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

## Table des matières



# 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

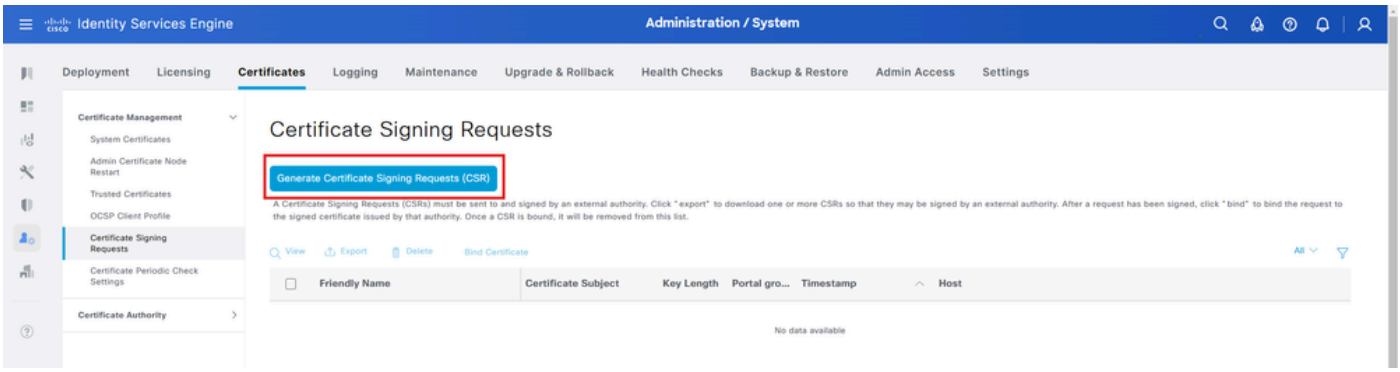
Étape 1 : Générer un certificat pxGrid ISEServer

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

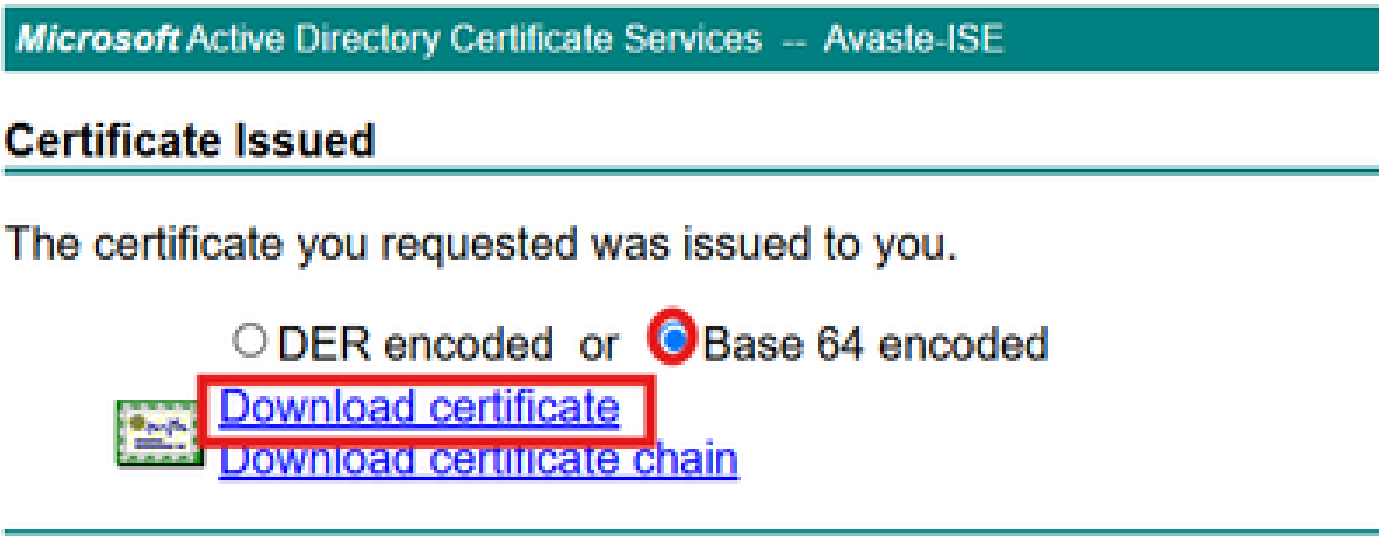
* Key Length: 4096

* Digest to Sign With: SHA-384

Certificate Policies

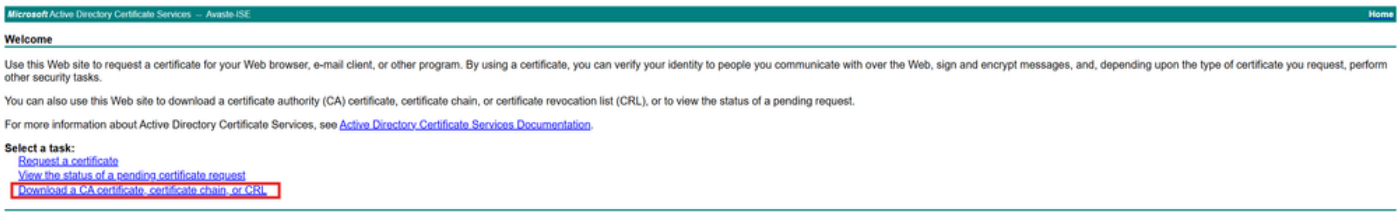
Le modèle de certificat pxGrid utilisé nécessite à la fois l'authentification du client et l'authentification du serveur dans le champ Enhanced Key Usage.

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

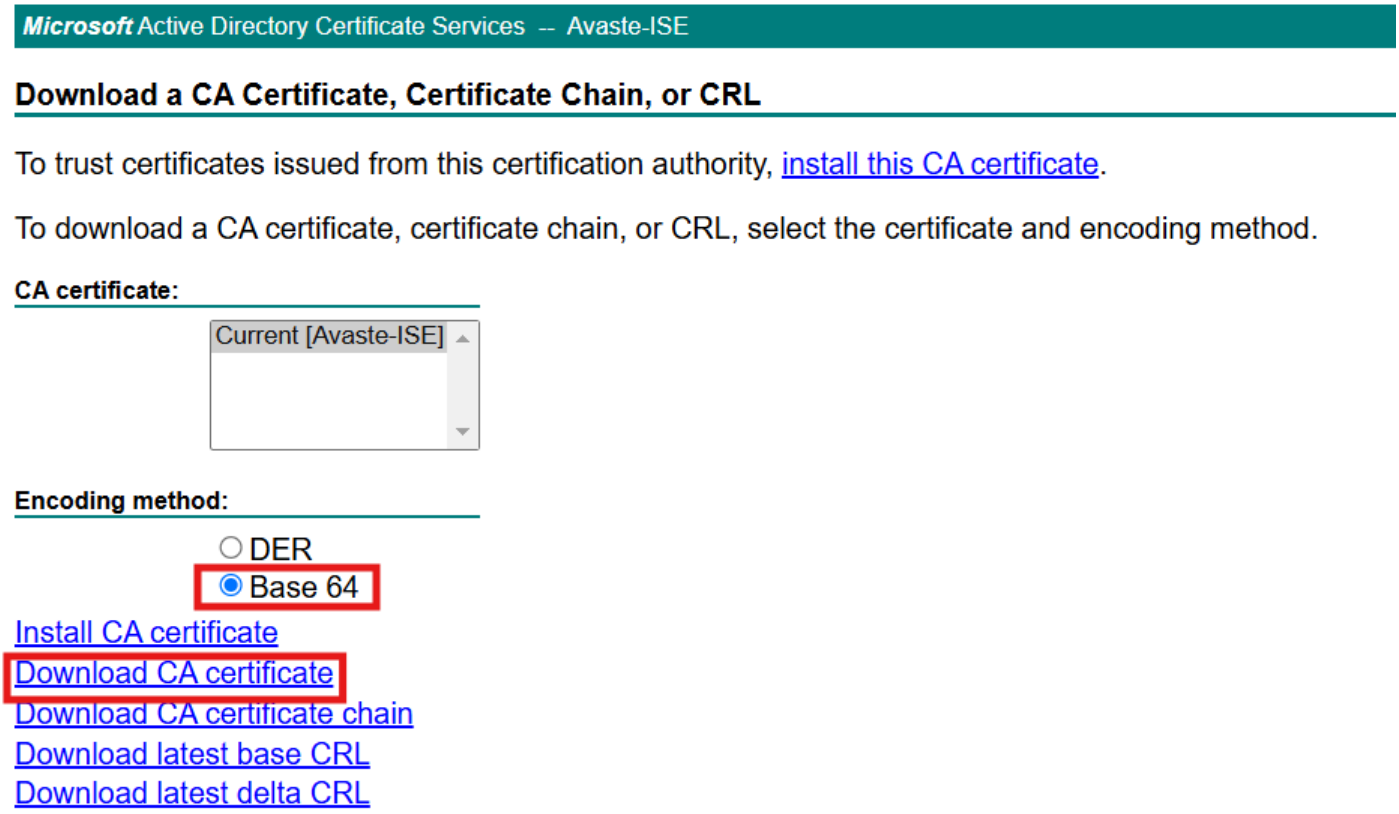



Étape 3 : Importer le certificat racine de l'autorité de certification dans l'ISE Trust Store

