骤1.导航至CSR创建并使用生成的私钥。

```
openssl req -new -key private-ec-key.pem -out MYCSR.csr
```

> **注意**：必须为CSR输入CN名称，并且必须与“Network”下定义的Clean接口的主机名匹配。DNS服务器上必须存在DNS条目，该条目解析了Clean接口主机名。



管理界面

步骤1.导航至CSR创建并使用生成的私钥。

```
openssl req -new -key private-ec-key.pem -out MYCSR.csr
```

注意：必须为CSR输入CN名称，并且必须与“Network”下定义的“admin interface”的“hostname”匹配。DNS服务器上必须存在DNS条目，该条目解析了干净的接口主机名。

步骤2. CSR由CA签署。以DER格式下载证书，其中包含CER扩展名。

步骤3.将CER转换为PEM。

```
openssl x509 -inform DER -outform PEM -in xxxx.cer -out yyyy.pem
```

CSR和CER到PEM的干净接口

```
C:\Users\Administrator\Downloads\TG\FMC>openssl req -new -key step7-1-private-ec
-key.pem -out clean-csr.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PPJ
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:WM[redacted].com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:C1sco@123
An optional company name []:PPJ

C:\Users\Administrator\Downloads\TG\FMC>openssl x509 -inform DER -outform PEM -i
n Clean-interface_CSR_CA-signed_DER_CER.cer -out Clean-interface_CSR_CA-signed_D
ER_PEM.pem
```

管理接口CSR和CER到PEM

```
C:\Users\Administrator\Downloads\TG\FMC>openssl req -new -key step7-1-private-ec
-key.pem -out Admin-interface_CSR.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PPJ
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:TG-[redacted].com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:C1sco@123
An optional company name []:PPJ

C:\Users\Administrator\Downloads\TG\FMC>openssl x509 -inform DER -outform PEM -i
n Admin-interface_CSR_CA-signed_DER_CER.cer -out Admin-interface_CSR_CA-signed_D
ER_PEM.pem
```

FMC证书的正确格式

如果您已经获得证书，并且证书为CER/CRT格式，并且使用文本编辑器时可读，您只需将扩展更改为PEM。

如果证书不可读，您需要将DER格式转换为PEM可读格式。

```
openssl x509 -inform DER -outform PEM -in xxxx.cer -out yyyy.pem
```

PEM

PEM可读格式示例，如图所示。

```
-----BEGIN CERTIFICATE-----
MIIFozCCA4ugAwIBAgITGQAAAALex/EgACaWIAAAAAAAAjANBgkqhkiG9w0BAQUF
ADAaMRgwFgYDVQQDEw9Ub21EZW1vIFJvb3QgQ0EwHhcNMTQwMjA3MTQwMTU3WhcN
MjQwMjA3MTQxMTU3WjBKMRIwEAYKCZImiZPyLGQBGRYCc2UxFzAVBgoJkiaJk/Is
ZAEZFgd0b21kZW1vMRswGQYDVQQDExJUb21EZW1vIE1zc3VpbmcgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDC8XmXxLHo0M/521CFtI4DSN6qVNAN
8jxujS4PSSRnQtaqpbjbcAZpvbYysNt2uwA40urkxY2nyn4SMy/21S4L9x10u8su
W+/4T2dcFgQKzFiNyqVkLop9vRKnCKjceD+FRKXbPCSZyy4Hhz/XCgwPRfaobx+q
aV1fSnW0[redacted]a2MHx60jf
BhdyONMrZxmQeYgFPUmd2o3x+lyq1406hIF7LLGFAoDdqi3R31D9OPb7+Dm2ezv0
OKkbCHdjl3inB3D1tg1L8mZeIEte+07RvlQXr33umO6zeYi4okbaHZLvAgMBAAGj
ggGwMIIBrDAQBgkrBgEEAYI3FQEEAwIBADAdBgNVHQ4EFgQU0+wPInpDnoqnuIlx
BtUbIGLdS1UwgYsGA1UdIASBgzCBgDB+BgorBgEEAYKdZwEBMHAwPgYIKwYBBQUH
AgIwMh4wAFQAbwBtAEQAZQBtAG8AIABQAG8AbABpAGMAeQAgAFMAdABhAHQAZQBt
AGUAbgB0MC4GCCsGAQUFBwIBFiJodHRwOi8vcGtpLnRvbWRlbW8uc2UvcGtpL2Nw
cy5odG0AMBkGCSsGAQQBgjcUAgQMHgoAUwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAP
BgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFL00e0rG2ExZ1dmboIuLwgGgPr5e
MEIGA1UdH[redacted]y5zZS9wa2kvVG9t
RGVtbyUyMFJvb3QlMjBDQS5jcmwwTQYIKwYBBQUHAQEEQTA/MD0GCCsGAQUFBzAC
hjFodHRwOi8vcGtpLnRvbWRlbW8uc2UvcGtpL1RvbURlbW81MjBSb290JTIwQ0Eu
Y3J0MA0GCSqGSIb3DQEBBQUAA4ICAQBBkNHalbX3kkpOXCV3nQ9R4CyG61WI90gL
57uGRcpulSqUu79OJ5s4xlW8rhm32db7qvHDPaYED23gudpOSHyUywZTFbwzm92c
e1wZpyJH6nsuqNFDTYQTdWAq8zwCrldcUFRW3O1mkPuhENjttqCIJ9KeLrwCaM/p
QVy7qWoTUl4/BY+OsLXDGURXrGejcVs8ZQy4bqhmh0TfelTcAOAX47pVt8XdnWFe
Vnu/rwuOnfvlyiWW62cknAATaagnLXdbFWIxnVSlbooZmYXXQqelFxJVlbhNdWM9
tgdq3t2qBXj3P7XiD+OWfzkABGMJrmki55LNpl0/oV+Kw3DuyGYLurq6TWWlJi8J
94GJm9VQBX1PylFQn0hILcxgr+LAIKX0PqXTyRCpl/UGH1ih05S1F4GvPEj0s1BA
ebRkDrN2vU+9kq8UXOhzxierQDmJkCOpSUWV6Pk6/OP72vxIuAQQNdY++cJRwzi+
adWp6cZBzW5h3OdKlyEDdjNB75rzQcwMlerYTABSIaK6KCTNb7OF4kTWlB5RlWqD
VXyboYEbf0ym5CiNmDKUXqQMI45FIztDhYjJqn1NeroJUZnUYa9y63zujy2uyQeG
EVWpXscPOfrcrCfSuvx0KsMiLxuclfVJyCAJqBMG++LgWxhb247CvhSDK2wZrq0+
Q70p0WaYww==
```

