Intégration d'ISE 3.3 à StealthWatch 7.5.1 à l'aide d'une CA externe

Table des matières

Introduction

Ce document décrit les procédures d'intégration d'ISE 3.3 avec Secure Network Analytics (StealthWatch) à l'aide de connexions pxGrid.

Conditions préalables

Cisco recommande des connaissances sur les sujets suivants :

- Plateforme de services d’identité
- Platform Exchange Grid (pxGrid)
- Secure Network Analytics (StealthWatch)
- Certificats TLS/SSL.
- PKI sur Windows Server 2016

Composants utilisés

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

- Identity Services Engine (ISE) version 3.3 correctif 4
- Analyses réseau sécurisées (StealthWatch) 7.5.1
- Windows Server 2016 en tant que serveur d'autorité de certification externe.

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.

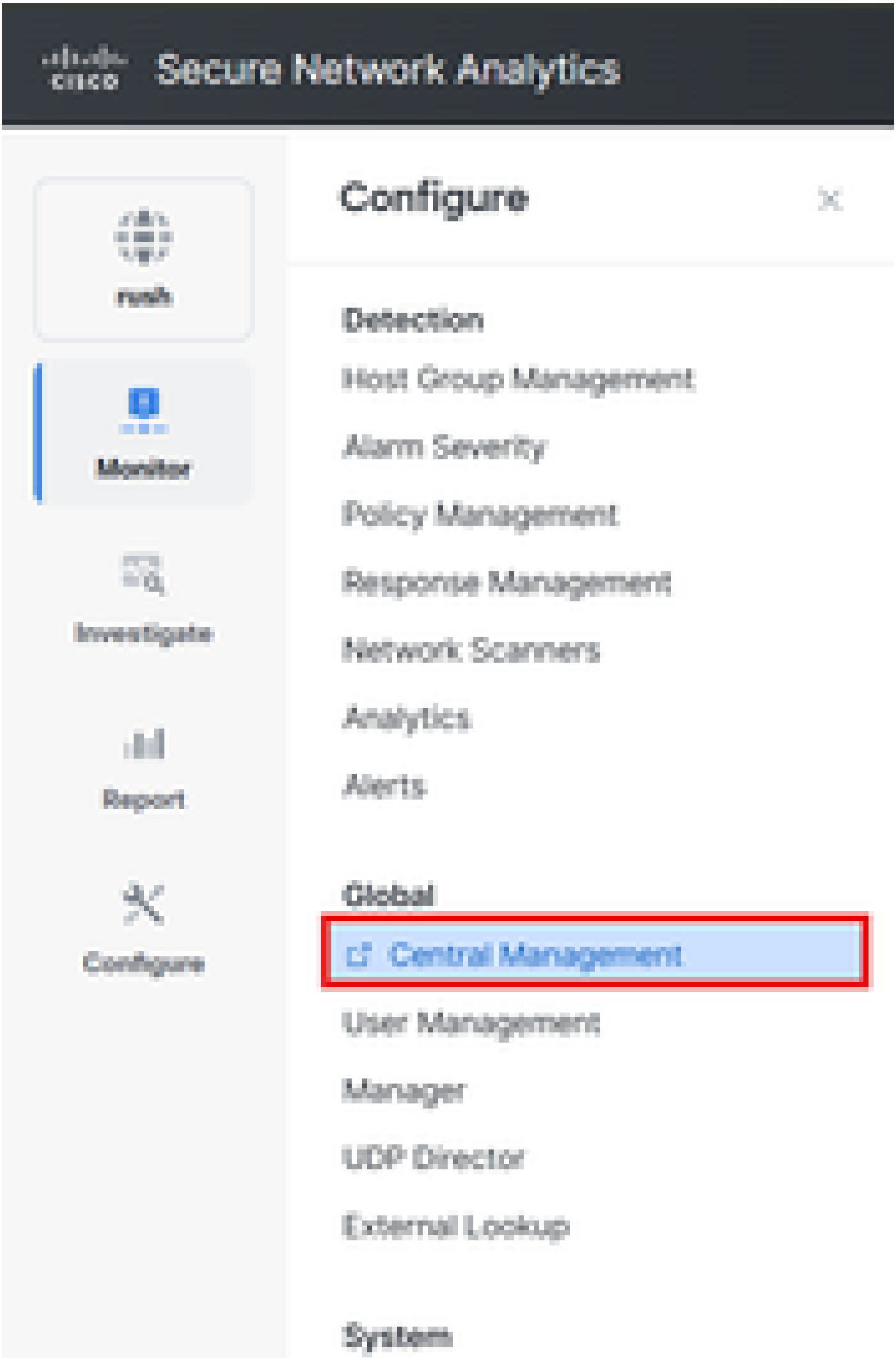
Configurer

Section A : Configuration du certificat Secure Network Analytics (StealthWatch)

Partie I - Génération d'un CSR pour le certificat client Secure Network Analytics pxGrid

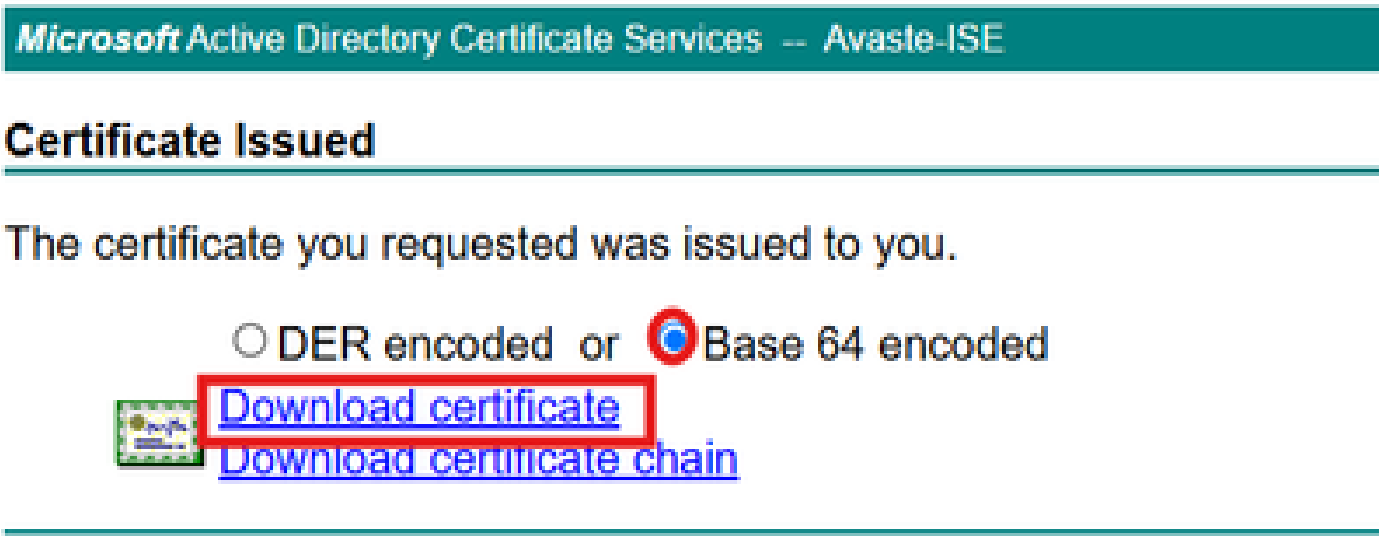
1. Connectez-vous à StealthWatch Management Console (SMC).

2. Dans le menu principal, sélectionnez Configure > Global > Central Management.


Secure Network Analytics
rush
Monitor
Investigate
Report
Configure
Configure
Detection
Host Group Management
Alarm Severity
Policy Management
Response Management
Network Scanners
Analytics
Alerts
Global
Central Management
User Management
Manager
UDP Director
External Lookup
System

Le modèle de certificat pxGrid utilisé nécessite à la fois l'authentification du client et l'authentification du serveur dans le champ « Utilisation améliorée de la clé ».

6. Téléchargez un certificat généré au format Base-64 et enregistrez-le sous pxGrid_client.cer.



PARTIE III - Ajout du certificat client Secure Network Analytics pxGrid au gestionnaire

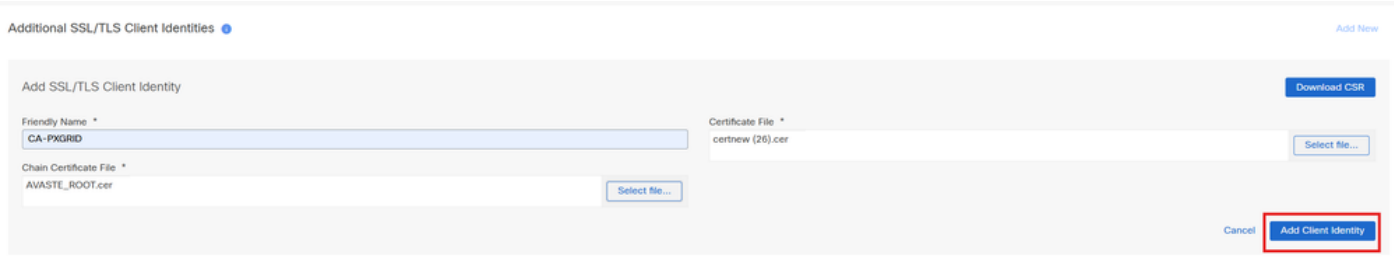
1. Accédez à la section Identités de client SSL/TLS supplémentaires de la configuration du gestionnaire dans Central Management.

2. La section Identités de client SSL/TLS supplémentaires contient un formulaire pour importer le certificat client créé.

3. Attribuez un nom convivial au certificat, puis cliquez sur Sélectionner un fichier pour localiser le fichier de certificat.

4. Sélectionnez le fichier .cer de l'autorité de certification racine ou de l'émetteur ou le fichier de chaîne de certificats (.pem / .cer / .crt) dans la section Fichier de certificat de chaîne.

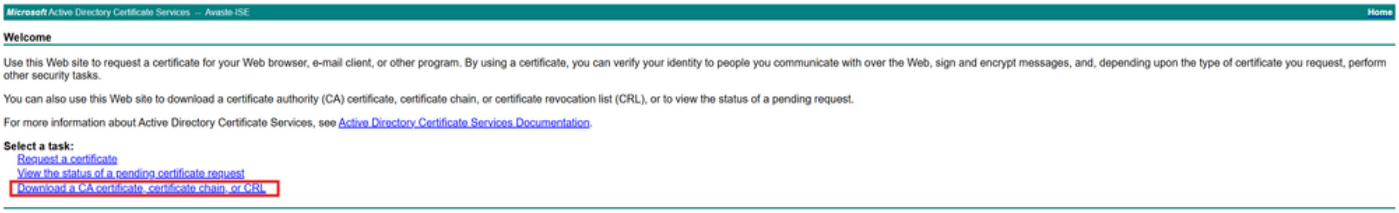
5. Cliquez sur Add Client Identity pour ajouter le certificat au système.



