

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

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Configurer](#)

[Section A : Configuration du certificat Secure Network Analytics \(StealthWatch\)](#)

[Partie I - Génération d'un CSR pour le certificat client Secure Network Analytics pxGrid](#)

[Partie II - Création d'un certificat client Secure Network Analytics pxGrid à l'aide d'une autorité de certification externe](#)

[PARTIE III - Ajout du certificat client Secure Network Analytics pxGrid au gestionnaire](#)

[PARTIE IV - Importation du certificat racine de l'autorité de certification dans le magasin de gestion de la confidentialité](#)

[Section B : Configuration du certificat Cisco Identity Services Engine3.3](#)

[PARTIE I - Génération d'un certificat pxGrid de serveur ISE](#)

[PARTIE II - Création d'un certificat pxGrid de serveur ISE à l'aide d'une autorité de certification externe](#)

[PARTIE III - Importation du certificat racine de l'autorité de certification dans l'ISE Trust Store](#)

[PARTIE IV - Liaison du certificat ISE à la demande de signature de certificat \(CSR\)](#)

[Intégrer](#)

[Vérifier](#)

[Dépannage](#)

[Problème de résolution DNS](#)

[Solution](#)

[Erreur CA inconnue ou certificat approuvé manquant](#)

[Solution](#)

[Défauts connus](#)

---

## 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 Configurer > Global > Central Management.



Dashboard



Monitor



Investigate



Report



Configure

## Configure X

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.

## Microsoft Active Directory Certificate Services – Avast-ISE

### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

#### 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.

Additional SSL/TLS Client Identities Add New

Add SSL/TLS Client Identity Download CSR

Friendly Name \* CA-PXGRID

Certificate File \* certnew (26).cer Select file...

Chain Certificate File \* AVASTE\_ROOT.cer Select file...

Cancel Add Client Identity

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.

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**[Request a certificate](#)[View the status of a pending certificate request](#)[Download a CA certificate, certificate chain, or CRL](#)

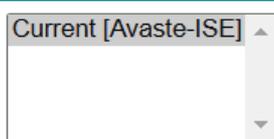
2. Sélectionnez le format Base-64, puis cliquez sur Télécharger le certificat CA.

3. Enregistrez le certificat en tant que CA\_Root.cer.

**Microsoft Active Directory Certificate Services -- Avaste-ISE****Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

**CA certificate:****Encoding method:** DER Base 64[Install CA certificate](#)[Download CA certificate](#)[Download CA certificate chain](#)[Download latest base CRL](#)[Download latest delta CRL](#)

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

5. Dans le menu principal, sélectionnez Configurer > 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.

Central Management Inventory Data Store Update Manager App Manager Smart Licensing Database

Inventory / Appliance Configuration  
Appliance Configuration - Manager  
smrc (10.106.127.50) / Last Updated: 2/8/2025, 5:30:58 PM by admin

Appliance Network Services **General**

Enable FIPS Encryption Libraries  
 Enable Common Criteria Encryption Libraries

**SMTP Configuration**

SMTP Server  
Port  
From Email  
User Name  
Password  
Encryption Type  
 SMTPS  STARTTLS  Un-Encrypted

**Backup Configuration Encryption**

Enable Encryption  
Backup Configuration Password  
Confirm Password

**External Services**

Enable Cisco Security Cloud Control  
 Enable Customer Success Metrics  
 Enable Threat Feed  
Feed Confidence Level: 7

**DoDIN Notifications**

Enable  
To Email \*

**Trust Store** Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
yy1nde2owmzmdu5indc2m2hizmu... cert	Secure Network Analytics	Secure Network Analytics	2024-06-20 20:17:15	2029-06-21 20:17:15	403c0116b1af4d3b71e9060afdba...	4096	Delete
fc751new.www.cisco.com	Secure Network Analytics	Secure Network Analytics	2024-06-23 12:14:09	2029-06-24 12:14:09	14e60739401a8e204c7f03b12279...	4096	Delete
AWS	Amazon	Amazon	2015-05-26 05:30:00	2038-01-17 05:30:00	66c9cf996f8c0a39e2f0788a43e69...	2048	Delete

5 items per page 1 - 3 of 3 items Page 1 of 1

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.

**Add Certification Authority Certificate**

Friendly Name \*  
AVASTEROOTCA

Certificate File \*  
AVASTE\_ROOT.cer

Select file...

