

Dépannage du certificat d'administration ISE expiré

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Certificat d'administration ISE \(expiré\)](#)

[Valider l'état du certificat admin](#)

[plan d'action](#)

[Dépannage](#)

[Cas d'utilisation 1 : Noeud secondaire désinscrit bloqué à l'état distribué \(ise-psn1\)](#)

[Valider l'état](#)

[Solution de contournement](#)

[Cas d'utilisation 2 : Interface utilisateur graphique du noeud secondaire désinscrit inaccessible \(ise-psn2\)](#)

[Valider l'état](#)

[Solution de contournement](#)

[Références](#)

[Pertinent](#)

Introduction

Ce document décrit comment dépanner et renouveler un certificat d'administration Cisco Identity Services Engine (ISE) expiré.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- Déploiement de Cisco ISE.
- Gestion des certificats dans Cisco ISE.

Composants utilisés

Les informations contenues dans ce document sont basées sur la version logicielle suivante :

- Cisco Identity Services Engine (ISE) version 3.3 Patch4.

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.

Informations générales

Ce document porte sur le déploiement distribué ; toutefois, vous pouvez utiliser le même plan de dépannage sur un noeud autonome.

Dans le déploiement distribué ISE, le noeud est soit le noeud d'administration principal (PPAN), soit le noeud secondaire.

Ce document utilise le certificat d'administration ISE comme certificat auto-signé afin de démontrer l'impact d'un certificat expiré, mais cette approche n'est pas recommandée pour un système de production. Il est préférable d'utiliser un certificat signé par l'autorité pour l'administration.

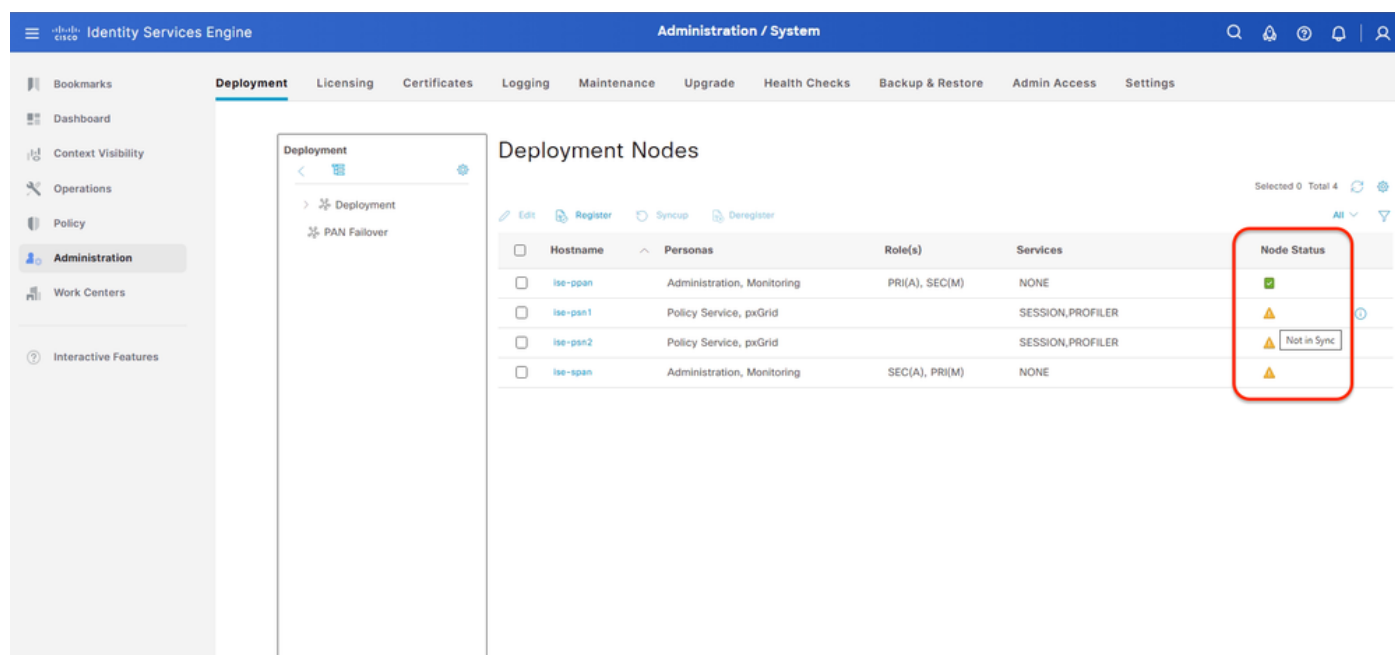
 Remarque : Cisco vous recommande de conserver votre certificat d'administrateur dans l'état d'intégrité et de planifier le renouvellement à l'avance. Consultez ce guide pour vous aider à suivre et à renouveler les certificats système ISE ([Configurer les renouvellements de certificats sur ISE](#)).

