Dépannage de l'intégration de Secure Malware Analytics Appliance avec FMC

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Problème
  - Scénario 1
  - Scénario 2
- Intégration
  - Certificats internes signés par l'autorité de certification pour l'interface Clean Admin
    - Nettoyer l'interface
    - Interface Admin
    - Nettoyer l'interface CSR et CER vers PEM
    - Admininterface CSR et CER vers PEM
- Format approprié du certificat pour FMC
  - PEM
  - DER
  - Différence entre les certificats créés sous Windows et sous Linux
- Téléchargement de certificat vers l'appliance Secure Malware Analytics et FMC
  - Télécharger le certificat pour une interface propre
  - Télécharger le certificat pour une interface d'administration
  - Télécharger le certificat vers FMC
- Informations connexes

Introduction

Ce document décrit en détail l'intégration de Secure Malware Analytics avec Firepower Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestion Firepower FMC
- Configuration de base de Secure Malware Appliance
- Créer des certificats d'autorité (CA)

- Linux/Unix

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FMC version 6.6.1
- Threat Grid 2.12.2
- CentOS 8

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

Dans ce scénario d'utilisation, vous pouvez voir 2 problèmes et deux codes d'erreur.

Scénario 1

L'intégration échoue avec des erreurs :

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

Quand il s'agit de ce problème, le problème est lié au certificat qui n'est pas téléchargé dans FMC en tant que chaîne complète. Étant donné que le certificat signé par l'autorité de certification a été utilisé, l'ensemble de la chaîne de certificats combinée en un seul fichier PEM doit être utilisé. En d'autres termes, vous commencez par Autorité de certification racine > Certificat intermédiaire (le cas échéant) > Clean Int. Reportez-vous à cet article du guide officiel qui décrit les exigences et la procédure.

S'il existe une chaîne de signature à plusieurs niveaux d'autorités de certification, tous les certificats intermédiaires requis et le certificat racine doivent être contenus dans un fichier unique qui est téléchargé vers le FMC.

- Tous les certificats doivent être codés en PEM.

- Les nouvelles lignes du fichier doivent être UNIX et non DOS.

- Si l'appliance Threat Grid présente un certificat auto-signé, téléchargez le certificat que vous avez téléchargé à partir de cette appliance.

- Si l'appliance Threat Grid présente un certificat signé par une autorité de certification, téléchargez le fichier qui contient la chaîne de signature de certificats.

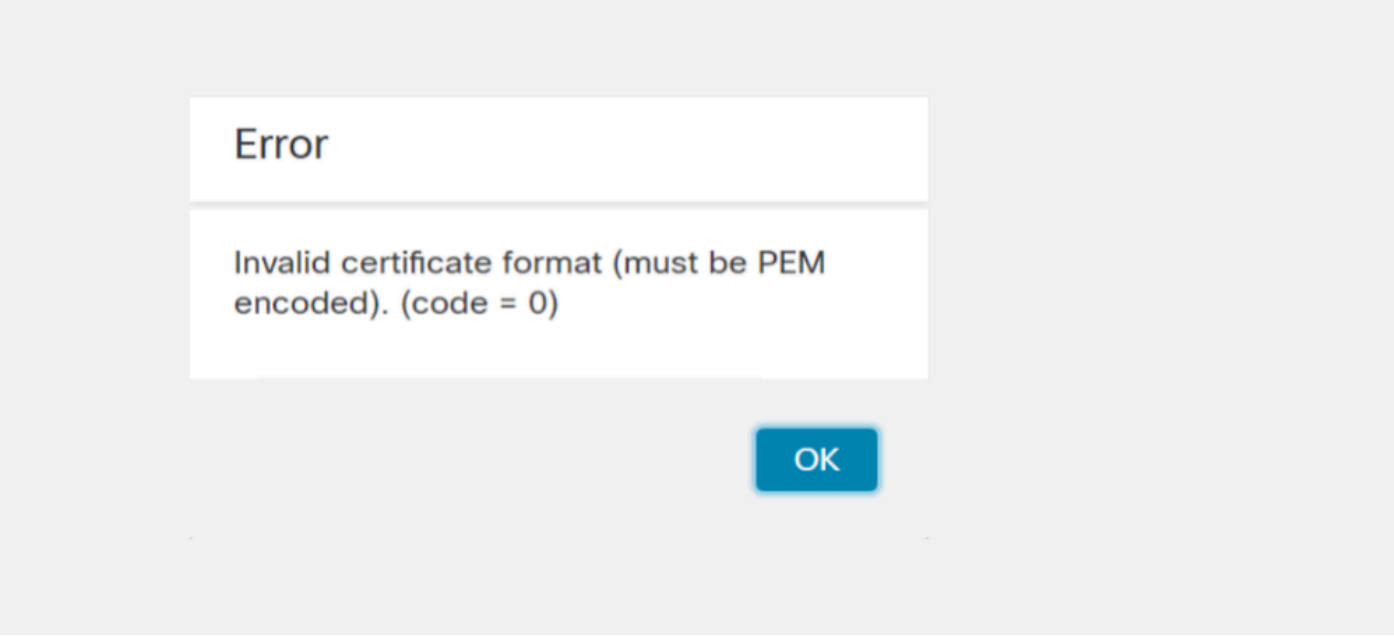
⚠ Mise en garde : Si vous avez régénéré le certificat auto-signé de l'appliance Secure Malware, assurez-vous que vous avez reconfiguré l'appliance de sorte qu'elle n'envoie le certificat mis à jour qu'après la connexion SSL.

Scénario 2

Erreur de format de certificat non valide

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

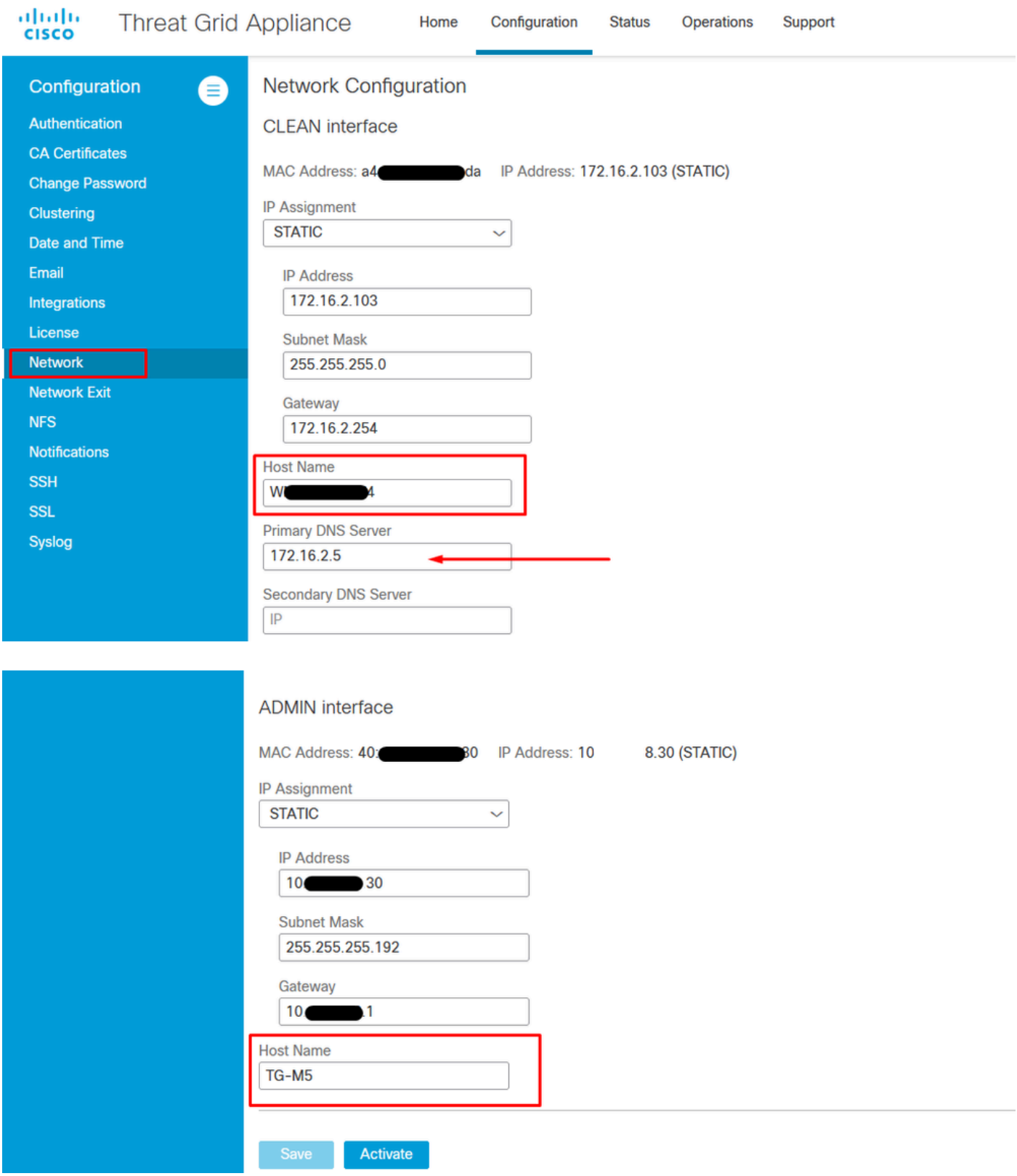
Erreur de format de certificat, comme indiqué dans l'image.