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



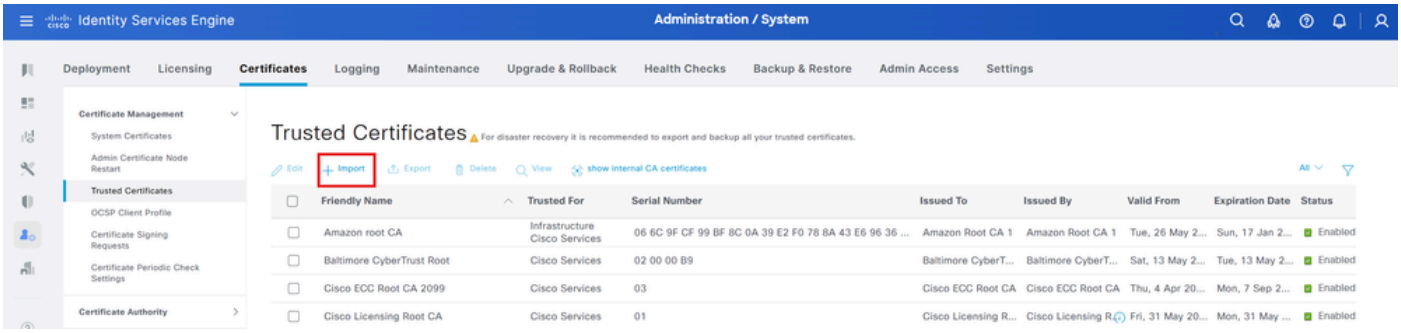

2. Sélectionnez le format Base-64, puis cliquez surTélécharger le certificat CA.




3.Enregistrez le certificat sous CA_Root.cer.

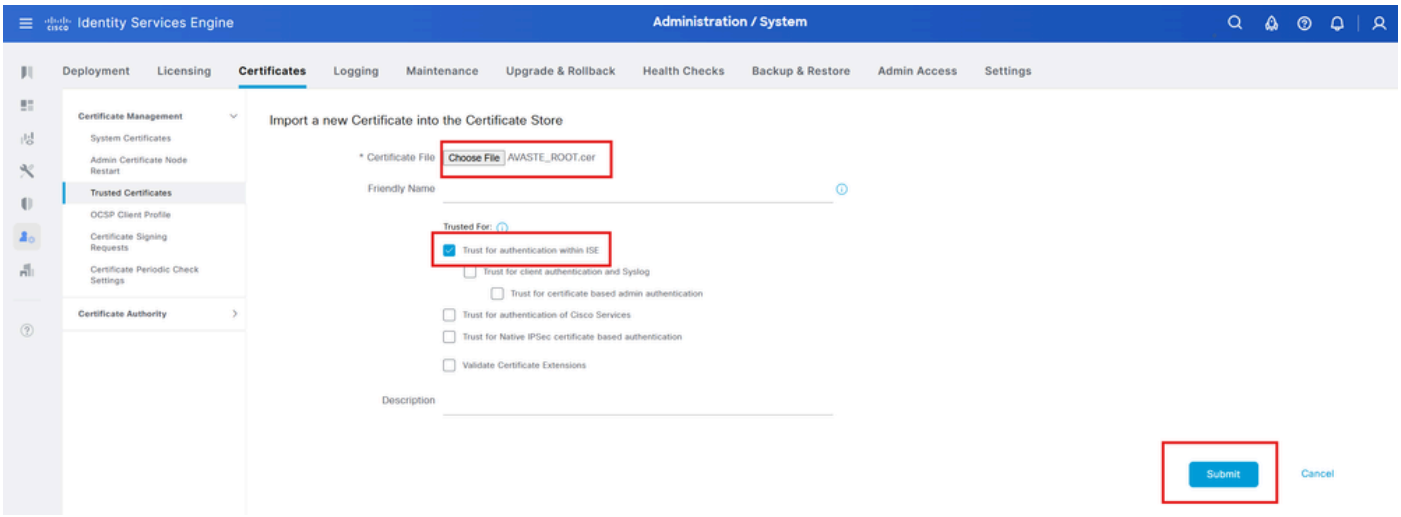
4.Connectez-vous à l'interface utilisateur graphique de Cisco Identity Services Engine (ISE).

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




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

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



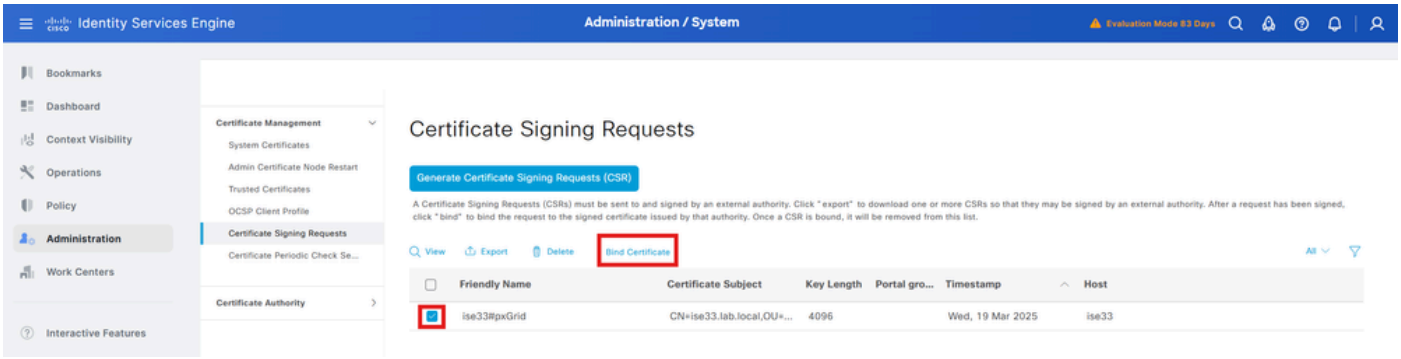

8. Cliquez sur Soumettre.

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).

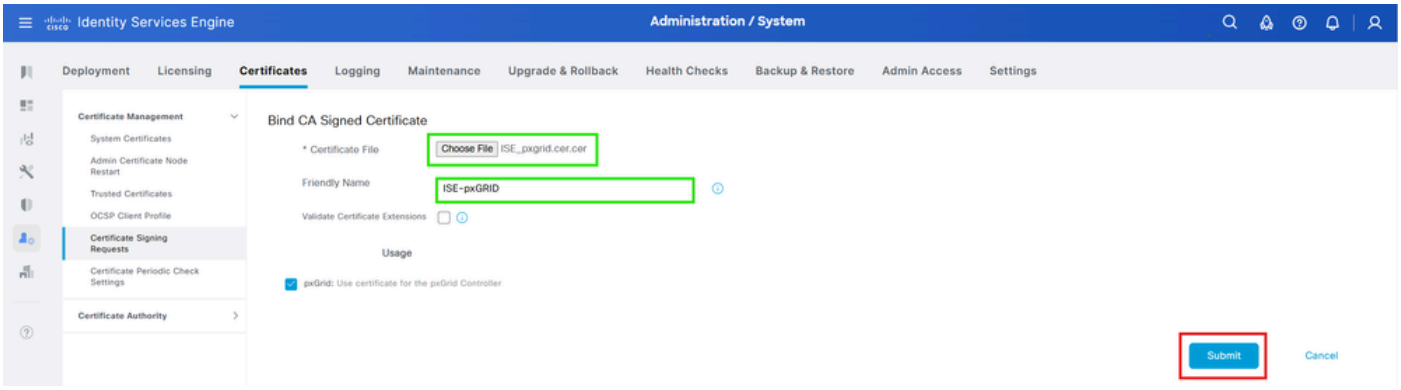
2. Sélectionnez Administration > Système > Certificats > Gestion des certificats > Demandes de signature de certificat.