DER

DER可读格式示例，如图所示

在Windows中创建的证书与在Linux中创建的证书之间的差异

您可以在记事本++中使用Compare 插件对两个证书进行简单的并排比较，#68行中的编码区别被删除。在左侧，您可以看到在Windows中创建的证书，在右侧，您可以找到在Linux计算机上生成的证书。左侧的回车符返回，使该证书PEM对FMC无效。但是，除记事本++中的一行外，无法区分文本编辑器中的区别。

将新创建/转换的RootCA和CLEAN接口的PEM证书复制到Linux计算机，并从PEM文件中删除回车。

```
sed -i 's/\r//'
```

示例, sed -i 's/\r//' OPADMIN.pem。

验证回车是否存在。

```
od -c
```

仍显示回车的证书，如图所示。

```
[admin@localhost Desktop]$ od -c MRJCA.cer
0000000   -   -   -   -   -   B   E   G   I   N       C   E   R   T   I
0000020   F   I   C   A   T   E   -   -   -   -   -  \r  \n   M   I   I
0000040   G   t   D   C   C   B   Z   y   g   A   w   I   B   A   g   I
0000060   T   R   Q   A   A   A   P   n   p   l   y   n   B   O   h   j
0000100   Z   a   w   A   E   A   A   A   A   +   T   A   N   B   g   k
0000120   q   h   k   i   G   9   w   0   B   A   Q   s   F  \r  \n   A
0000140   D   B   O   M   R   U   w   E   w   Y   K   C   Z   I   m   i
0000160   Z   P   y   L   G   Q   B   G   R   Y   F   T   G   9   j   Y
0000200   U   w   x   F   z   A   V   B   g   o   J   k   i   a   J   k
0000220   /   I   s   Z   A   E   Z   F   g   d   P   c   2   9   j  \r
0000240  \n   L   W   p   v   M   R   w   w   G   g   Y   D   V   Q   Q
0000260   D   E   x   N   P   c   2   9   j   L   W   p   v   L   U   N
0000300   D   T   l   R   E   Q   z   A   y   L   U   N   B   M   B   4
0000320   X   D   T   I   x   M   D   Q   w   N   D   I   x   M   j   U
0000340   x  \r  \n   M   l   o   X   D   T   I   z   M   D   Q   w   N
0000360   D   I   x   M   j   U   x   M   l   o   w   J   j   E   k   M
0000400   C   I   G   A   1   U   E   A   x   M   b   T   V   J   K   L
0000420   U   F   N   U   C   1   U   R   y   1   N   N   S   0   w   M
0000440   S   5   q  \r  \n   d   C   5   q   d   G   d   y   b   3   V
0000460   w   M   I   I   B   I   j   A   N   B   g   k   q   h   k   i
0000500   G   9   w   0   B   A   Q   E   F   A   A   O   C   A   Q   8
0000520   A   M   I   I   B   C   g   K   C   A   Q   E   A   s   g   4
0000540   Z   s   m   o   Y  \r  \n   w   T   2   Q   Y   O   7   h   h
0000560   z   d   8   b   +   K   b   s   U   M   c   Q   Q   0   5   0
0000600   p   o   g   q   v   e   1   Q   5   2   G   7   T   m   w   e
0000620   +   v   m   q   +   E   Y   H   W   b   B   T   g   D   9   9
0000640   K   D   l   x   R   o   l  \r  \n   O   S   y   I   g   3   W
0000660   k   i   l   M   p   I   l   u   P   i   0   E   U   H   d   A
0000700   c   2   T   q   A   d   w   O   r   e   E   M   k   H   l   F
0000720   n   Q   5   4   G   J   l   w   Z   6   S   o   h   I   9   J
0000740   2   8   h   /   L   k   R   f   8  \r  \n   Z   3   5   B   q
0000760   q   F   o   x   p   s   8   s   0   k   p   7   1   o   7   H
0001000   A   1   b   x   q   b   4   5   t   t   U   U   N   n   /   i
```