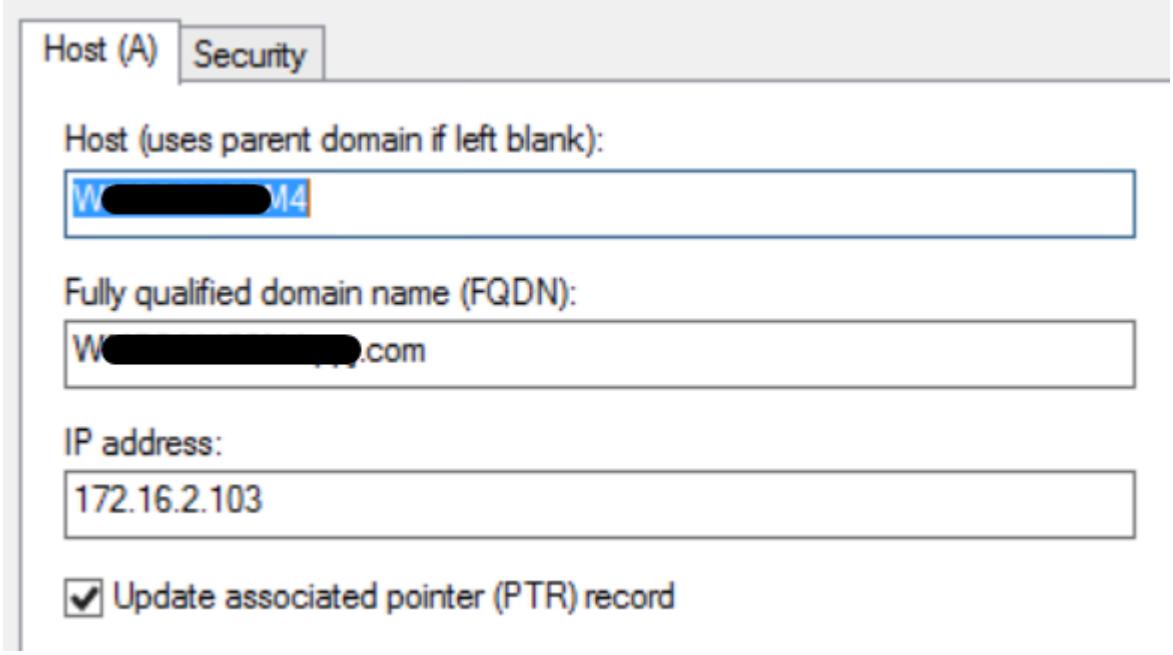


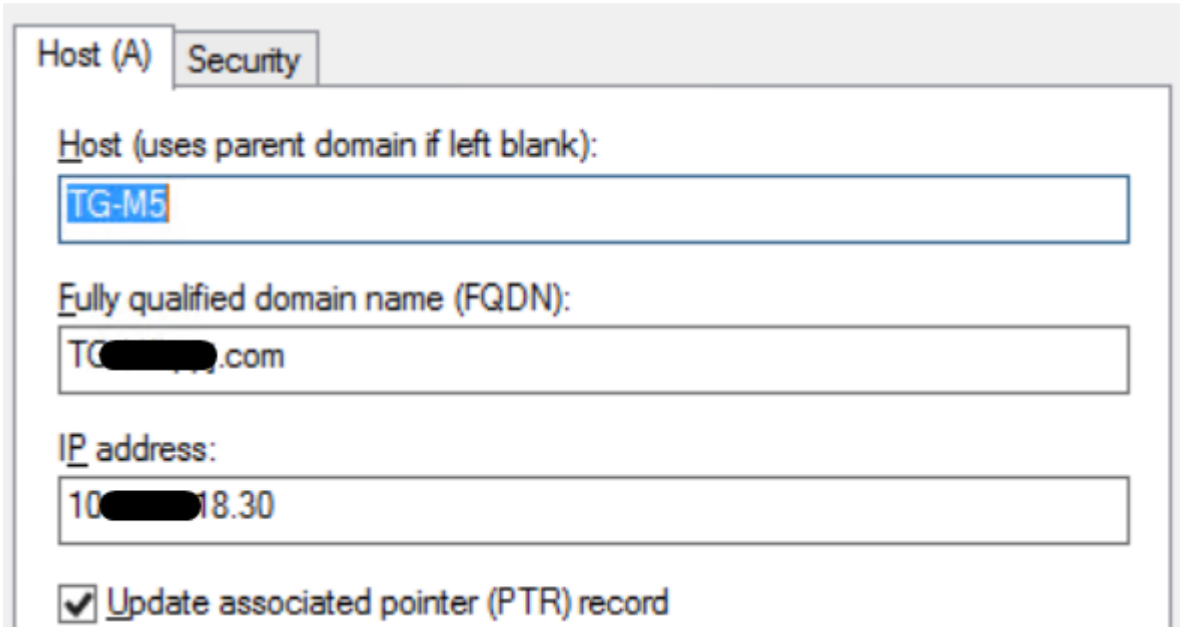
Cette erreur est due au mauvais formatage du certificat PEM combiné créé sur l'ordinateur Windows qui utilise OpenSSL. Il est fortement recommandé d'utiliser une machine Linux pour créer ce certificat.

Intégration

Étape 1. Configurez la TGA, comme indiqué dans les images.