Certificat d'administration ISE (expiré)

Valider l'état du certificat admin

Étape 1. Vérifiez l'état du déploiement. Accédez à Administration > System > Deployment.

Vous pouvez vérifier l'état des noeuds secondaires, comme indiqué, les trois noeuds secondaires sont (Non synchronisé).



Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	
ise-psn1	Policy Service, pxGrid		SESSION, PROFILER	 Not in Sync
ise-psn2	Policy Service, pxGrid		SESSION, PROFILER	 Not in Sync
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	 Not in Sync

Étape 2. Vérifiez les alarmes. Accédez à Tableau de bord > Alarmes > (Certificat expiré).

Pour confirmer quel noeud et quel certificat a expiré.



Remarque : Si le noeud d'administration principal (PPAN) a expiré avant un noeud secondaire, vous ne pouvez pas voir d'alarmes de ce noeud, c'est ce qui s'est produit pour le noeud d'administration secondaire (SPAN) dans cette alarme.

Identity Services Engine

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Alarms: Certificate Expired

Description

This certificate has expired! ISE may fail when attempting to establish secure communications with clients. Inter-node communication may also be affected

Suggested Actions

Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can just delete the certificate if it is no longer used. For a system certificate, navigate to Administration > System > Certificate > System Certificates to view details. For a trusted certificate, navigate to Administration > System > Certificate > Trusted Certificates to view details

Rows/Page 3

1

Go

3 Total Rows

Time Stamp

Description

Details

☐ Jan 23 2025 16:00:13.466 PM	Local certificate Default self-signed server certificate expired on Thu; 23 Jan 2025 Server=ise-ppan	
☐ Jan 22 2025 16:37:23.498 PM	Local certificate Default self-signed server certificate expired on Thu; 23 Jan 2025 Server=ise-pan1	
☐ Jan 22 2025 16:36:53.545 PM	Local certificate Default self-signed server certificate expired on Thu; 23 Jan 2025 Server=ise-pan2	

Alarmes (certificat expiré)

Étape 3 : vérification de l'état du certificat d'administration Accédez à Administration > Système > Certificats > Gestion des certificats > Certificats système > Noeud Développer.

1. Noeud d'administration principal (PPAN) :

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade 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 Se...

Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Edit + Generate Self Signed Certificate + Import Export Delete View

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-ppan.kdiab2.local	ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdiab2.local	SAML		SAML_ise-ppan.kdiab2.local	SAML_ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=Certificate Services System Certificate, Certificate Services Endpoint Sub CA - Ise-ppan#00003	pxGrid		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - Ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=ISE Messaging Service, Certificate Services Endpoint Sub CA - Ise-ppan#00004	ISE Messaging Service		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - Ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
ise-psn1 ise-psn2 ise-span							

État du certificat d'administration PPAN

2. Noeuds secondaires.

Pour les noeuds secondaires, il peut s'agir d'une option sur deux et dans les deux cas, vous devez appliquer le même plan d'action :

A. Peut développer le certificat système du noeud et confirmer que le certificat admin a expiré :

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade 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 Se...