Cancel Add Certificate

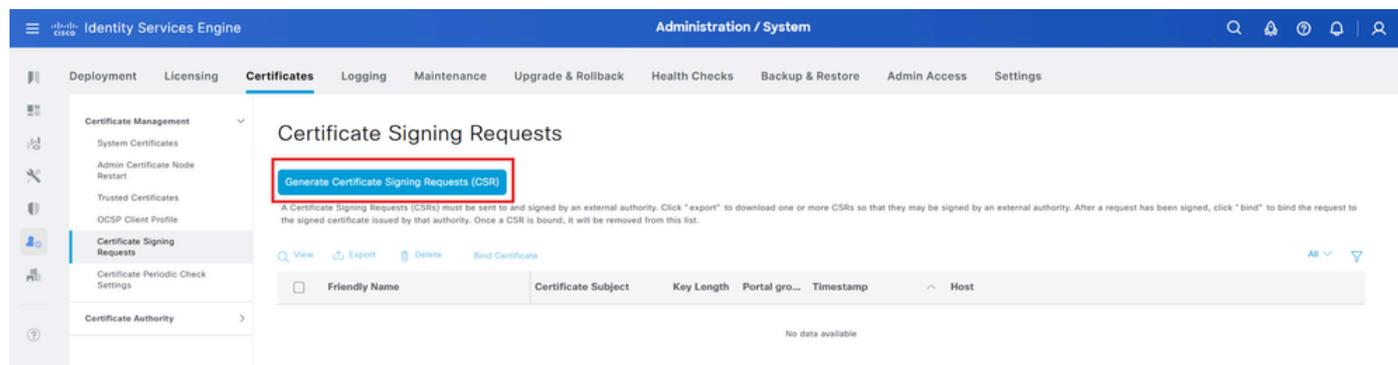
13. Cliquez sur Apply Settings pour enregistrer les modifications.

## 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.

**Usage**  
Certificate(s) will be used for

Allow Wildcard Certificates

**Node(s)**  
Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> avasteise271	avasteise271#pxGrid

**Subject**

Common Name (CN)  
SFQDNS

Organizational Unit (OU)  
AAA

Organization (O)  
Cisco

City (L)  
Bangalore

State (ST)  
KA

Country (C)  
IN

Subject Alternative Name (SAN)

DNS Name	avasteise271.avaste.local	-	+
IP Address	10.127.197.128	-	+

\* Key type  
RSA

\* Key Length  
4096

\* Digest to Sign With  
SHA-384

Certificate Policies

8. Cliquez sur Exporter et enregistrez le fichier localement.

✕

**Successfully generated CSR(s)** 

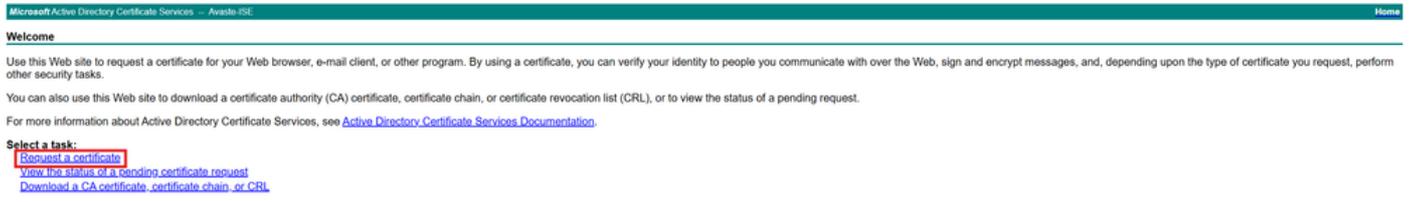
**Certificate Signing request(s) generated:**

**avasteise271#pxGrid**

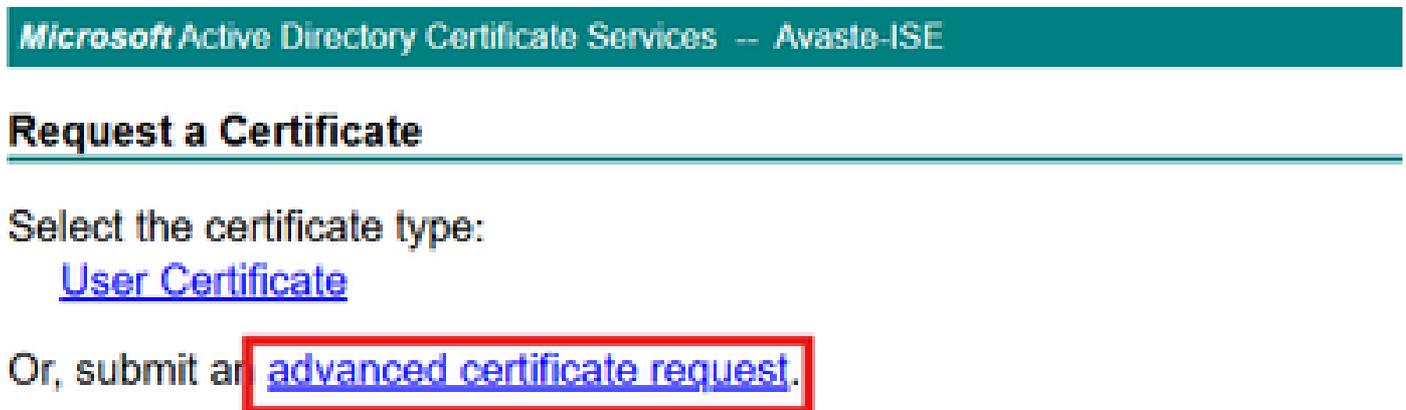
**Click Export to download CSR(s) or OK to return to list of CSR(s) screen**