Threat Grid Appliance
Home
Configuration
Status
Operations
Support
Configuration
Authentication
CA Certificates
Change Password
Clustering
Date and Time
Email
Integrations
License
Network
Network Exit
NFS
Notifications
SSH
SSL
Syslog
Network Configuration
CLEAN interface
MAC Address: a4[redacted]da
IP Address: 172.16.2.103 (STATIC)
IP Assignment
STATIC
IP Address
172.16.2.103
Subnet Mask
255.255.255.0
Gateway
172.16.2.254
Host Name
W[redacted]4
Primary DNS Server
172.16.2.5
Secondary DNS Server
IP
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





Certificats internes signés par l'autorité de certification pour l'interface Clean Admin

Étape 1 : génération de la clé privée utilisée pour l'interface d'administration et pour l'interface propre

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

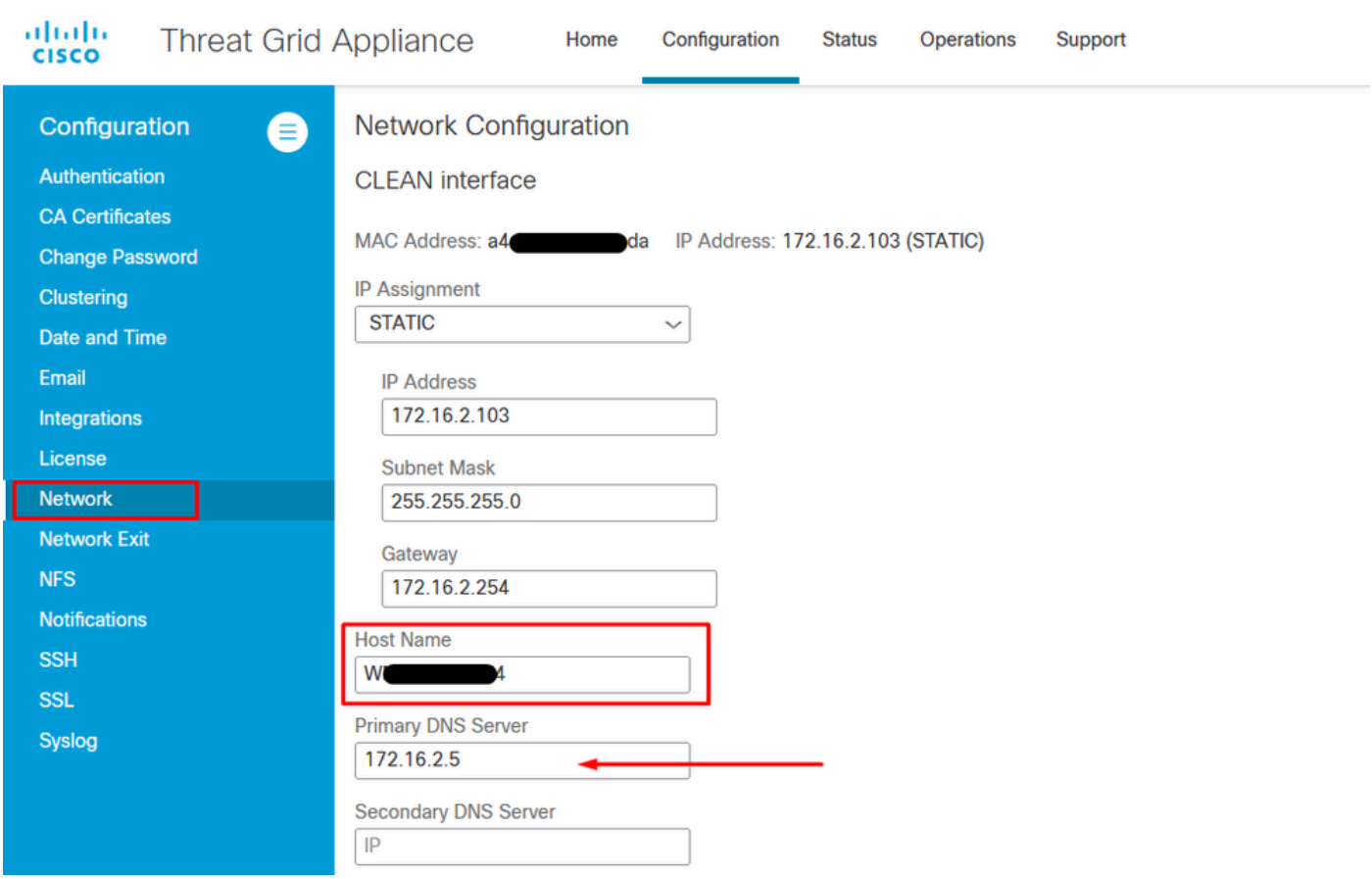
Étape 2. Génération de CSR

Nettoyer l'interface

Étape 1. Accédez à la création CSR et utilisez la clé privée générée.

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

Remarque : Le nom CN doit être entré pour CSR et doit correspondre au nom d'hôte de l'interface Clean définie sous « Network ». Une entrée DNS doit être présente sur le serveur DNS qui résout le nom d'hôte de l'interface Clean.

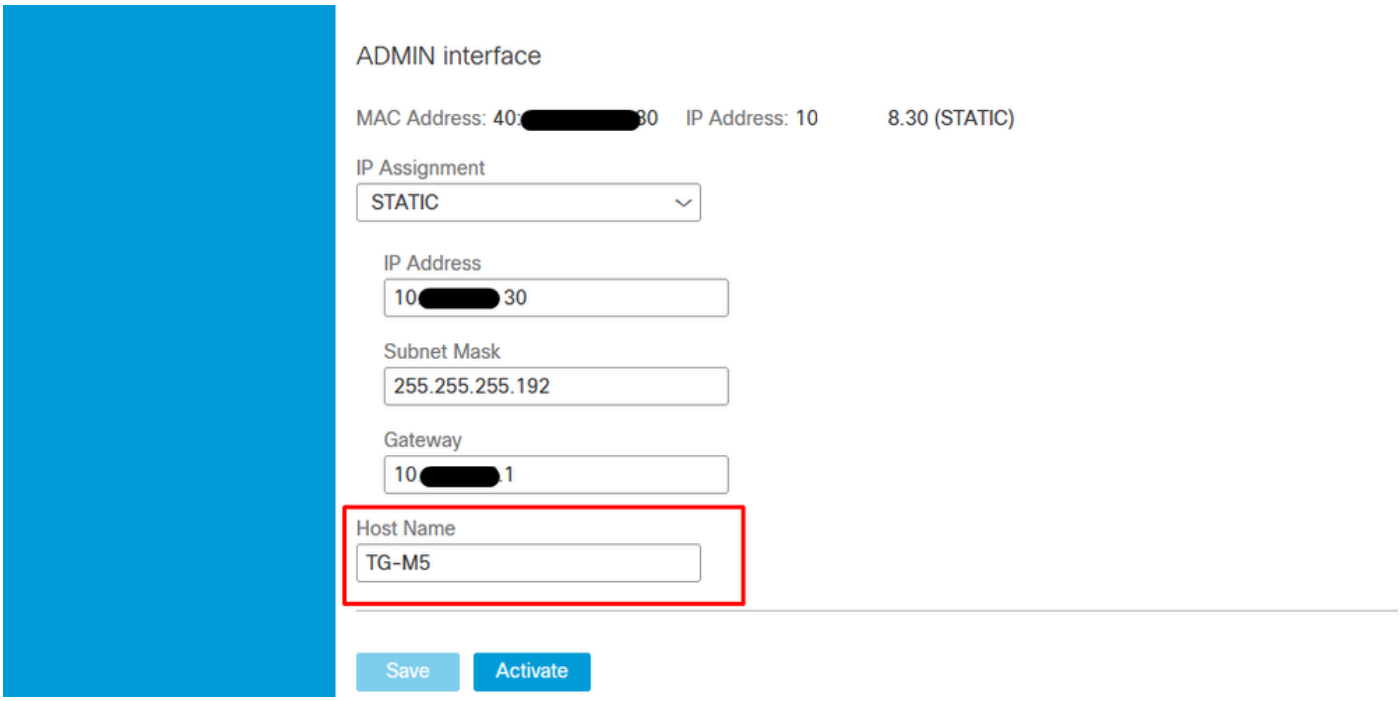


Interface Admin

Étape 1. Accédez à la création CSR et utilisez la clé privée générée.

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

Remarque : Le nom CN doit être saisi pour CSR et doit correspondre au « nom d'hôte » de l'« interface d'administration » défini sous « Réseau ». Une entrée DNS doit être présente sur le serveur DNS qui résout le nom d'hôte de l'interface propre.