在通过Linux计算机运行证书之后。

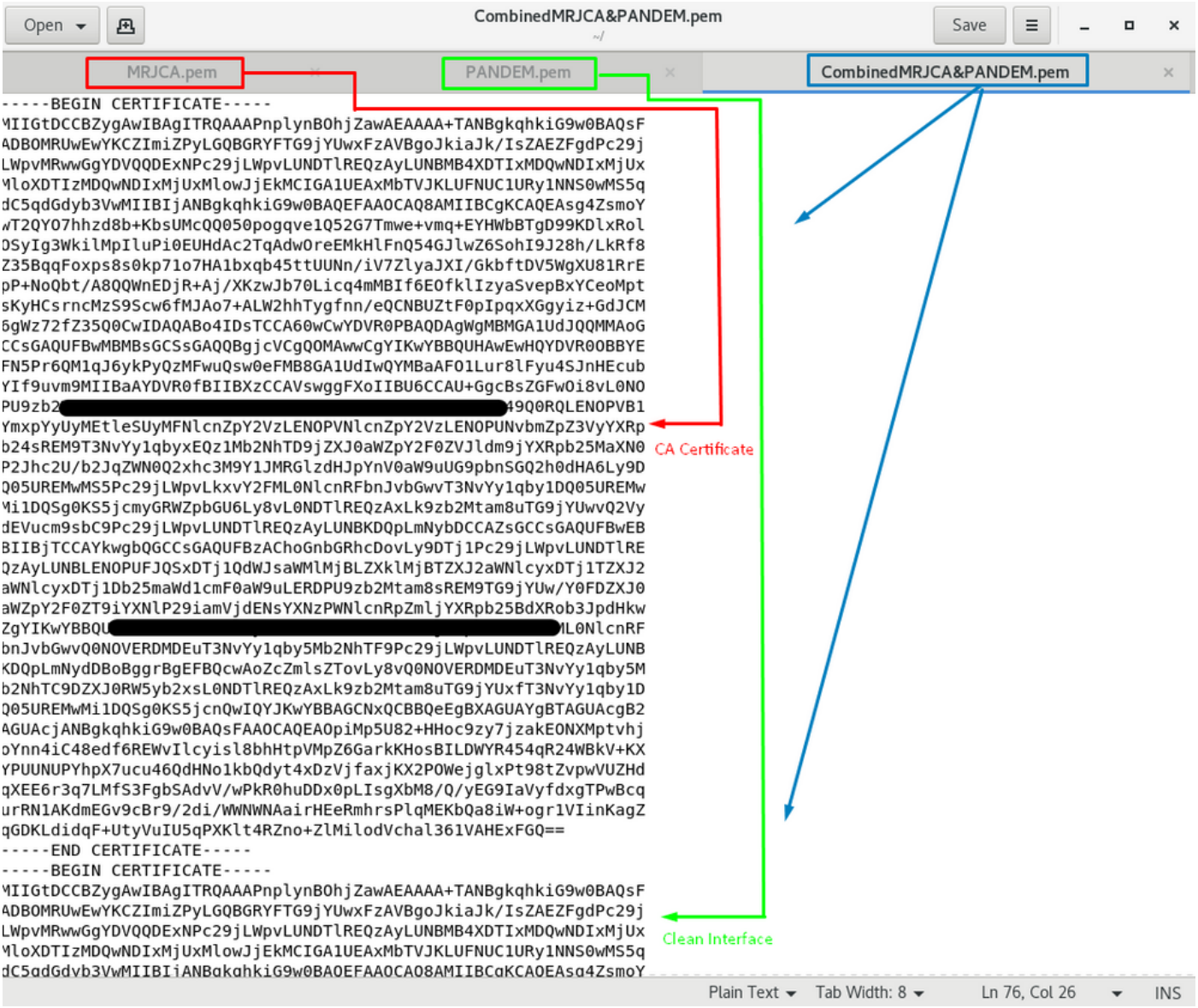
```
[admin@localhost Desktop]$ od -c MRJCA.pem
0000000   -   -   -   -   -   B   E   G   I   N       C   E   R   T   I
0000020   F   I   C   A   T   E   -   -   -   -   -  \n   M   I   I   G
0000040   t   D   C   C   B   Z   y   g   A   w   I   B   A   g   I   T
0000060   R   Q   A   A   A   P   n   p   l   y   n   B   O   h   j   Z
0000100   a   w   A   E   A   A   A   A   +   T   A   N   B   g   k   q
0000120   h   k   i   G   9   w   0   B   A   Q   s   F  \n   A   D   B
0000140   O   M   R   U   w   E   w   Y   K   C   Z   I   m   i   Z   P
0000160   y   L   G   Q   B   G   R   Y   F   T   G   9   j   Y   U   w
0000200   x   F   z   A   V   B   g   o   J   k   i   a   J   k   /   I
0000220   s   Z   A   E   Z   F   g   d   P   c   2   9   j  \n   L   W
0000240   p   v   M   R   w   w   G   g   Y   D   V   Q   Q   D   E   x
0000260   N   P   c   2   9   j   L   W   p   v   L   U   N   D   T   l
0000300   R   E   Q   z   A   y   L   U   N   B   M   B   4   X   D   T
0000320   I   x   M   D   Q   w   N   D   I   x   M   j   U   x  \n   M
0000340   l   o   X   D   T   I   z   M   D   Q   w   N   D   I   x   M
0000360   j   U   x   M   l   o   w   J   j   E   k   M   C   I   G   A
0000400   1   U   E   A   x   M   b   T   V   J   K   L   U   F   N   U
0000420   C   1   U   R   y   1   N   N   S   0   w   M   S   5   q  \n
0000440   d   C   5   q   d   G   d   y   b   3   V   w   M   I   I   B
0000460   I   j   A   N   B   g   k   q   h   k   i   G   9   w   0   B
0000500   A   Q   E   F   A   A   O   C   A   Q   8   A   M   I   I   B
0000520   C   g   K   C   A   Q   E   A   s   g   4   Z   s   m   o   Y
0000540  \n   w   T   2   Q   Y   O   7   h   h   z   d   8   b   +   K
0000560   b   s   U   M   c   Q   Q   0   5   0   p   o   g   q   v   e
0000600   1   Q   5   2   G   7   T   m   w   e   +   v   m   q   +   E
0000620   Y   H   W   b   B   T   g   D   9   9   K   D   l   x   R   o
0000640   l  \n   O   S   y   I   g   3   W   k   i   l   M   p   I   l
0000660   u   P   i   0   E   U   H   d   A   c   2   T   q   A   d   w
0000700   O   r   e   E   M   k   H   l   F   n   Q   5   4   G   J   l
0000720   w   Z   6   S   o   h   I   9   J   2   8   h   /   L   k   R
0000740   f   8  \n   Z   3   5   B   q   q   F   o   x   p   s   8   s
0000760   0   k   p   7   1   o   7   H   A   1   b   x   q   b   4   5
0001000   t   t   U   U   N   n   /   i   V   7   Z   l   y   a   J   X
```