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




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

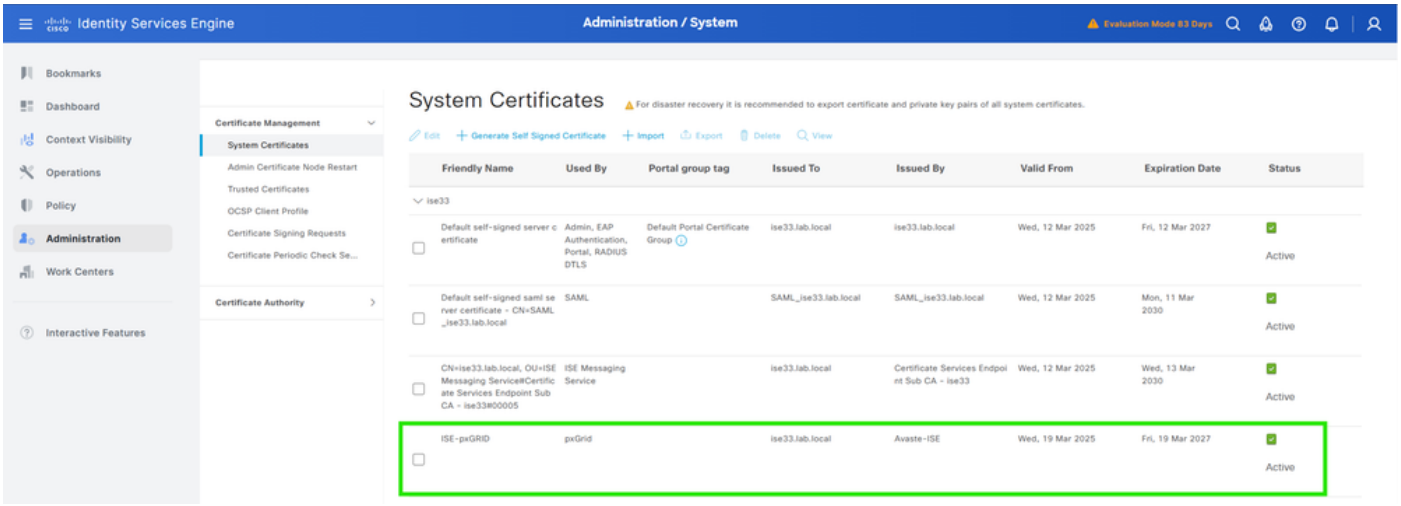
5. Attribuez un nom convivial au certificat, puis cliquez sur Envoyer.




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

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

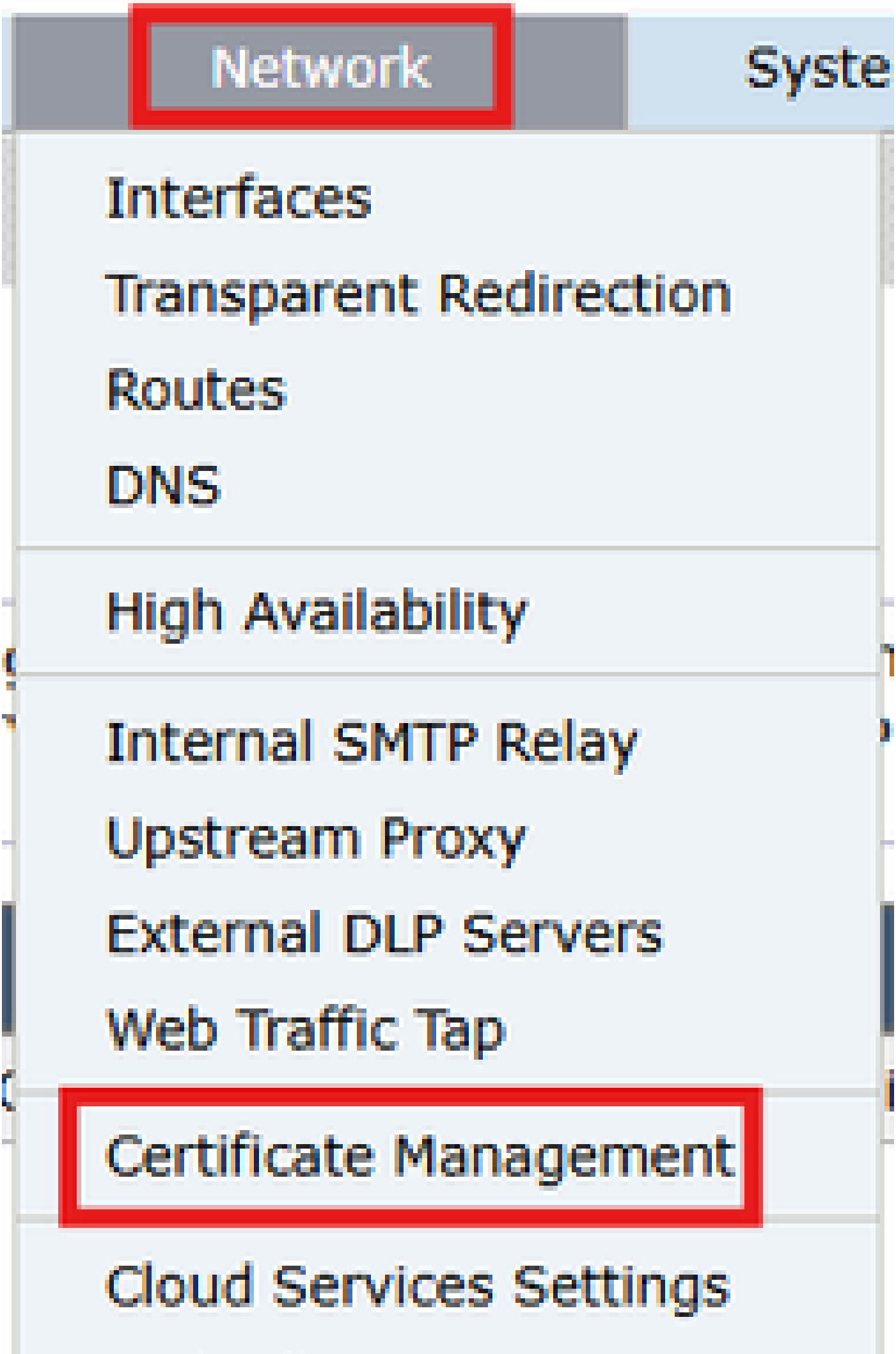
9. Vous pouvez voir le certificat pxGrid créé signé par l'autorité de certification externe dans la liste.