Étape 2. Le CSR doit être signé par l'AC. Téléchargez le certificat au format DER avec l'extension CER.

Étape 3. Convertissez CER en PEM.

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

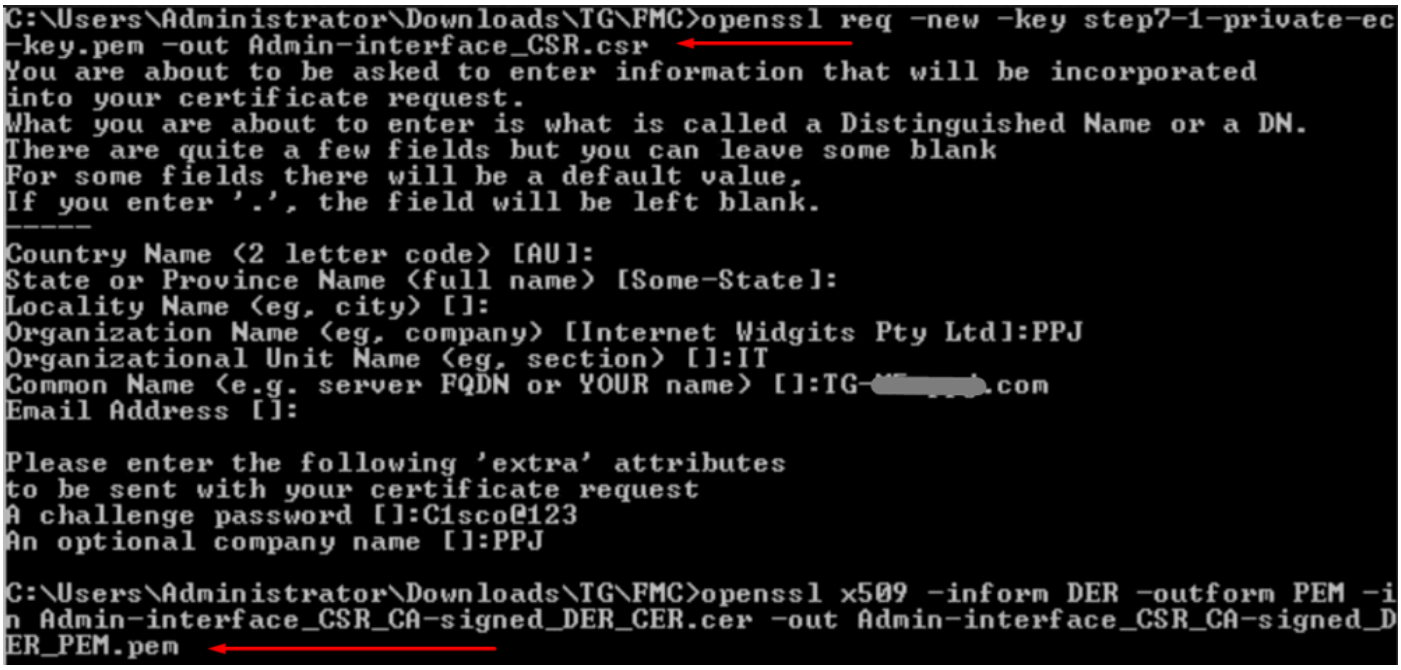
Nettoyer l'interface CSR et CER vers PEM

```
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
```

Interface d'administration CSR et CER vers PEM



Format approprié du certificat pour FMC

Si vous avez déjà reçu des certificats et qu'ils sont au format CER/CRT et lisibles lorsqu'un éditeur de texte est utilisé, vous pouvez simplement changer l'extension en PEM.

Si le certificat n'est pas lisible, vous devez convertir le format DER en format PEM lisible.

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

PEM

Exemple de format lisible par PEM, comme illustré dans l'image.



DER

Exemple de format lisible par DER, comme illustré dans l'image



Différence entre les certificats créés sous Windows et sous Linux

Une simple comparaison côte à côte des deux certificats l'un à côté de l'autre, vous pouvez utiliser le plug-in Compare dans Notepad ++ a masqué la différence encodée dans la ligne #68. Sur la gauche, vous pouvez voir le certificat créé dans Windows, sur la droite, vous pouvez trouver le certificat généré sur la machine Linux. Celui de gauche a un retour chariot qui rend ce certificat PEM non valide pour FMC. Cependant, vous ne pouvez pas faire la différence dans l'éditeur de texte, à l'exception de cette ligne dans le Bloc-notes ++.



Copiez le certificat PEM nouvellement créé/converti pour l'interface RootCA et CLEAN sur votre machine Linux et supprimez le retour chariot du fichier PEM.

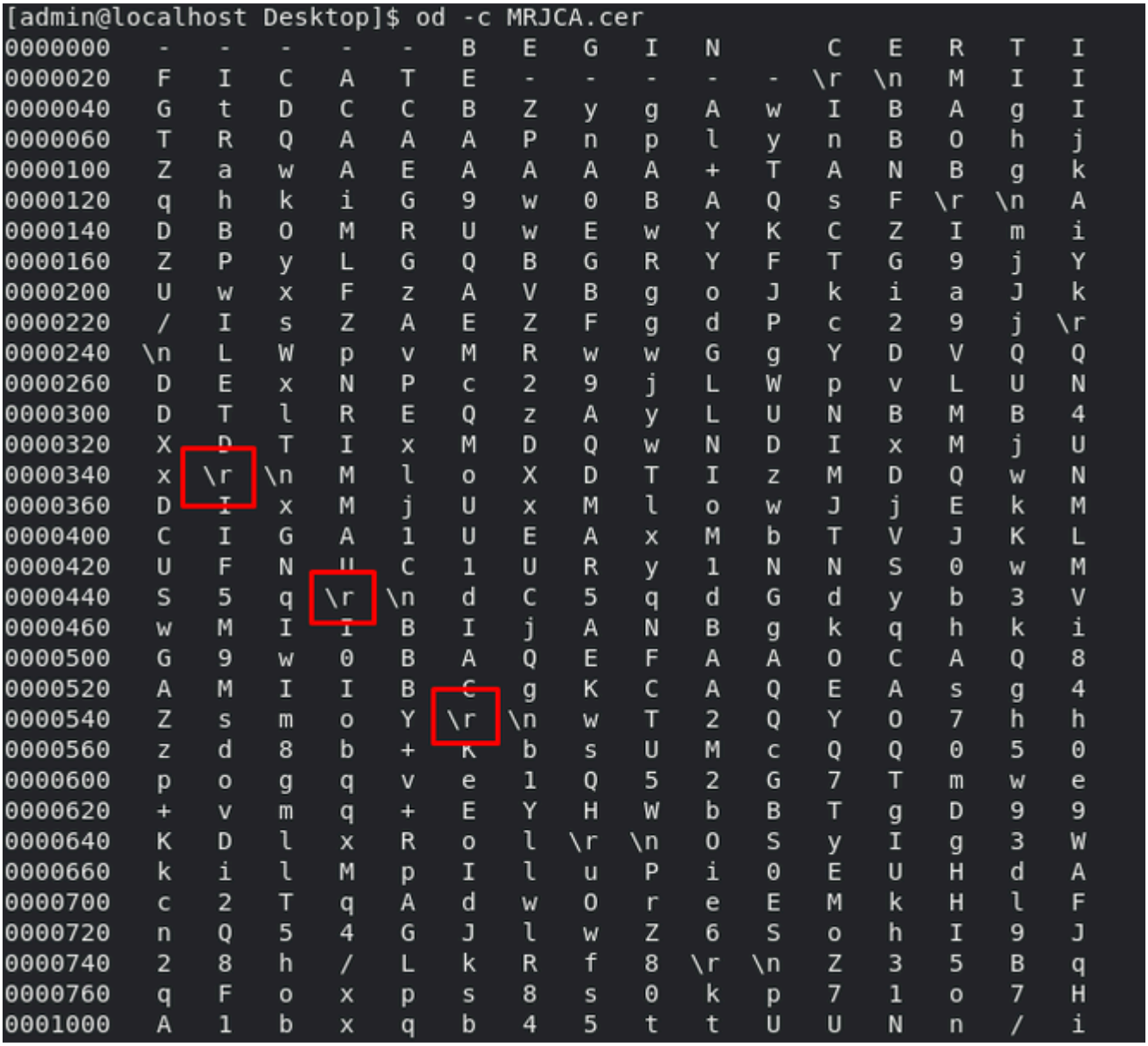
```
sed -i 's/\r//'
```

Exemple, sed -i 's/\r//' OPADMIN.pem.