6. Cliquez sur Apply Settings pour enregistrer les modifications.

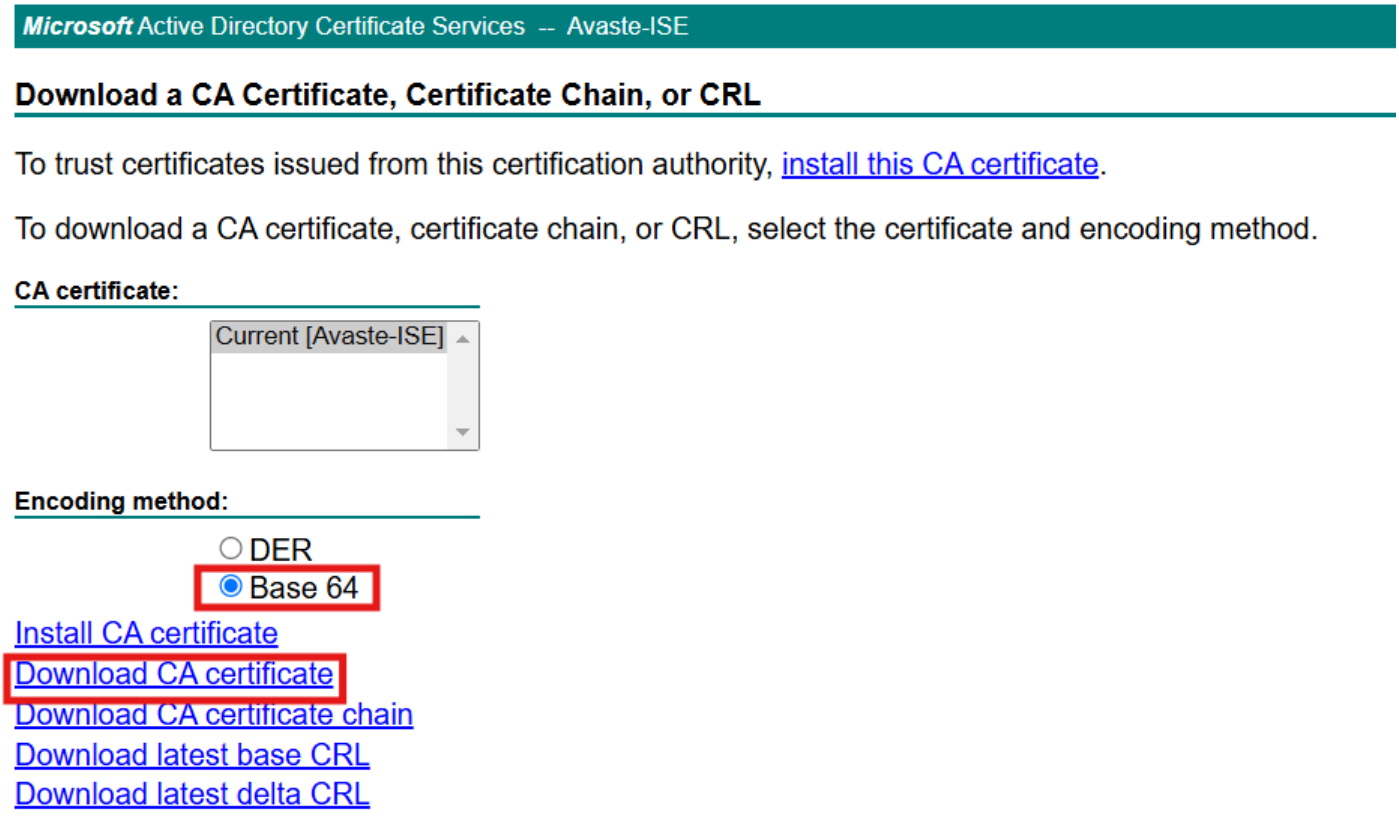
PARTIE IV - Importation du certificat racine de l'autorité de certification dans le magasin de gestion de la confidentialité

1. Accédez à la page d'accueil du service de certificats Active Directory MS et sélectionnez Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation de certificats.



2. Sélectionnez le format Base-64, puis cliquez sur Télécharger le certificat CA.

3. Enregistrez le certificat en tant que CA_Root.cer.



4. Connectez-vous à la console de gestion StealthWatch (SMC).

5. Dans le menu principal, sélectionnez Configure > Global > Central Management.

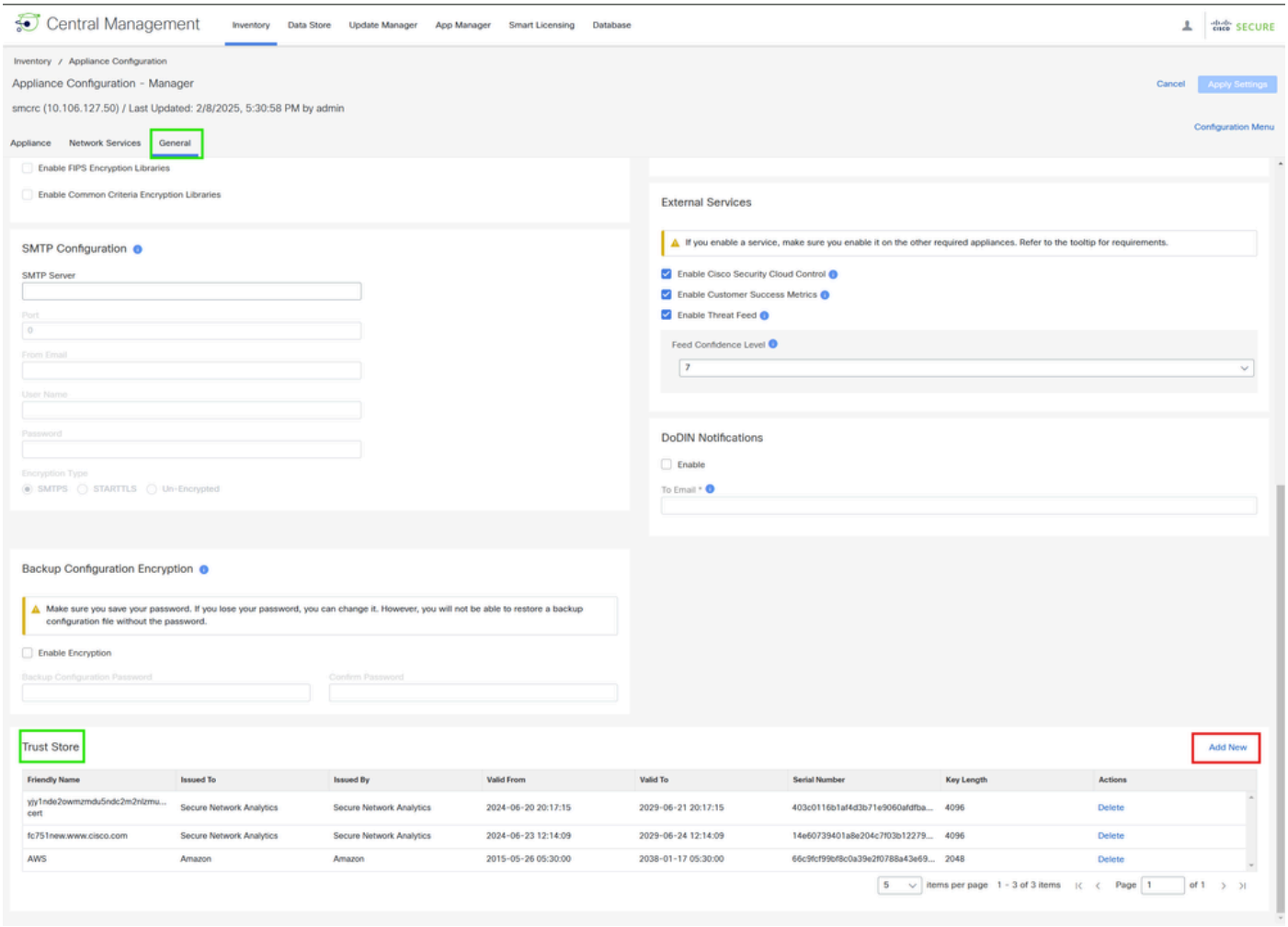
6. Sur la page Inventaire, cliquez sur l'icône (points de suspension) du manager.

7. Choisissez Modifier la configuration du matériel.

8. Sélectionnez l'onglet Général.

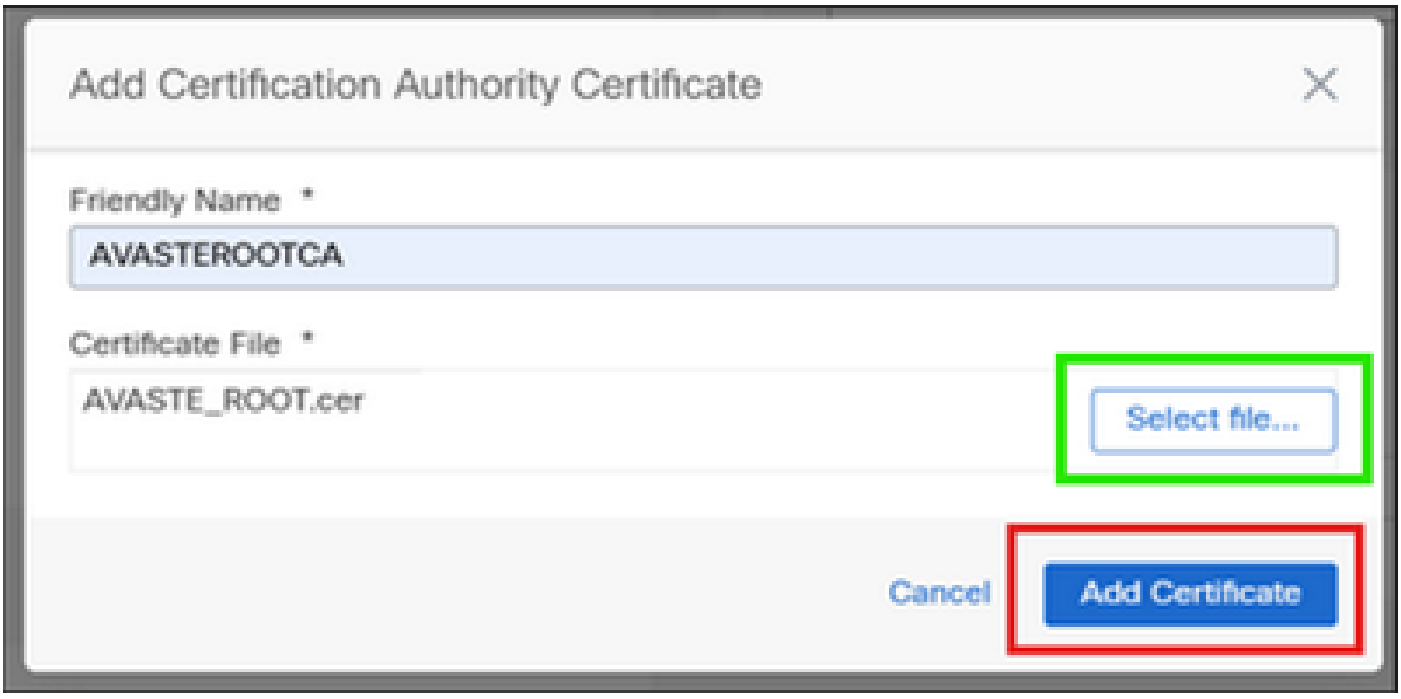
9. Accédez à la section Magasin de confiance et importez le certificat CA_Root.cer précédemment exporté.

