

# Intégration d'ISE 3.3 avec WSA à l'aide d'une CA externe

## Table des matières

---

### [Introduction](#)

### [Conditions préalables](#)

#### [Exigences](#)

#### [Composants utilisés](#)

### [Configurer](#)

#### [Section A : Configuration du certificat Cisco Identity Services Engine 3.3](#)

##### [Étape 1 : Générer un certificat ISE Server pxGrid](#)

##### [Étape 2 : Créer un certificat pxGrid de serveur ISE à l'aide d'une autorité de certification externe](#)

##### [Étape 3 : Importer le certificat racine de l'autorité de certification dans l'ISE Trust Store](#)

##### [Étape 4 : Liaison du certificat ISE à la demande de signature de certificat \(CSR\).](#)

#### [Section B : Ajout du certificat racine CA au magasin de certificats de confiance WSA](#)

### [Intégration](#)

#### [Section A : Activez WSA pour l'intégration ISE et générez un CSR pour le certificat client WSA.](#)

#### [Section B : Signature d'un CSR client WSA à l'aide d'une CA externe](#)

#### [Section C : Liaison du certificat client WSA à la demande de signature de certificat \(CSR\) et intégration.](#)

### [Vérifier](#)

### [Dépannage](#)

#### [Problème](#)

#### [Solution](#)

### [Défauts connus](#)

---

## Introduction

Ce document décrit les procédures d'intégration d'ISE 3.3 avec Cisco Secure Web Appliance (WSA) à l'aide de connexions pxGrid.

## Conditions préalables

### Exigences

Cisco recommande des connaissances sur les sujets suivants :

- Plateforme de services d'identité
- Appareil Web sécurisé Cisco (WSA)
- Platform Exchange Grid (pxGrid)
- 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
- Appliance Web sécurisé Cisco version 15.2.0-116
- 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.

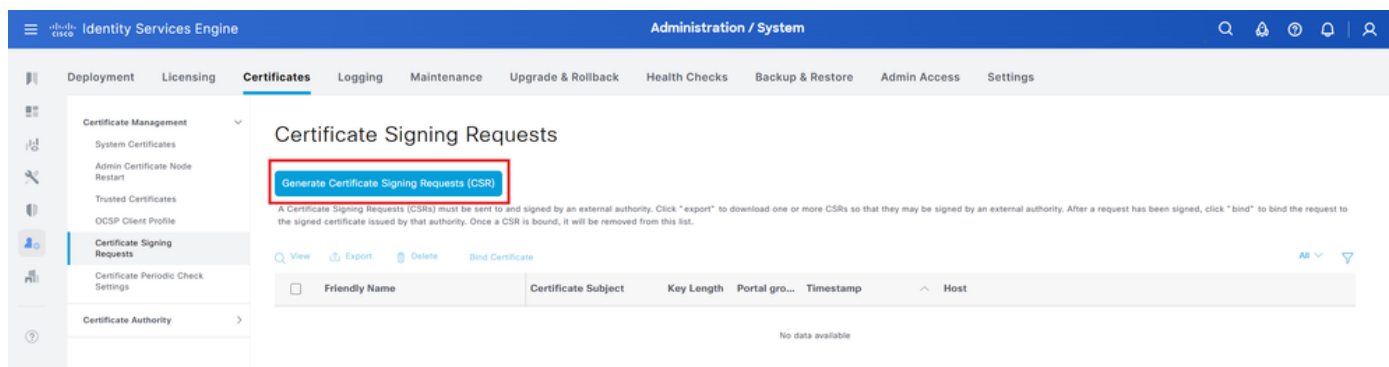
## Configurer

### Section A : Configuration du certificat Cisco Identity Services Engine 3.3

Étape 1 : Générer un certificat pxGrid ISEServer

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. SelectPxGridin le(s) certificat(s) est utilisé pour le champ.
5. Sélectionnez le noeud ISE pour lequel le certificat est généré.
6. Remplissez les détails des autres certificats si nécessaire.
7. Cliquez sur Générer.

## Usage

Certificate(s) will be used for

pxGrid

Allow Wildcard Certificates

☐

## Node(s)

Generate CSR's for these Nodes:

Node

CSR Friendly Name



ise33

ise33#pxGrid

## Subject

Common Name (CN)

\$FQDN\$



Organizational Unit (OU)

AAA



Organization (O)

Cisco



City (L)

Bangalore

State (ST)

KA

Country (C)

IN

Subject Alternative Name (SAN)



DNS Name



ise33.lab.local



IP Address



10.127.197.128



\* Key type

RSA



\* Key Length

4096



\* Digest to Sign With

SHA-384



Certificate Policies

Le modèle de certificat pxGrid utilisé nécessite à la fois l'authentification du client et l'authentification du serveur dans le champ Enhanced Key Usage.

6. Téléchargez le certificat généré au format Base-64 et enregistrez-le sous ISE\_pxGrid.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](#)

Étape 3 : Importer le 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 -- Avast-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](#)

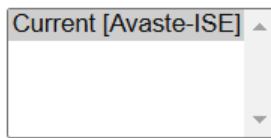
2. Sélectionnez le format Base-64, puis cliquez sur Télécharger le certificat CA.