Vérifiez si le retour chariot est présent.

```
od -c
```

Les certificats qui ont encore un retour chariot sont présentés, comme le montre l'image.



```
[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
```

Certificat après avoir exécuté cela sur une machine Linux.

```
[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
```

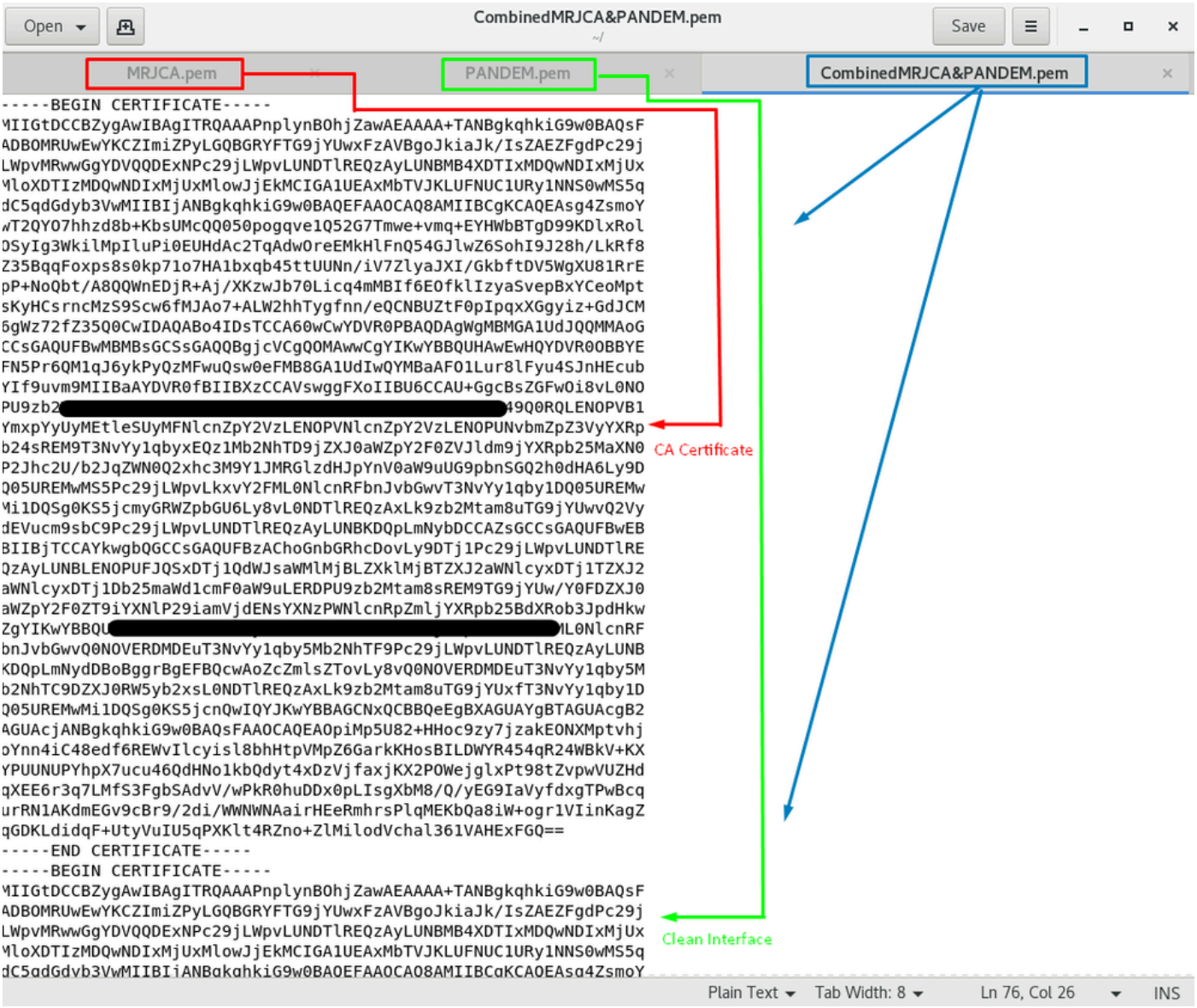
Pour FMC, combinez Root_CA et le certificat no-carry sur une machine Linux à l'aide de la commande suivante.

```
cat

        >
```

Par exemple, cat Clean-interface_CSR_CA-signed_DER_CER_PEM_no-carry.pem Root-CA.pem > combine.pem.

Ou vous pouvez également ouvrir un nouvel éditeur de texte dans votre machine Linux et combiner les deux certificats Clean avec retour chariot supprimé dans un fichier et l'enregistrer avec l'extension .PEM. Vous devez avoir votre certificat CA en haut et le certificat Clean Interface en bas.

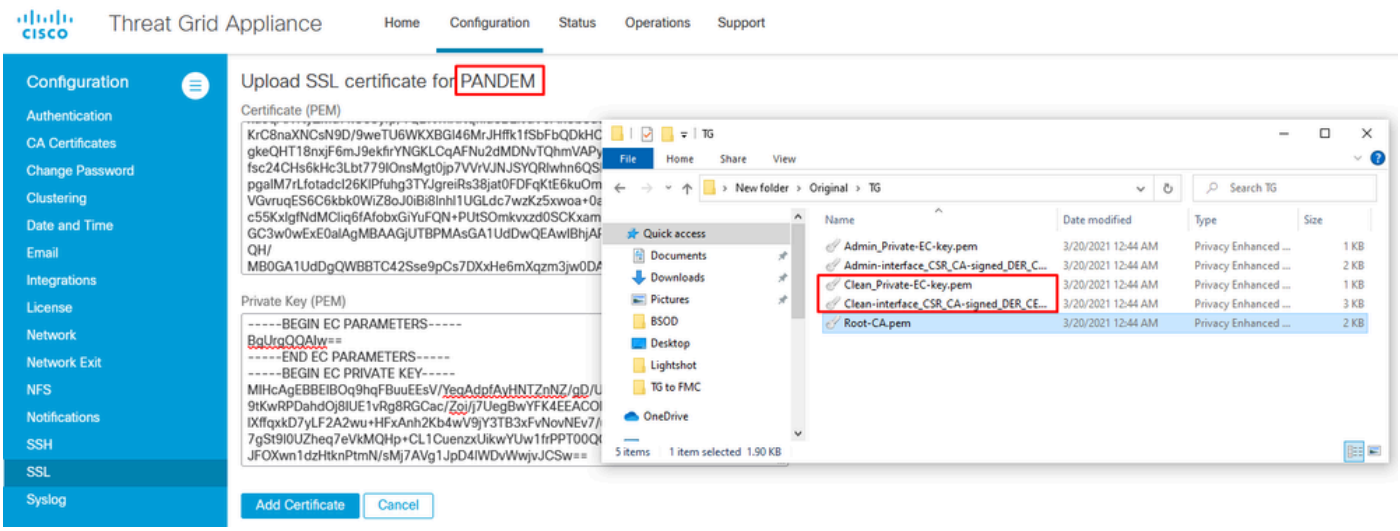


Il doit s'agir de votre certificat que vous téléchargez ultérieurement sur votre FMC pour l'intégrer à l'appliance TG.

