Configuration de l'intégration ISE 2.4 et FMC 6.2.3 pxGrid

Table des matières

Introduction

Ce document décrit le processus de configuration pour l'intégration de l'ISE pxGrid version 2.4 et de FMC version 6.2.3.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE 2.4
- FMC 6.2.3
- LDAP (Active Directory/Lightweight Directory Access Protocol)

Composants utilisés

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

logiciel suivantes :

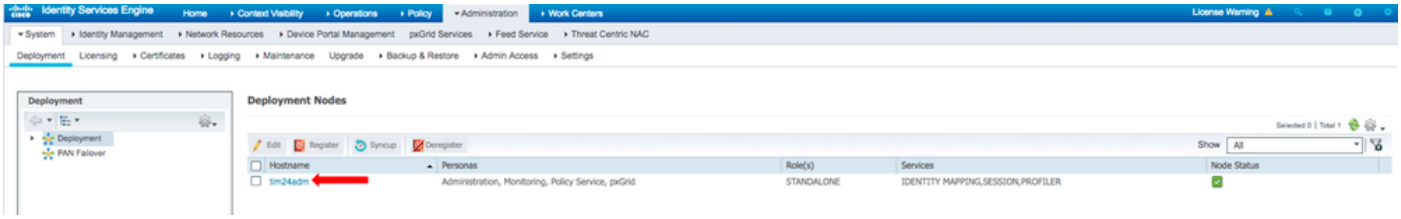
- ISE autonome 2.4
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid version 2.4
- Firepower Management Center (FMC) version 6.2.3

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.

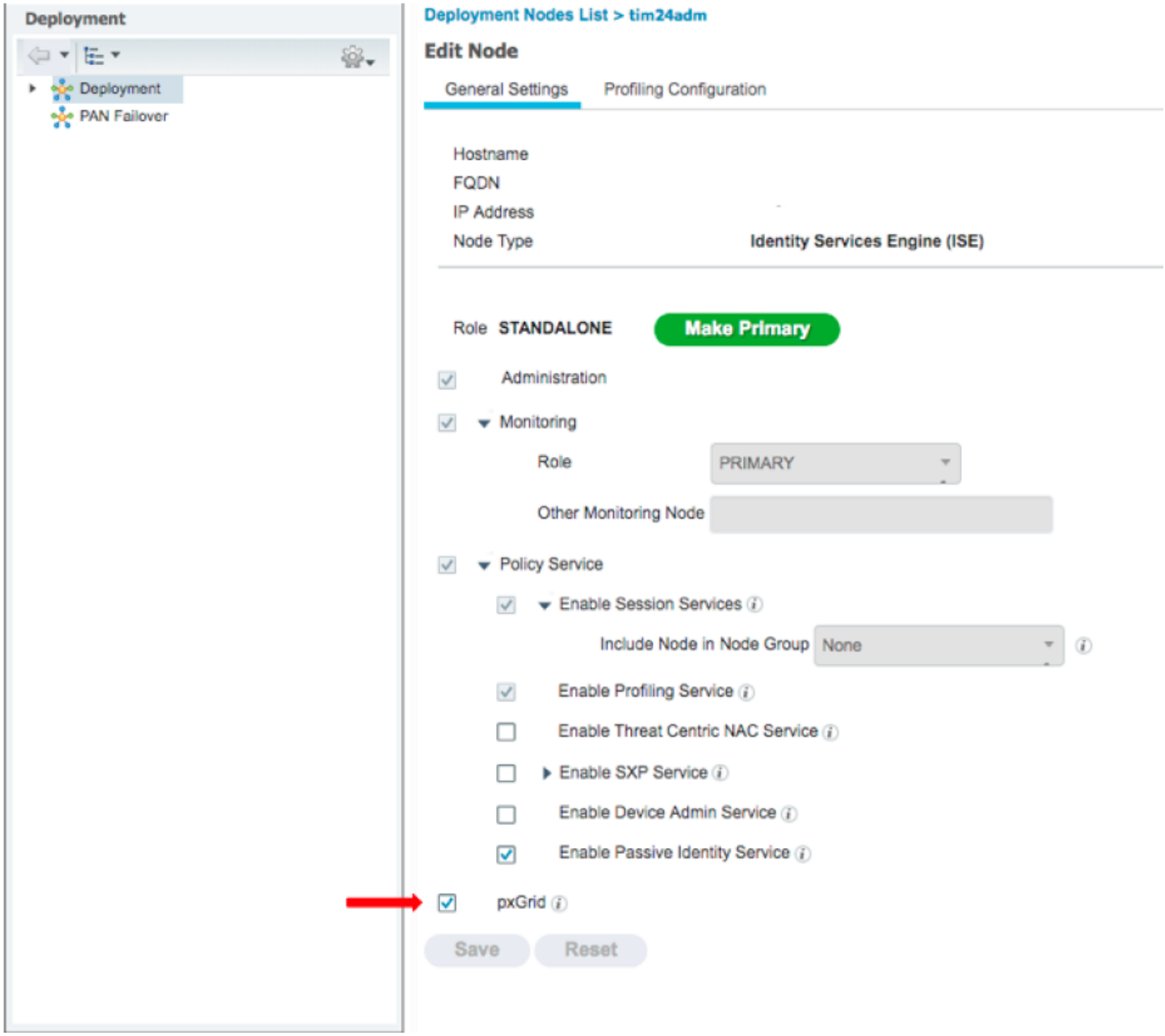
Configuration d'ISE

Étape 1. Activer les services pxGrid

1. Connectez-vous à l'interface utilisateur graphique d'administration ISE, accédez à **Administration > Deployment.**
2. Sélectionnez le noeud ISE à utiliser pour le profil pxGrid.



3. Activez le service pxGrid et cliquez sur **Save** comme indiqué dans l'image.



4. Vérifiez que les services pxGrid s'exécutent à partir de l'interface de ligne de commande.

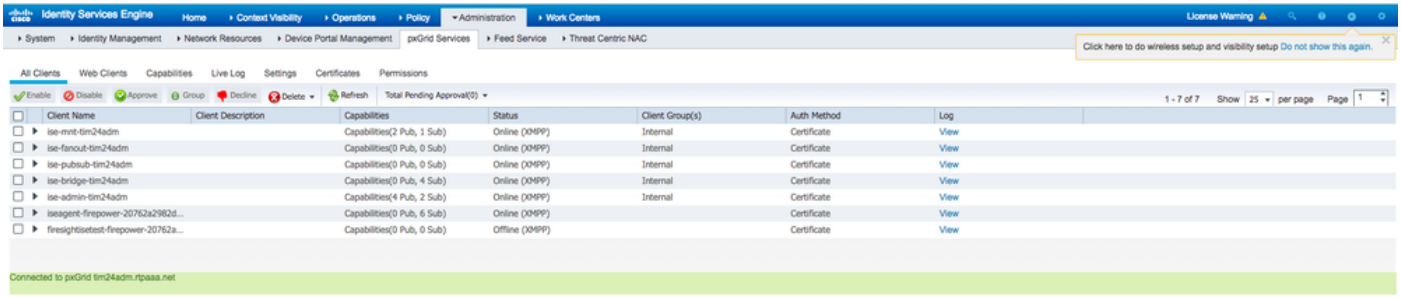
Remarque : le processus nécessite jusqu'à 5 minutes pour que les services pxGrid démarrent et déterminent l'état de haute disponibilité (HA) si plus d'un noeud pxGrid est utilisé.

5. Connectez SSH à l'interface de ligne de commande du noeud ISE pxGrid et vérifiez l'état de l'application.

```
# show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#
```

6. Accédez à l'interface utilisateur graphique de l'administrateur ISE et vérifiez que les services sont en ligne et fonctionnent. Accédez à **Administration > pxGrid Services**.