## 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:



Encoding method:

☐ DER

☒ Base 64

[Install CA certificate](#)

[Download CA certificate](#)

[Download CA certificate chain](#)

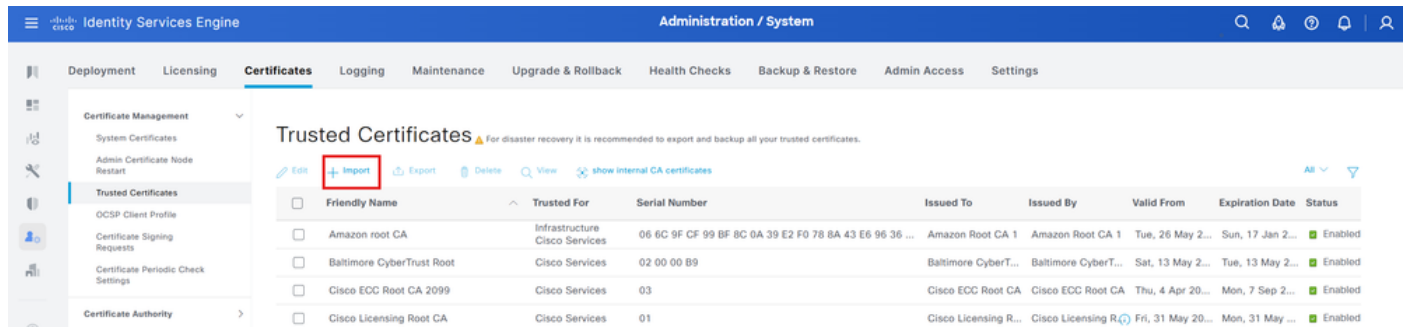
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Enregistrez le certificat sous 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.



The screenshot shows the 'Trusted Certificates' page in the Cisco ISE Administration console. The page title is 'Trusted Certificates' with a warning icon and text: 'For disaster recovery it is recommended to export and backup all your trusted certificates.' Below the title are action buttons: 'Edit', 'Import' (highlighted with a red box), 'Export', 'Delete', 'View', and 'show internal CA certificates'. A table lists the trusted certificates with columns: 'Friendly Name', 'Trusted For', 'Serial Number', 'Issued To', 'Issued By', 'Valid From', 'Expiration Date', and 'Status'.

| Friendly Name                                      | Trusted For                   | Serial Number                                          | Issued To            | Issued By            | Valid From        | Expiration Date  | Status  |
|----------------------------------------------------|-------------------------------|--------------------------------------------------------|----------------------|----------------------|-------------------|------------------|---------|
| <input type="checkbox"/> Amazon root CA            | Infrastructure Cisco Services | 06 6C 9F 9F 99 BF 8C 0A 39 E2 F0 78 8A 43 E6 96 36 ... | Amazon Root CA 1     | Amazon Root CA 1     | Tue, 26 May 2...  | Sun, 17 Jan 2... | Enabled |
| <input type="checkbox"/> Baltimore CyberTrust Root | Cisco Services                | 02 00 00 B9                                            | Baltimore CyberT...  | Baltimore CyberT...  | Sat, 13 May 2...  | Tue, 13 May 2... | Enabled |
| <input type="checkbox"/> Cisco ECC Root CA 2099    | Cisco Services                | 03                                                     | Cisco ECC Root CA    | Cisco ECC Root CA    | Thu, 4 Apr 20...  | Mon, 7 Sep 2...  | Enabled |
| <input type="checkbox"/> Cisco Licensing Root CA   | Cisco Services                | 01                                                     | Cisco Licensing R... | Cisco Licensing R... | Fri, 31 May 20... | Mon, 31 May ...  | Enabled |

6. Sélectionnez Importer > fichier de certificat et Importer le certificat racine.

7. Assurez-vous que la case Trust for authentication within ISE est cochée.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Settings Certificate Authority

Import a new Certificate into the Certificate Store

\* Certificate File **Choose File** AWASTE\_ROOT.cer

Friendly Name

Trusted For:

☒ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

☐ Trust for authentication of Cisco Services

☐ Trust for Native IPsec certificate based authentication

☐ Validate Certificate Extensions

Description

**Submit** Cancel

8. Cliquez sur Soumettre.

Étape 4 : 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 > Système > Certificats > Gestion des certificats > Demandes de signature de certificat.

3. Sélectionnez le CSR généré dans la section précédente, puis cliquez sur Lier le certificat.

Identity Services Engine Administration / System Evaluation Mode 83 Days

Bookmarks Dashboard Context Visibility Operations Policy **Administration** Work Centers Interactive Features

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile **Certificate Signing Requests** Certificate Periodic Check Settings Certificate Authority

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete **Bind Certificate**

| <input type="checkbox"/>            | Friendly Name | Certificate Subject       | Key Length | Portal gro... | Timestamp        | Host  |
|-------------------------------------|---------------|---------------------------|------------|---------------|------------------|-------|
| <input checked="" type="checkbox"/> | ise33pxGrid   | CN=ise33.lab.local,OU=... | 4096       |               | Wed, 19 Mar 2025 | ise33 |

4. Dans le formulaire 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.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Settings Certificate Authority

Bind CA Signed Certificate

\* Certificate File **Choose File** ISE\_pxgrid.cer.cer

Friendly Name **ISE-pxGRID**

Validate Certificate Extensions ☐

Usage

☒ pxGrid: Use certificate for the pxGrid Controller

**Submit** Cancel

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

8. Sélectionnez Administration > Système > Certificats > Certificats système.

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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Features. The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below this, there are tabs for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', 'Delete', and 'View'. A table lists the system certificates:

| Friendly Name                                                         | Used By                                        | Portal group tag                 | Issued To            | Issued By                                    | Valid From       | Expiration Date  | Status |
|-----------------------------------------------------------------------|------------------------------------------------|----------------------------------|----------------------|----------------------------------------------|------------------|------------------|--------|
| Default self-signed server certificate                                | Admin, EAP Authentication, Portal, RADIUS DTLS | Default Portal Certificate Group | ise33.lab.local      | ise33.lab.local                              | Wed, 12 Mar 2025 | Fri, 12 Mar 2027 | Active |
| Default self-signed saml server certificate - CN=SAML_ise33.lab.local | SAML                                           |                                  | SAML_ise33.lab.local | SAML_ise33.lab.local                         | Wed, 12 Mar 2025 | Mon, 11 Mar 2030 | Active |
| CN=ise33.lab.local, OU=ISE Messaging Service                          | ISE Messaging Service                          |                                  | ise33.lab.local      | Certificate Services Endpoint Sub CA - ise33 | Wed, 12 Mar 2025 | Wed, 13 Mar 2030 | Active |
| ISE-pxGRID                                                            | pxGrid                                         |                                  | ise33.lab.local      | Avaste-ISE                                   | Wed, 19 Mar 2025 | Fri, 19 Mar 2027 | Active |