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

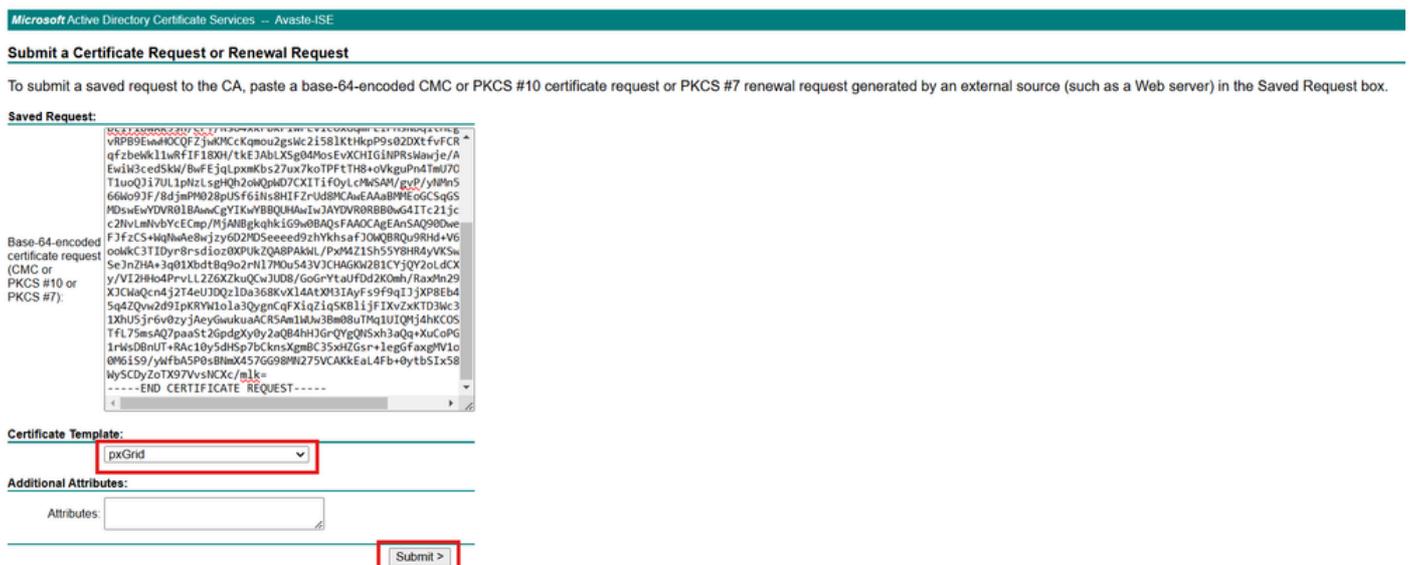
1. Accédez au service de certificats MS Active Directory, <https://server/certsrv/>, où server is IP or DNS of your MS Server.
2. Cliquez sur Demander un certificat.



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.

## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

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.

Microsoft Active Directory Certificate Services -- Avaste-ISE Home

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

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

## Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

### CA certificate:

Current [Avaste-ISE] ▲

▼

### Encoding method:

DER

Base 64

[Install CA certificate](#)

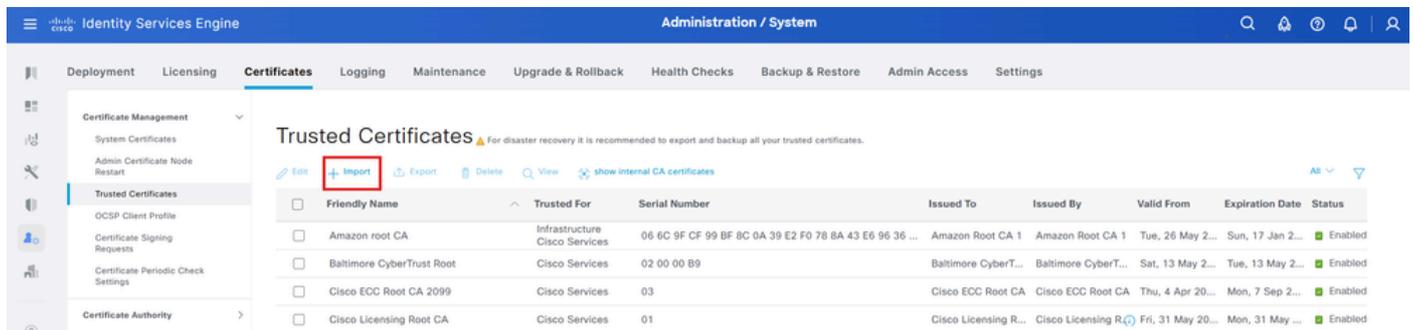
[Download CA certificate](#)