对于FMC，在Linux计算机上将Root_CA和无回车证书组合使用下一个命令。

```
cat
```

示例, cat Clean-interface_CSR_CA-signed_DER_CER_PEM_no-carriage.pem Root-CA.pem > combine.pem。

或者，您也可以在Linux计算机中打开新的文本编辑器，将Clean证书和回车合并到一个文件中，并使用.PEM扩展名保存。您的CA证书必须位于顶部，而Clean Interface证书位于底部。

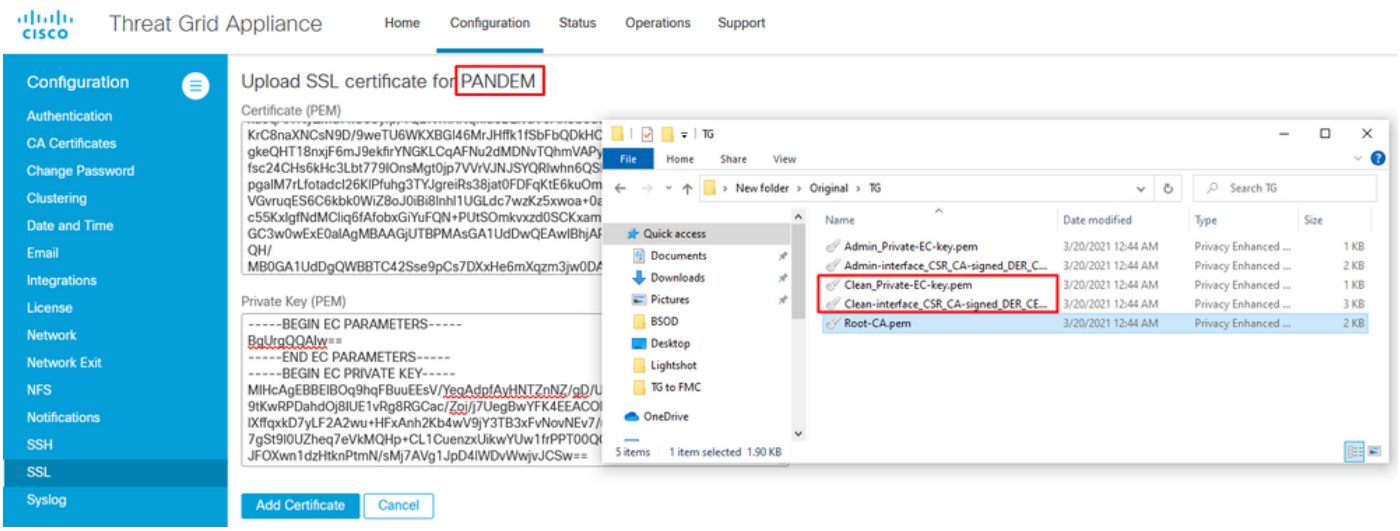


这必须是您稍后上传到FMC的证书，以便与TG设备集成。

证书上传到TG设备和FMC

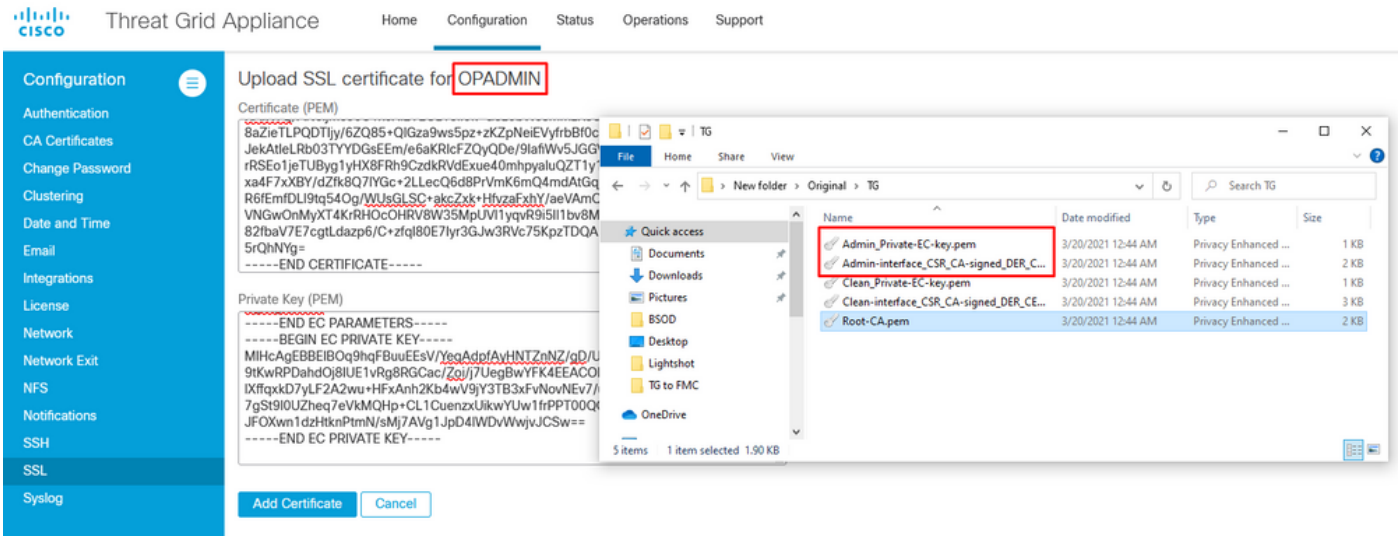