10. Cliquez sur Ajouter nouveau.



11. Attribuez un nom convivial au certificat, puis cliquez sur Sélectionner un fichier... pour sélectionner le certificat de l'autorité de certification ISE exporté précédemment.

12. Cliquez sur Add Certificate pour enregistrer les modifications.



13. Cliquez sur Apply Settings pour enregistrer les modifications.

Section B : Configuration du certificat Cisco Identity Services Engine 3.3

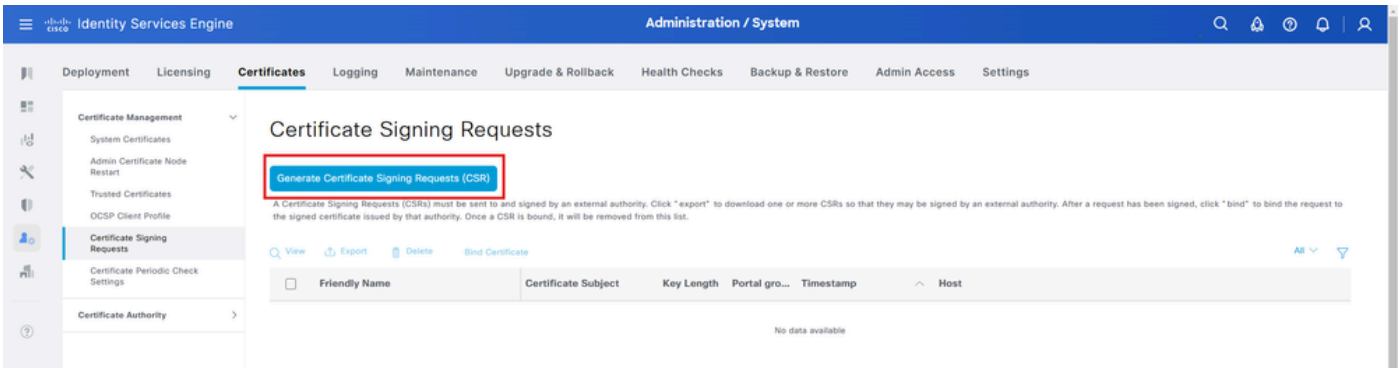
PARTIE I - Génération d'un certificat ISE Server pxGrid

Générez un CSR pour un certificat pxGrid de serveur ISE :

1. Connectez-vous à l'interface utilisateur graphique de Cisco Identity Services Engine (ISE).

2. Accédez à Administration > Système > Certificats > Gestion des certificats > Demandes de signature de certificat.

3. Sélectionnez Générer une demande de signature de certificat (CSR).

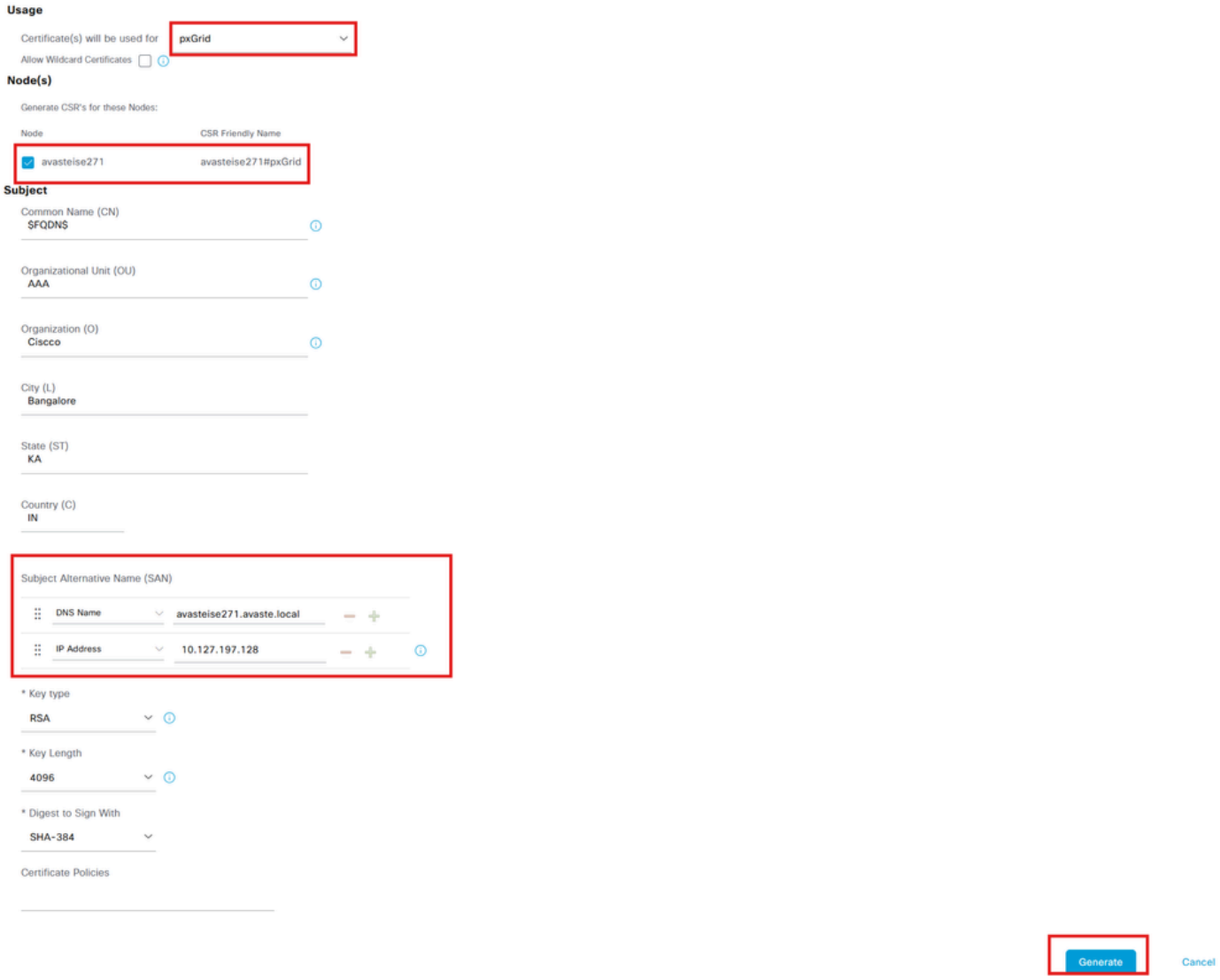


4. Sélectionnez pxGrid dans le champ Certificate(s) is used for.

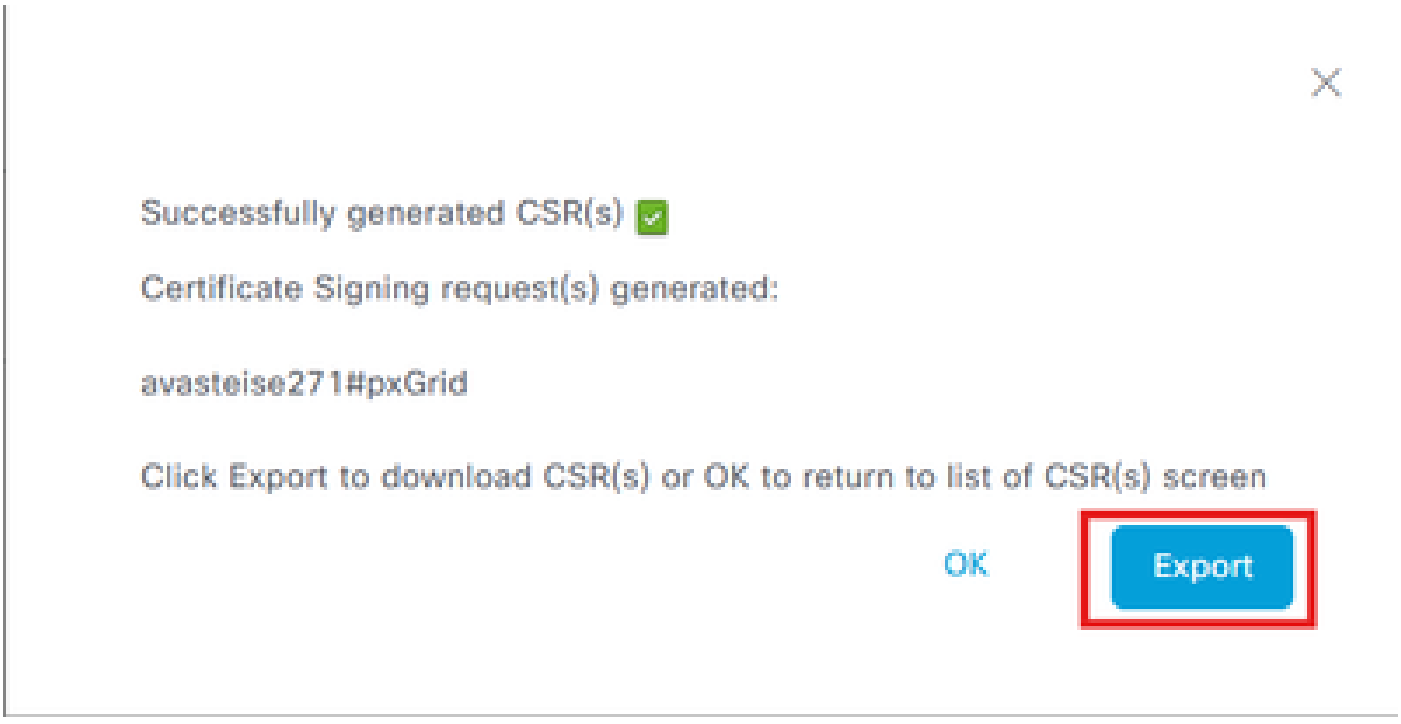
5. Sélectionnez le noeud ISE pour lequel le certificat est généré.