[Download CA certificate chain](#)

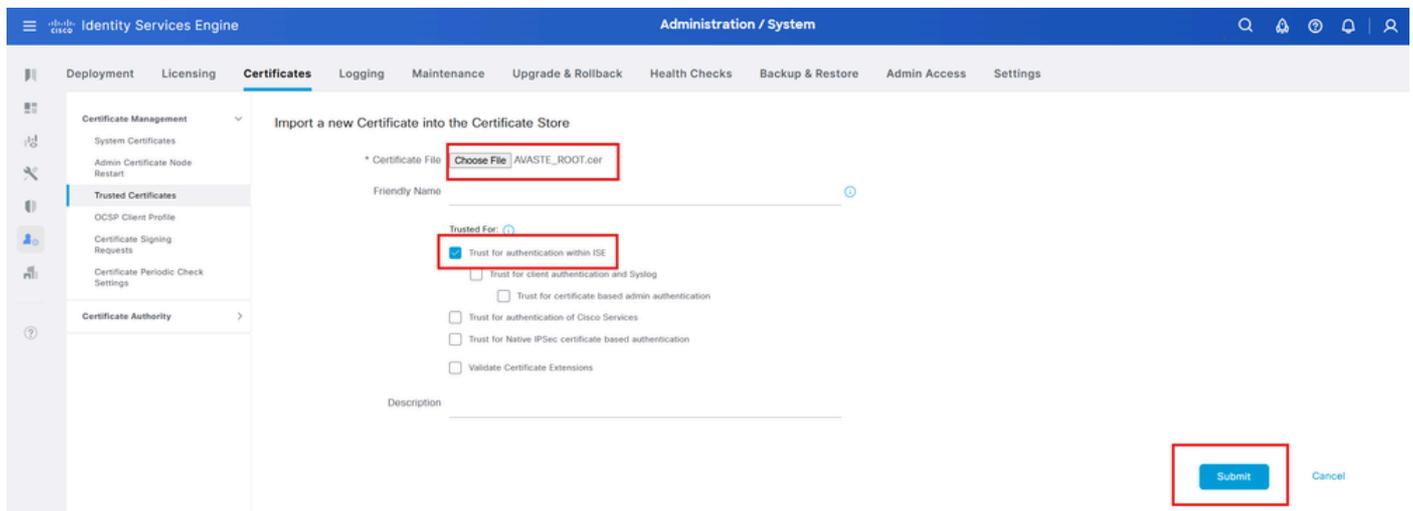
[Download latest base CRL](#)

[Download latest delta CRL](#)

- Enregistrez le certificat en tant que CA\_Root.cer.
- Connectez-vous à l'interface utilisateur graphique de Cisco Identity Services Engine (ISE).
- Sélectionnez Administration > Système > Certificats > Gestion des certificats > Certificats approuvés.



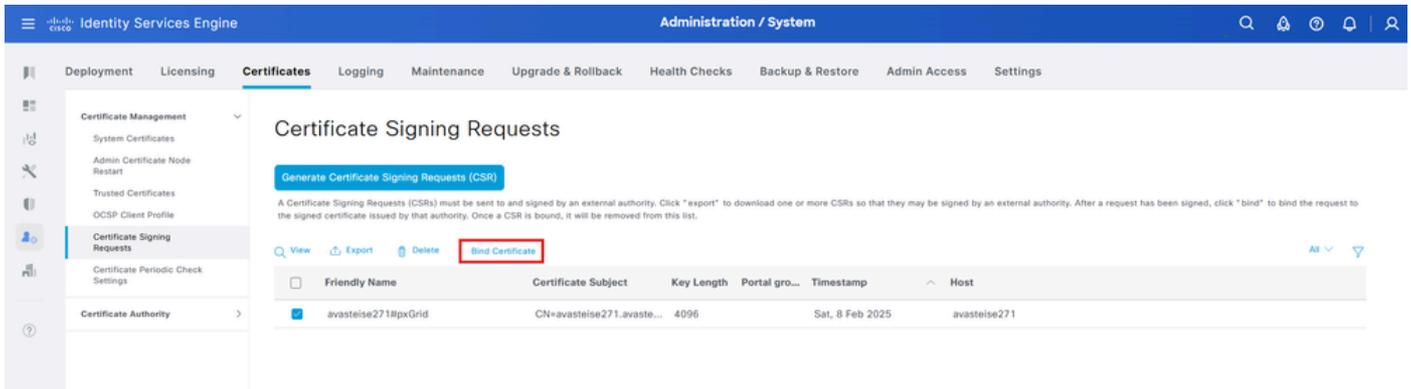
- Sélectionnez Import > Certificate file et Import the root certificate.
- Assurez-vous que la case Approuver l'authentification dans ISE est cochée.