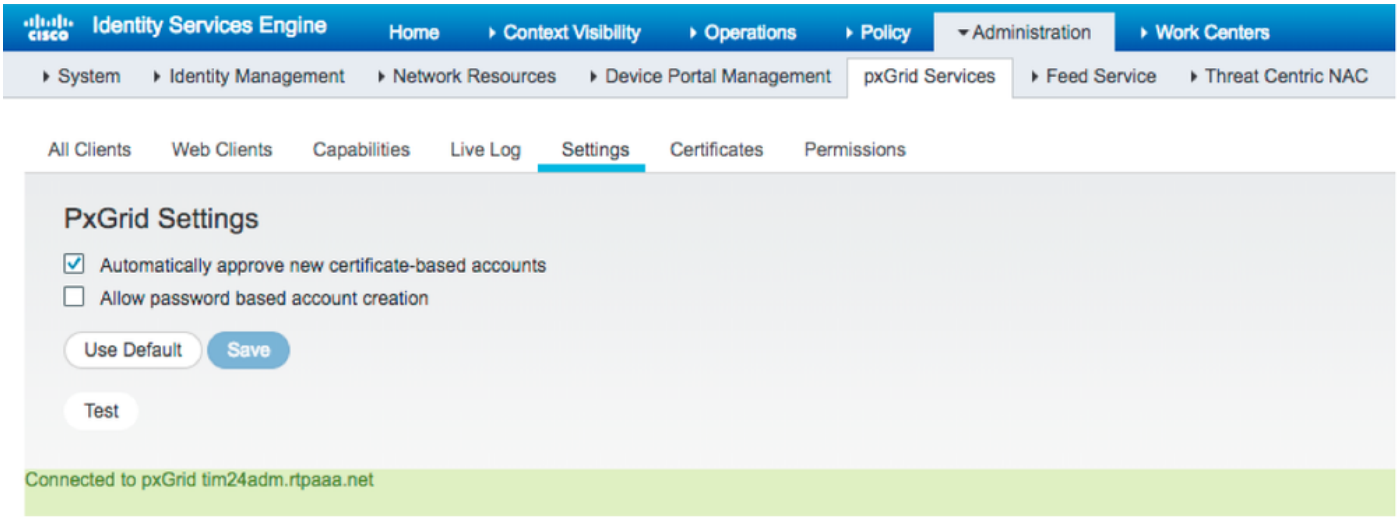
7. En bas de la page, ISE affiche **Connected to pxGrid <pxGrid node FQDN>**.



Étape 2. Configurer ISE pour approuver tous les comptes basés sur des certificats pxGrid

1. Accédez à **Administration > pxGrid Services > Settings.**

2. Cochez la case « Approuver automatiquement les nouveaux comptes basés sur un certificat » et cliquez sur **Enregistrer**.



> **Remarque** : si cette option n'est pas activée, l'administrateur doit approuver manuellement la connexion FMC à ISE.

Étape 3. Exporter les certificats d'administration ISE MNT et pxGrid CA

1. Accédez à **Administration > Certificats > Certificats système**.

2. Développez le noeud Surveillance principale (MNT) s'il n'est pas activé sur le noeud Administration principale.

3. Sélectionnez le certificat avec le champ « Utilisé par l'administrateur ».

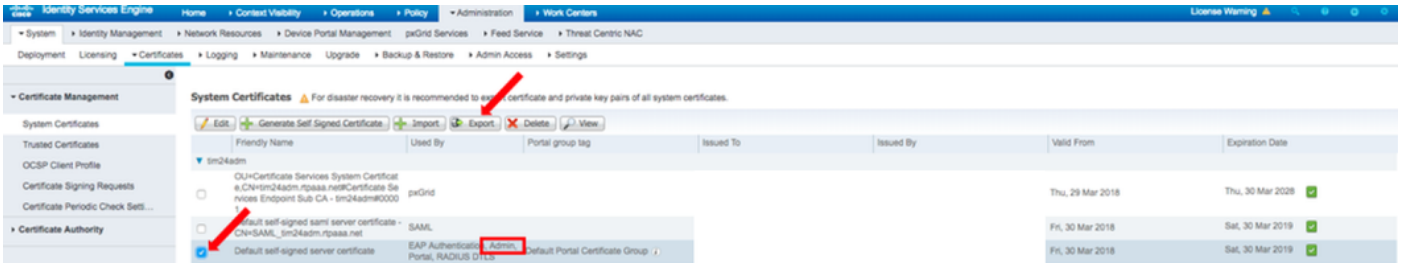
> **Remarque** : ce guide utilise le certificat auto-signé ISE par défaut pour l'administration. Si vous utilisez un certificat d'administration signé par une autorité de certification, exportez l'autorité de certification racine qui a signé le certificat d'administration sur le noeud MNT ISE.

4. Cliquez sur **Exporter**.

5. Choisissez l'option Exporter le certificat et la clé privée.

6. Définissez une clé de chiffrement.

7. **Exportez** et **enregistrez** le fichier comme indiqué dans l'image.

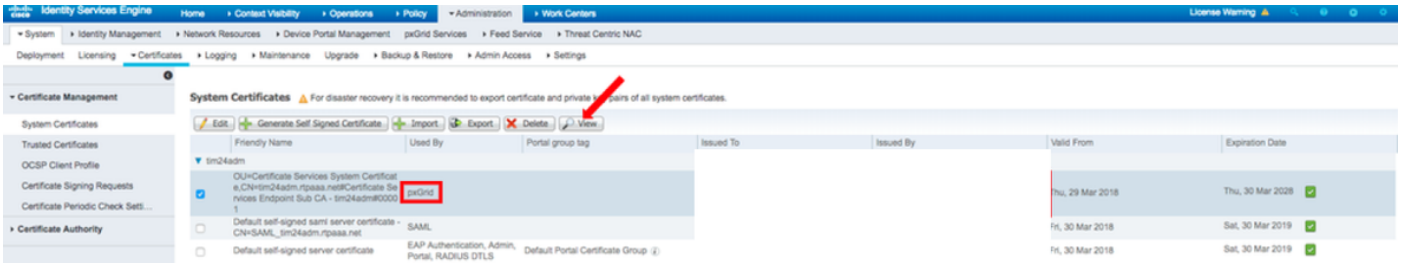


9. Revenez à l'écran ISE System Certificates (Certificats système ISE).

10. Déterminez le champ Émis par sur le certificat avec l'utilisation « pxGrid » dans la colonne Utilisé par.

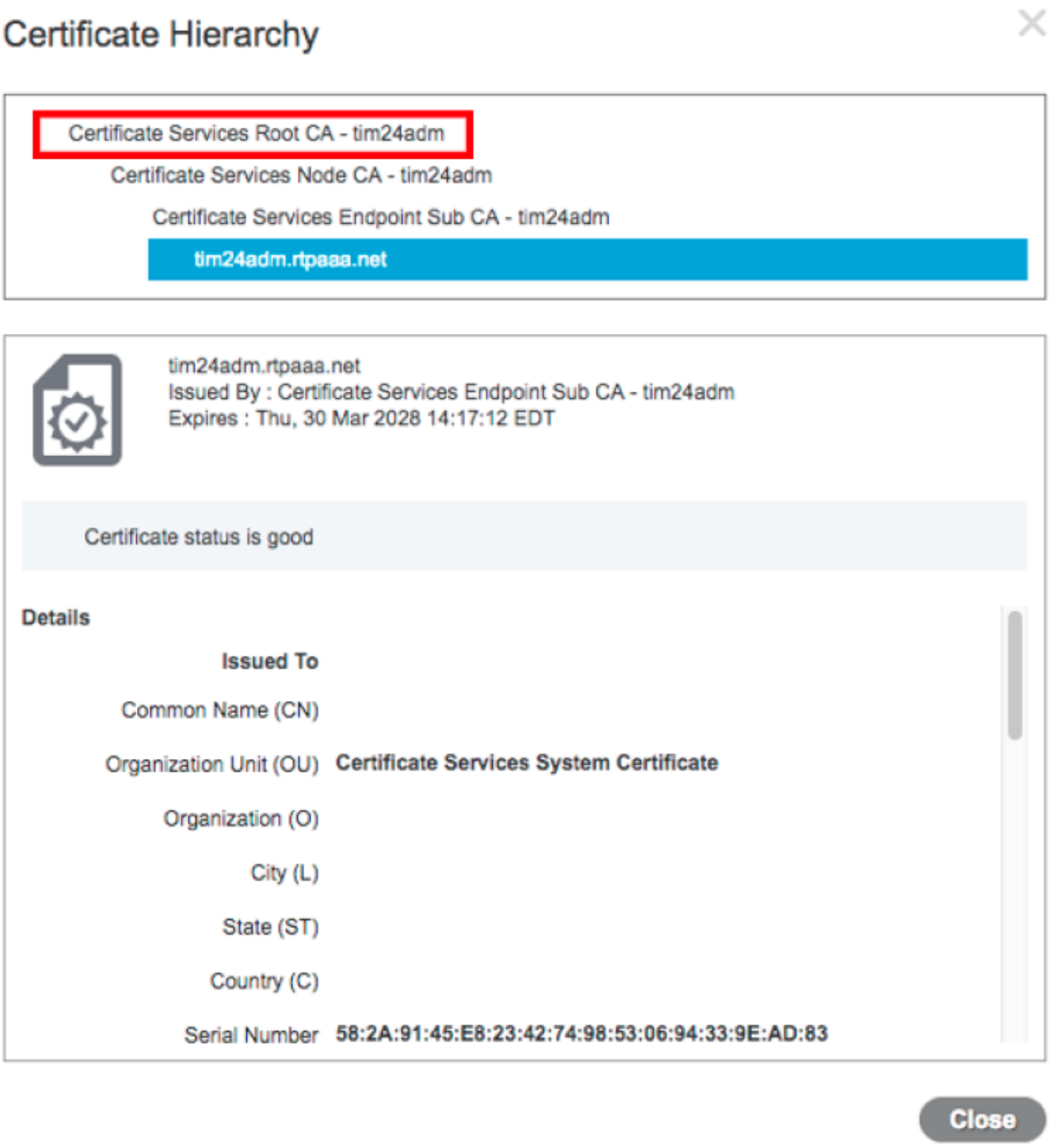
> **Remarque** : dans les versions antérieures d'ISE, il s'agissait d'un certificat auto-signé, mais à partir de la version 2.2, ce certificat est émis par la chaîne d'autorité de certification ISE interne par défaut.