## Section B : Ajout du certificat racine CA au magasin de certificats de confiance WSA

Ajouter un certificat racine CA au magasin de confiance WSA :

1. Connectez-vous à l'interface utilisateur graphique du dispositif de sécurité Web (WSA).
2. Accédez à Réseau > Gestion des certificats > Gérer les certificats racines de confiance.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

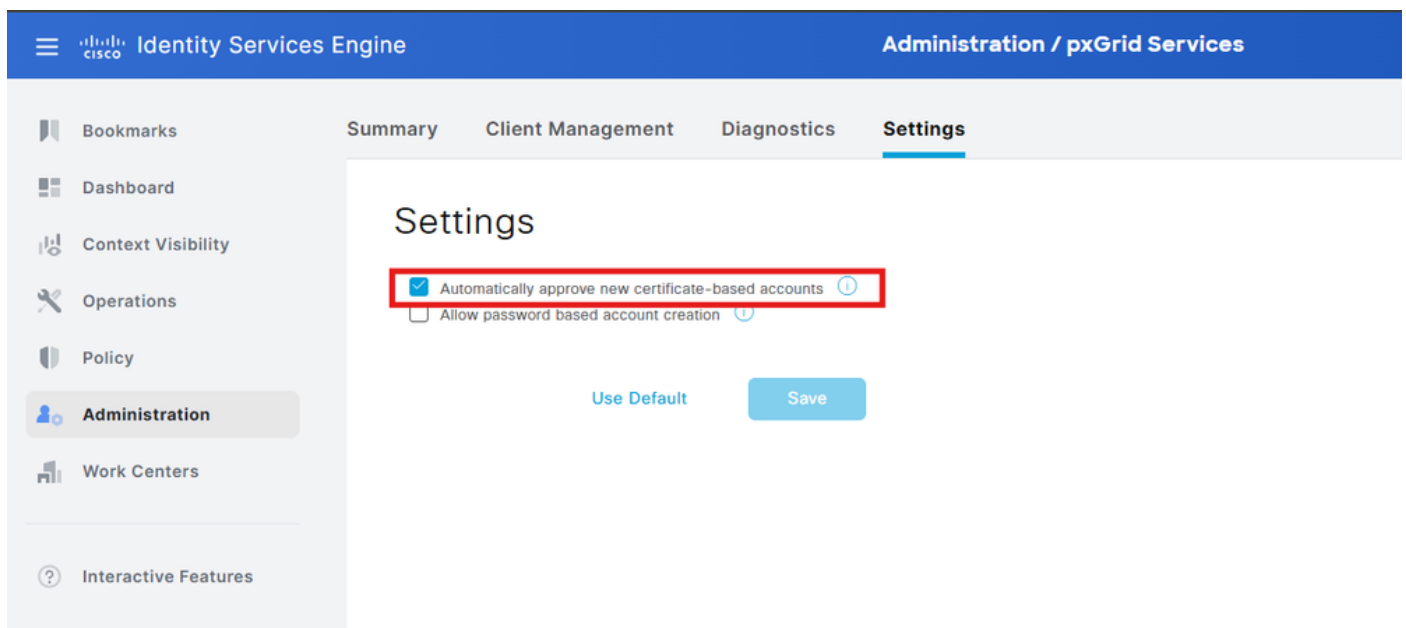
External DLP Servers

Web Traffic Tap

Certificate Management

Cloud Services Settings

Approuvez automatiquement les nouveaux comptes basés sur des certificats pour la demande du client à l'approbation automatique et à l'enregistrement.



Section A : Activez WSA pour l'intégration ISE et générez un CSR pour le certificat client WSA.

1. Connectez-vous à l'interface utilisateur graphique du dispositif de sécurité Web (WSA).

2. Accédez à Réseau > Services d'identification > Moteur de service d'identification.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