Téléchargement de certificat vers l'appliance Secure Malware Analytics et FMC

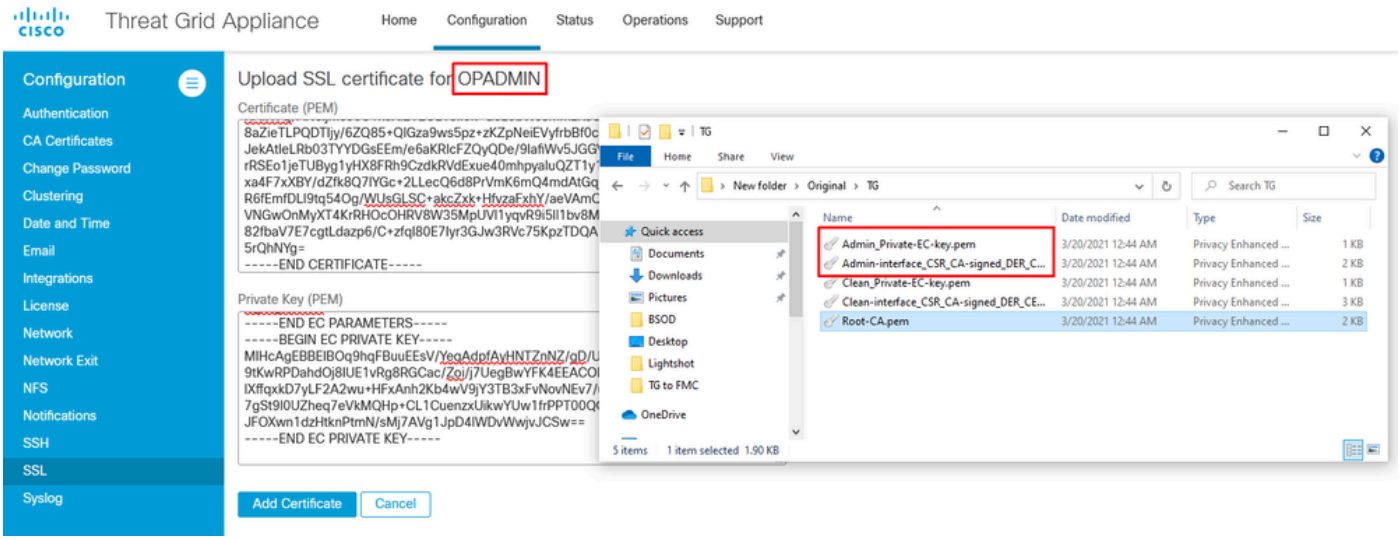
Télécharger le certificat pour une interface propre

Accédez à Configuration > SSL > PANDEM - Actions Upload New Certificate > Add Certificate, comme indiqué dans l'image.



Télécharger le certificat pour une interface d'administration

Accédez à Configuration > SSL > OPADMIN - Actions Upload New Certificate > Add Certificate, comme indiqué dans l'image.



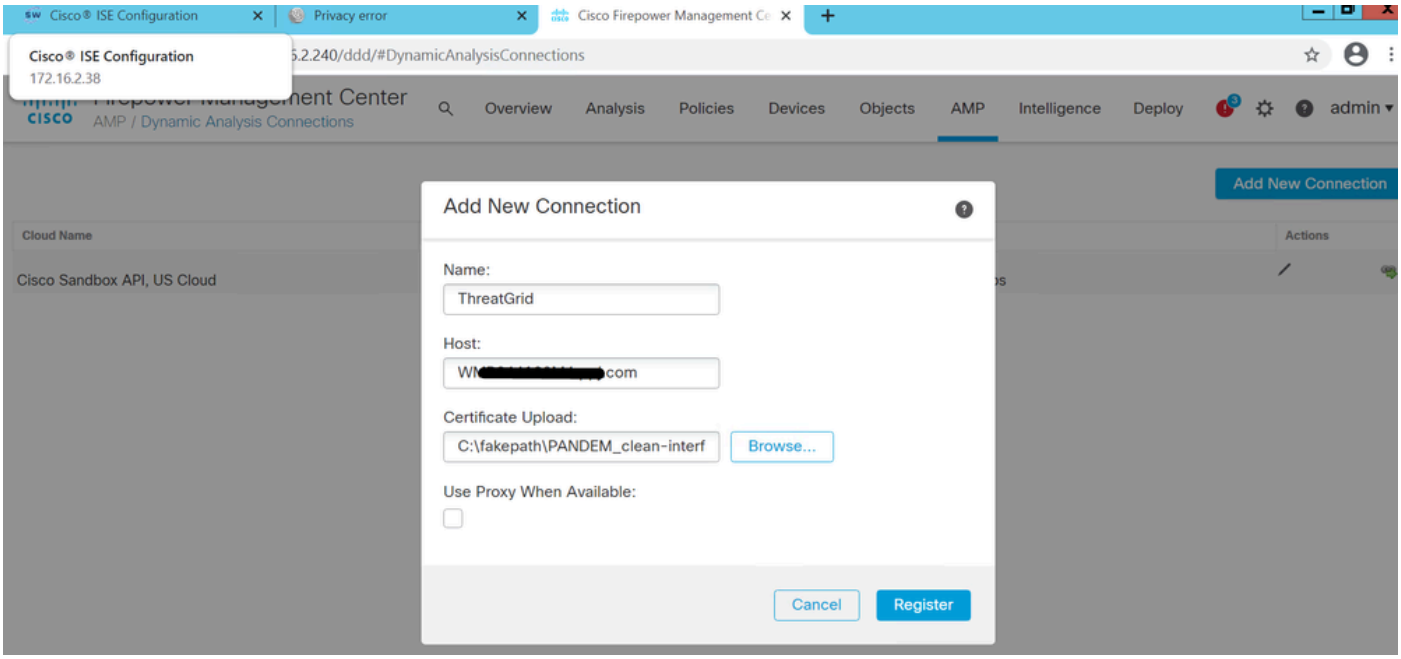
Télécharger le certificat vers FMC

Afin de télécharger le certificat sur le FMC, accédez à AMP > Dynamic Analysis Connections > Add New Connection, puis remplissez les informations requises.