11. Sélectionnez le certificat et cliquez sur **Afficher** comme indiqué dans l'image.



12. Déterminez le certificat de niveau supérieur (racine). Dans ce cas, il s'agit de **"Certificate Services Root CA - tim24adm".**

13. Fermez la fenêtre d'affichage des certificats comme indiqué dans l'image.

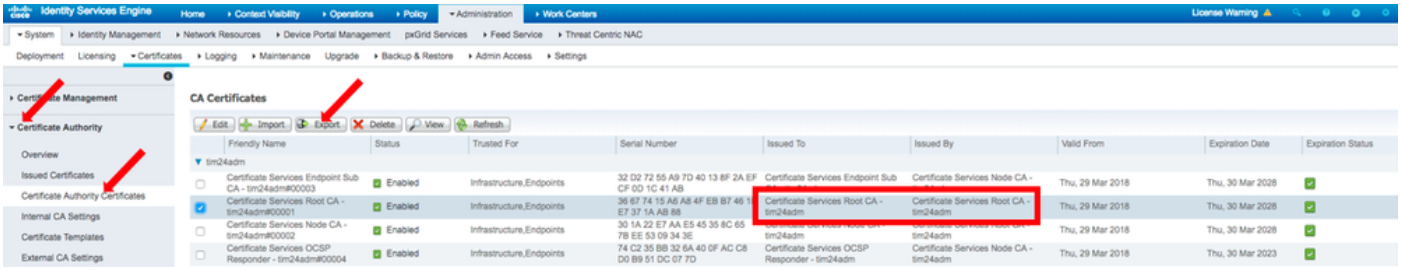


---

14. Développez le menu ISE Certificate Authority.

15. Sélectionnez **Certificats d'autorité de certification**.

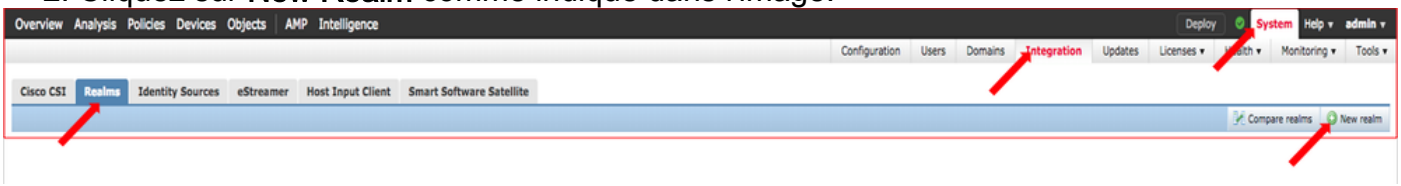
16. Sélectionnez le certificat racine identifié et cliquez sur **Exporter.** Enregistrez ensuite le certificat d'autorité de certification racine pxGrid comme indiqué dans l'image.



Configurer FMC

Étape 4. Ajouter un nouveau domaine à FMC

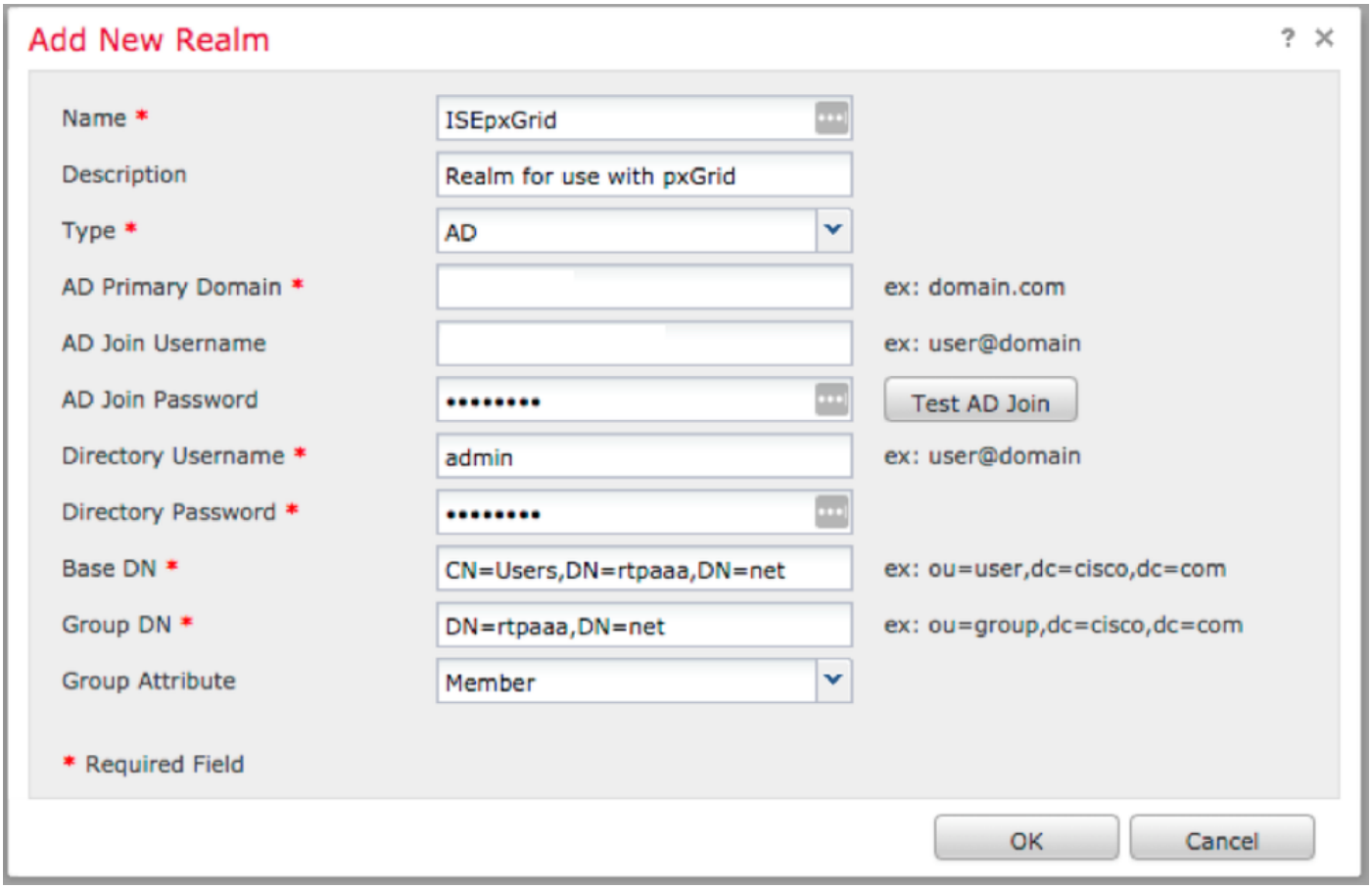
1. Accédez à l'interface utilisateur graphique de FMC et accédez à **System > Integration > Realms**.
2. Cliquez sur **New Realm** comme indiqué dans l'image.



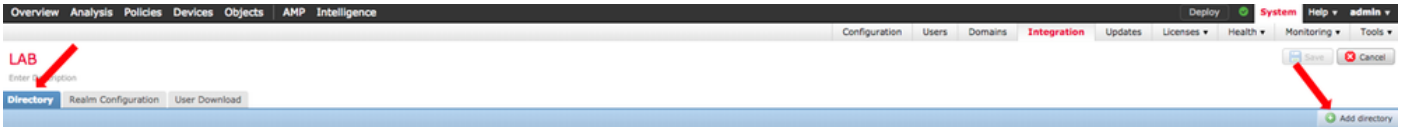
3. Remplissez le formulaire et cliquez sur le bouton Tester la connexion à Active Directory (AD).

> **Remarque** : le nom d'utilisateur de la jointure Active Directory doit être au format UPN (User Principal Name), sinon le test échoue.