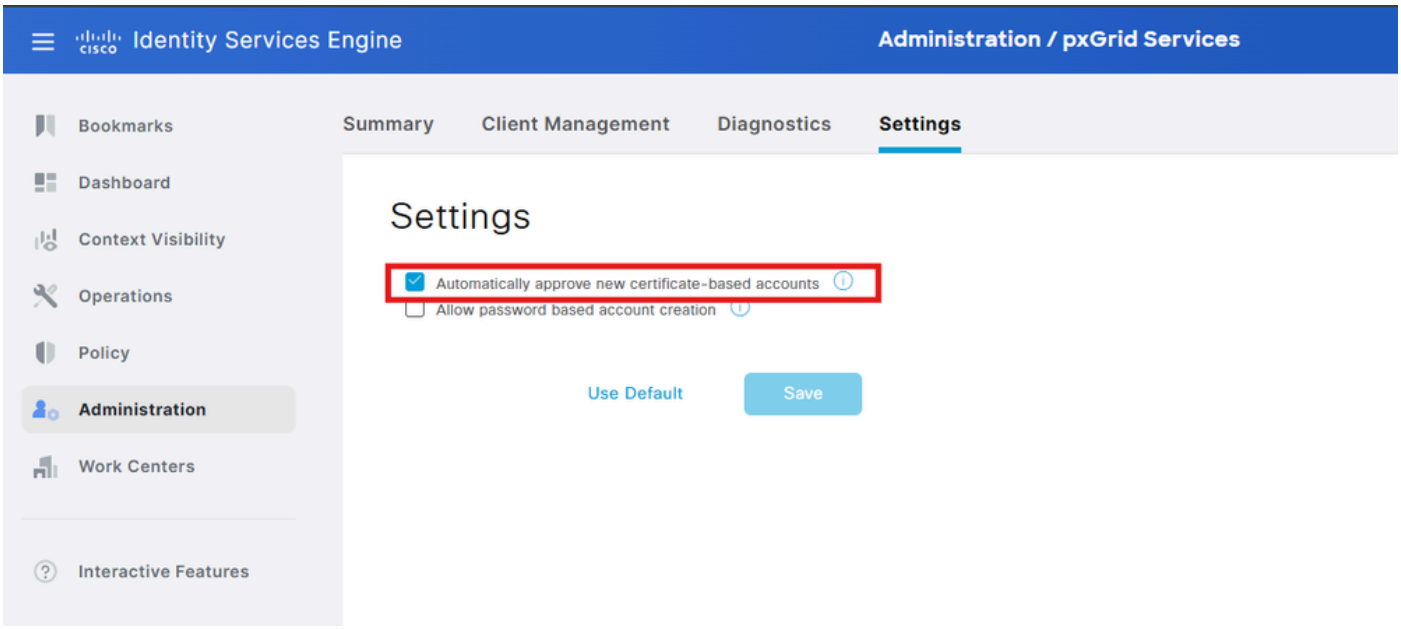

## Section B : Ajout du certificat racine CA au magasin de certificats de confiance WSA

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
Syste
Interfaces
Transparent Redirection
Routes
DNS
High Availability
Internal SMTP Relay
Upstream Proxy
External DLP Servers
Web Traffic Tap
Certificate Management
Cloud Services Settings

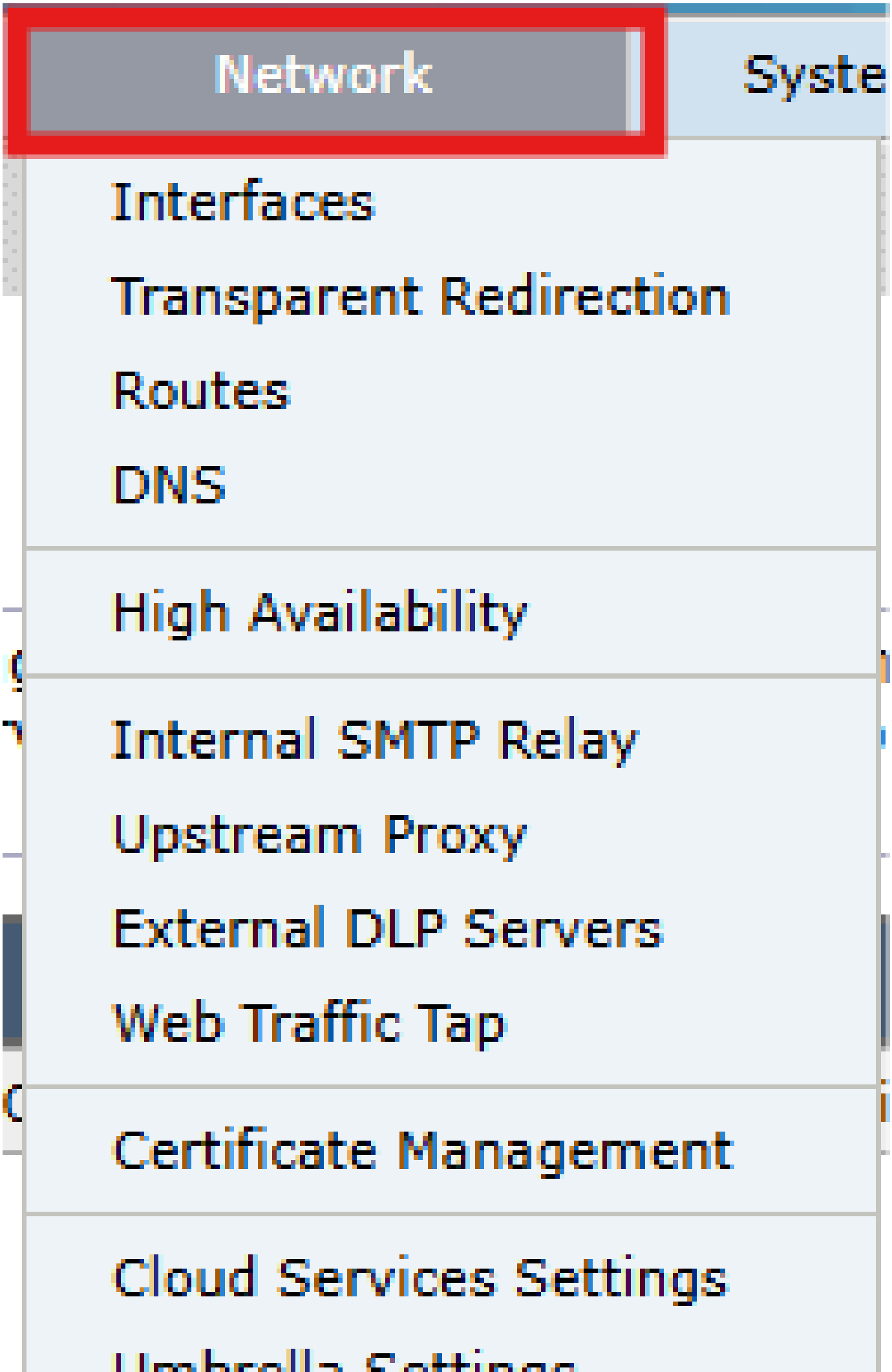
Approuvez automatiquement les nouveaux comptes basés sur des certificats pour la demande du client à l'approbation automatique et à l'enregistrement.




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

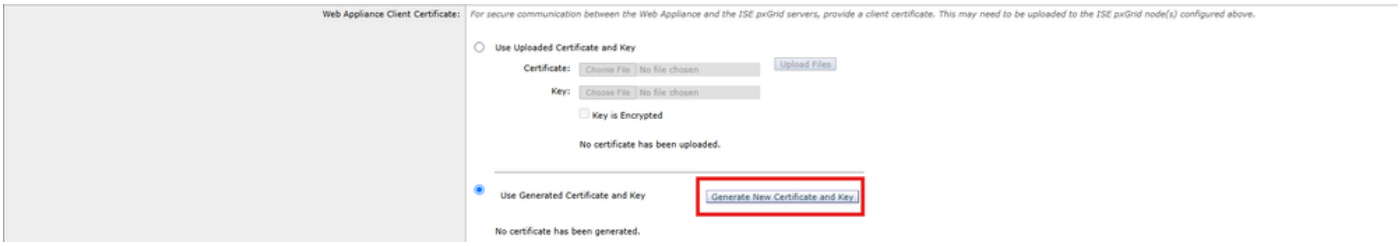
1.Connectez-vous à l'interface utilisateur graphique du dispositif de sécurité Web (WSA).