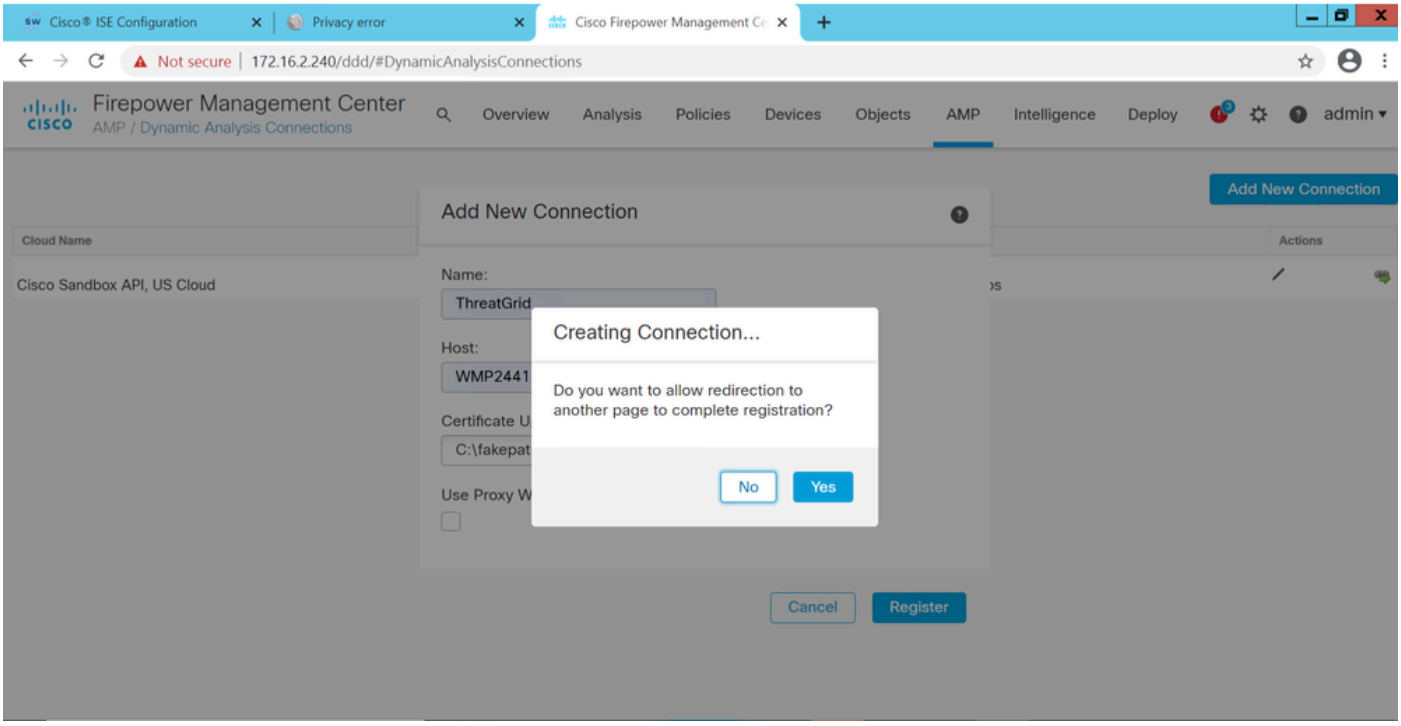
Name : Tout nom à identifier.

Hôte : Clean-interface FQDN tel que défini lors de la génération du CSR pour clean-interface

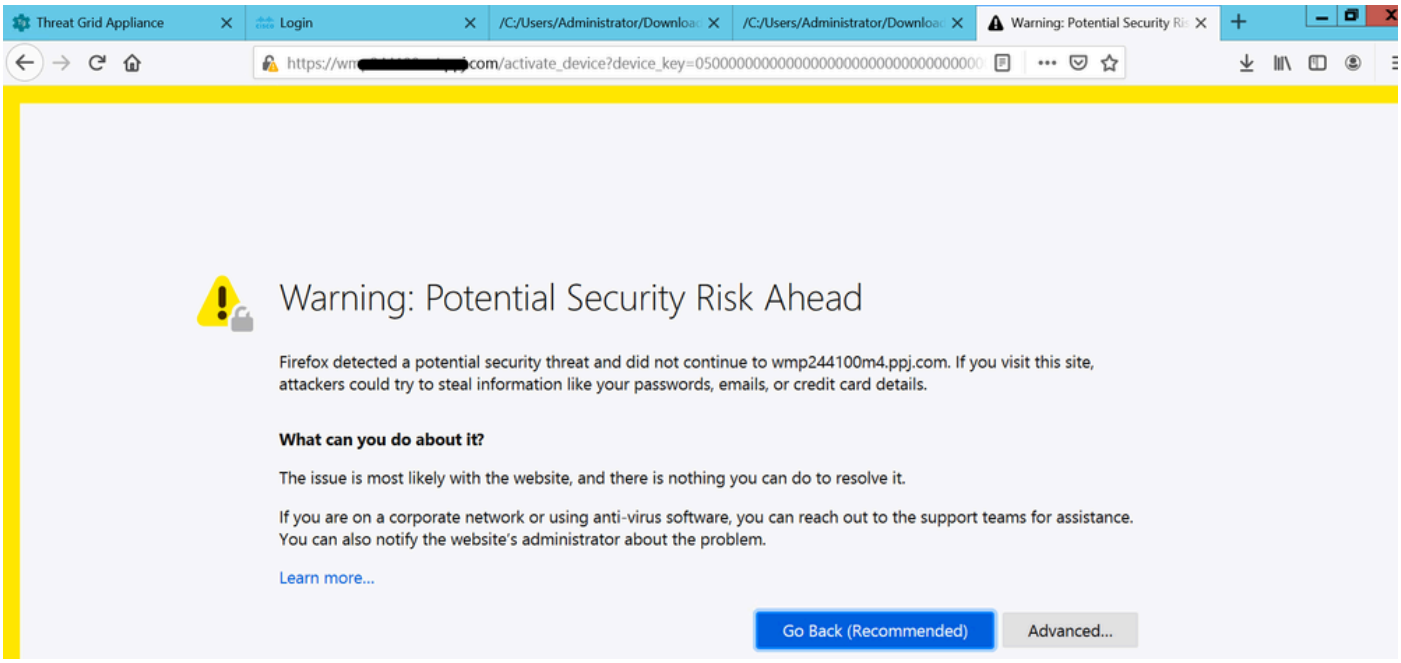
Certificat: Le certificat combiné de ROOT_CA et de clean interface_no-transport.

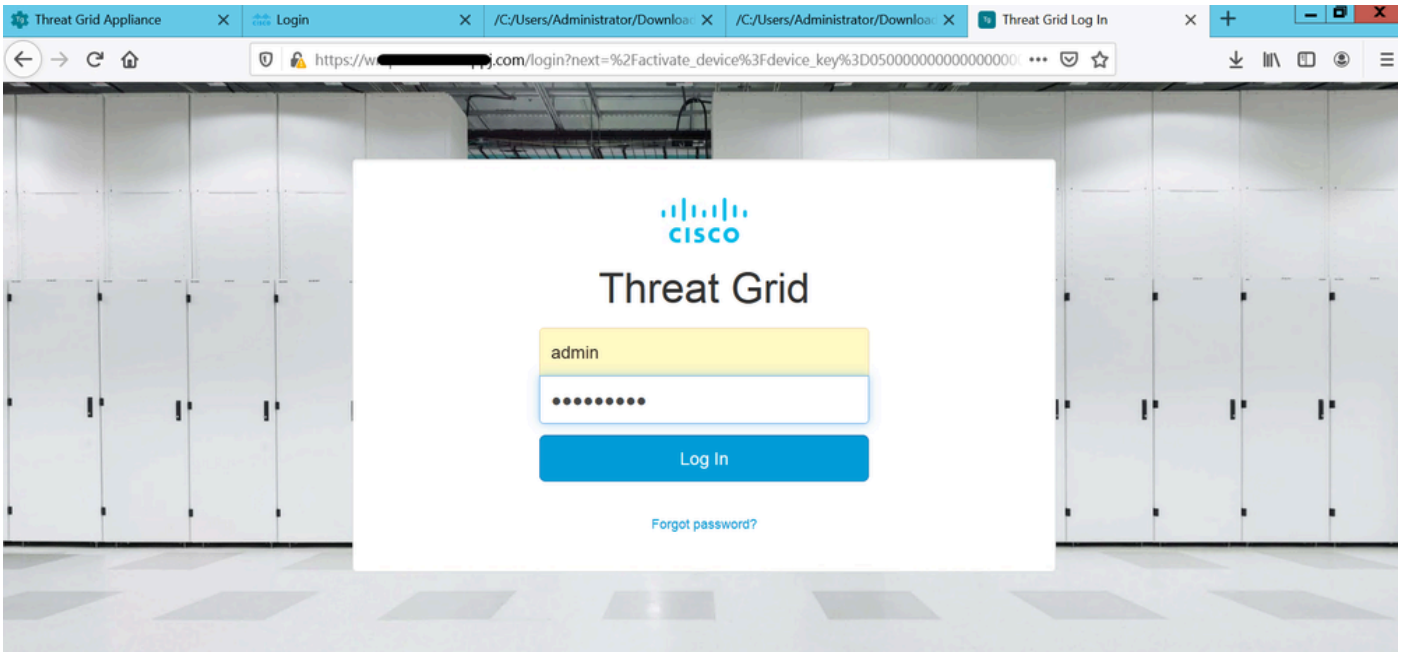


Une fois la nouvelle connexion enregistrée, une fenêtre contextuelle s'affiche, cliquez sur le bouton Yes (Oui).