4. Si le test de la jointure Active Directory réussit, cliquez sur **OK**.



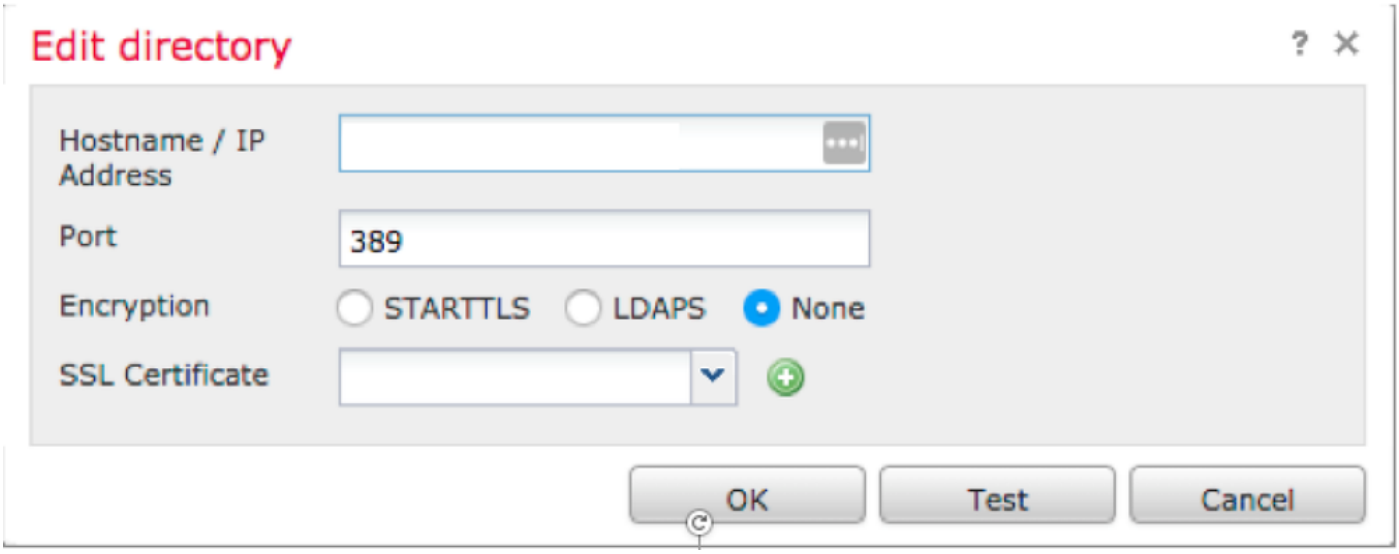
5. Cliquez sur l'onglet **Répertoire**, puis cliquez sur **Ajouter un répertoire** comme indiqué dans l'image.

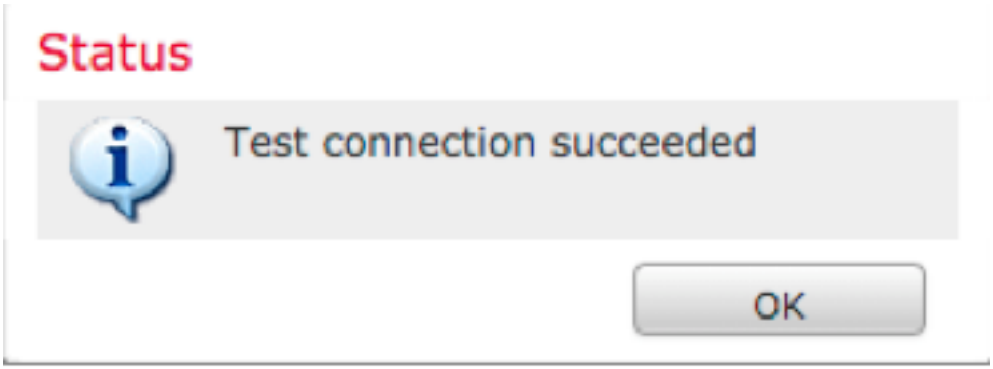


6. Configurez IP/Hostname et testez la connexion.

> **Remarque** : si le test échoue, vérifiez les informations d'identification dans l'onglet Configuration du domaine.

7. Cliquez sur **OK**.

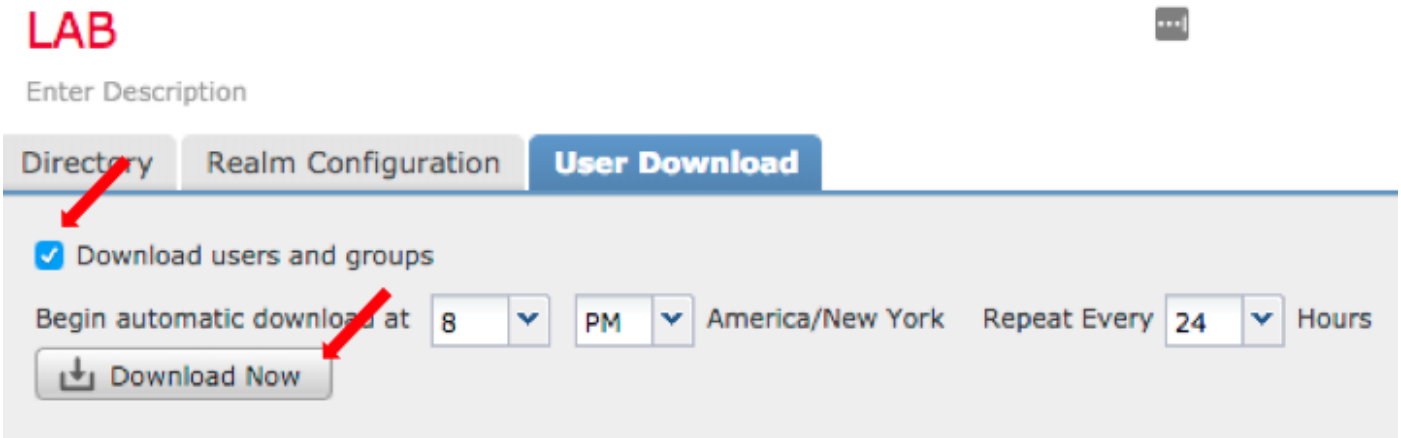




8. Cliquez sur l'onglet **Téléchargement utilisateur**.

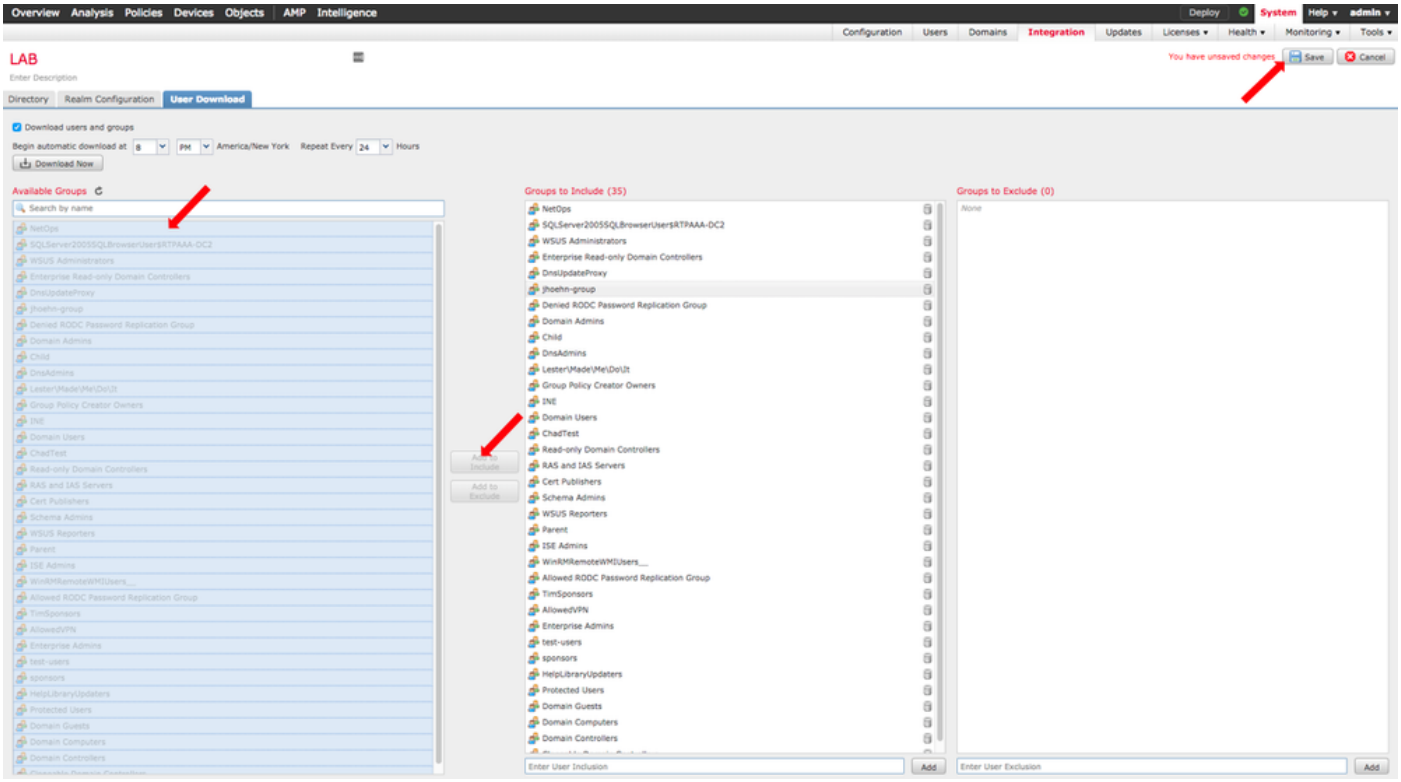
9. Si cette option n'est pas déjà sélectionnée, activez le téléchargement des utilisateurs et des groupes