Web Traffic Tap

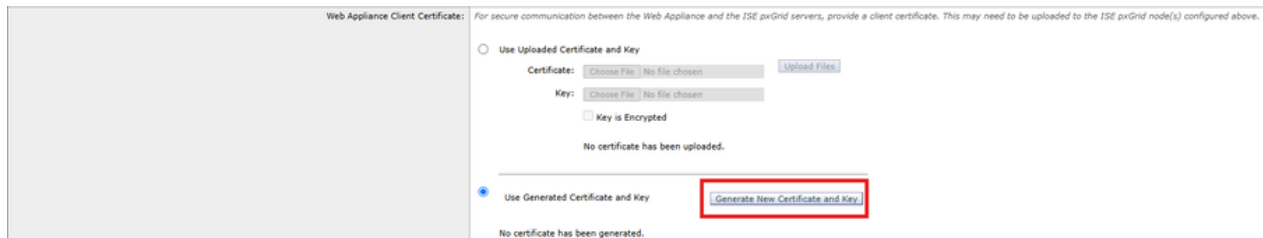
Certificate Management

Cloud Services Settings

Umbrella Settings

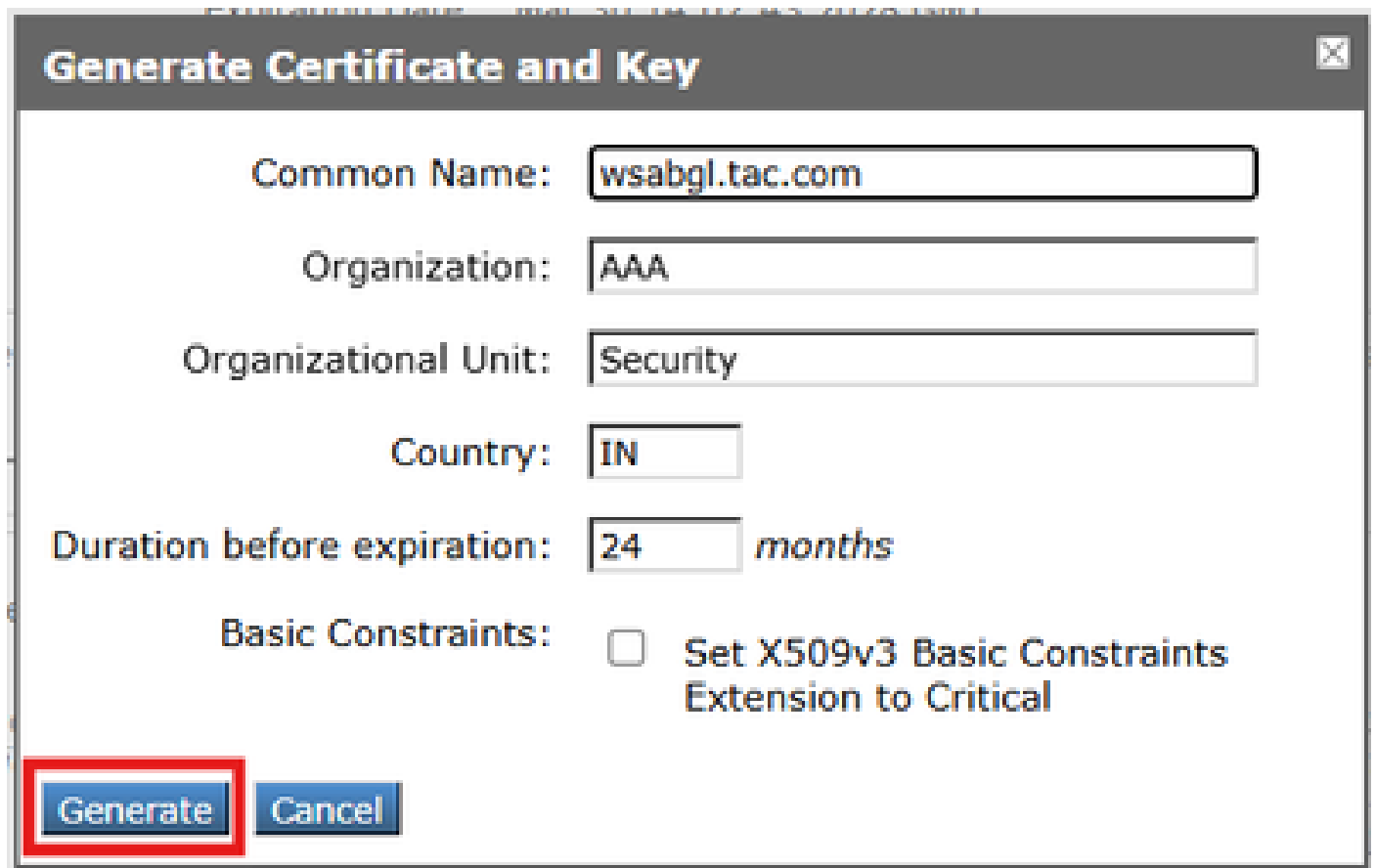
Il ne peut y avoir que deux noeuds pxGrid par déploiement ISE. Il s'agit d'une configuration pxGrid Active-Standby ; un seul noeud ISE+pxGrid peut être actif à la fois. Dans une configuration pxGrid Active-Standby, toutes les informations passent par le PPAN, où le deuxième noeud ISE+pxGrid reste inactif.

8. Faites défiler la page jusqu'à la section Web Appliance Client Certificate et cliquez sur Generate New Certificate and Key.