- Cliquez sur Soumettre.

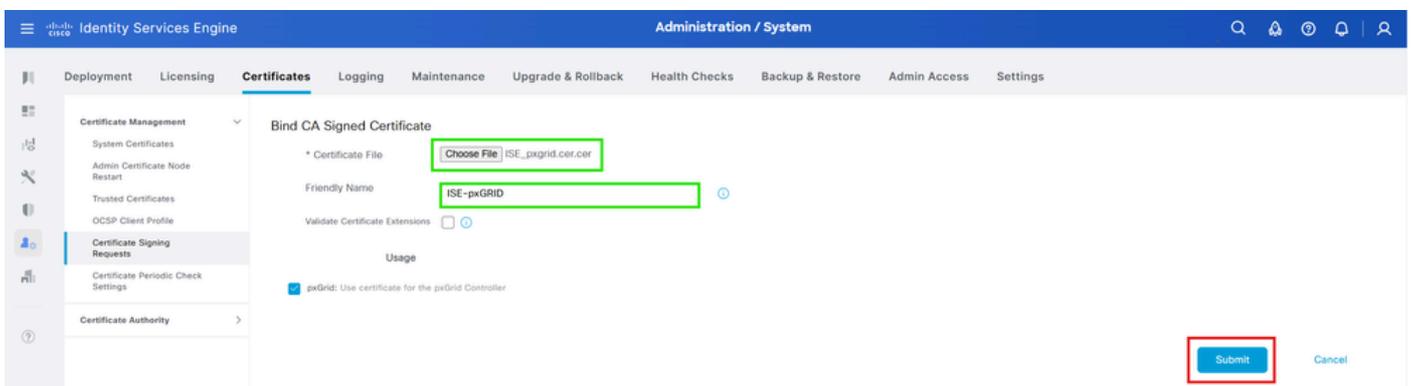
#### PARTIE IV - Liaison du certificat ISE à la demande de signature de certificat (CSR)

- Connectez-vous à l'interface utilisateur graphique de Cisco Identity Services Engine (ISE).
- Sélectionnez Administration > System > Certificates > Certificate Management > Certificate Signing Requests.
- 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.

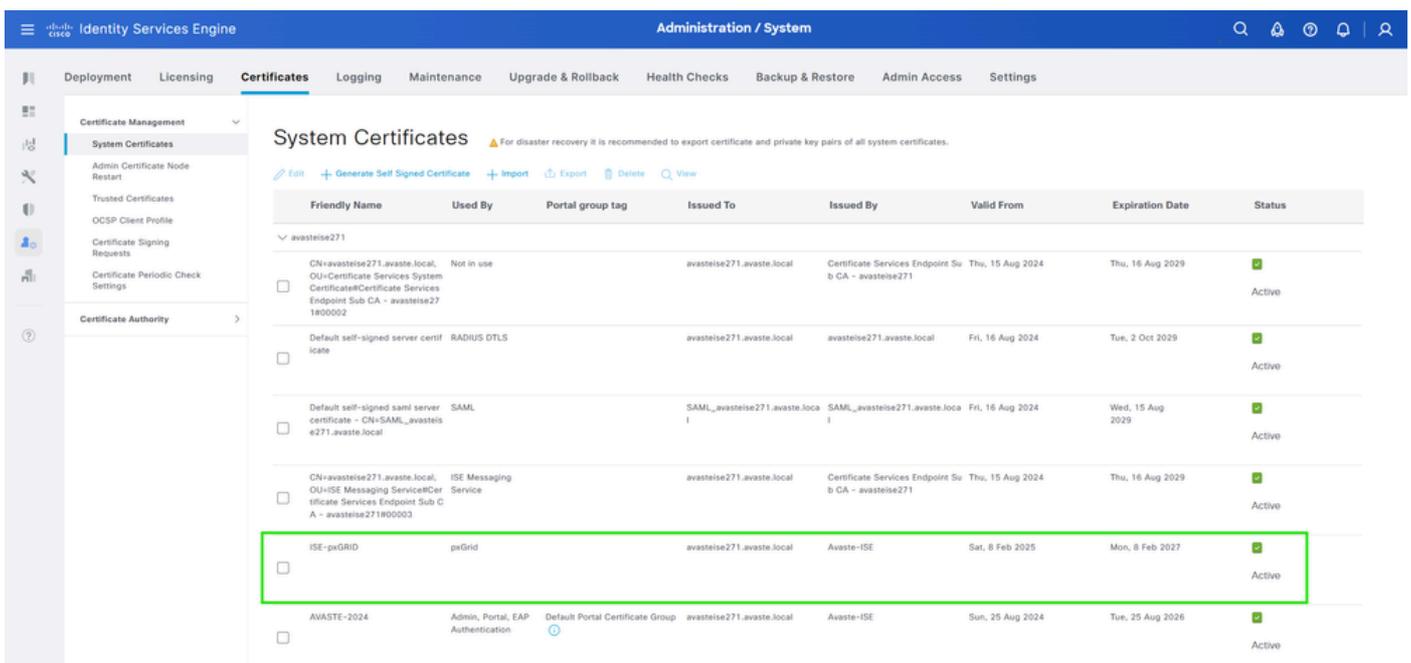
5. Attribuez un nom convivial au certificat, puis cliquez sur Envoyer.