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

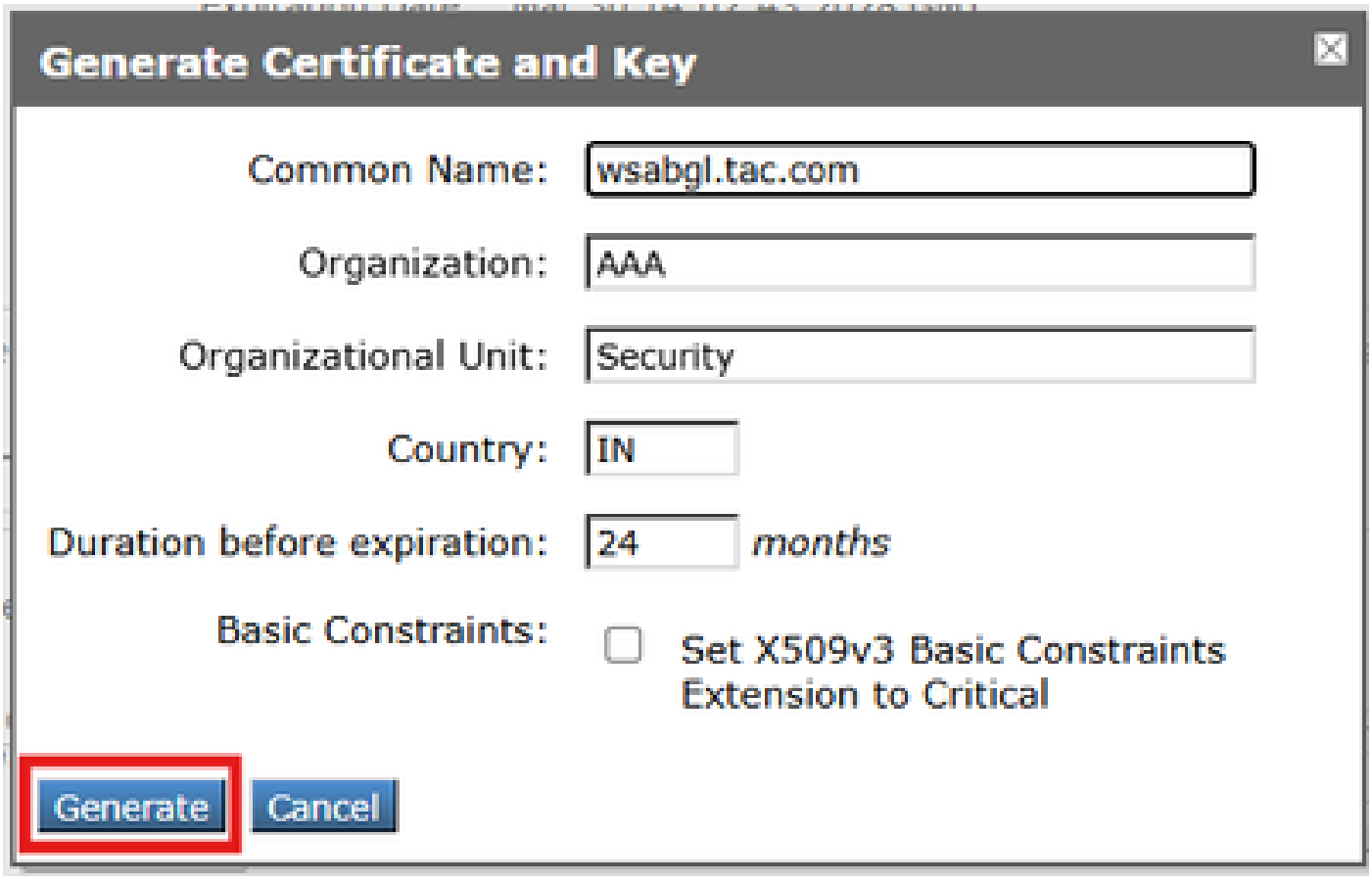

Network
Syste
Interfaces
Transparent Redirection
Routes
DNS
High Availability
Internal SMTP Relay
Upstream Proxy
External DLP Servers
Web Traffic Tap
Certificate Management
Cloud Services Settings

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.

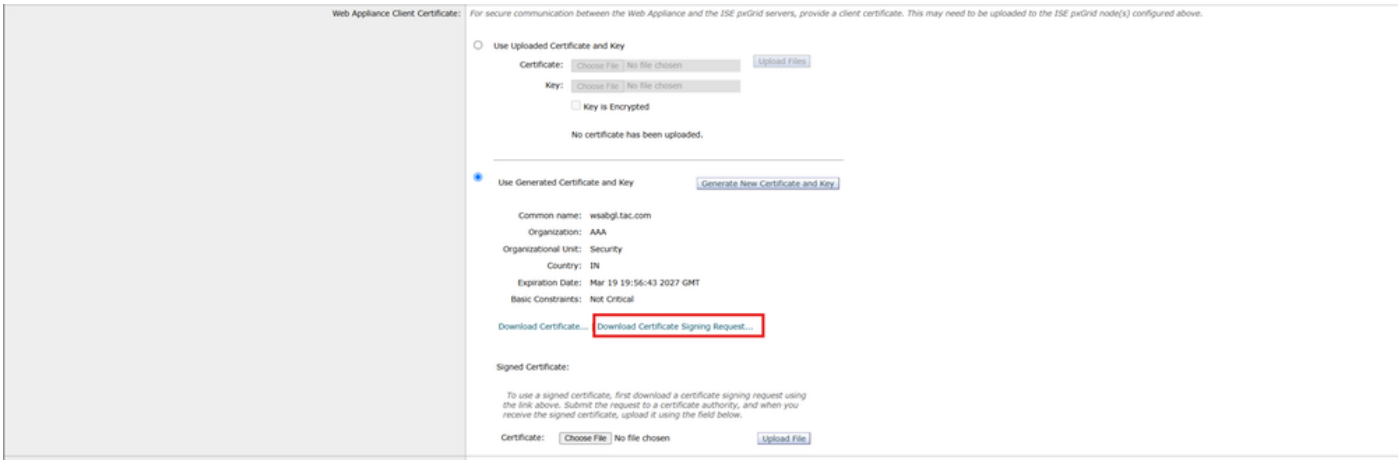



9. Remplissez les détails du certificat si nécessaire et cliquez sur Générer.



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).

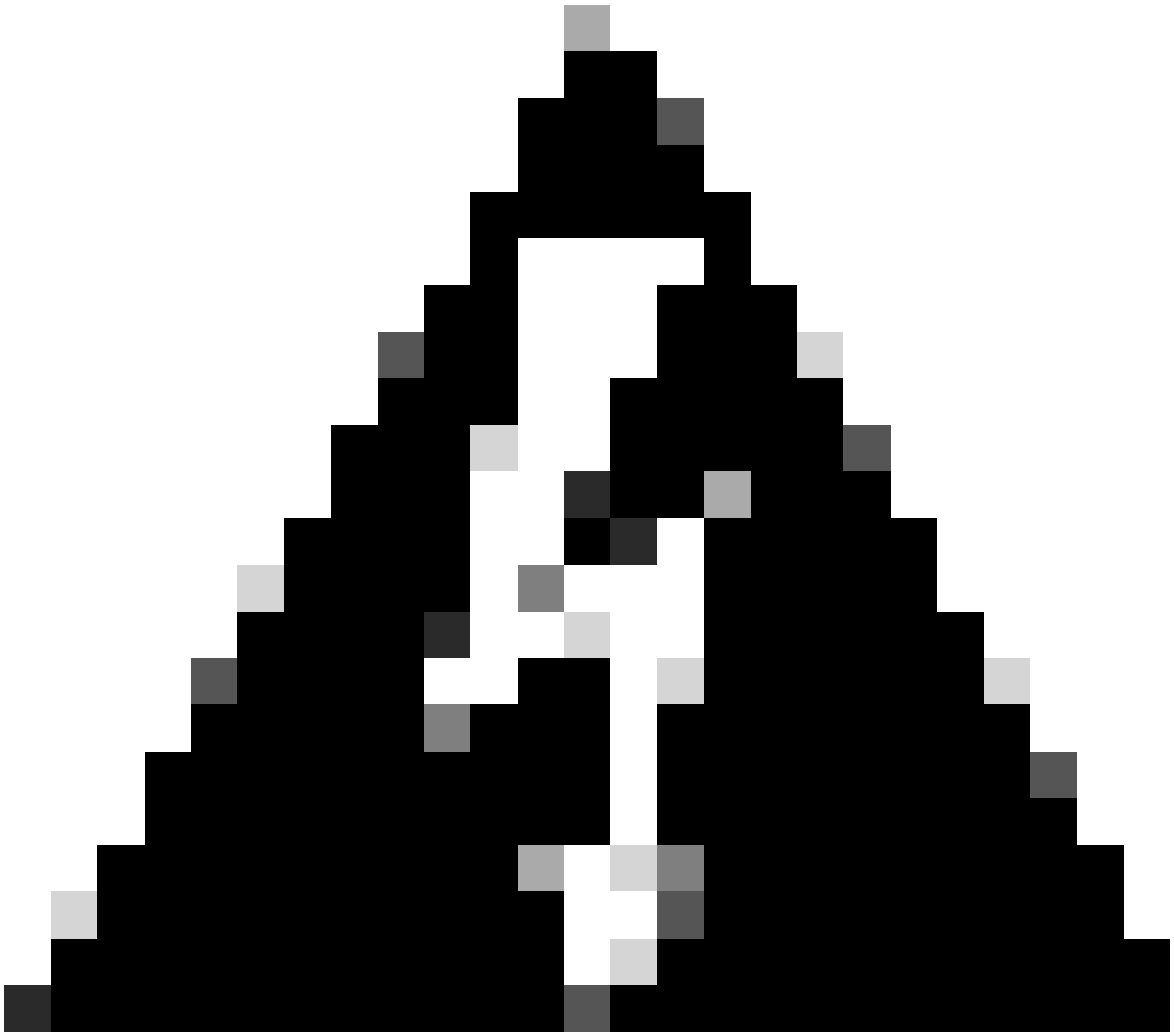
10. Cliquez sur Télécharger la demande de signature de certificat.