10. Cliquez sur Télécharger maintenant



11. Une fois la liste renseignée, ajoutez les groupes souhaités et sélectionnez **Ajouter à inclure**.

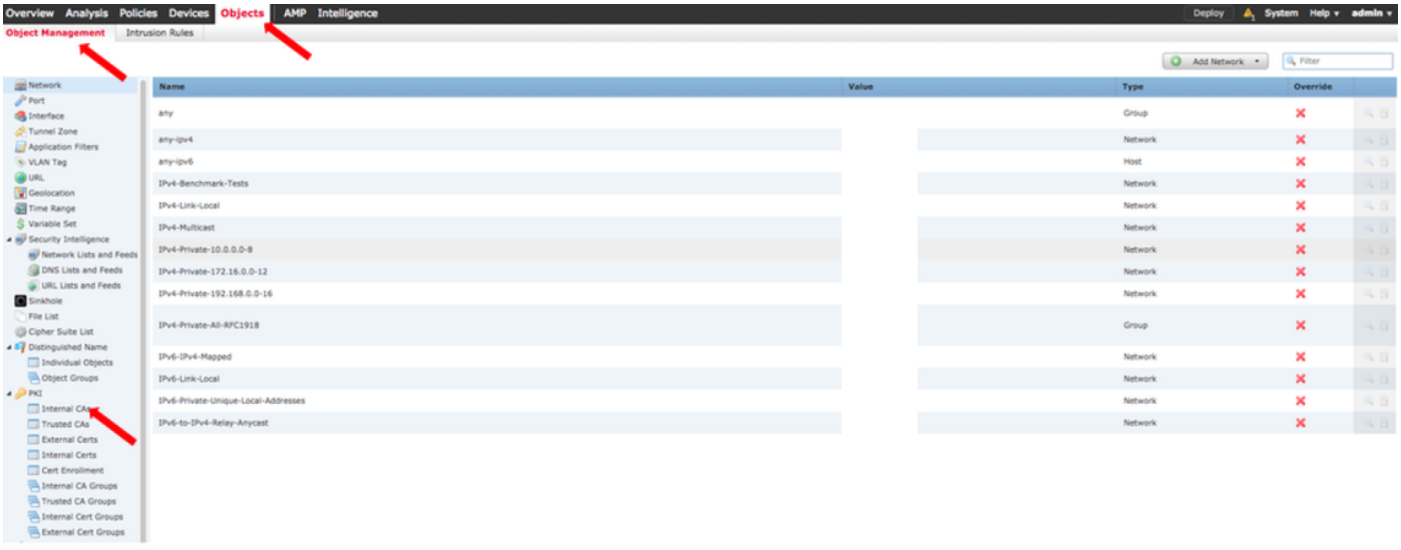
12. Enregistrez la **configuration** du **domaine**.



13. Activez l'état du domaine.

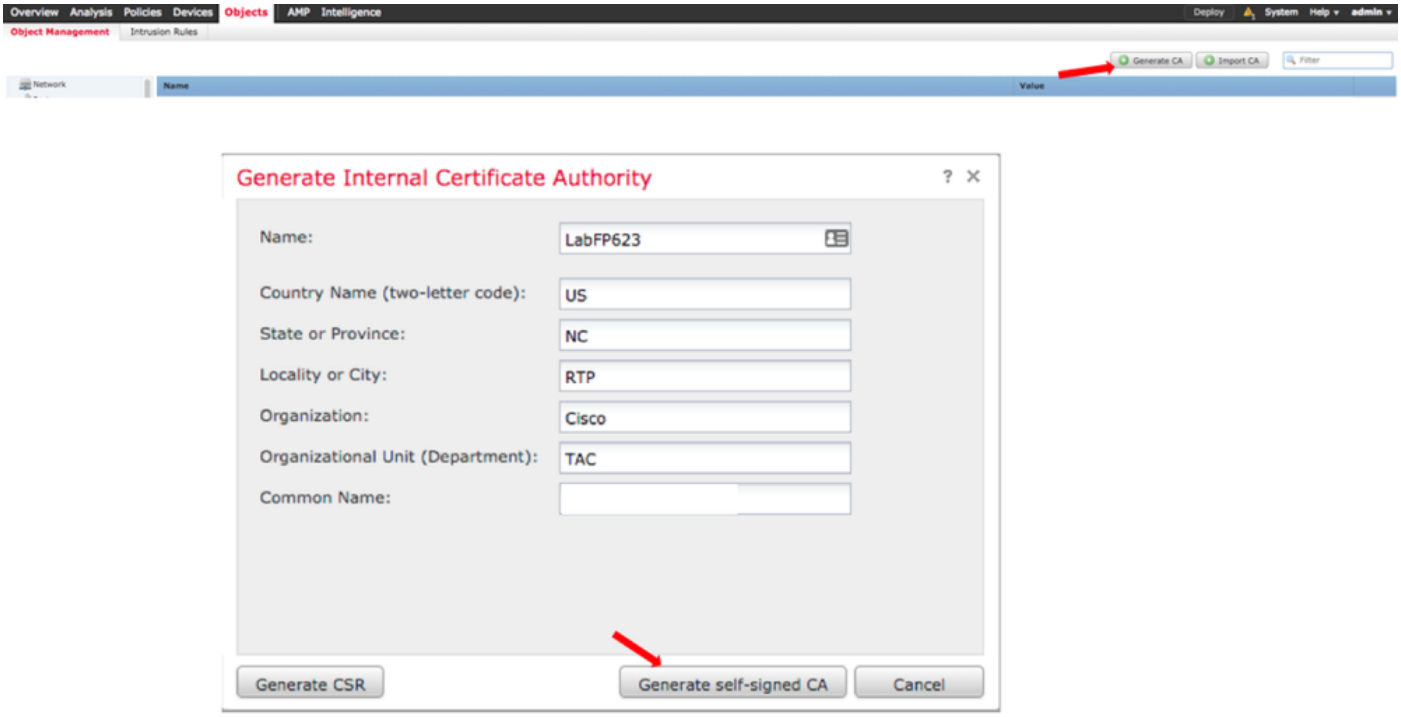
Étape 5. Générer un certificat CA FMC

1. Accédez à **Objets > Gestion des objets > Autorités de certification internes** comme indiqué dans l'image.



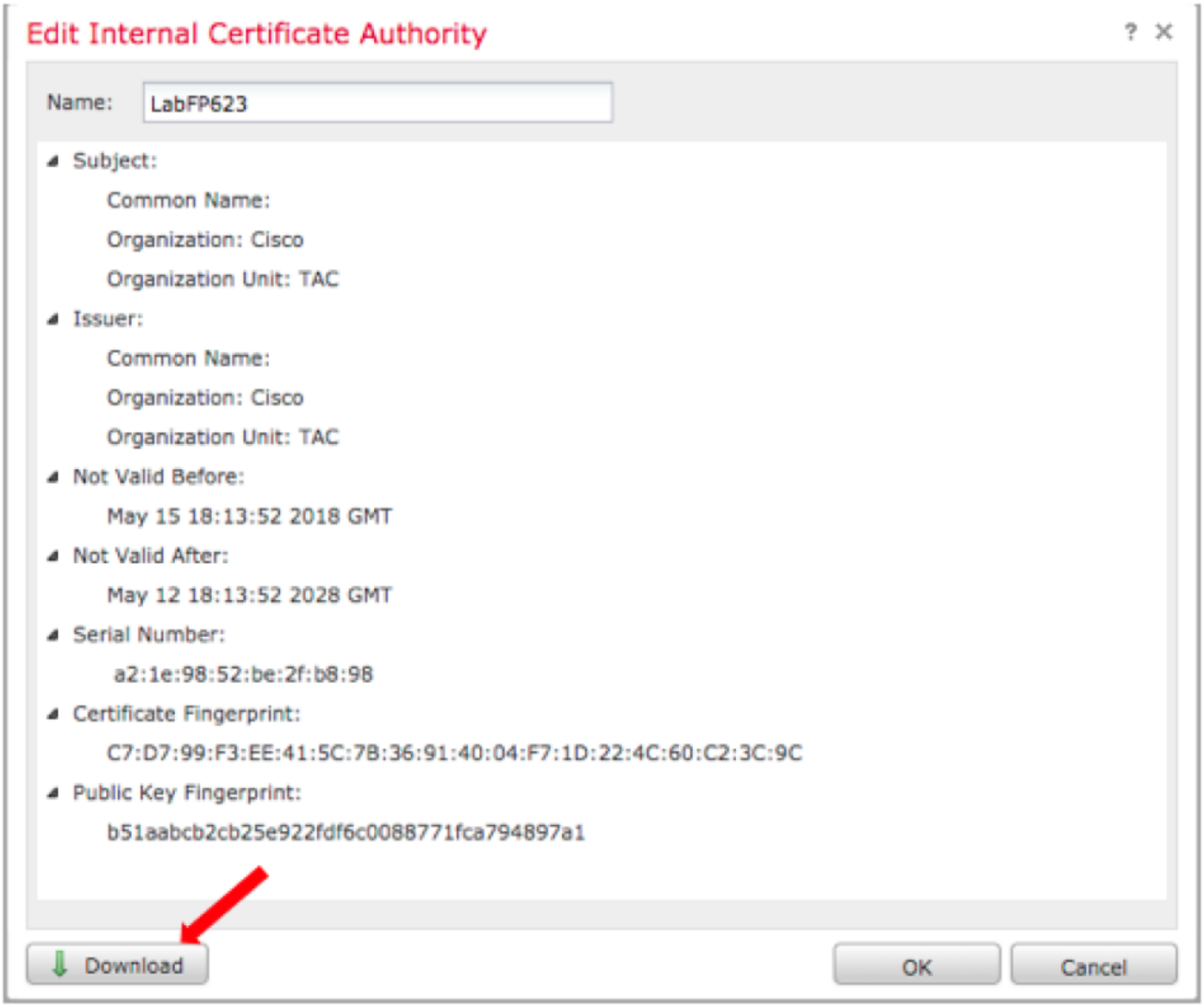
2. Cliquez sur **Generate CA**.