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.

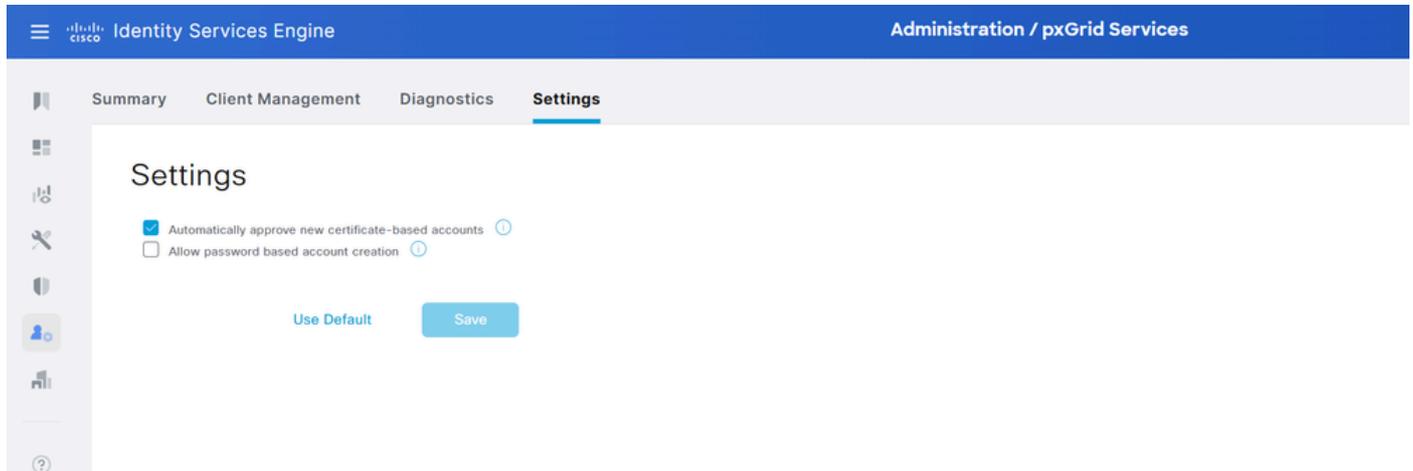


Les certificats sont maintenant déployés, passez à l'intégration.

## Intégrer

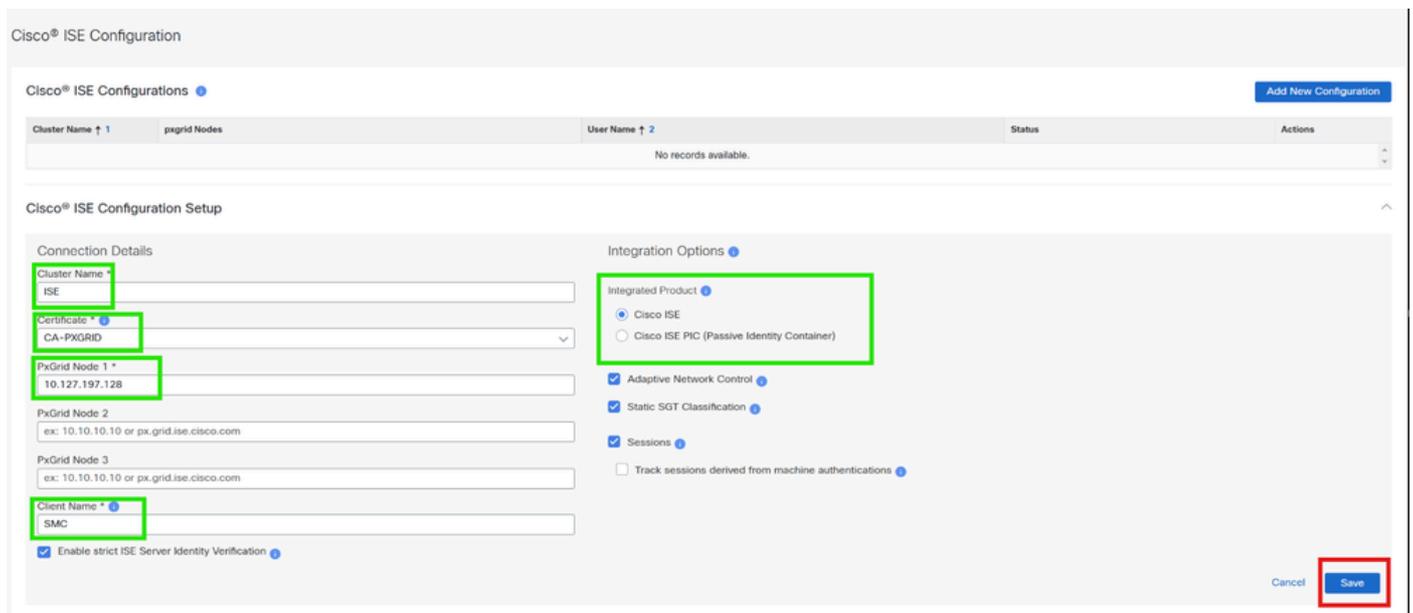
Avant de procéder à l'intégration, assurez-vous que :