Certificate Authority

System Certificates

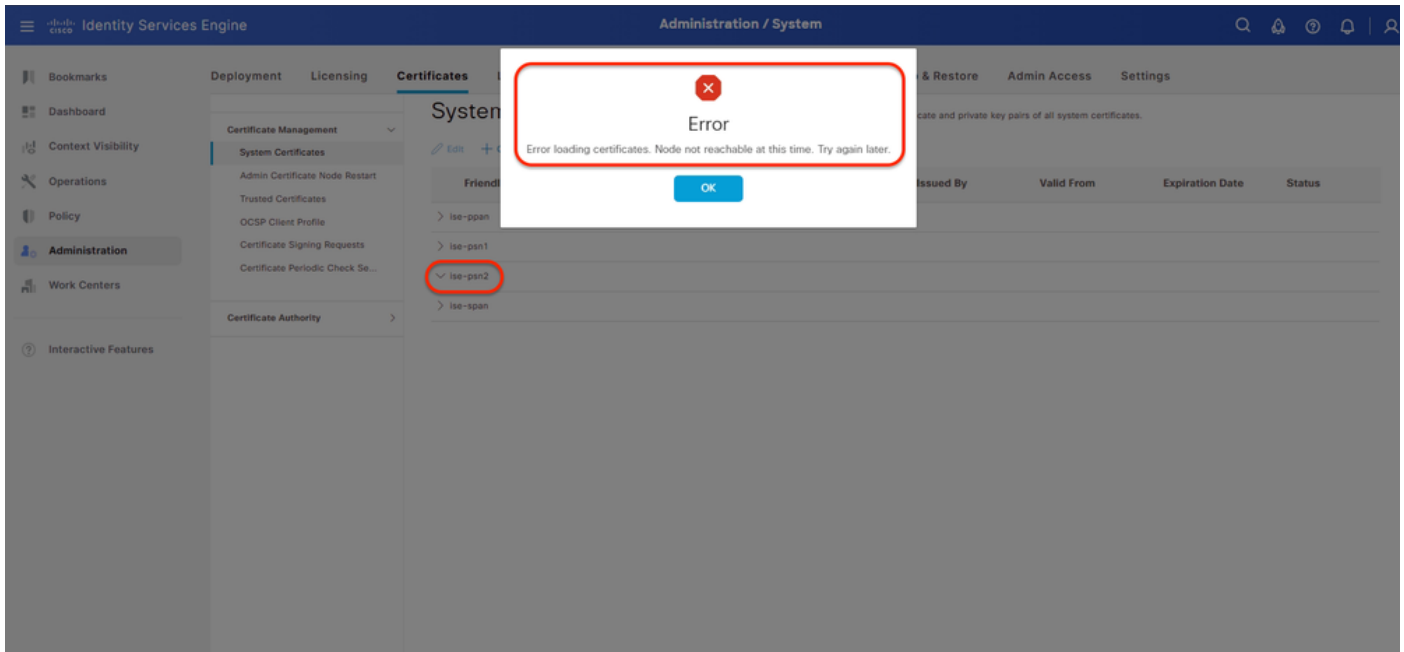
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Edit + Generate Self Signed Certificate + Import Export Delete View

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-ppan							
ise-psn1							
ise-psn2							
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-span.kdiab2.local	ise-span.kdiab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdiab2.local	SAML		SAML_ise-ppan.kdiab2.local	SAML_ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-span.kdiab2.local, OU=Certificate Services System Certificate, Certificate Services Endpoint Sub CA - Ise-span#00005	pxGrid		ise-span.kdiab2.local	Certificate Services Endpoint Sub CA - Ise-span	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-span.kdiab2.local, OU=ISE Messaging Service, Certificate Services Endpoint Sub CA - Ise-span#00006	ISE Messaging Service		ise-span.kdiab2.local	Certificate Services Endpoint Sub CA - Ise-span	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

État du certificat d'administration du noeud secondaire

B. Lancer l'erreur ("Erreur lors du chargement des certificats. Noeud inaccessible pour le moment. Réessayez ultérieurement.") comme indiqué pour (ise-psn2



Noeud secondaire inaccessible

plan d'action

Après avoir confirmé l'expiration du certificat d'administration pour les 4 noeuds, vous devez appliquer ces étapes :

Étape 1 : annulation de l'enregistrement de tous les noeuds secondaires du déploiement distribué (uniquement si le certificat d'administration a expiré)

Accédez à Administration > System > Deployment > Check [✓] des noeuds secondaires et cliquez sur Derregister.

 Remarque : L'annulation de l'enregistrement du noeud signifie qu'il est passé à autonome, puis vous pouvez renouveler le certificat d'administration sur ce noeud.

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	OK
ise-psn1	Policy Service, pxGrid		SESSION, PROFILER	Warning
ise-psn2	Policy Service, pxGrid		SESSION, PROFILER	Warning
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	OK

Annuler l'enregistrement des noeuds secondaires

Remarque : N'oubliez pas de ne plus enregistrer que les noeuds secondaires où le certificat d'administration a déjà expiré et de conserver le reste. Dans ce document, tous les noeuds secondaires ont expiré.

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), PRI(M)	NONE	OK

Tous les noeuds secondaires sont désenregistrés

Étape 2 : renouvellement du certificat d'administration du noeud principal d'administration (PPAN)

1. Accédez à Administration > System > Certificates > Certificate Management > System Certificates > Cliquez sur +Generate Self Signed Certificate:

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade 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 Se...

Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

[Edit](#) [+ Generate Self Signed Certificate](#) [+ Import](#) [Export](#) [Delete](#) [View](#)

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-ppan.kdlab2.local	ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdlab2.local	SAML		SAML_ise-ppan.kdlab2.local	SAML_ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ise-ppan#00003	pxGrid		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=ISE Messaging Service Ice#Certificate Services Endpoint Sub CA - ise-ppan#00004	ISE Messaging Service		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

Générer un nouveau certificat d'administration auto-signé

2. Sélectionnez le noeud d'administration principal (PPAN) (ise-ppan) et remplissez les informations de certificat :

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade 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 Se...