上传安全接口的证书

导航至Configuration > SSL > PANDEM - Actions Upload New Certificate > Add Certificate，如图所示。



上传管理员接口的证书

导航至**Configuration > SSL > OPADMIN - Actions Upload New Certificate > Add Certificate**，如图所示。



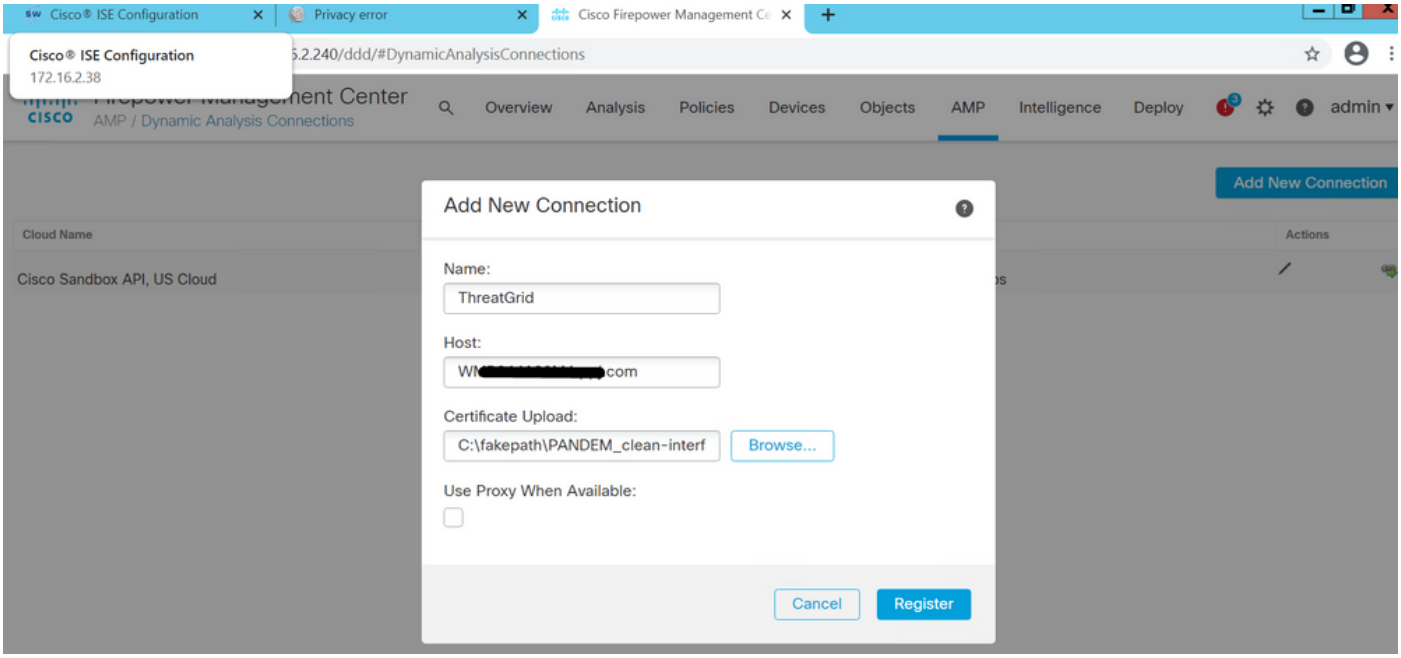
将证书上传到FMC

要将证书上传到FMC，请导航至**AMP > Dynamic Analysis Connections > Add New Connection**，然后填写所需信息。