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.

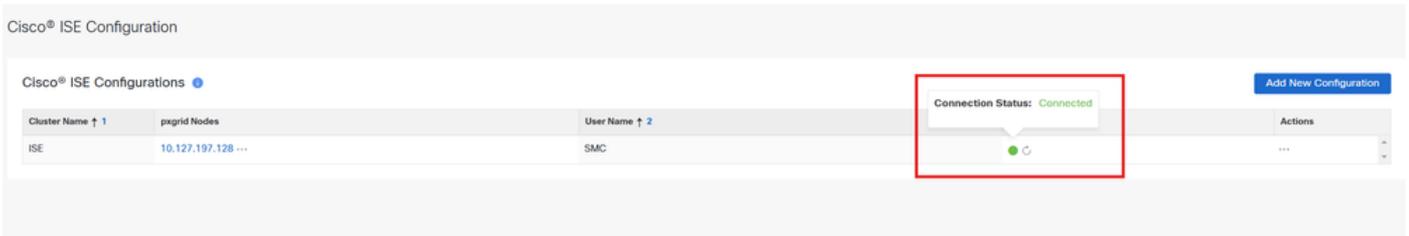


## Vérifier

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

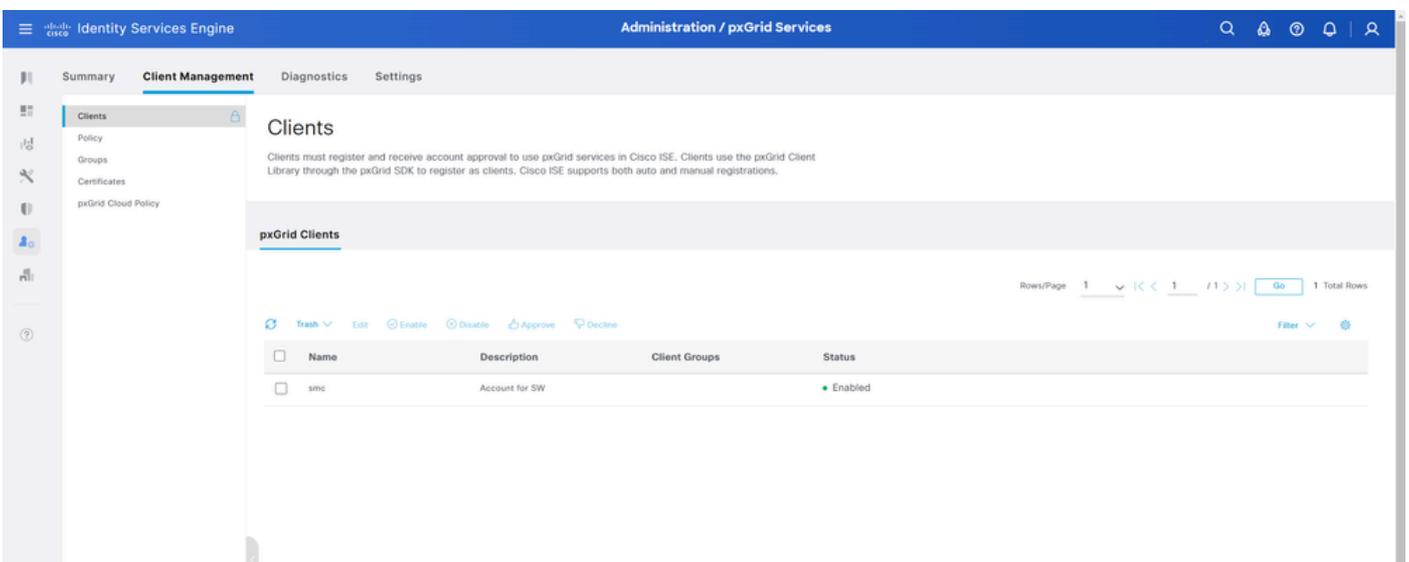
1. Retournez à la page Configuration ISE dans Web App et actualisez la page.