11. Cliquez sur Soumettre.

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

---



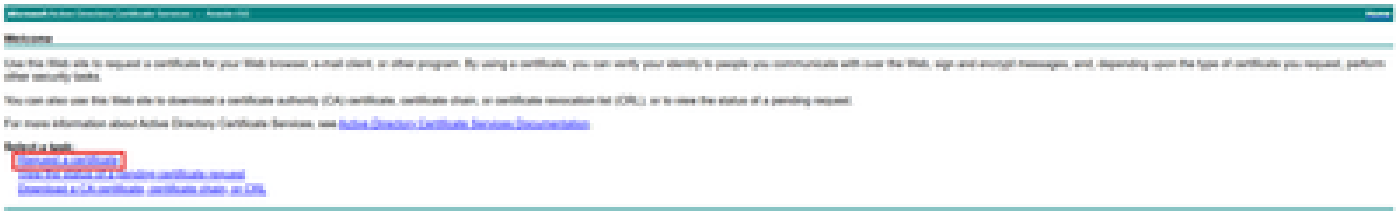
Avertissement : Si vous n'envoyez pas et ne validez pas les modifications mentionnées et que vous téléchargez directement le certificat signé et effectuez la validation, vous risquez de rencontrer des problèmes lors de l'intégration.

---

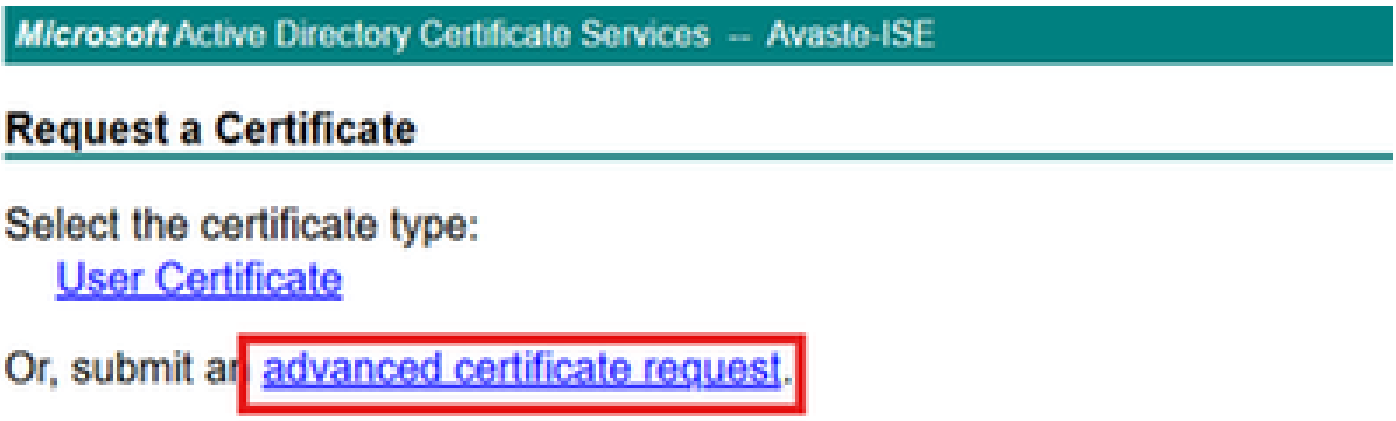
Section B : Signer un CSR client WSA à l'aide d'une CA externe

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.