6. Complétez les détails des autres certificats si nécessaire.

7. Cliquez sur Générer.



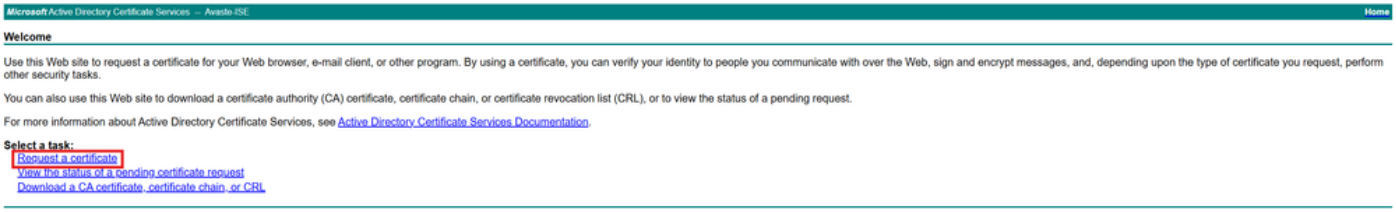
8. Cliquez sur Exporter et enregistrez le fichier localement.



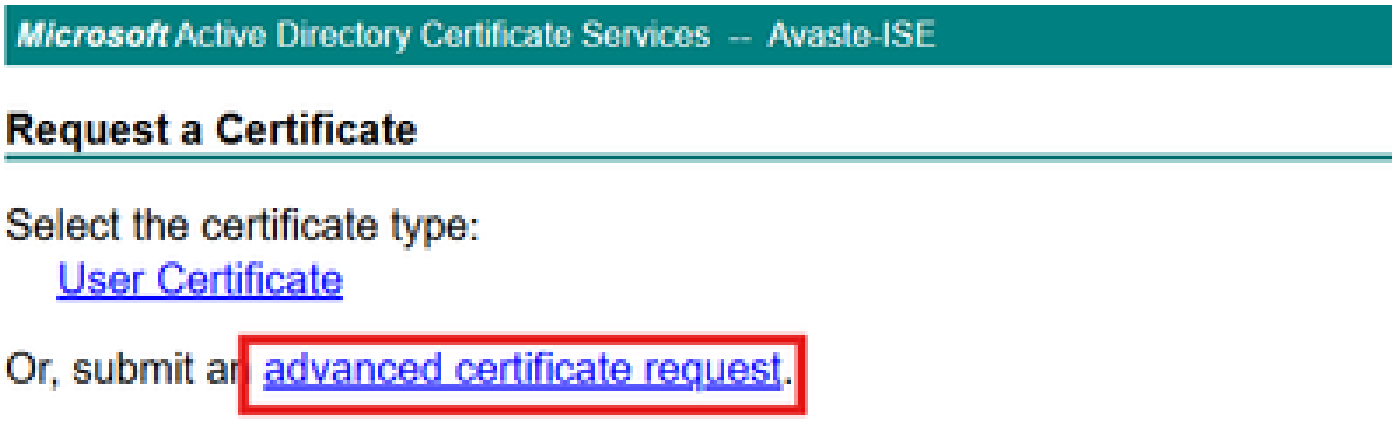
PARTIE II - Création d'un certificat pxGrid de serveur ISE à l'aide d'une autorité de certification externe

1. Accédez au service de certificats MS Active Directory, https://server/certsrv/, où server is IP or DNS of your MS Server.

2. Cliquez sur Demander un certificat.

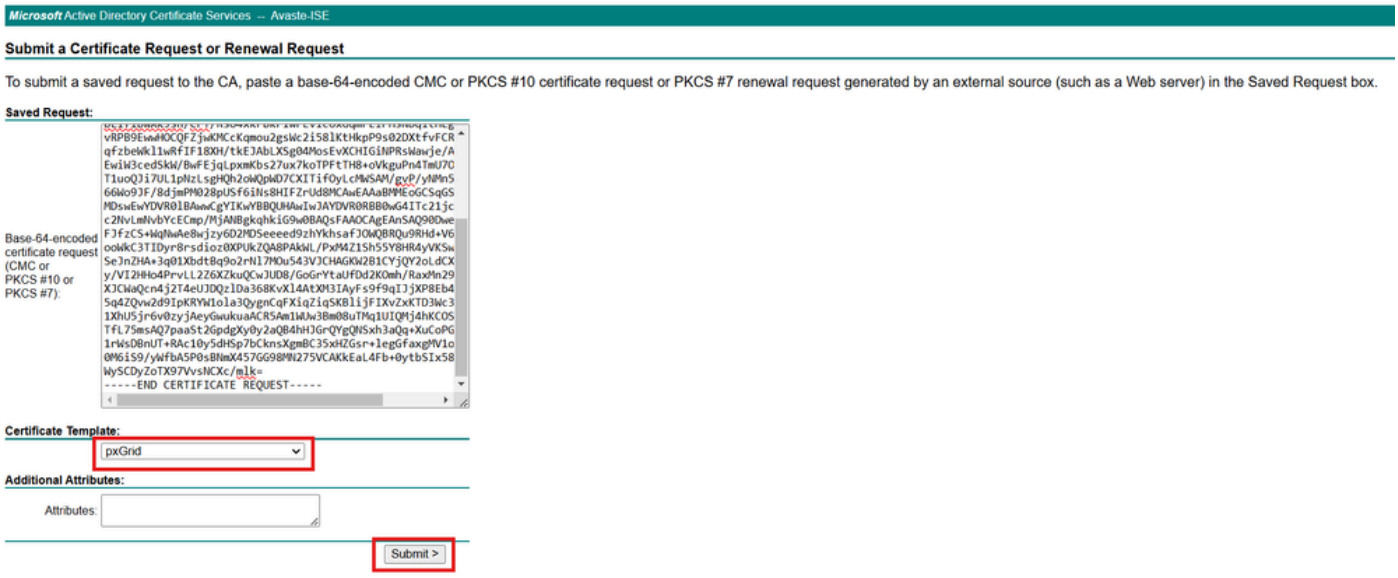


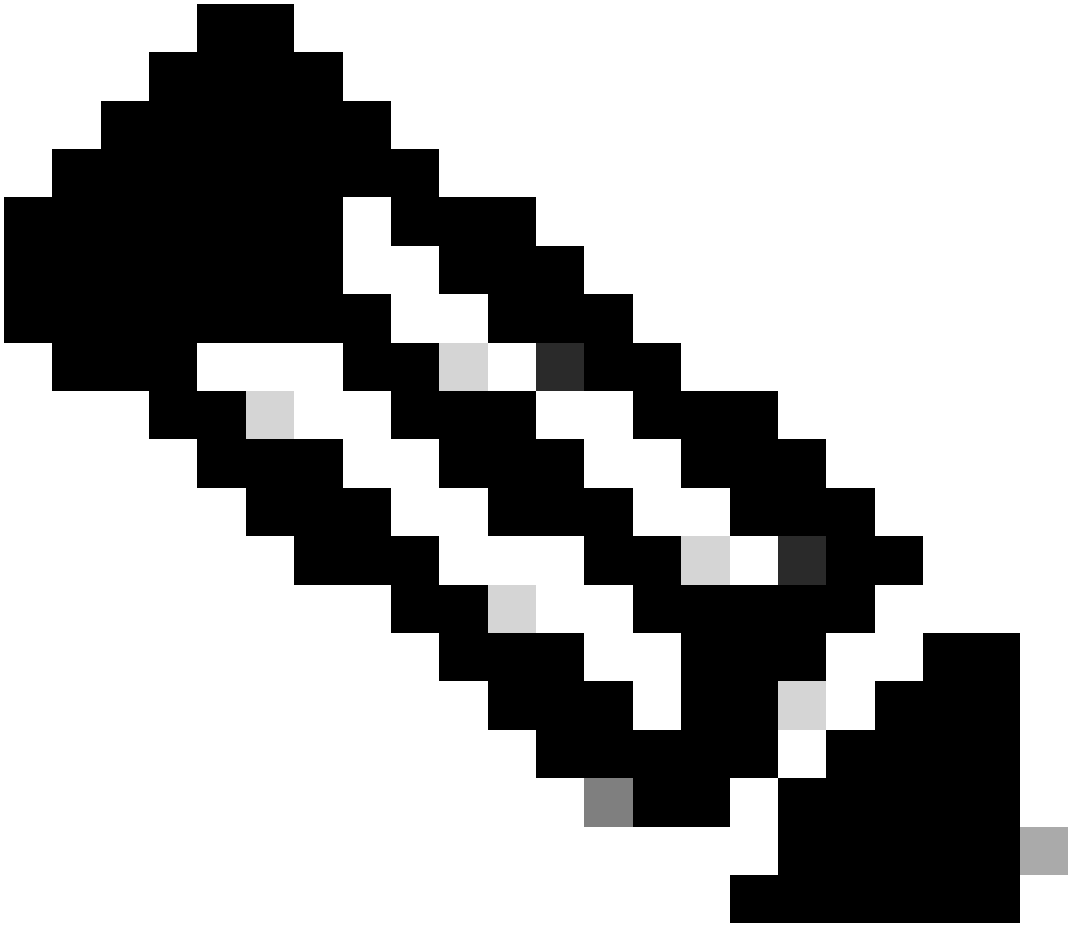
3. Choisissez de soumettre une demande de certificat avancée.