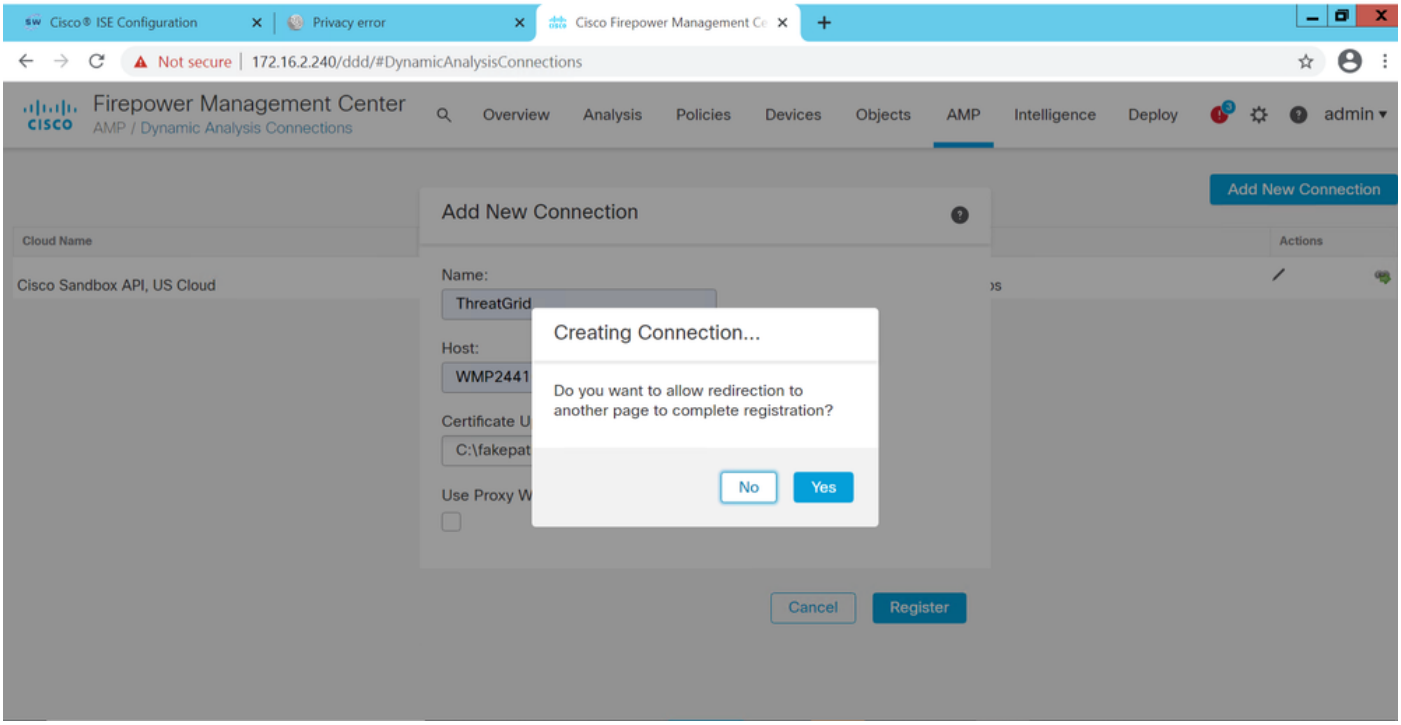
名称：任何要标识的名称。

主机：生成clean-interface的CSR时定义的clean-interface FQDN

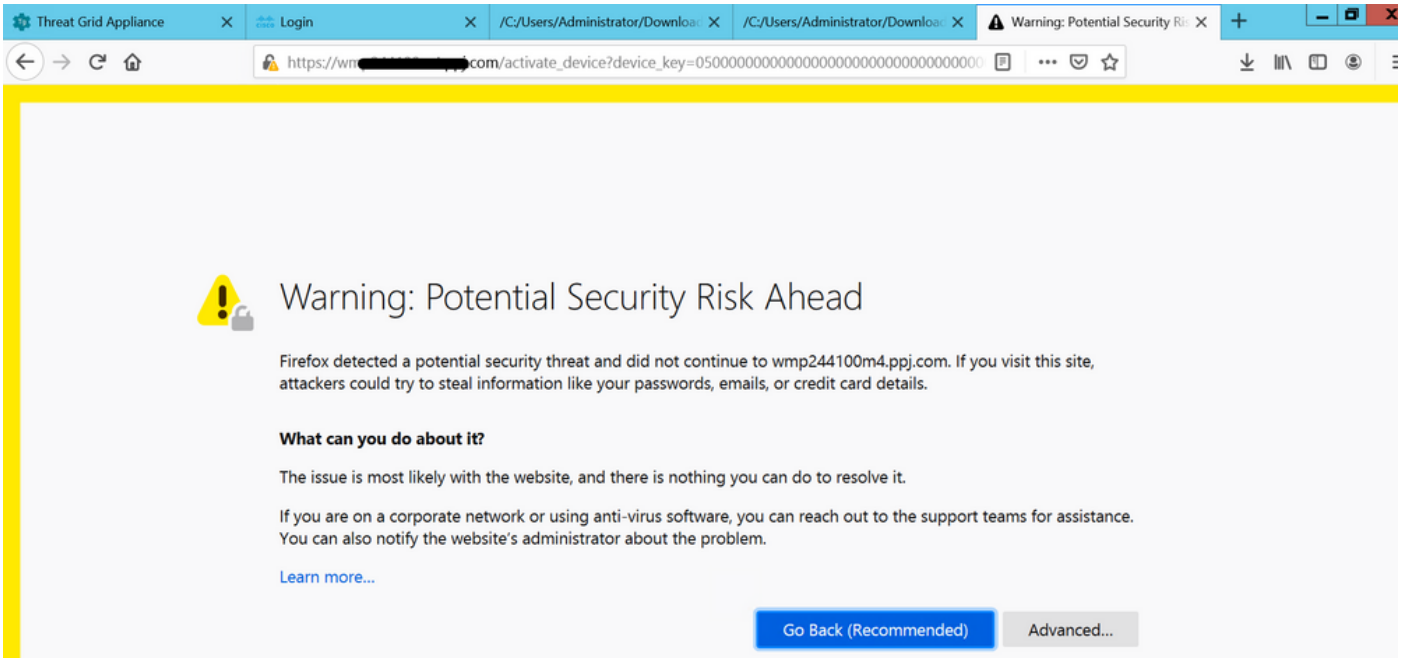
证书:ROOT_CA和clean interface_no-carriage的组合证书。