3. Remplissez le formulaire et cliquez sur **Generate self-signed CA**.



4. Une fois la génération terminée, cliquez sur le crayon à droite du certificat CA généré, comme illustré dans l'image.

5. Cliquez sur **Télécharger**.



6. Configurez et confirmez le mot de passe de cryptage, puis cliquez sur **OK**.

7. Enregistrez le fichier PKCS (Public-Key Cryptography Standards) p12 dans votre système de fichiers local.

Étape 6. Extraire le certificat et la clé privée du certificat généré à l'aide d'OpenSSL

Ceci est fait soit sur la racine du FMC, soit sur n'importe quel client capable de commandes OpenSSL. Cet exemple utilise un shell Linux standard.

1. Utilisez **openssl** afin d'extraire le certificat (CER) et la clé privée (PVK) du fichier p12.

2. Extrayez le fichier CER, puis configurez la clé d'exportation de certificat à partir de la génération de certificat sur FMC.

```
~$ openssl pkcs12 -nokeys -clcerts -in <filename.p12> -out <filename.cer>
Password:
Last login: Tue May 15 18:46:41 UTC 2018
Enter Import Password:
MAC verified OK
```

3. Extrayez le fichier PVK, configurez la clé d'exportation de certificat, puis définissez une

nouvelle phrase de passe PEM et confirmez.

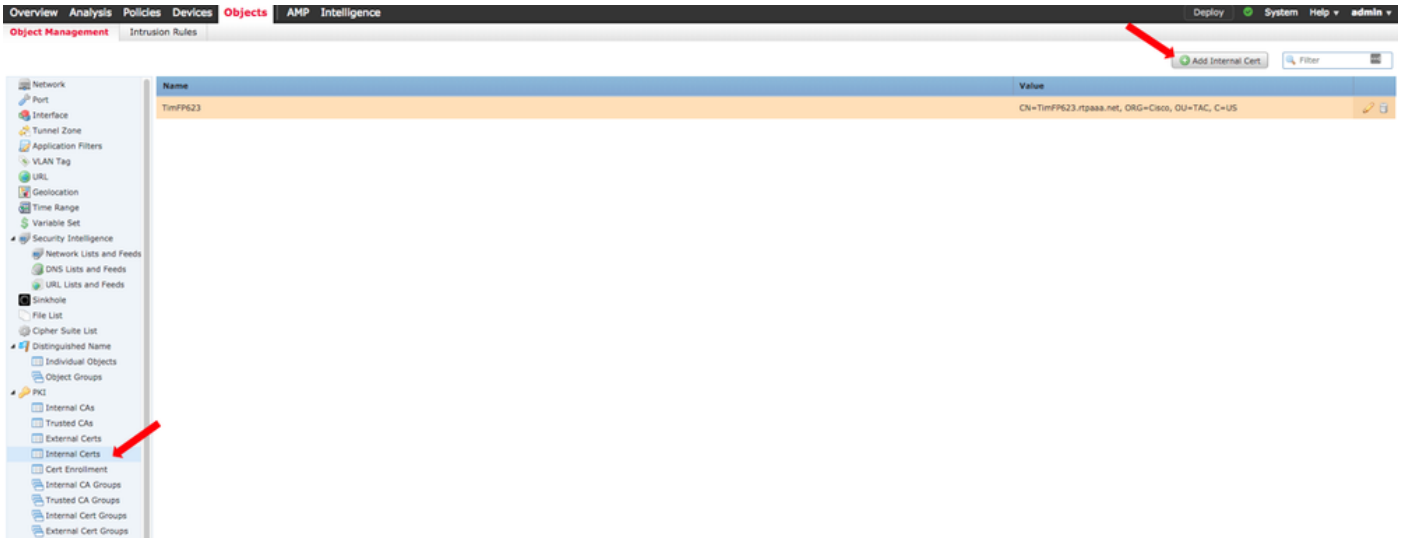
```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
Password:   Last login: Tue May 15 18:46:41 UTC 2018   Enter Import Password:   MAC verified OK
```

4. Cette phrase PEM est nécessaire à l'étape suivante.

Étape 7. Installer le certificat dans FMC

1. Accédez à **Objets > Gestion des objets > PKI > Certs internes**.

2. Cliquez sur **Add Internal Cert** comme indiqué dans l'image.



3. Configurez un nom pour le certificat interne.

4. Accédez à l'emplacement du fichier CER et sélectionnez-le. Une fois que les données de certificat sont renseignées, sélectionnez la seconde.

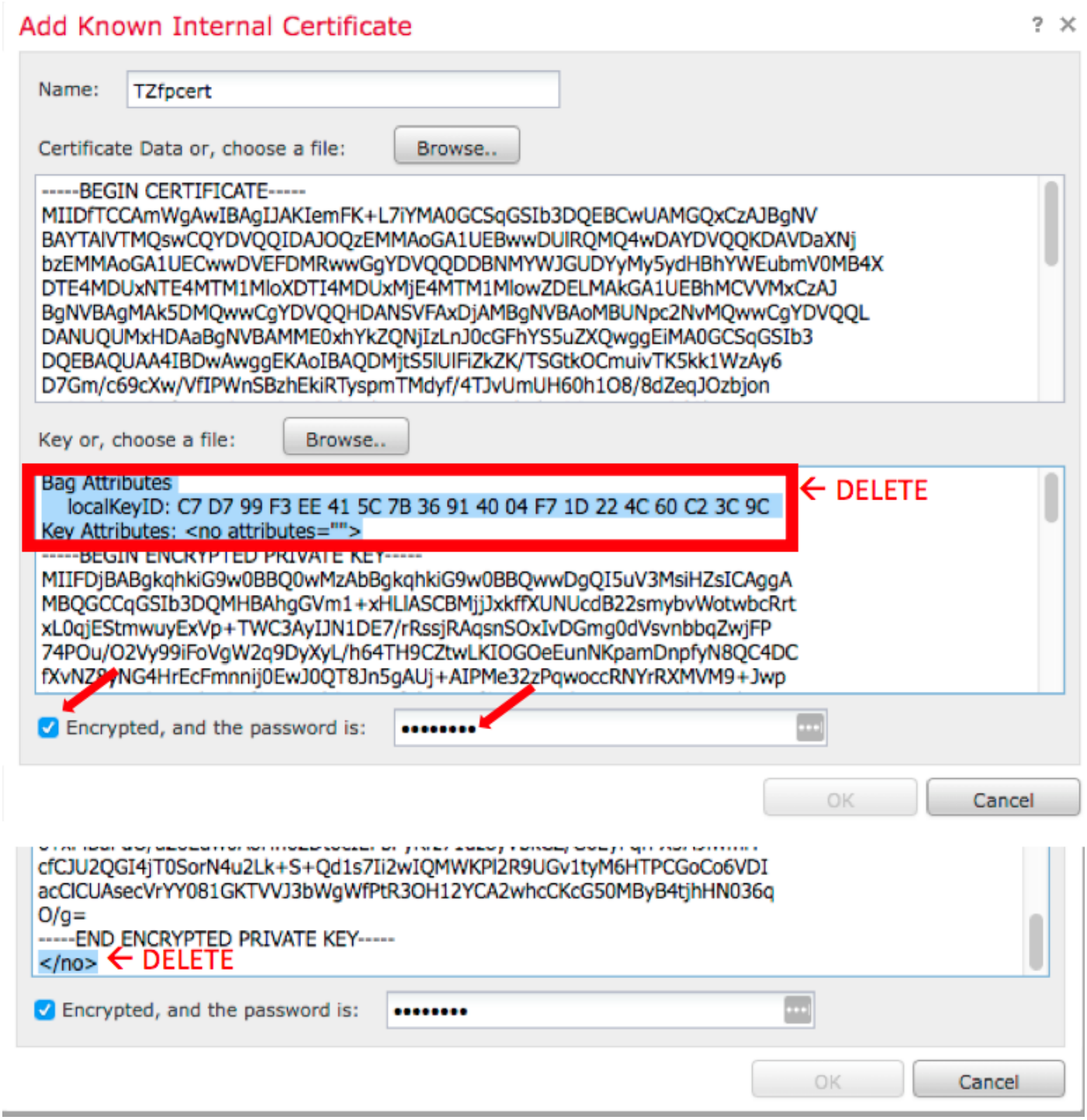
5. Parcourez **Option** et sélectionnez le fichier PVK.