4. Copiez le contenu du CSR généré dans la section précédente dans le champ Requête enregistrée.

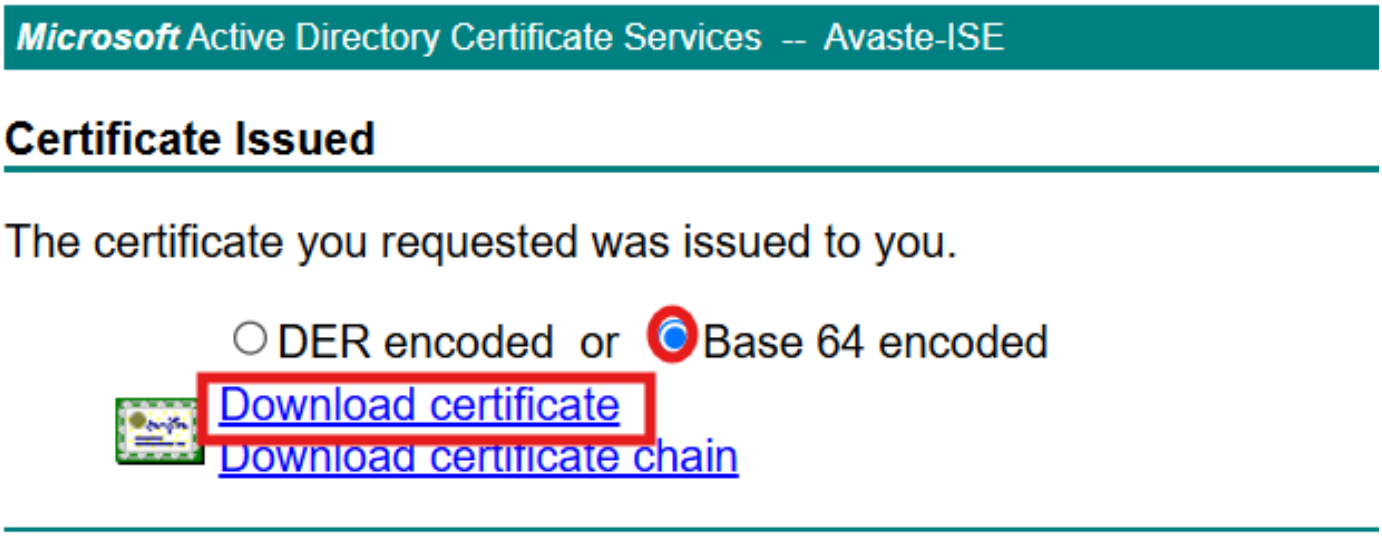
5. Sélectionnez pxGrid comme modèle de certificat, puis cliquez sur Envoyer.





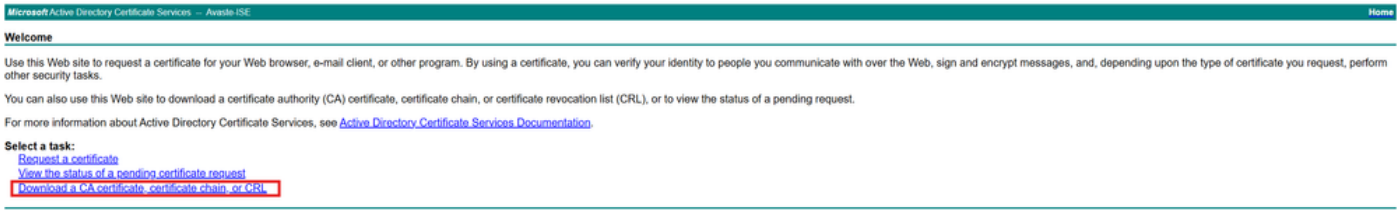
Remarque : Le modèle de certificat pxGrid utilisé nécessite à la fois l'authentification du client et l'authentification du serveur dans le champ « Utilisation améliorée de la clé ».

6. Téléchargez le certificat généré au format Base-64 et enregistrez-le sous le nom ISE_pxGrid.cer.

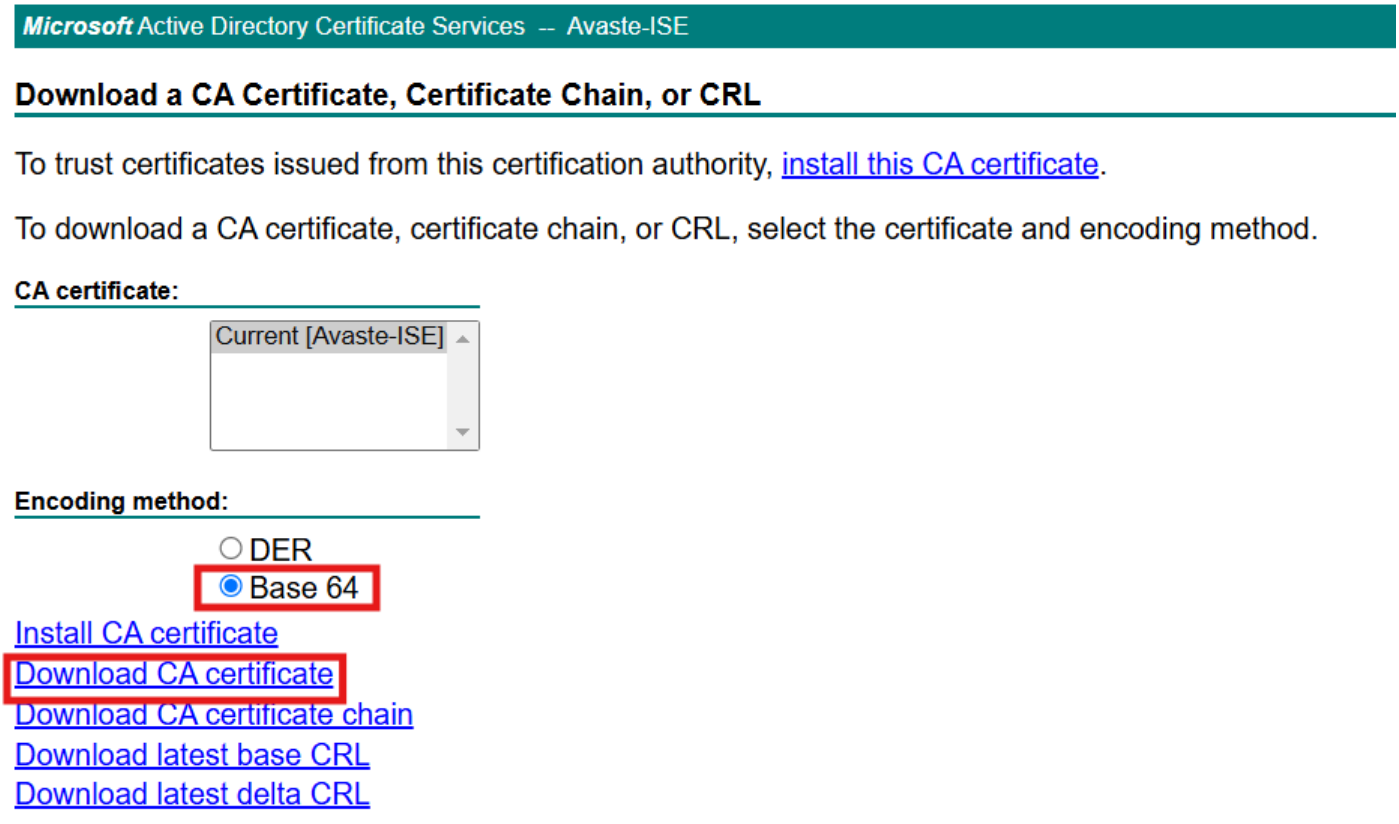


PARTIE III - Importation du certificat racine de l'autorité de certification dans l'ISE Trust Store

1. Accédez à la page d'accueil du service de certificats MS Active Directory et sélectionnez Télécharger un certificat CA, une chaîne de certificats ou une liste de révocation de certificats.



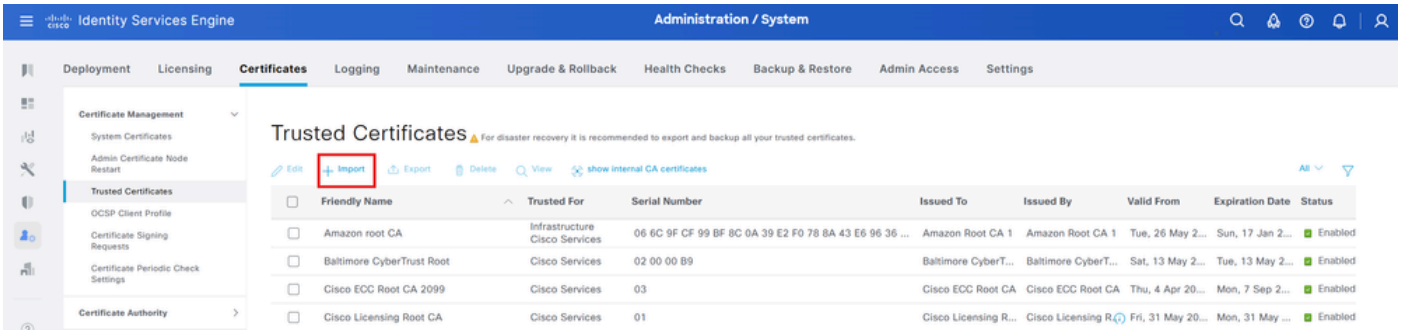
2. Sélectionnez le format Base-64, puis cliquez sur Télécharger le certificat CA.



3. Enregistrez le certificat en tant que CA_Root.cer.

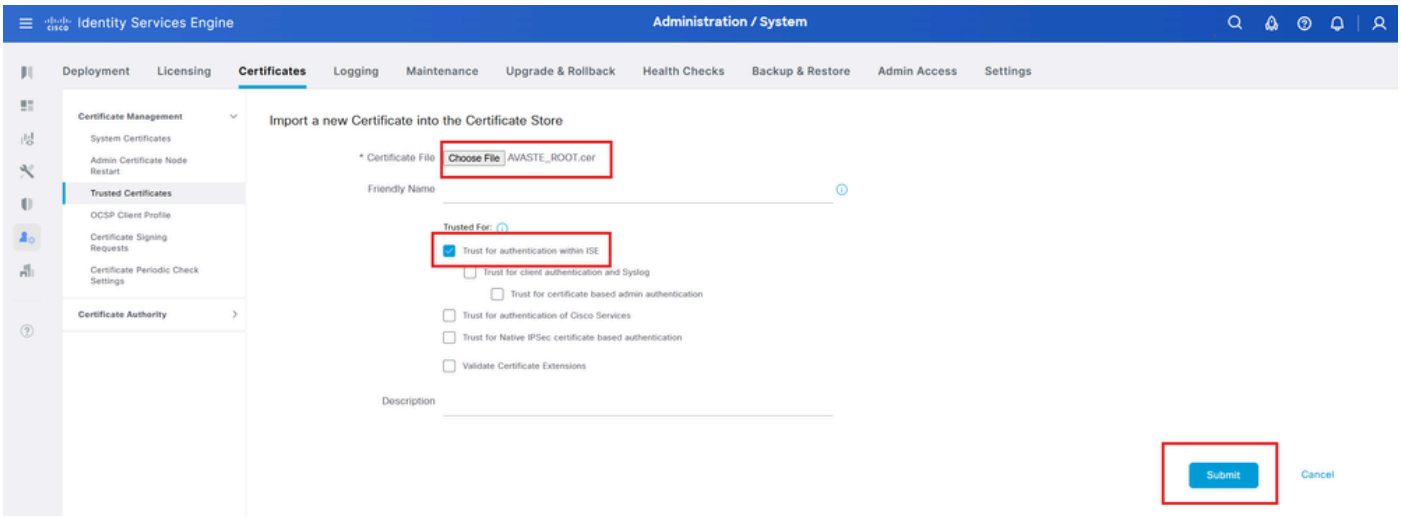
4. Connectez-vous à l'interface utilisateur graphique de Cisco Identity Services Engine (ISE).