Certificate Authority

Generate Self Signed Certificate

* Select Node **ise-ppan**

Subject

Common Name (CN)
\$FQDN\$

Organizational Unit (OU)
Tech

Organization (O)
KD

City (L)

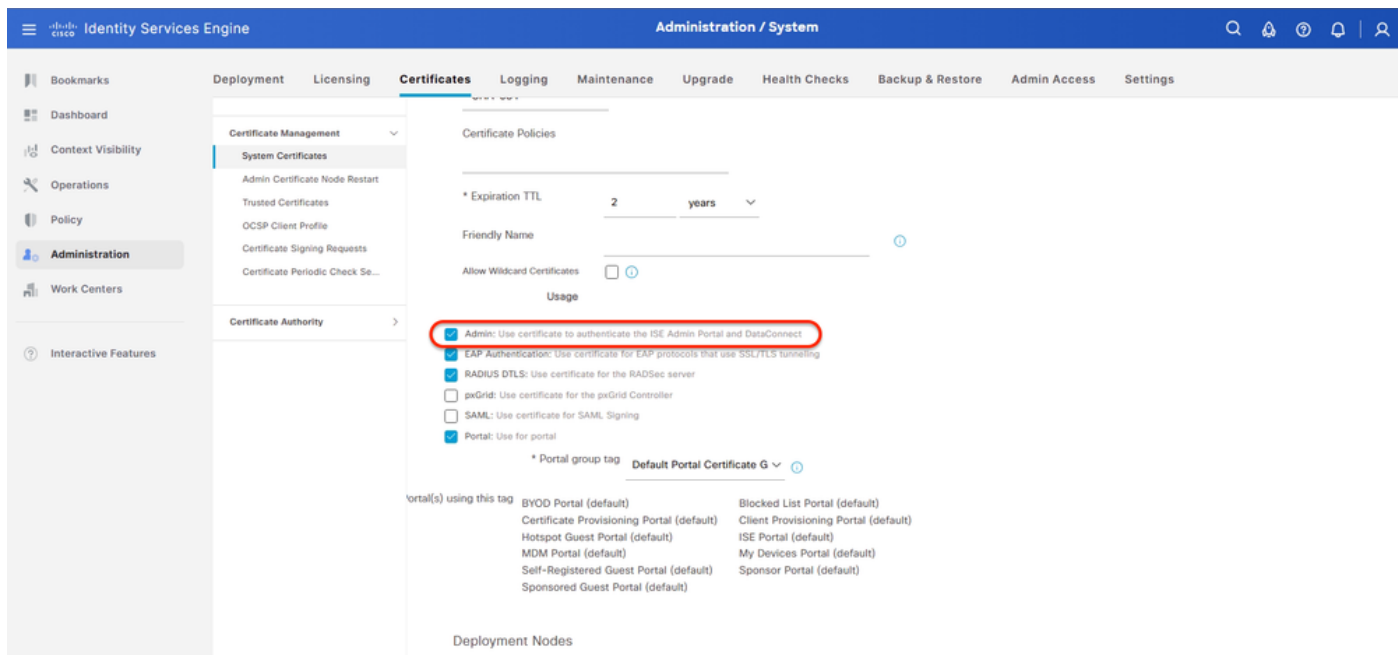
State (ST)

Country (C)

Subject Alternative Name (SAN)

Sélectionnez le noeud d'administration principal (PPAN)