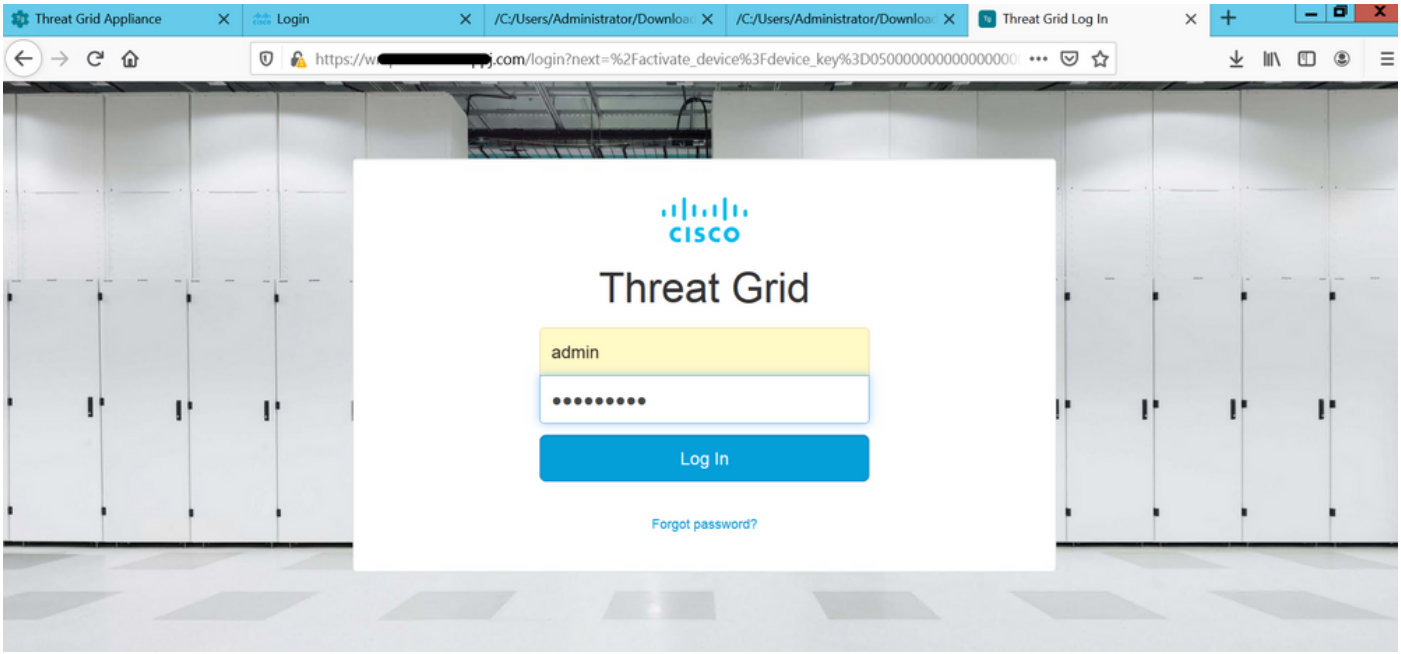


注册新连接后，将显示弹出窗口，单击“是”按钮。

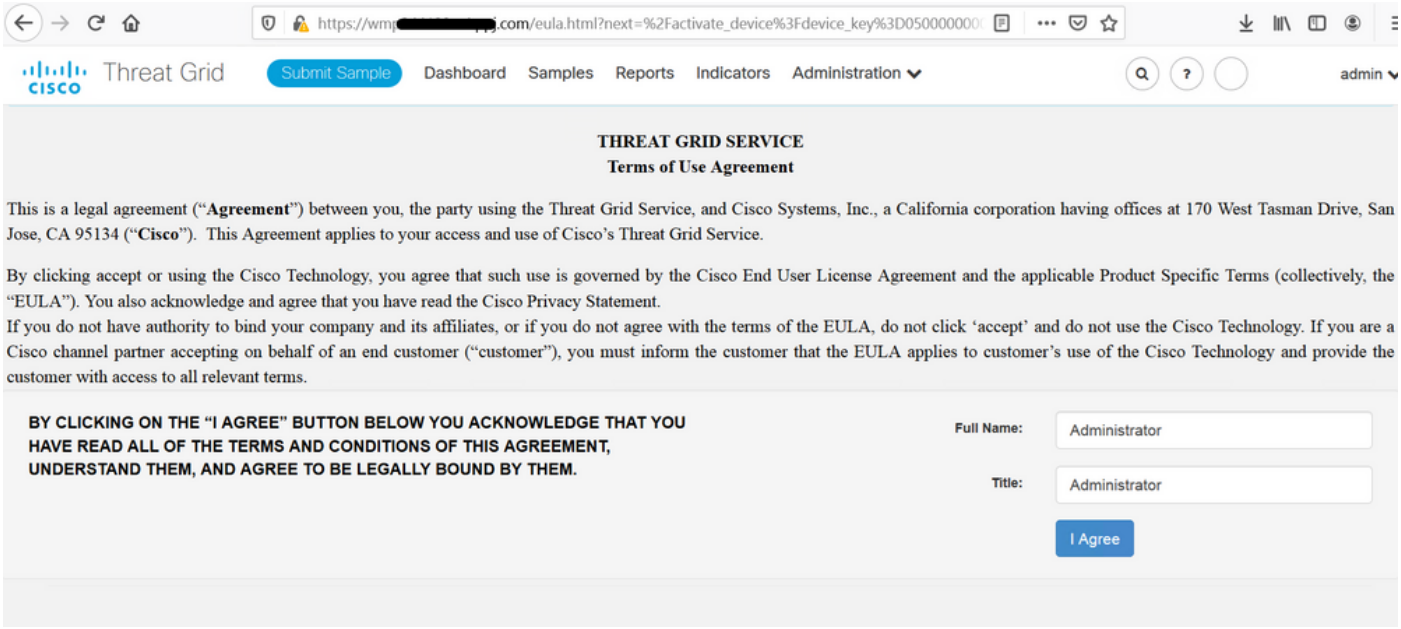


页面重定向到TG Clean界面和登录提示，如图所示。

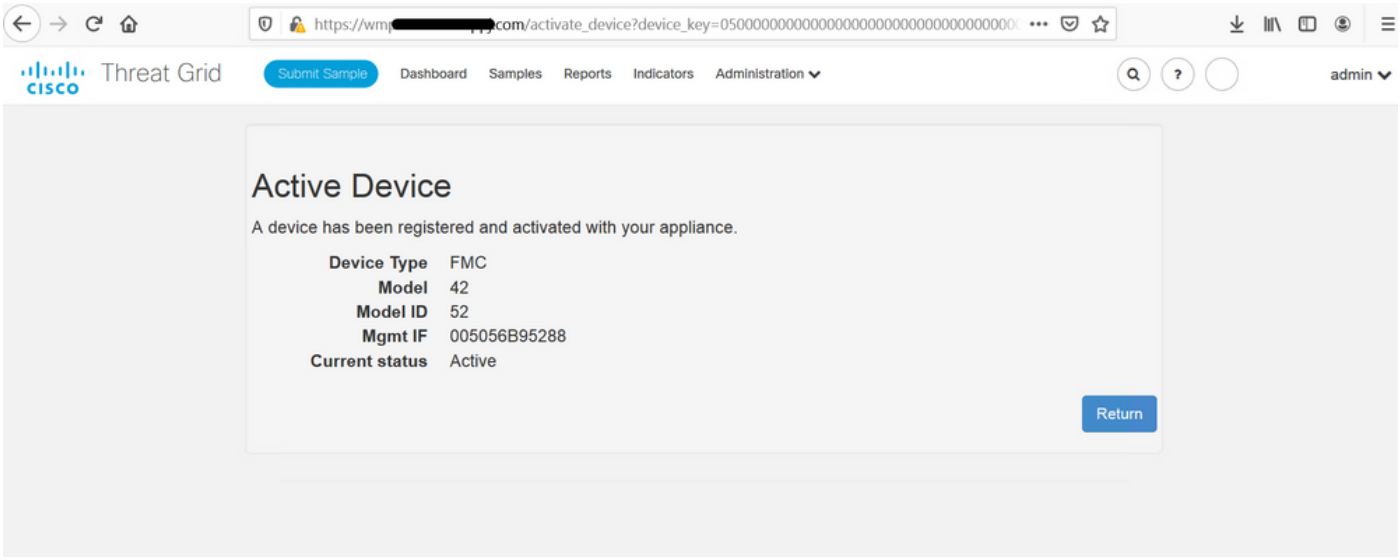

Threat Grid Appliance
Login
Warning: Potential Security Risk Ahead
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to wmp244100m4.ppj.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it.