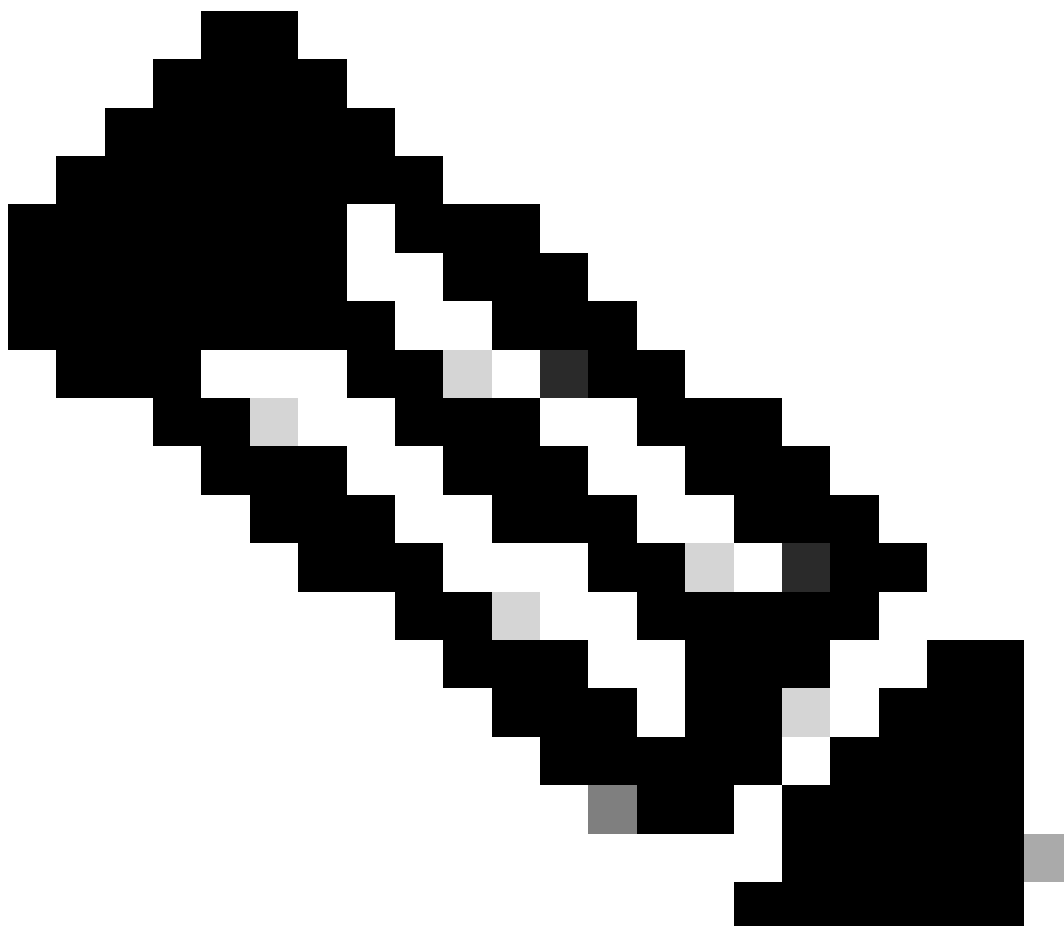


The screenshot shows the 'Web Appliance Client Certificate' configuration page. It has two main sections: 'Use Uploaded Certificate and Key' and 'Use Generated Certificate and Key'. The first section is currently selected with a radio button. It contains fields for 'Certificate' and 'Key', each with a 'Choose File' button and an 'Upload Files' button. Below these fields, it says 'No certificate has been uploaded.' The second section, 'Use Generated Certificate and Key', is currently unselected. It contains a button labeled 'Generate New Certificate and Key' which is highlighted with a red rectangle. Below this button, it says 'No certificate has been generated.'

9. Remplissez les détails du certificat si nécessaire et cliquez sur Générer.



The screenshot shows a dialog box titled 'Generate Certificate and Key'. It contains several input fields for certificate details: 'Common Name' (wsabgl.tac.com), 'Organization' (AAA), 'Organizational Unit' (Security), 'Country' (IN), and 'Duration before expiration' (24 months). There is also a checkbox for 'Basic Constraints' with the label 'Set X509v3 Basic Constraints Extension to Critical'. At the bottom left, there are two buttons: 'Generate' (highlighted with a red rectangle) and 'Cancel'.



Remarque : La durée du certificat doit être un entier compris entre 24 et 60 mois et le pays doit être un code de pays ISO à deux caractères (lettres majuscules uniquement).

10. Cliquez sur Télécharger la demande de signature de certificat.

Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

☐ Use Uploaded Certificate and Key

Certificate:  No file chosen

Key:  No file chosen

☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

Common name: wsibgl.tac.com

Organization: AAA

Organizational Unit: Security

Country: IN

Expiration Date: Mar 19 19:56:43 2027 GMT

Basic Constraints: Not Critical

Download Certificate...

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:  No file chosen

11. Cliquez sur Soumettre.

12. Cliquez sur Valider les modifications pour appliquer les modifications.

---



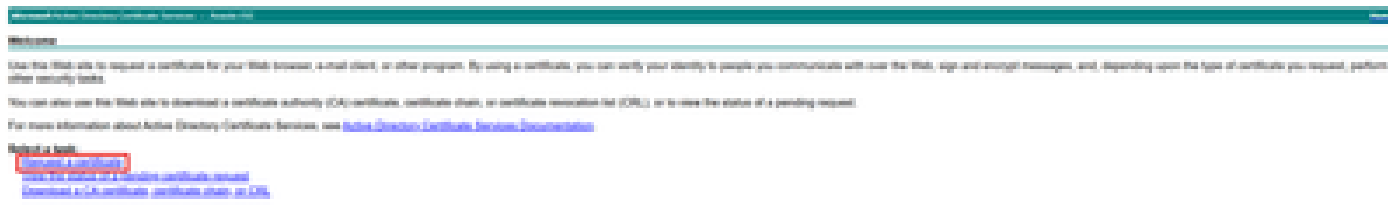
Avertissement : Si vous n'envoyez pas et ne validez pas les modifications mentionnées et que vous téléchargez directement le certificat signé et effectuez la validation, vous risquez de rencontrer des problèmes lors de l'intégration.

---

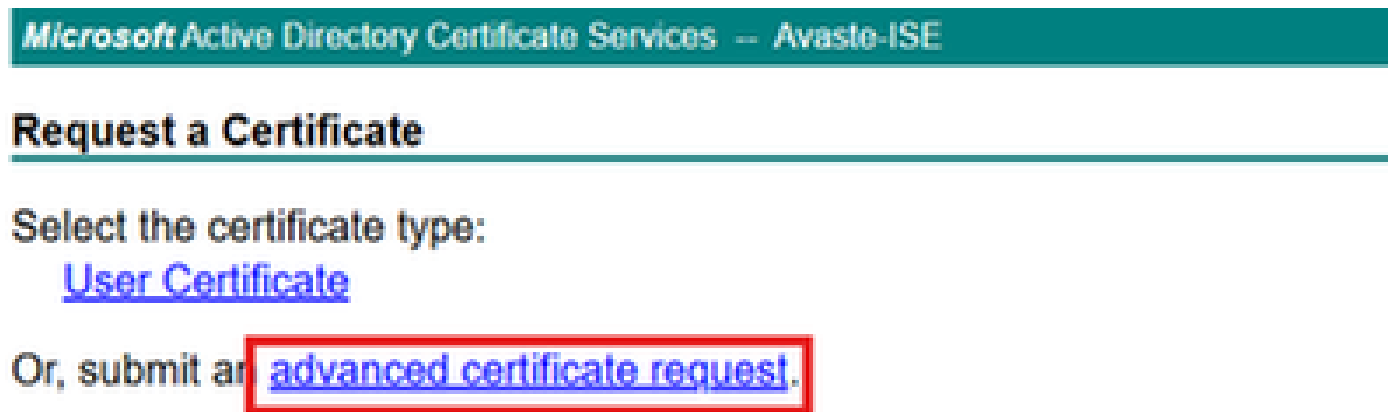
#### Section B : Signer un CSR client WSA à l'aide d'une CA externe

1. Accédez au service de certificats Active Directory MS, <https://server/certsrv/>, où le serveur est IP ou DNS de votre serveur MS.