5. Sélectionnez Administration > Système > Certificats > Gestion des certificats > Certificats approuvés.



6. Sélectionnez Import > Certificate file et Import the root certificate.

7. Assurez-vous que la case Approuver l'authentification dans ISE est cochée.



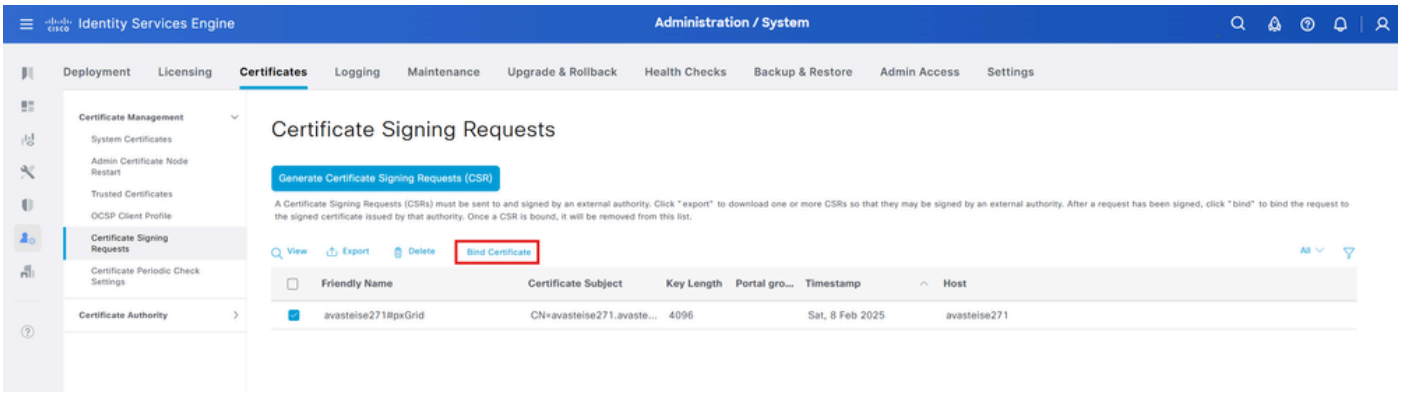
8. Cliquez sur Soumettre.

PARTIE IV - Liaison du certificat ISE à la demande de signature de certificat (CSR)

1. Connectez-vous à l'interface utilisateur graphique de Cisco Identity Services Engine (ISE).

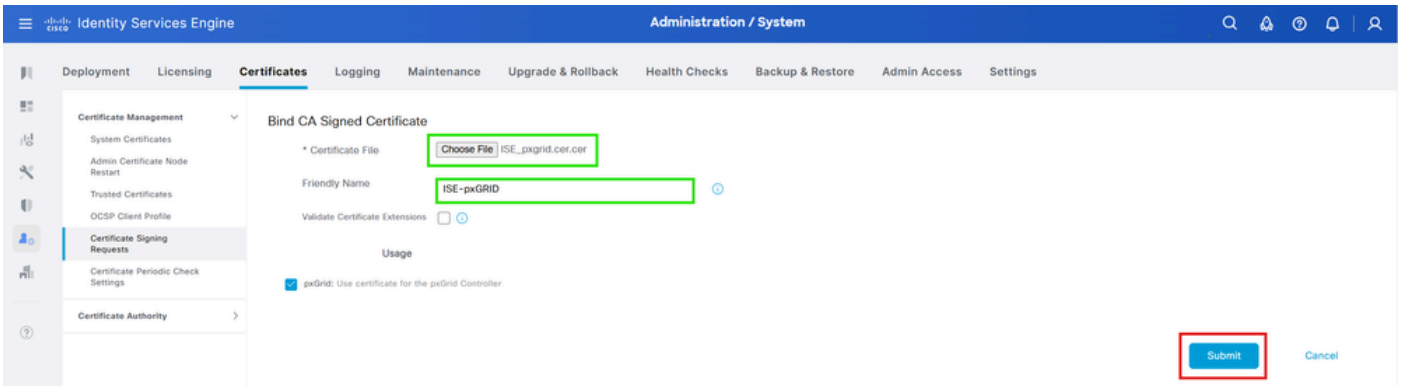
2. Sélectionnez Administration > System > Certificates > Certificate Management > Certificate Signing Requests.

3. Sélectionnez le CSR généré dans la section précédente, puis cliquez sur Bind Certificate.



4. Dans l'écran Lier le certificat signé par l'autorité de certification, sélectionnez le certificat ISE_pxGrid.cer généré précédemment.

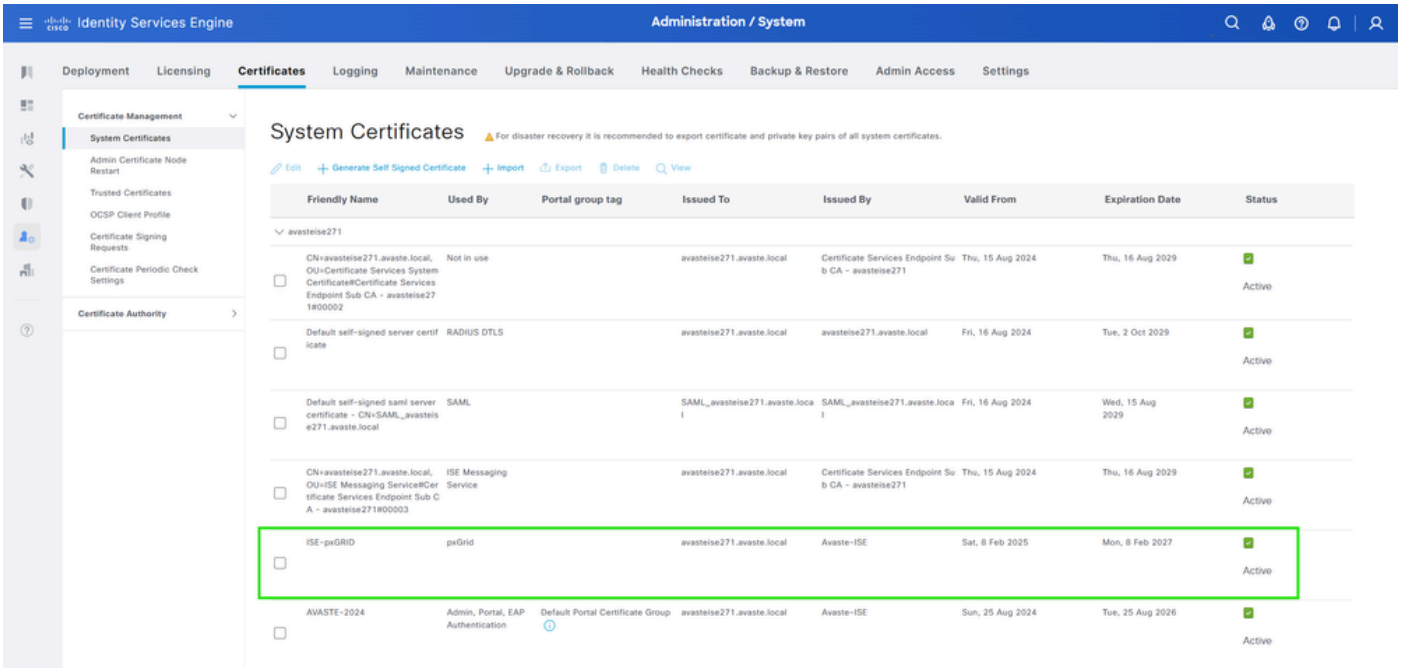
5. Attribuez un nom convivial au certificat, puis cliquez sur Envoyer.



7. Cliquez sur Oui si le système vous demande de remplacer le certificat.

8. Sélectionnez Administration > System > Certificates > System Certificates.

9. Vous pouvez voir le certificat pxGrid créé signé par l'autorité de certification externe dans la liste.

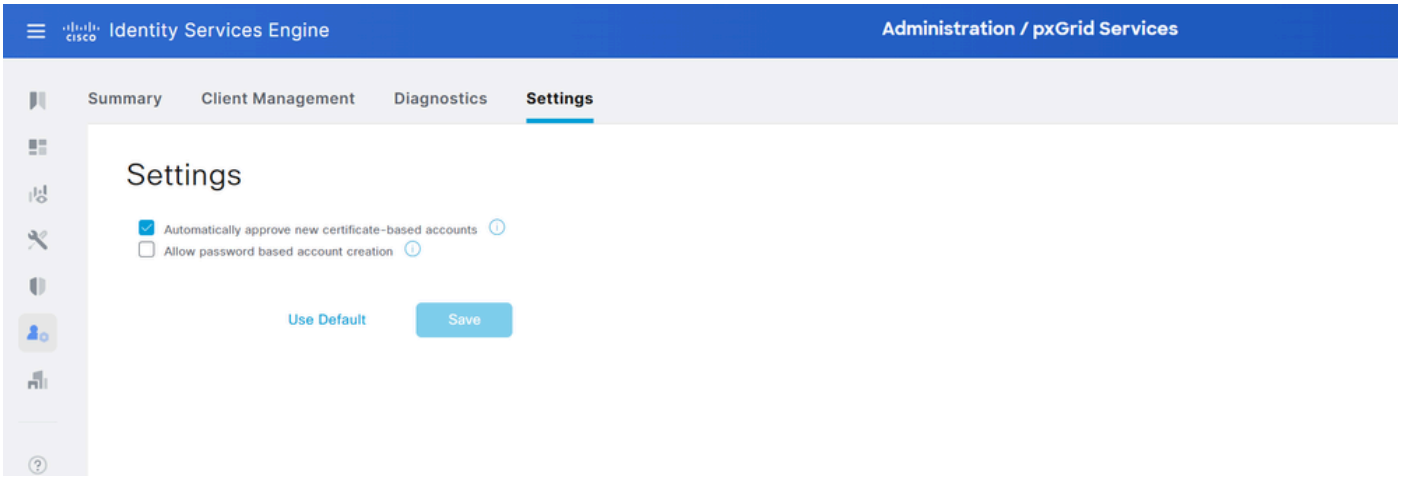


Les certificats sont maintenant déployés, passez à l'intégration.