6. Supprimez tous les "attributs de sac" et toutes les valeurs de fin de la section PVK. Le PVK commence par **-----BEGIN ENCRYPTED PRIVATE KEY—** et se termine par **-----END ENCRYPTED PRIVATE KEY—**.

> **Remarque** : vous ne pouvez pas cliquer sur **OK** si le texte PVK comporte des caractères en dehors des traits d'union de début et de fin.

7. Cochez la case Chiffré et configurez le mot de passe créé lors de l'exportation du PVK à l'étape 6.

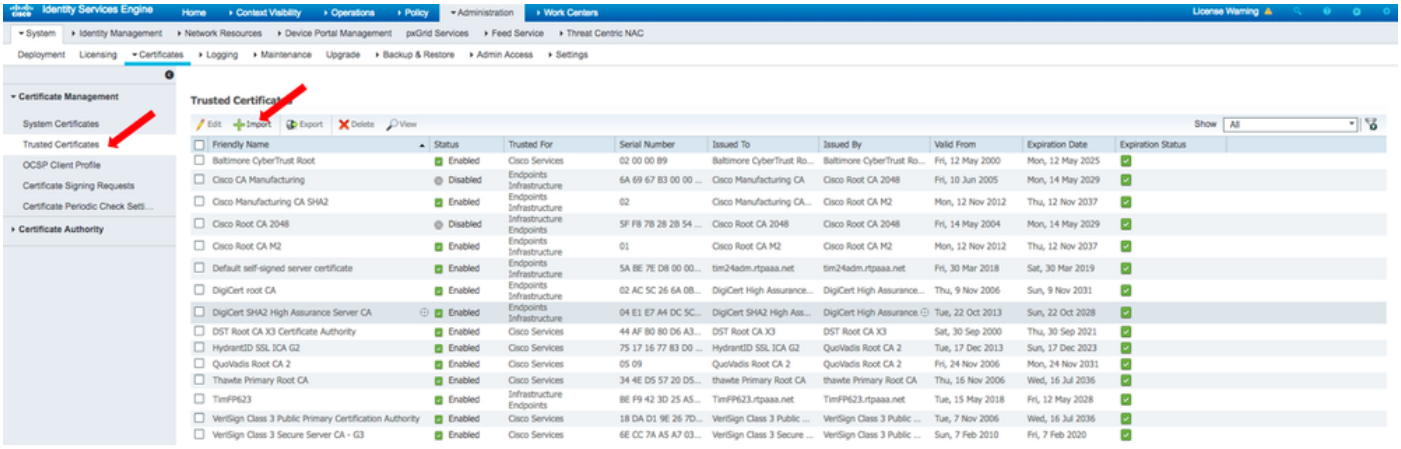
8. Cliquez sur **OK**.



Étape 8. Importer le certificat FMC dans ISE

1. Accédez à l'**interface utilisateur graphique d'ISE** et sélectionnez **Administration > System > Certificates > Trusted Certificates**.

2. Cliquez sur **Importer**.



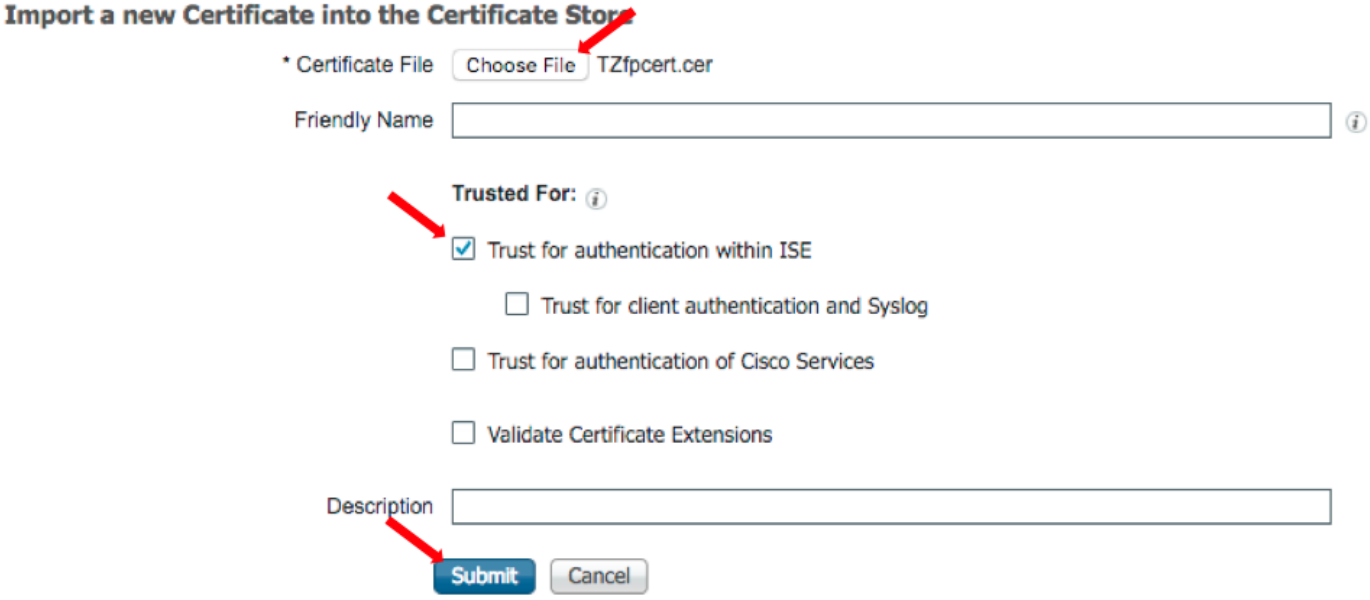
3. Cliquez sur **Choose File** et sélectionnez le fichier FMC CER sur votre système local.

   Facultatif : configurez un nom convivial.

4. Vérifiez **Trust** pour l'authentification au sein d'ISE.

   Facultatif : configurez une description.

5. Cliquez sur **Submit** comme indiqué dans l'image.



Étape 9. Configurer la connexion pxGrid sur FMC

1. Accédez à **System > Integration > Identity Sources** comme indiqué dans l'image.

2. Cliquez sur **ISE**.

3. Configurez l'adresse IP ou le nom d'hôte du noeud ISE pxGrid.

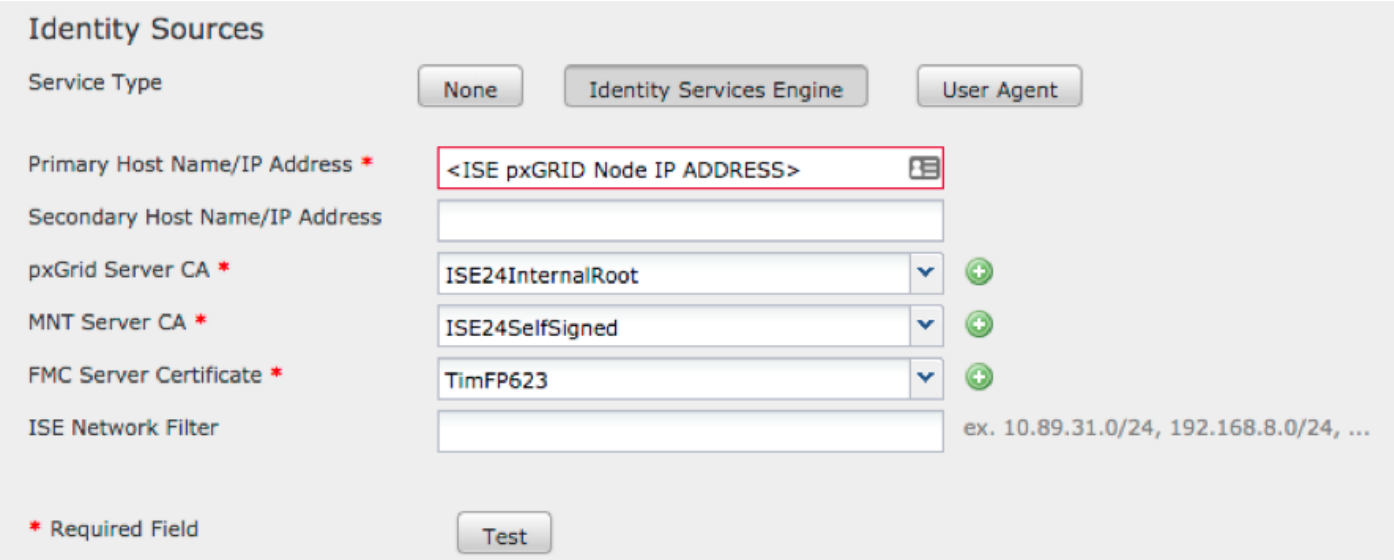
4. Sélectionnez le signe + à droite de l'autorité de certification pxGrid Server.