2. Cliquez sur Demander un certificat.

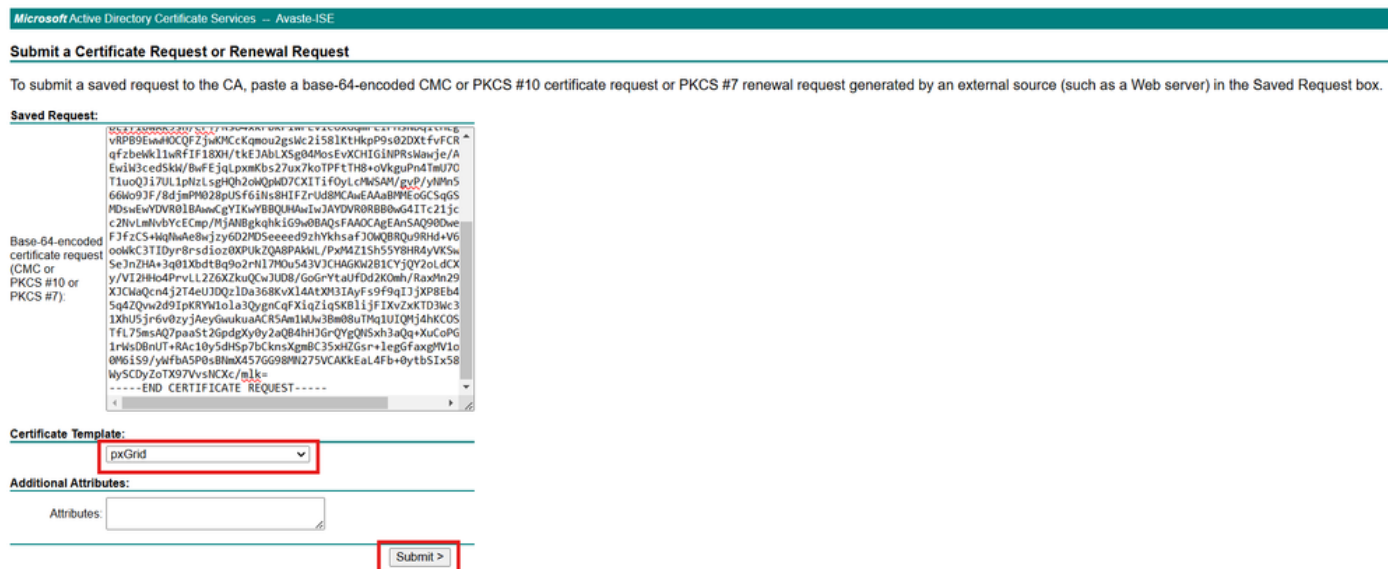


3. Choisissez de soumettre une demande de certificat avancée.



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

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





Remarque : Remarque : Le modèle de certificat pxGrid utilisé nécessite à la fois l'authentification du client et l'authentification du serveur dans le champ Enhanced Key Usage.

---

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

## Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Section C : Liaison du certificat client WSA à la demande de signature de certificat (CSR) et intégration.

1. Accédez à l'interface utilisateur graphique de l'appliance de sécurité Web (WSA).
2. Accédez à Réseau > Services d'identification > Moteur de service d'identification.
3. Cliquez sur Edit Settings.
4. Accédez à la section Certificat client de l'appareil Web.
5. Dans la section signed certificate, Upload the signed certificate WSA-Client.cer

☒

Use Generated Certificate and Key

Generate New Certificate and Key

Common name: wsabgl.tac.com

Organization: AAA

Organizational Unit: Security

Country: IN

Expiration Date: Mar 19 14:21:32 2027 GMT

Basic Constraints: Not Critical

Download Certificate... | Download Certificate Signing Request...

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:

Choose File WSA-Client.cer.cer

Upload File

6. Cliquez sur Envoyer.

7. Cliquez sur Commit Changes pour appliquer les modifications.

8. Cliquez sur Modifier les paramètres.

9. Faites défiler pour tester la communication avec les noeuds ISE et cliquez sur Start Test, qui peut se traduire par :

Tester la communication avec les noeuds ISE

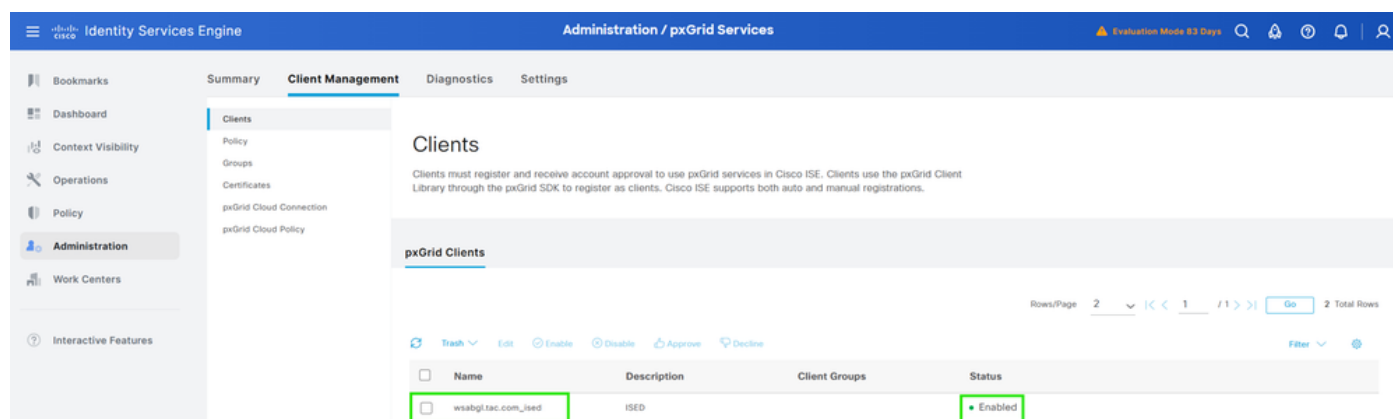
Tester la communication avec les noeuds ISE

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved '10.127.197.128' address: 10.127.197.128
Validating WSA client certificate ...
Success: Certificate validation successful
Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful
Checking connection to ISE pxGrid Node(s) ...
Trying primary PxGrid server...
SXP not enabled.
ERS not enabled.
Preparing TLS connection...
Completed TLS handshake with PxGrid successfully.
Trying download user-session from (https://ise33.lab.local:8910)...
Failure: Failed to download user-sessions.
Trying download SGT from (https://ise33.lab.local:8910)...
Able to Download 17 SGTs.
Skipping all SXP related service requests as SXP is not configured.
Success: Connection to ISE pxGrid Node was successful.
Test completed successfully.
```

## Vérifier

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

Cela génère le WSA en tant que client pxgrid avec le status Enabled.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar indicates 'Administration / pxGrid Services'. The left sidebar shows the 'Administration' menu. The main content area is titled 'Clients' and includes a sub-header 'pxGrid Clients'. Below this, there is a table with the following columns: Name, Description, Client Groups, and Status. The table contains one entry: 'wsa@tac.com\_iseif' with a description of 'ISED' and a status of 'Enabled'. The 'Enabled' status is highlighted with a green box. The table also includes a checkbox for each row and a 'Filter' button.

| Name                                       | Description | Client Groups | Status                                      |
|--------------------------------------------|-------------|---------------|---------------------------------------------|
| <input type="checkbox"/> wsa@tac.com_iseif | ISED        |               | <input checked="" type="checkbox"/> Enabled |

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

## Websocket > Clients :

| Client Name         | Connect To | Session Id | Certificate                                              | Subscriptions                                       |
|---------------------|------------|------------|----------------------------------------------------------|-----------------------------------------------------|
| -ise-admin-ise33    | ise33      | ise33:0    | CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=... | /topic/com.cisco.ise.pxgrid.admin.log               |
| -ise-fanout-ise33   | ise33      | ise33:1    | CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=... | /topic/wildcard                                     |
| -ise-mnt-ise33      | ise33      | ise33:2    | CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=... | /topic/com.cisco.ise.session.internal               |
| -ise-fanout-ise33   | ise33      | ise33:3    | CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=... | /topic/distributed                                  |
| wsabgl.tac.com_ised | ise33      | ise33:4    | CN=wsabgl.tac.com, OU=Security, O=AAA, C=IN              | /topic/com.cisco.ise.session                        |
| wsabgl.tac.com_ised | ise33      | ise33:5    | CN=wsabgl.tac.com, OU=Security, O=AAA, C=IN              | /topic/com.cisco.ise.config.trustsec.security.group |
| -ise-internal_test  | ise33      | ise33:6    | CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=... | /topic/com.cisco.ise.session                        |

Cisco ISE Pxgrid-server.log niveau TRACE.reference.

<#root>

```
{ "timestamp":1742395398803, "level":"INFO", "type":"WS_SERVER_CONNECTED", "host":"ise33", "client":
```

**wsabgl.lab.local\_ised**

```
", "server":"wss://ise33.lab.local:8910/pxgrid/ise/pubsub", "message":"WebSocket connected. session\u003d
TRACE [Thread-8][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Drop. exclude=[id=3, cl
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- Authenticating null
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- Certs up to date. user=~ise-pu
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- preAuthenticatedPrincipal = ~i
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- X.509 client authentication ce
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- Authentication
```

**success**

```
: PreAuthenticatedAuthenticationToken [Principal=org.springframework.security.core.userdetails.User [Us
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.data.AuthzDaoImpl -:::- requestNodeName=wsabgl.lab.local
DEBUG [Thread-13][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Adding subscription=[
INFO [Thread-13][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Pubsub subscribe. subscrip
TRACE [WsIseClientConnection-804][ ] cpm.pxgrid.ws.client.WsEndpoint -:::- Send. session=[id=34eae1
```

**"wsabgl.lab.local\_ised**