Intégrer

Avant de procéder à l'intégration, assurez-vous que :

Pour Cisco ISE, sous Administration > pxGrid Services > Settings and Check Approuvez automatiquement les nouveaux comptes basés sur des certificats pour la demande du client à l'approbation automatique et à l'enregistrement.

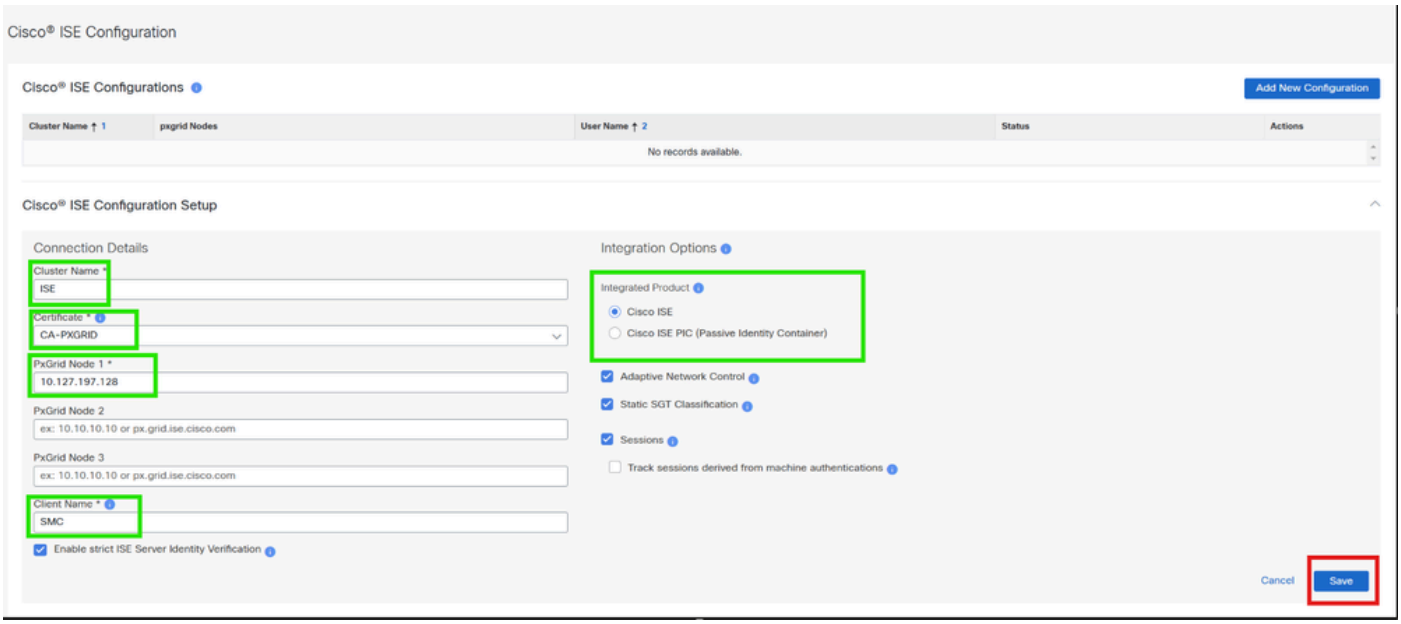


Sur la console de gestion StealthWatch (SMC), pour ouvrir la page de configuration ISE :

1. Sélectionnez Configure > Integrations > Cisco ISE.

2. Dans le coin supérieur droit de la page, cliquez sur Add new configuration.

3. Entrez le nom du cluster, sélectionnez le certificat et le produit d'intégration, pxGrid noeud IP et cliquez sur Enregistrer.



Vérifier

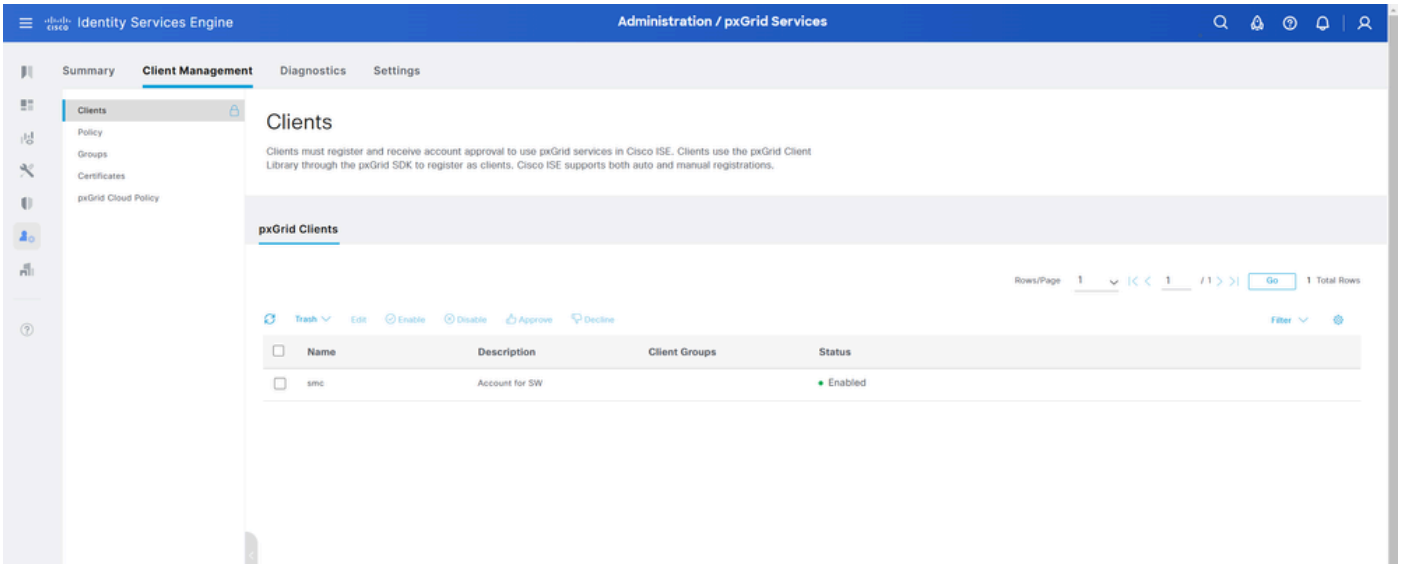
Actualisez la page de configuration ISE sur la console de gestion StealthWatch (SMC).

1. Retournez à la page Configuration ISE dans Web App et actualisez la page.

2. Vérifiez que l'indicateur d'état du noeud situé à côté du champ d'adresse IP applicable est vert, ce qui indique qu'une connexion au cluster ISE ou ISE-PIC a été établie.

Sur Cisco ISE, accédez à Administration > pxGrid Services > Client Management > Clients.

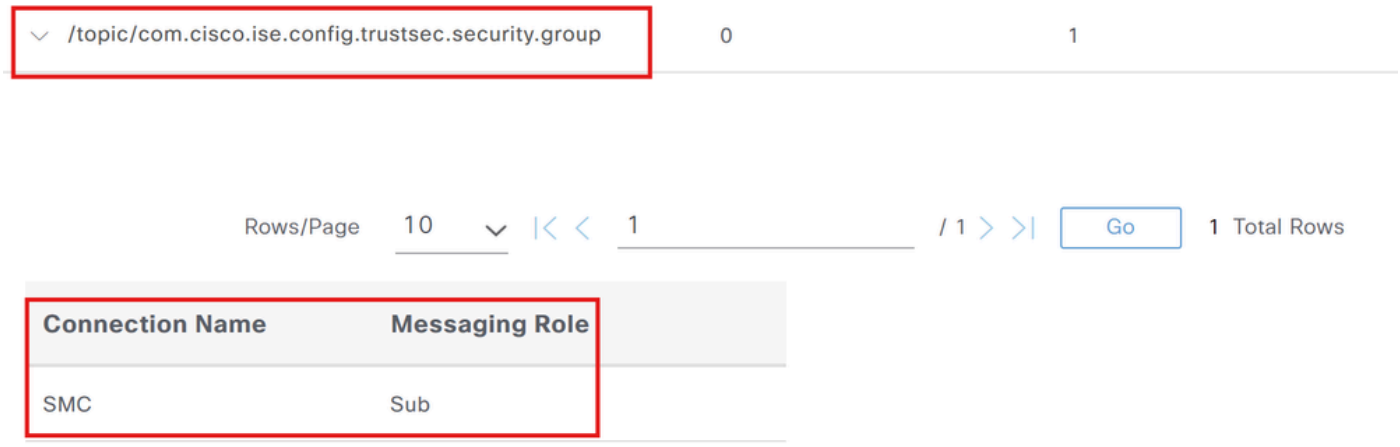
Cela génère le SMC en tant que client pxgrid avec l'état Enabled.



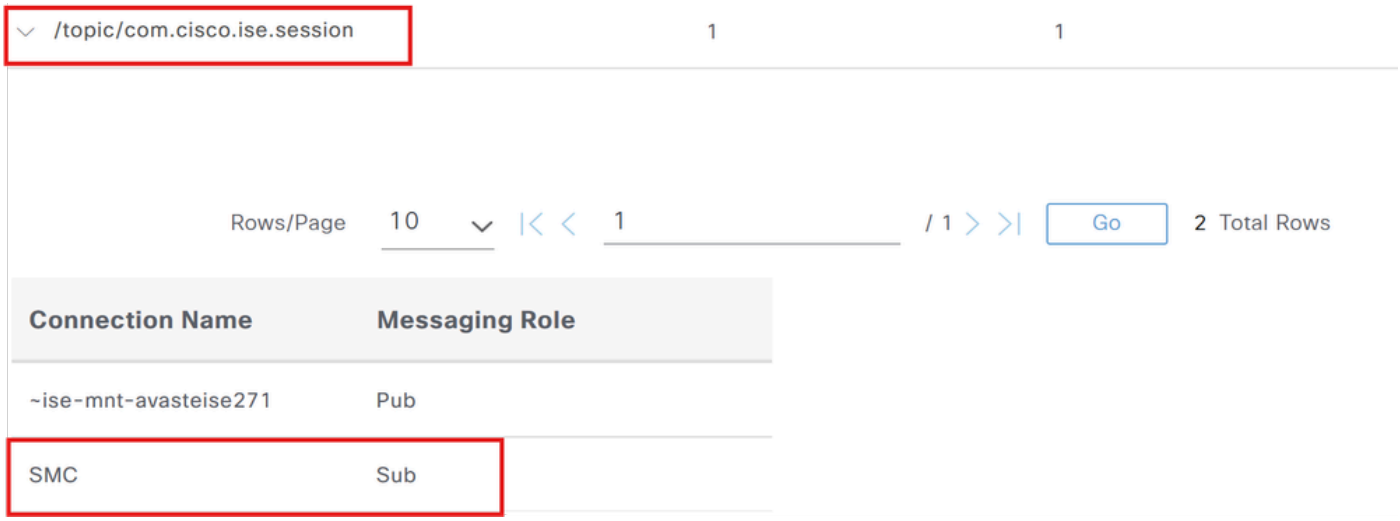
Pour vérifier l'abonnement à la rubrique sur Cisco ISE, accédez à Administration > pxGrid Services > Diagnostics > Websocket > Topics

Un SMC s'abonne à ces rubriques.