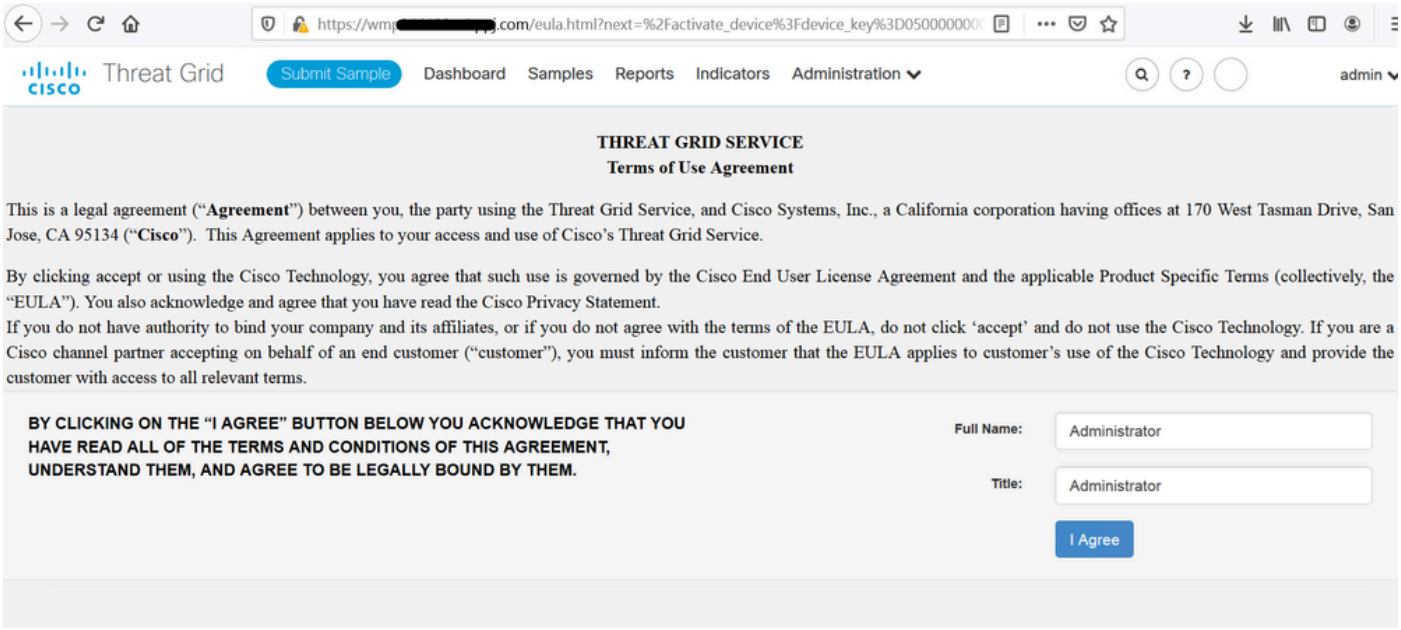


La page redirige vers l'interface Secure Malware Analytics Clean et l'invite de connexion, comme indiqué dans les images.

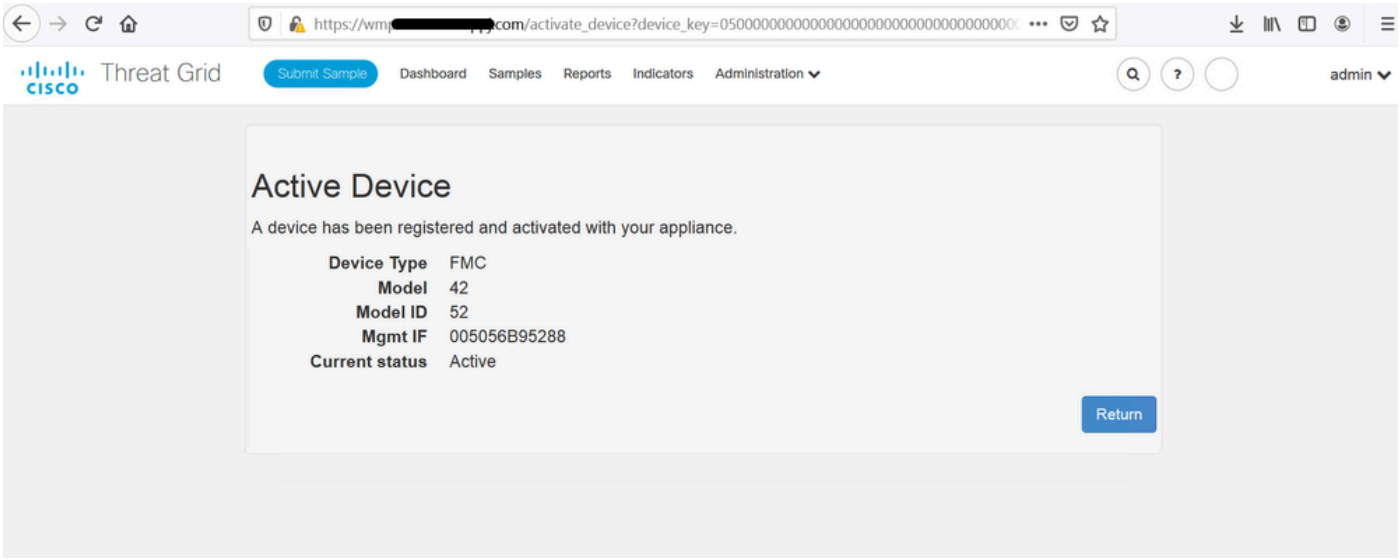




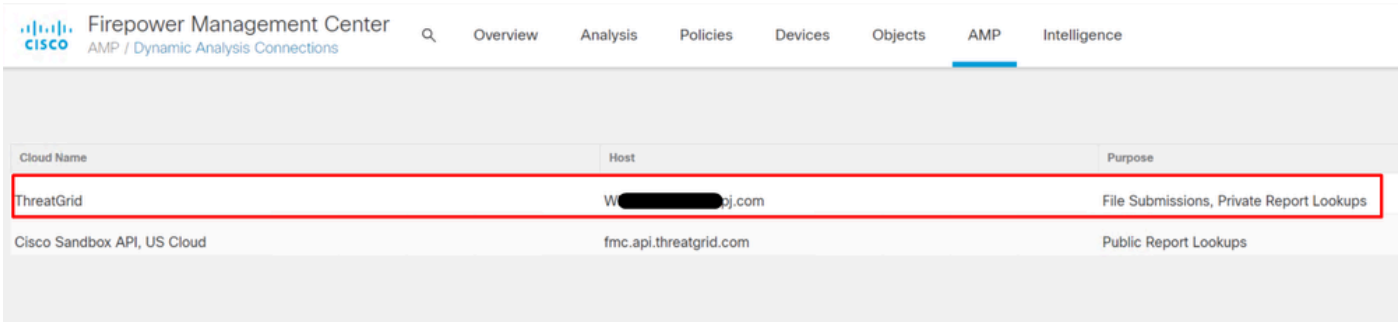
Acceptez le CLUF.



Une intégration réussie affiche un périphérique actif, comme illustré dans l'image.



Cliquez sur Retour, revenez à FMC avec une intégration Secure Malware Analytics réussie, comme illustré dans l'image.



Informations connexes

- Guide de configuration de Firepower Management Center, version 6.6

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.