```
", "server":"wss://ise33.lab.local:8910/pxgrid/ise/pubsub", "message":"Pubsub subscribe. subscription\u003d
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Received frame=[command=SE
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Authorized to send (cached
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Distribute from=[id=0,
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Distribute distributed
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Distribute distributed
TRACE [sub-sender-1][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::- Send. subscription=[id=
TRACE [sub-sender-0][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::- Send. subscription=[id=
DEBUG [Grizzly(1)][ ] cpm.pxgrid.ws.client.WsSubscriber -:::- onStompMessage session=[id=34eae17d-5
DEBUG [Grizzly(1)][ ] cpm.pxgrid.ws.client.WsSubscriber -:::- onStompMessage session=[id=4b4d7de4-b
TRACE [Grizzly(1)][ ] cpm.pxgrid.ws.client.WsEndpoint -:::- Send. session=[id=dd1d138d-a640-4f4f-bd
TRACE [Grizzly(1)][ ] cpm.pxgridwebapp.ws.distributed.FanoutDistributor -:::- DownstreamHandler sen
TRACE [Thread-10][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Received frame=[command=S
```

TRACE [Thread-10][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Authorized to send (cached

## Dépannage

### Problème

Problème CA inconnu. Sur le WSA, le test de la connexion ISE échoue avec une erreur. Échec: La connexion au serveur ISE PxGrid a expiré.

#### Test Communication with ISE Server

Start Test

Validating ISE Portal certificate ...

Success: Certificate validation successful

Checking connection to ISE PxGrid server...

**Failure: Connection to ISE PxGrid server timed out**

**Test interrupted: Fatal error occurred, see details above.**

Cisco ISE Pxgrid-server.log niveau TRACE.reference.

<#root>

#### ERROR

[Thread-8][[]] cisco.cpm.pxgrid.cert.LoggingTrustManagerWrapper -:::-- checkClientTrusted exception.  
unable to find valid certification path to requested target principle=CN=wsabgl.lab.local, OU=Security,

TRACE [WsIseClientConnection-804][[]] cpm.pxgrid.ws.client.WsEndpoint -:::-- Send. session=[id=34eae1  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Received frame=[command=SE  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Authorized to send (cached  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::-- Distribute from=[id=0,  
unable to find valid certification path to requested target

principle\u003dCN\u003dwsabgl.lab.local, OU\u003dSecurity, O\u003dAAA, C\u003dIN"}  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::-- Distribute distributed  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::-- Distribute distributed  
TRACE [sub-sender-1][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::-- Send. subscription=[id=  
DEBUG [Grizzly(2)][[]] cpm.pxgrid.ws.client.WsSubscriber -:::-- onStompMessage session=[id=4b4d7de4-b  
TRACE [Grizzly(2)][[]] cpm.pxgrid.ws.client.WsEndpoint -:::-- Send. session=[id=dd1d138d-a640-4f4f-bd

La raison de l'échec peut être vue avec les captures de paquets,

| Source         | Destination    | Protocol | Length | Info                                                                                                           |
|----------------|----------------|----------|--------|----------------------------------------------------------------------------------------------------------------|
| 10.76.105.168  | 10.127.197.128 | TCP      | 74     | 42883 → 8910 [SYN] Seq=0 Win=65535 Len=0 MSS=1254 WS=64 SACK_PERM TSval=984988989 TSecr=0                      |
| 10.127.197.128 | 10.76.105.168  | TCP      | 74     | 8910 → 42883 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1459800712 TSecr=984988989 WS=128 |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [ACK] Seq=1 Ack=1 Win=66496 Len=0 TSval=984988999 TSecr=1459800712                                |
| 10.76.105.168  | 10.127.197.128 | TLSv1.2  | 583    | Client Hello (SNI=10.127.197.128)                                                                              |
| 10.127.197.128 | 10.76.105.168  | TCP      | 66     | 8910 → 42883 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=1459800715 TSecr=984988999                              |
| 10.127.197.128 | 10.76.105.168  | TLSv1.2  | 4818   | Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done                         |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [ACK] Seq=518 Ack=1243 Win=65280 Len=0 TSval=984989019 TSecr=1459800739                           |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [ACK] Seq=518 Ack=2485 Win=65280 Len=0 TSval=984989019 TSecr=1459800739                           |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [ACK] Seq=518 Ack=3727 Win=64064 Len=0 TSval=984989019 TSecr=1459800739                           |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [ACK] Seq=518 Ack=4753 Win=65472 Len=0 TSval=984989019 TSecr=1459800739                           |
| 10.76.105.168  | 10.127.197.128 | TLSv1.2  | 1526   | Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message          |
| 10.127.197.128 | 10.76.105.168  | TCP      | 66     | 8910 → 42883 [ACK] Seq=4753 Ack=1978 Win=33024 Len=0 TSval=1459800761 TSecr=984989039                          |
| 10.127.197.128 | 10.76.105.168  | TLSv1.2  | 73     | Alert (Level: Fatal, Description: Certificate Unknown)                                                         |
| 10.127.197.128 | 10.76.105.168  | TCP      | 66     | 8910 → 42883 [FIN, ACK] Seq=4760 Ack=1978 Win=33024 Len=0 TSval=1459800769 TSecr=984989039                     |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [ACK] Seq=1978 Ack=4760 Win=66496 Len=0 TSval=984989049 TSecr=1459800769                          |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [ACK] Seq=1978 Ack=4761 Win=66496 Len=0 TSval=984989049 TSecr=1459800769                          |
| 10.76.105.168  | 10.127.197.128 | TCP      | 66     | 42883 → 8910 [FIN, ACK] Seq=1978 Ack=4761 Win=66496 Len=0 TSval=984989049 TSecr=1459800769                     |
| 10.127.197.128 | 10.76.105.168  | TCP      | 66     | 8910 → 42883 [ACK] Seq=4761 Ack=1979 Win=33024 Len=0 TSval=1459800770 TSecr=984989049                          |

## Solution

1. Assurez-vous que le certificat signé de l'appliance Web est correctement lié sur le WSA et que les modifications ont été validées.
2. Assurez-vous que le certificat de l'émetteur ou de l'autorité de certification racine du certificat du client WSA fait partie du magasin de confiance sur Cisco ISE.

## Défauts connus

| ID de débogage Cisco                    | Description                                                   |
|-----------------------------------------|---------------------------------------------------------------|
| <a href="#">ID de bogue Cisco 23986</a> | La requête API Pxgrid getUserGroups renvoie une réponse vide. |
| <a href="#">ID de bogue Cisco 77321</a> | WSA reçoit des SID au lieu de groupes AD d'ISE.               |

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.