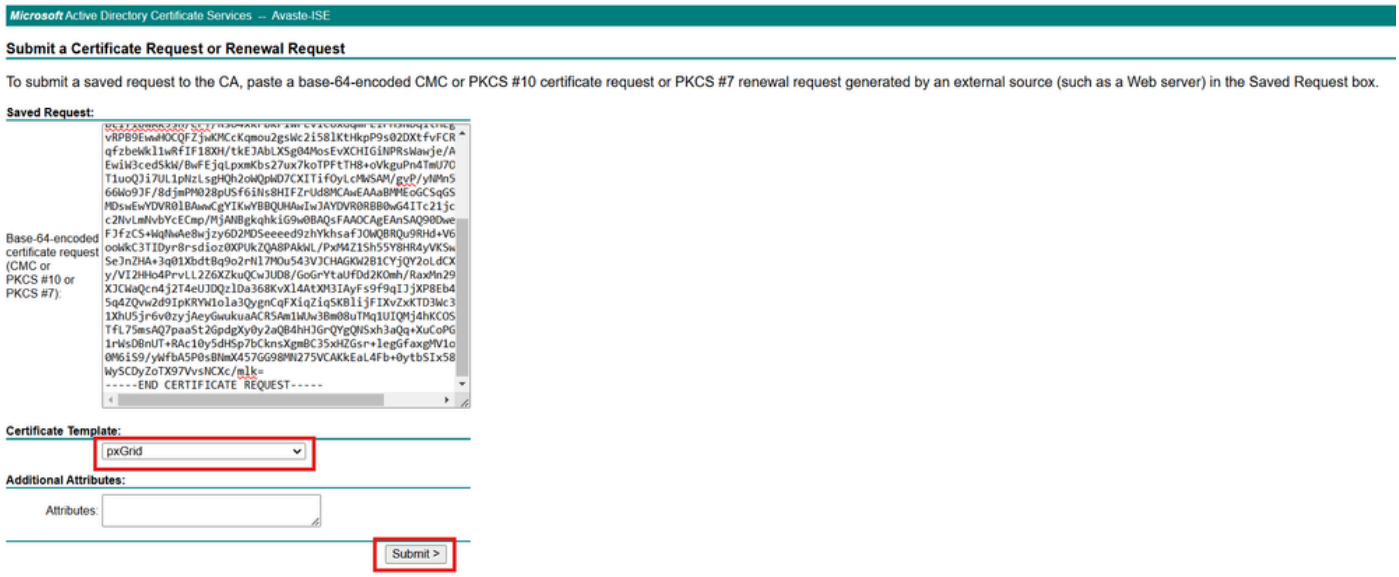


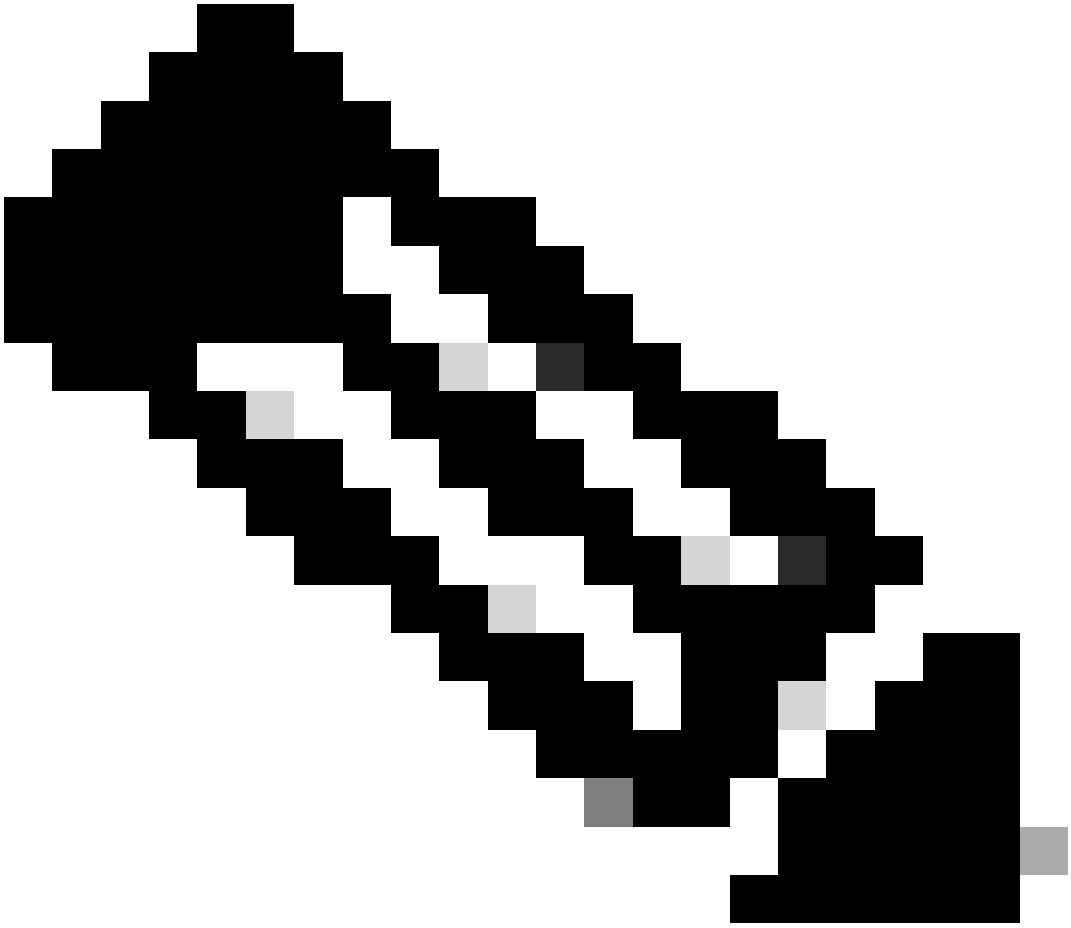
3. Choisissez de soumettre une demande de certificat avancée.




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

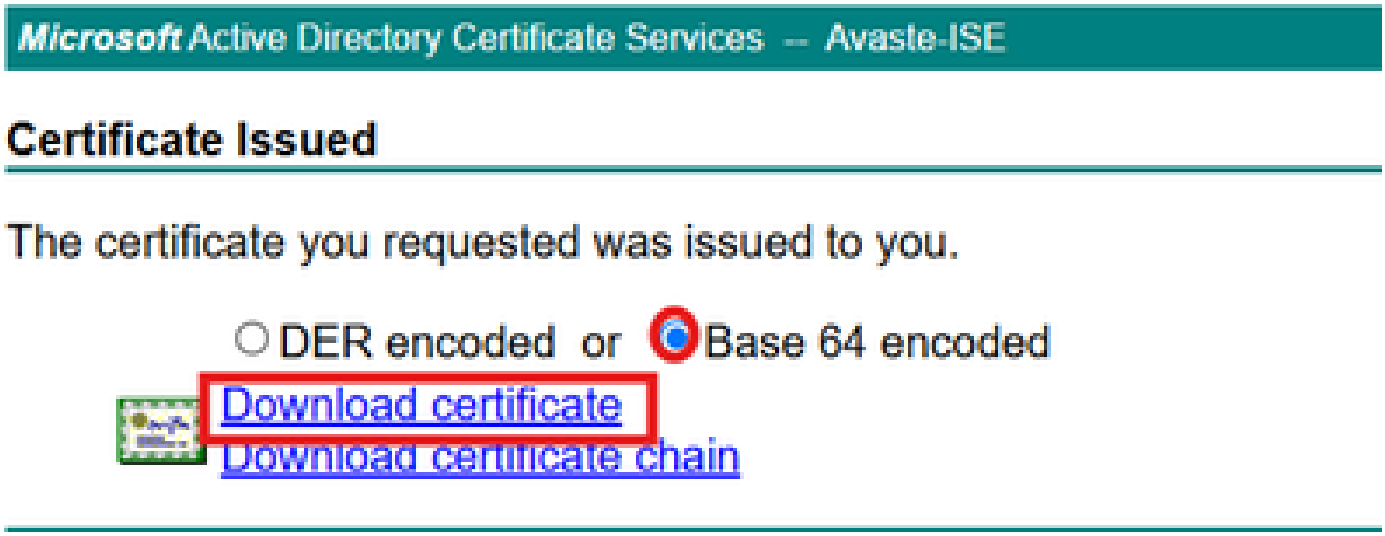
5. Sélectionnez pxGrilles comme modèle de certificat, puis cliquez sur Envoyer.





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.




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

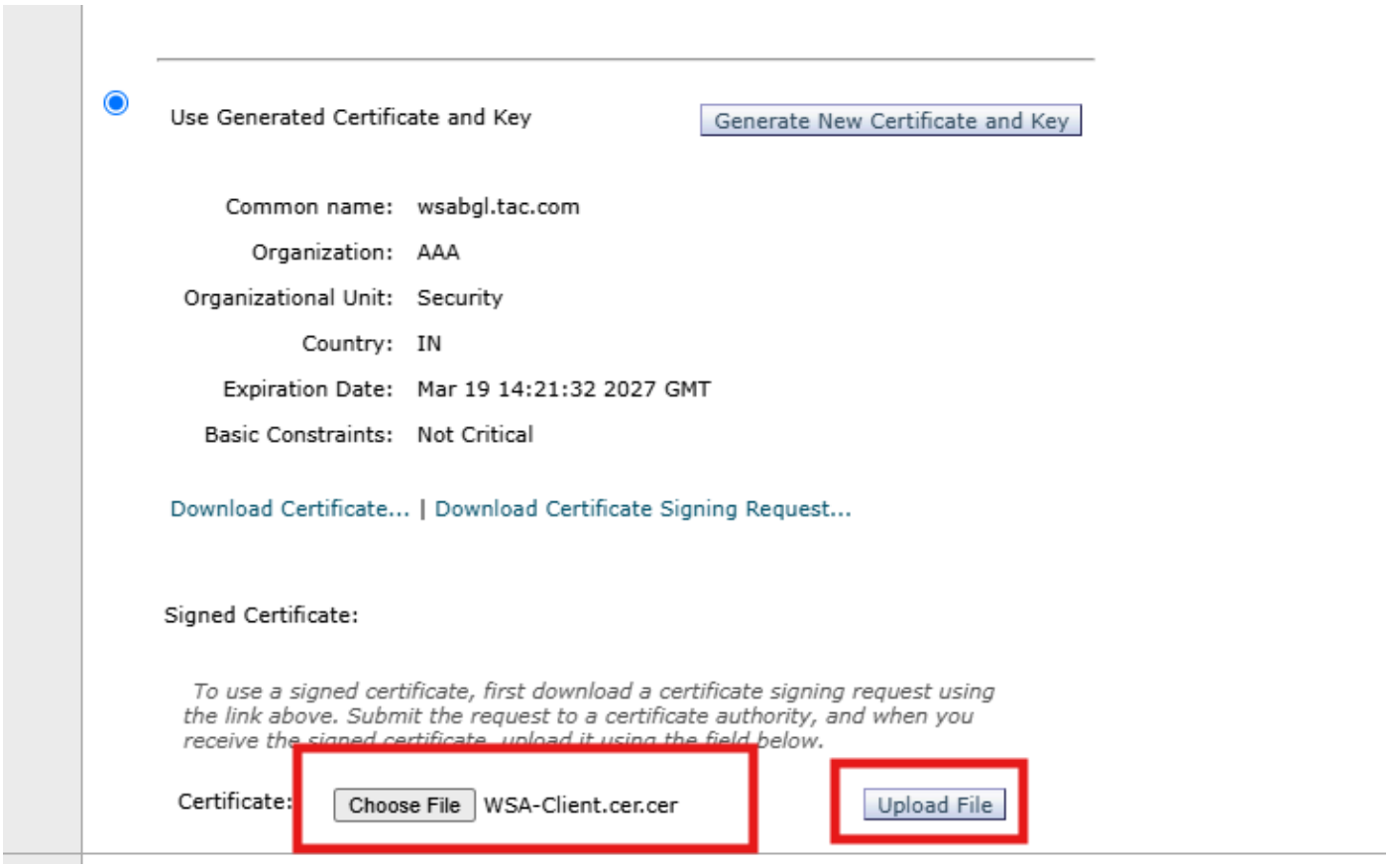
1. Accédez à l'interface utilisateur graphique de l'appliance de sécurité Web (WSA).