5. Nommez le fichier d'autorité de certification du serveur, puis accédez à l'autorité de certification de signature racine pxGrid collectée à l'étape 3. et cliquez sur **Enregistrer**.

6. Sélectionnez le signe **+** à droite de l'autorité de certification du serveur MNT.

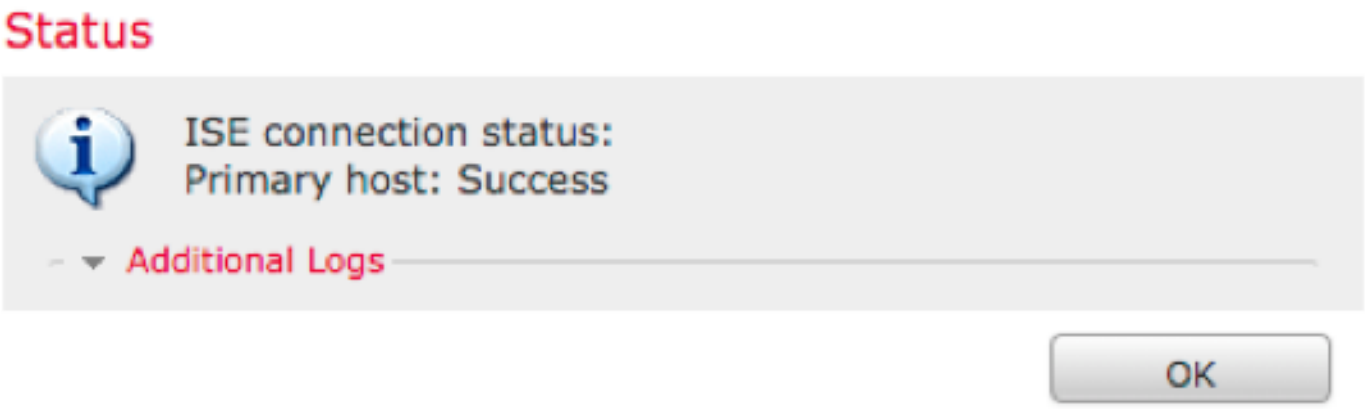
7. Nommez le fichier d'autorité de certification du serveur, puis accédez au certificat Admin collecté à l'étape 3. et cliquez sur **Enregistrer**.

8. Sélectionnez le fichier **FMC CER** dans la liste déroulante.



9. Cliquez sur **Test**.

10. Si le test réussit, cliquez sur **OK**, puis sur **Save** en haut à droite de l'écran.



> **Remarque** : lorsque vous exécutez deux noeuds ISE pxGrid, il est normal qu'un hôte affiche Success et un autre Failure, car pxGrid ne s'exécute activement que sur un noeud ISE à la fois. Cela dépend de la configuration si l'hôte principal peut afficher Échec et l'hôte secondaire, Succès. Tout dépend du noeud dans ISE qui est le noeud pxGrid actif.

Vérifier

Vérification dans ISE

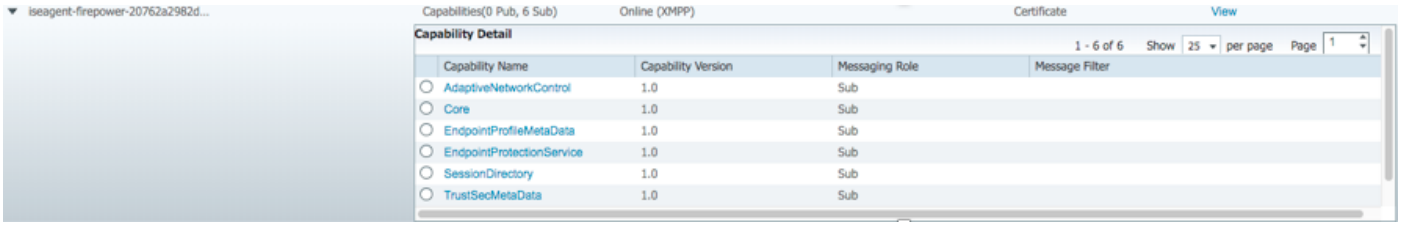
1. Ouvrez l'**interface utilisateur graphique d'ISE** et accédez à **Administration > pxGrid Services**.

En cas de réussite, deux connexions firepower sont répertoriées dans la liste des clients. Un pour le FMC réel (iseagent-hostname-33bytes) et un pour le périphérique de test (firesightisetest-hostname-33bytes).

La connexion iseagent-firepower affiche six (6) sous-réseaux et apparaît en ligne.

La connexion firesightisetest-firepower affiche zéro (0) sous-réseau et apparaît hors ligne.

La vue étendue du client iseagent-firepower affiche les six abonnements.

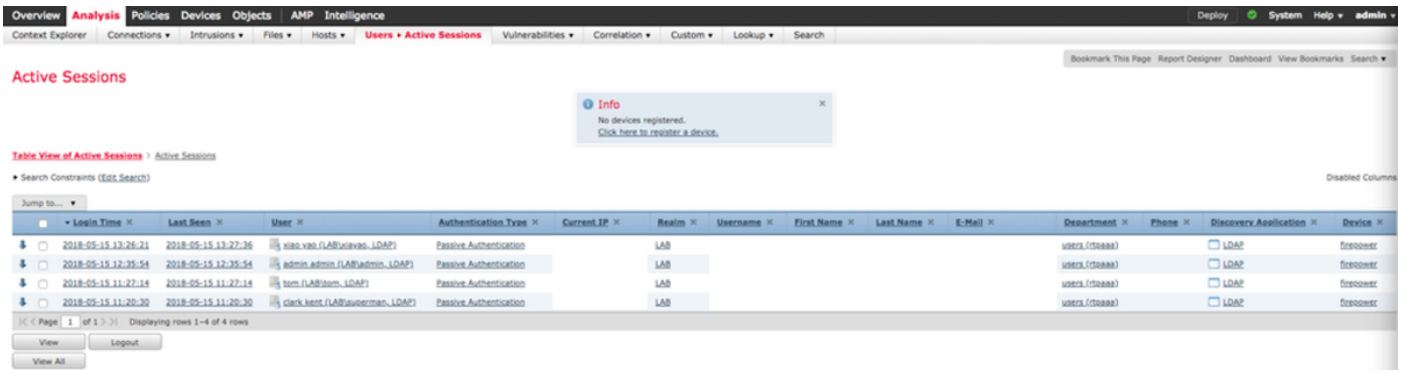


> **Remarque** : en raison du bogue Cisco IDCSCvo75376 il existe une limitation de nom d'hôte et le téléchargement en masse échoue. Le bouton de test du FMC affiche un échec de connectivité. Cela concerne 2.3p6, 2.4p6 et 2.6. La recommandation actuelle est d'exécuter 2.3 patch 5 ou 2.4 patch 5 jusqu'à ce qu'un patch officiel soit publié.

Vérification dans FMC

1. Ouvrez l'interface utilisateur graphique de FMC et accédez à **Analysis > Users > Active Sessions**.

Toutes les sessions actives publiées via la fonctionnalité d'annuaire de sessions dans ISE sont affichées dans le tableau Sessions actives sur FMC.



En mode sudo de l'interface de ligne de commande FMC, la **session adi_cli** affiche les

informations de session utilisateur envoyées par ISE à FMC.

```
ssh admin@<FMC IP ADDRESS>
Password:
Last login: Tue May 15 19:03:01 UTC 2018 from dhcp-172-18-250-115.cisco.com on ssh
Last login: Wed May 16 16:28:50 2018 from dhcp-172-18-250-115.cisco.com

Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.3 (build 13)
Cisco Firepower Management Center for VMWare v6.2.3 (build 83)

admin@firepower:~$ sudo -i
Password:
Last login: Wed May 16 16:01:01 UTC 2018 on cron
root@firepower:~# adi_cli session

received user session: username tom, ip ::ffff:172.18.250.148, location_ip ::ffff:10.36.150.11,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
received user session: username xiayao, ip ::ffff:10.36.148.98, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username admin, ip ::ffff:10.36.150.24, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username administrator, ip ::ffff:172.18.124.200, location_ip ::,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

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.