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...


Threat Grid Appliance
Login
Threat Grid Log In
CISCO
Threat Grid
admin
Log In
Forgot password?

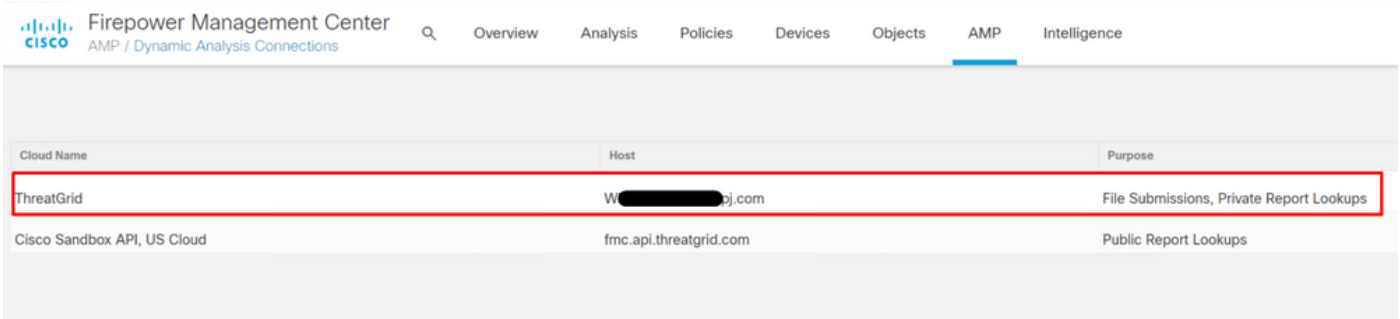
接受EULA。



如图所示，成功集成可显示活动设备。



单击**Return(返回)**，返回TG集成成功的FMC，如图所示。



相关信息

- [Firepower管理中心配置指南，版本6.6]
- [技术支持和文档 - Cisco Systems]