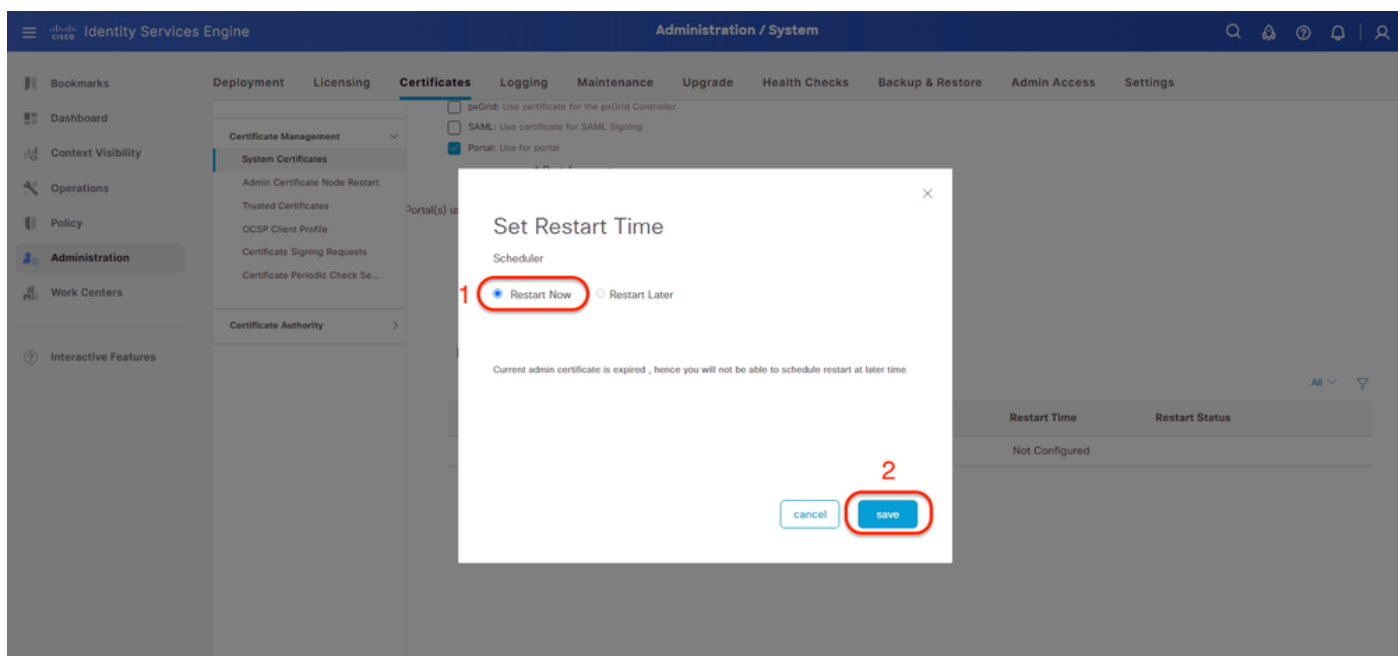
3. Vérifiez [✓] l'utilisation Admin.



Utilisation admin

4. Définissez l'heure de redémarrage sur Redémarrer maintenant pour le noeud d'administration principal (PPAN). Définissez tous les noeuds du déploiement sur Redémarrer maintenant ou Redémarrer ultérieurement.

Une fois que vous avez renouvelé un certificat d'administration (un certificat configuré pour une utilisation d'administration) sur le noeud principal d'administration (PPAN), tous les noeuds de votre déploiement doivent être redémarrés.



Définir l'heure de redémarrage sur Maintenant

5. Cliquez sur Soumettre.



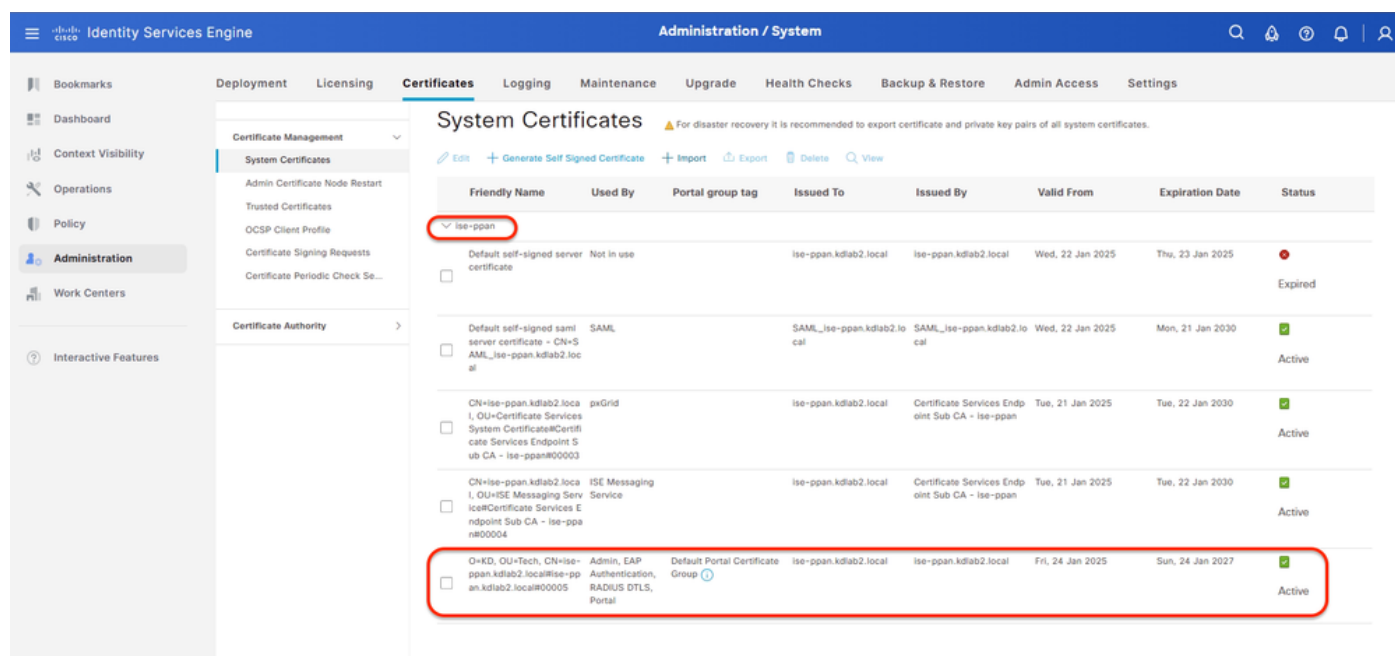
Remarque : Une fois que vous avez renouvelé un certificat d'administration (un certificat