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



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

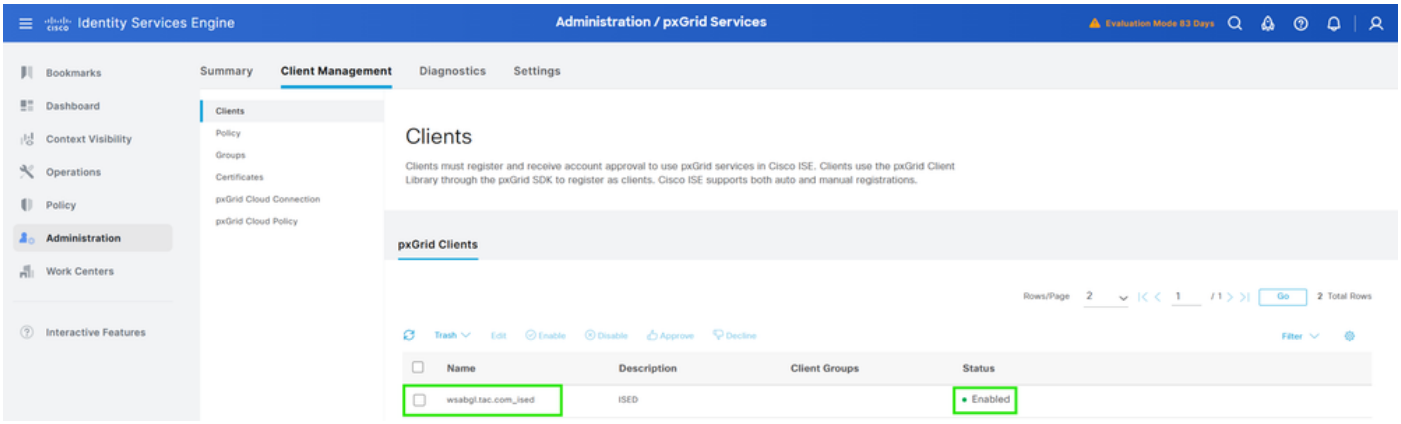
Tester la communication avec les noeuds ISE

```
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

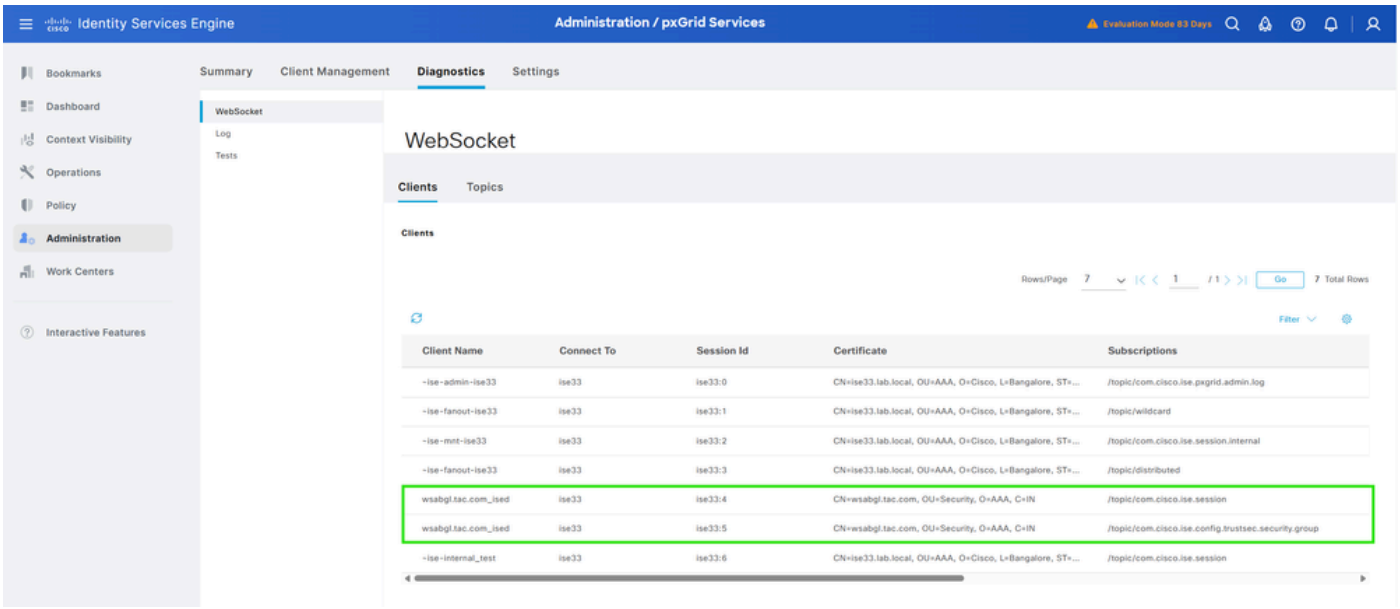
Sur Cisco ISE, accédez à Administration > pxGrid Services > Client Management > Clients.

Cela génère le WSA en tant que client pxgrid avec le statusEnabled.




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

Websocket > Clients :




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\u00
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 (cache
```

# 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.


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

### <#root>

**ERROR**

```
 [Thread-8][[]] cisco.cpm.pxgrid.cert.LoggingTrustManagerWrapper -:::::- checkClientTrusted exception.
```

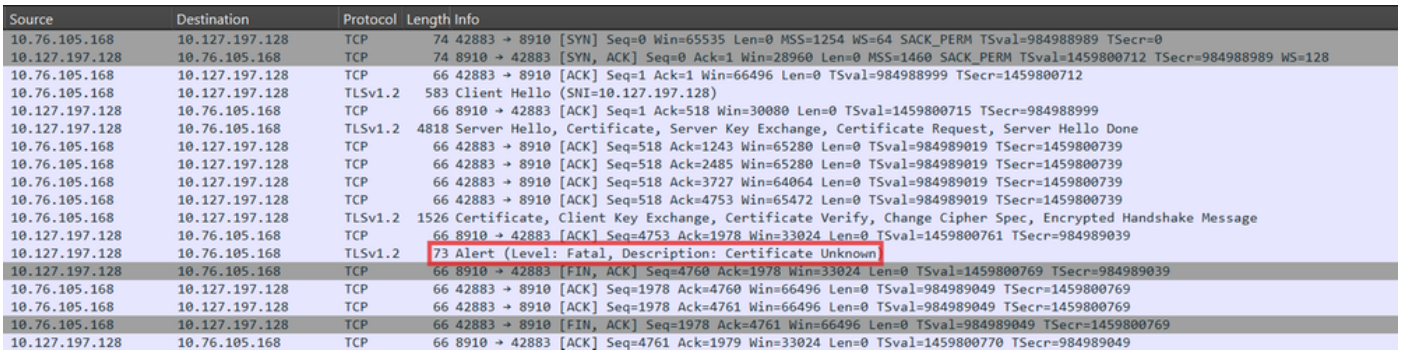
**unable to find valid certification path to requested target principle=CN=wsabgl.lab.local, OU=Security,**

```
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 |
|---|---|
| ID de bogue Cisco 23986 | La requête API Pxgrid getUserGroups renvoie une réponse vide. |
| ID de bogue Cisco 77321 | 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.