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

▼ /topic/com.cisco.ise.config.trustsec.security.group	0	1
---	---	---

Rows/Page 10 |<< 1 / 1 >> |  1 Total Rows

Connection Name	Messaging Role
SMC	Sub

### Rubrique du répertoire de session ISE

▼ /topic/com.cisco.ise.session	1	1
--------------------------------	---	---

Rows/Page 10 |<< 1 / 1 >> |  2 Total Rows

Connection Name	Messaging Role
-ise-mnt-avasteise271	Pub
SMC	Sub

### Rubrique Liaisons ISE SXP

▼ /topic/com.cisco.ise.sxp.binding	0	1
------------------------------------	---	---

Rows/Page 10 |<< 1 / 1 >> |  1 Total Rows

Connection Name	Messaging Role
SMC	Sub

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

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

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

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

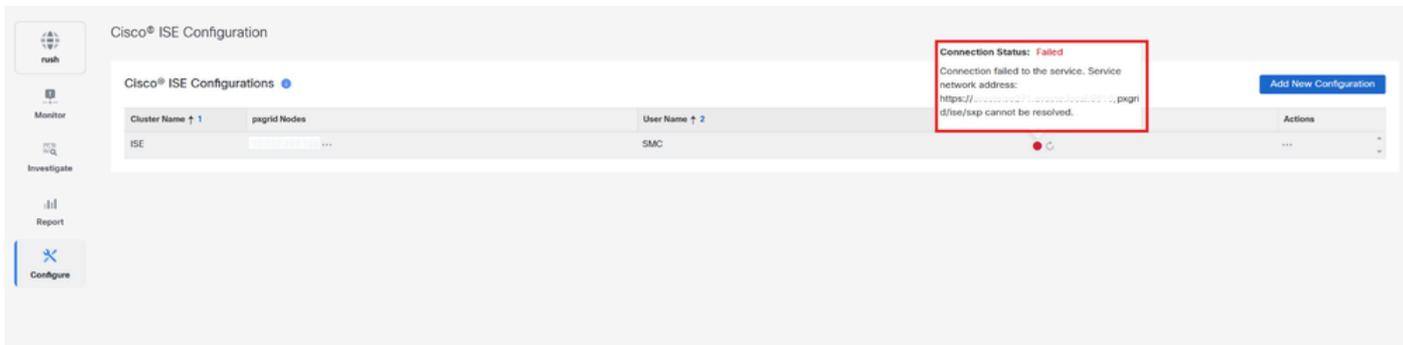
] from=[id=7,client=~ise-admin-avasteise271,server=wss://avasteise271.avaste.local:8910/pxgr
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

```

## 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://isehostnameeme.domain.com:8910/pxgrid/ise/pubsub> 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 Configurer > 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 SMCMsvcvise-client.log. Chemin :  
 catlancopepe/var/logs/containesvcvise-client.log

```
snasmc1 docker/svc-ise-client[1453]: java.util.concurrent.ExecutionException: javax.net.ssl.SSLException
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.reportGet(CompletableFuture.java:395)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(CompletableFuture.java:2065)
snasmc1 docker/svc-ise-client[1453]: at org.springframework.web.socket.client.jetty.JettyWebSocketClient.doHandshake(JettyWebSocketClient.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.FutureTask.run(FutureTask.java:284)
```

```

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.TlsFatalAlert
snasmc1 docker/svc-ise-client[1453]: at org.bouncycastle.jsse.provider.ProvSSLEngine.unwrap(ProvSSLEngine.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/javax.net.ssl.SSLContext.unwrap(SSLContext.java:637)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.unwrap(SslConnection.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.fill(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.process(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.receive(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpChannelOverHTTP.receive(HttpChannelOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpConnectionOverHTTP.onFillable(HttpConnectionOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(AbstractConnection$ReadCallback.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFillable(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.SelectableChannelEndPoint$1.run(SelectableChannelEndPoint$1.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPool$Runner.java:100)
snasmc1 docker/svc-ise-client[1453]: ... 1 more
snasmc1 docker/svc-ise-client[1453]: Suppressed: javax.net.ssl.SSLHandshakeException: org.bouncycastle.tls.TlsFatalAlert

```

## Solution

1. Connectez-vous à la console de gestion StealthWatch (SMC).
2. Dans le menu principal, sélectionnez Configurer > 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
<a href="#">ID de bogue Cisco 18119</a>	ISE sélectionne un paquet Hello de serveur ITLS de chiffrement non pris en charge
<a href="#">ID de bogue Cisco 01634</a>	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.