 configuré pour une utilisation d'administration) sur le noeud principal d'administration (PPAN), tous les noeuds de votre déploiement doivent être redémarrés. Vous pouvez redémarrer chaque noeud immédiatement ou programmer les redémarrages ultérieurement. Cette fonction vous permet de vous assurer qu'aucun processus en cours d'exécution n'est interrompu par les redémarrages automatiques, ce qui vous permet de mieux contrôler le processus.

Vous pouvez afficher et modifier les redémarrages planifiés dans la fenêtre Administration > System > Certificates > Admin Certificate Node Restart, qui est disponible à partir de Cisco ISE version 3.3.

6. Vérifiez le nouveau certificat d'administration du noeud d'administration principal (PPAN).

Accédez à Administration > System > Certificates > Certificate Management > System Certificates > Expand (ise-ppan).



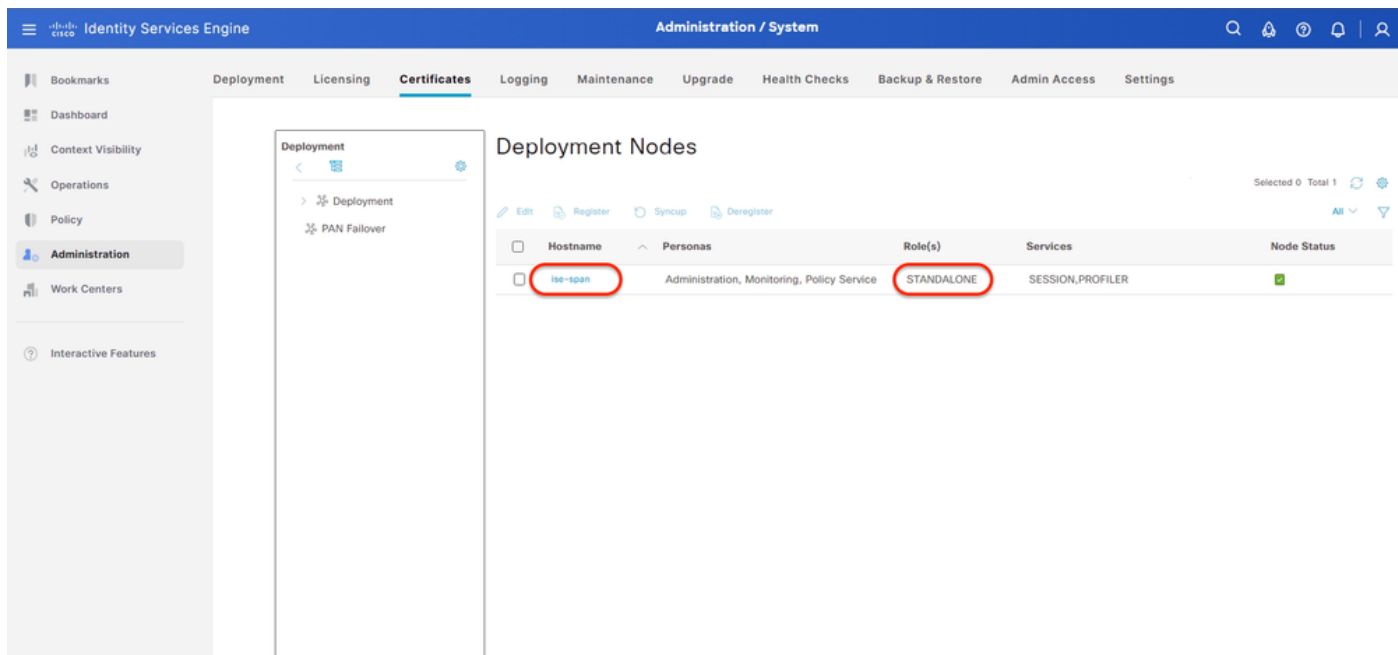
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Not in use		ise-ppan.kdiab2.local	ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdiab2.local	SAML		SAML_ise-ppan.kdiab2.local	SAML_ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=Certificate Services, System Certificate Services Endpoint Sub CA - ise-ppan#00003	paGrid		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=ISE Messaging Service, Endpoint Sub CA - ise-ppan#00004	ISE Messaging Service		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
O=ED, OU=Tech, CN=ise-ppan.kdiab2.local, OU=ise-ppan.kdiab2.local#00005	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ise-ppan.kdiab2.local	ise-ppan.kdiab2.local	Fri, 24 Jan 2025	Sun, 24 Jan 2027	Active