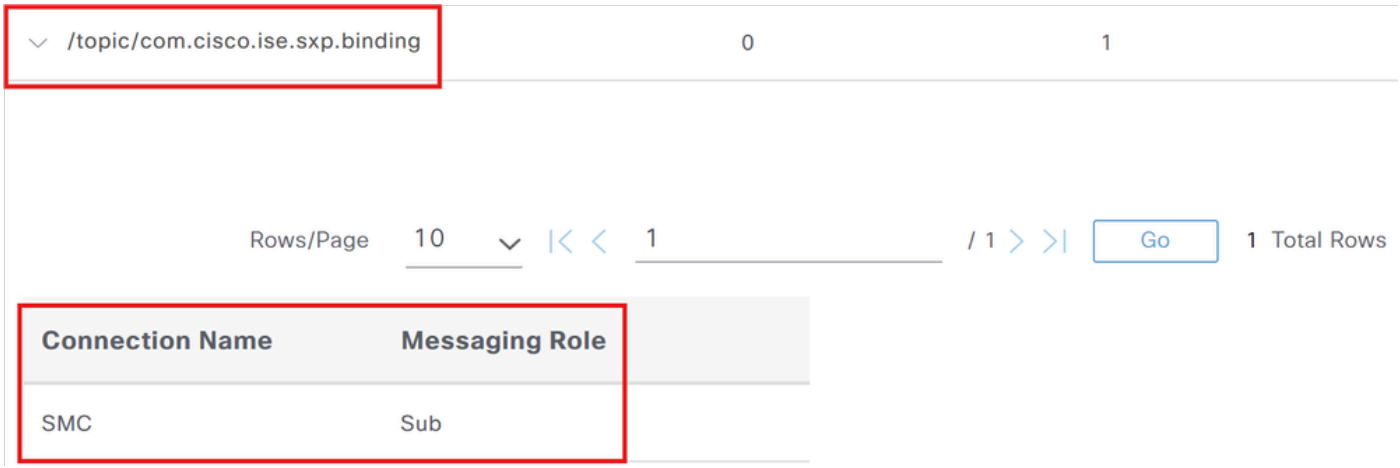
Rubrique Trustsec SGT



Rubrique du répertoire de session ISE



Rubrique Liaisons ISE SXP



Cisco ISE Pxgrid-server.log dans le niveau TRACE.

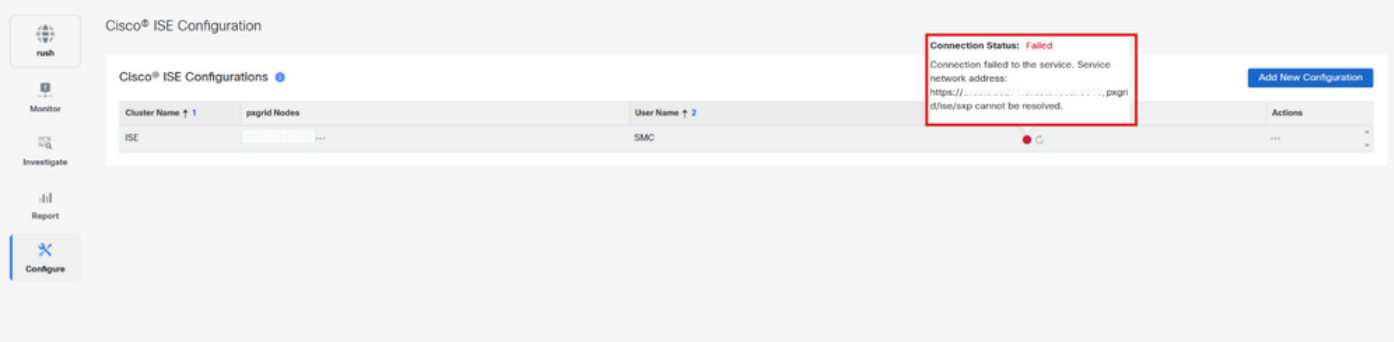
```
2025-02-08 18:07:11,086 TRACE  [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE  [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,110 DEBUG  [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
```

```
2025-02-08 18:07:11,111 DEBUG  [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG  [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG  [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG  [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,112 DEBUG  [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.data.AuthzDaoImpl -:::::
2025-02-08 18:07:11,321 DEBUG  [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut



       ]
2025-02-08 18:07:11,322 DEBUG  [pxgrid-http-pool20][[]] cisco.cpm.pxgridwebapp.config.AuthzEvaluator -:
2025-02-08 18:07:11,322 INFO   [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint



        ] session=[id=8,client=SMC,server=wss://avasteise271.avaste.local:8910/pxgrid/ise/pubsub]
2025-02-08 18:07:11,323 TRACE  [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,323 TRACE  [WsIseClientConnection-1010][[]] cpm.pxgrid.ws.client.WsEndpoint -::::::
2025-02-08 18:07:11,323 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,323 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut



         ]
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut



          ]
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut
2025-02-08 18:07:11,324 TRACE  [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -::::::



           ] from=[id=7,client=~ise-admin-avasteise271,server=wss://avasteise271.avaste.local:8910/pxgr
2025-02-08 18:07:11,324 TRACE  [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -::::::
```

Dépannage

Problème de résolution DNS

Le message d'erreur suivant s'affiche : « Connection Status ; Échec de la connexion au service. Adresse réseau du service : https:isehostnameme.domain.com:891pxgridiisessxpxp ne peut pas être résolu":



Solution

Idéalement, cette erreur doit être corrigée sur le serveur DNS pour les recherches directes et inversées de ce nom de domaine complet ISE. Mais une solution de contournement temporaire peut être ajoutée pour la résolution locale :

1. Connectez-vous à la console de gestion StealthWatch (SMC).

2. Dans le menu principal, sélectionnez Configure > Global > Central Management.

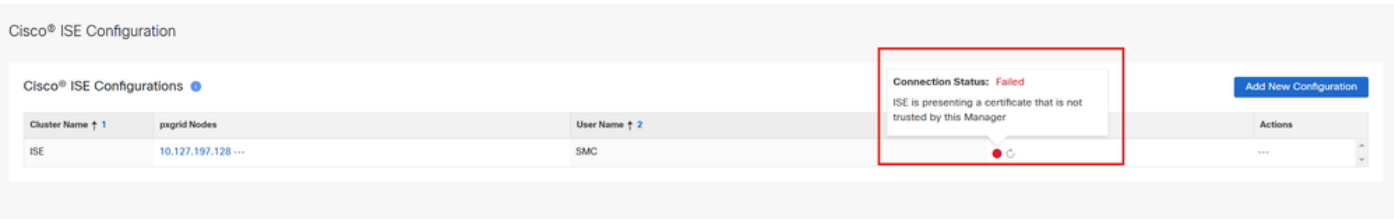
3. Sur la page Inventaire, cliquez sur l'icône (points de suspension) du manager.

4. Choisissez Modifier la configuration du matériel.

5. Onglet Network Services et ajoutez une entrée de résolution locale pour ce FQDN ISE.

Erreur CA inconnue ou certificat approuvé manquant

Cela produit un message d'erreur comme "ISE présente un certificat qui n'est pas approuvé par ce gestionnaire" :



Une référence de journal similaire peut être vue dans le fichier SMCMsvcvisese-client.log. Chemin : catlancopepe/var/logs/containesvcvisese-client.log

```
snasmc1 docker/svc-ise-client[1453]: java.util.concurrent.ExecutionException: javax.net.ssl.SSLExceptio
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.reportGet(Comp
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(Completabl
snasmc1 docker/svc-ise-client[1453]: at org.springframework.web.socket.client.jetty.JettyWebSocketClien
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.FutureTask.run(FutureTask.java:2
```

```
snasmc1 docker/svc-ise-client[1453]: at java.base/java.lang.Thread.run(Thread.java:829)
snasmc1 docker/svc-ise-client[1453]: Caused by: javax.net.ssl.SSLException: org.bouncycastle.tls.TlsFat
snasmc1 docker/svc-ise-client[1453]: at org.bouncycastle.jsse.provider.ProvSSLEngine.unwrap(ProvSSLEngi
snasmc1 docker/svc-ise-client[1453]: at java.base/javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:637)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.unwrap(SslConnection.jav
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.fill(S
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.process(Http
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.receive(Http
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpChannelOverHTTP.receive(HttpC
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpConnectionOverHTTP.onFillable
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:10
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFill
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$2.succeeded(SslConnectio
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:10
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.SelectableChannelEndPoint$1.run(Selectable
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThr
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(Queue
snasmc1 docker/svc-ise-client[1453]: ... 1 more
snasmc1 docker/svc-ise-client[1453]: Suppressed: javax.net.ssl.SSLHandshakeException: org.bouncycastle.
```

Solution

1. Connectez-vous à la console de gestion StealthWatch (SMC).

2. Dans le menu principal, sélectionnez Configure > Global > Central Management.

3. Sur la page Inventaire, cliquez sur l'icône (points de suspension) du manager.

4. Choisissez Modifier la configuration du matériel.

5. Sélectionnez l'onglet Général.

6. Accédez à la section Magasin de confiance et assurez-vous que l'émetteur du certificat Pxgridid de Cisco ISE fait partie du magasin de confiance.

Défauts connus

ID de bogue	Description
ID de bogue Cisco 18119	ISE sélectionne un paquet Hello de serveur ITLS de chiffrement non pris en charge
ID de bogue Cisco 01634	Impossible de mettre en quarantaine les périphériques en utilisant la condition EPS

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.