Nouveau certificat d'administration (ise-ppan)

Étape 3 : renouvellement du certificat d'administration des noeuds secondaires

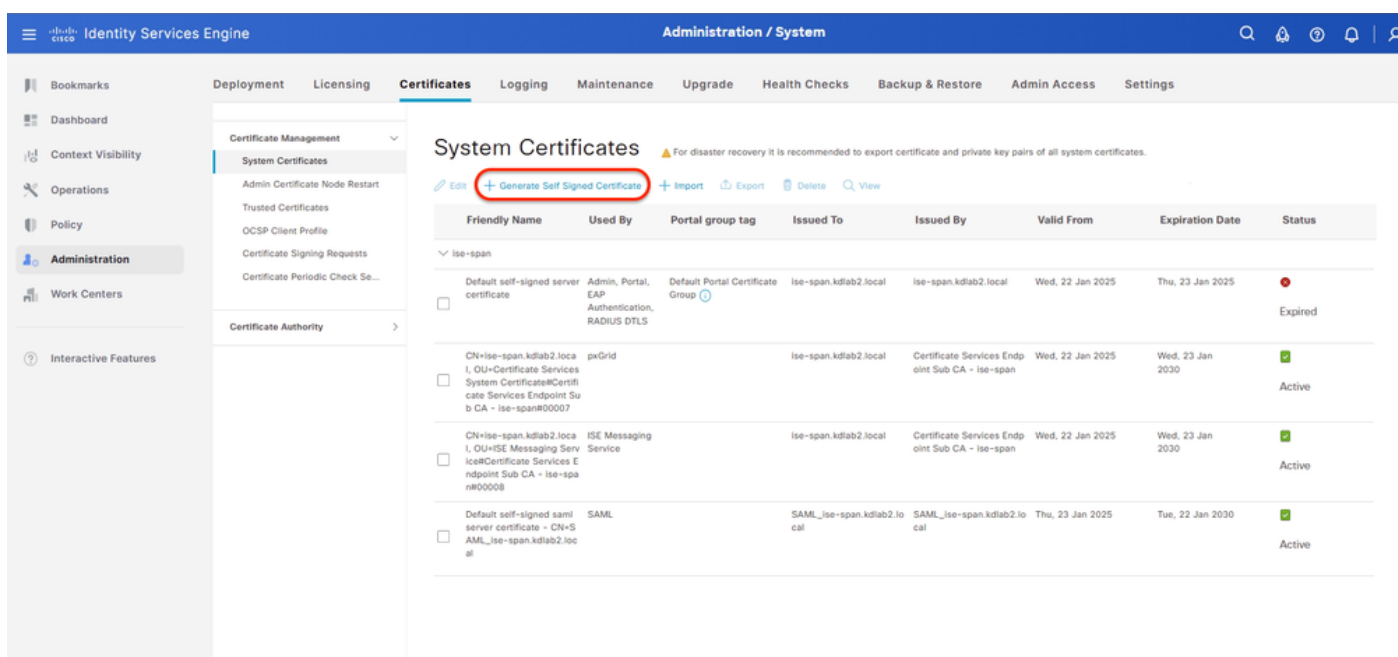
1. Confirmez le noeud secondaire sur le déploiement autonome après la désinscription du déploiement distribué.

Parcourez le noeud via l'interface utilisateur graphique (<https://<FQDN/IP>>) et accédez à Administration > System > Deployment.



(ise-span) sur le déploiement autonome

2. Accédez à Administration > System > Certificates > Certificate Management > System Certificates > Cliquez sur +Generate Self Signed Certificate.



Générer un nouveau certificat d'administration auto-signé

3. Sélectionnez le (ise-span) et remplissez les informations de certificat.

Identity Services Engine Administration / System

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 Se...

Certificate Authority

Generate Self Signed Certificate

* Select Node **ise-span**

Subject

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

Sélectionnez le noeud

4. Vérifiez [✓] l'utilisation Admin.

Identity Services Engine Administration / System

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 Se...

Certificate Authority

* Digest to Sign With **SHA-384**

Certificate Policies

* Expiration TTL **2** years

Friendly Name

Allow Wildcard Certificates ☐

Usage

☒ Admin: Use certificate to authenticate the ISE Admin Portal and DataConnect

☒ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

☒ RADIUS DTLS: Use certificate for the RADSec server

☐ pxGrid: Use certificate for the pxGrid Controller

☐ SAML: Use certificate for SAML Signing

☒ Portal: Use for portal

* Portal group tag **Default Portal Certificate G**

Portal(s) using this tag

BYOD Portal (default)	Blocked List Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	ISE Portal (default)
MDM Portal (default)	My Devices Portal (default)
Self-Registered Guest Portal (default)	Sponsor Portal (default)
Sponsored Guest Portal (default)	

Utilisation admin



Remarque : La modification du certificat du rôle admin sur le noeud ISE redémarre les services.

5. Cliquez sur Soumettre.

6. Vérifiez le nouveau certificat d'administration sur (ise-span).

Naviguez jusqu'à Administration > Système > Certificats > Gestion des certificats > Certificats système > Développer (portée.

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Actions: Edit, Generate Self Signed Certificate, Import, Export, Delete, View

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-span							
Default self-signed server certificate	Not in use		ise-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
O=ED, OU=Tech, CN=ise-span.kdlab2.local@ise-span.kdlab2.local@00009	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ise-span.kdlab2.local	ise-span.kdlab2.local	Fri, 24 Jan 2025	Sun, 24 Jan 2027	Active
CN=ise-span.kdlab2.local, OU=Certificate Services System CertificateEndpoint Sub CA - ise-span@00007	pxGrid		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=ISE Messaging Service, CN=Certificate Services Endpoint Sub CA - ise-span@00008	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
Default self-signed saml server certificate - CN=SAML_ise-span.kdlab2.local	SAML		SAML_ise-span.kdlab2.local	SAML_ise-span.kdlab2.local	Thu, 23 Jan 2025	Tue, 22 Jan 2030	Active

Nouveau certificat d'administration (ise-span)

Étape 4 : enregistrement des noeuds secondaires dans le déploiement distribué

Configurez vos profils et rôles de déploiement comme avant (Admin, MNT, PSN, etc.).

1. À partir de l'interface graphique du noeud principal d'administration (PPAN), accédez à Administration > System > Deployment > cliquez sur Register.

Deployment Nodes

Selected 0 Total 1

Actions: Edit, Register, Sync, Deregister

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), PRI(M)	NONE	Active

Interface graphique utilisateur du noeud d'administration principal (PPAN)

2. Saisissez le nom de domaine complet et les informations d'identification du noeud secondaire (Nom d'utilisateur/Mot de passe).

Entrez le nom de domaine complet (FQDN) pouvant être résolu par DNS du noeud autonome que vous allez enregistrer. Le nom de domaine complet du (PPAN) et le noeud en cours

d'enregistrement doivent pouvoir être résolus l'un par rapport à l'autre.

Saisir l'accès au noeud secondaire

3. Activez la personne et les services appropriés.

Enregistrer le noeud secondaire (ise-span)

Étape 5 : vérification de l'état du déploiement

Accédez à Administration > System > Deployment.

Identity Services Engine Administration / System

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

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

Deployment > Deployment > PAN Failover

Deployment Nodes

Selected 0 Total 2

Edit Register Syncup Deregister

☐	Hostname	Personas	Role(s)	Services	Node Status
☐	ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✔
☐	ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	✔

(ise-span) Ajouté au déploiement

Dépannage

Cas d'utilisation 1 : Noeud secondaire désinscrit bloqué à l'état distribué (ise-psn1)

Valider l'état

Étape 1 : confirmation de l'état du déploiement distribué

Dans l'interface graphique du noeud d'administration principal (PPAN), accédez à Administration > System > Deployment. Vous pouvez confirmer que ce noeud (ise-psn1) est déjà désinscrit.

Identity Services Engine Administration / System

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

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

Deployment > Deployment > PAN Failover

Deployment Nodes

Selected 0 Total 2

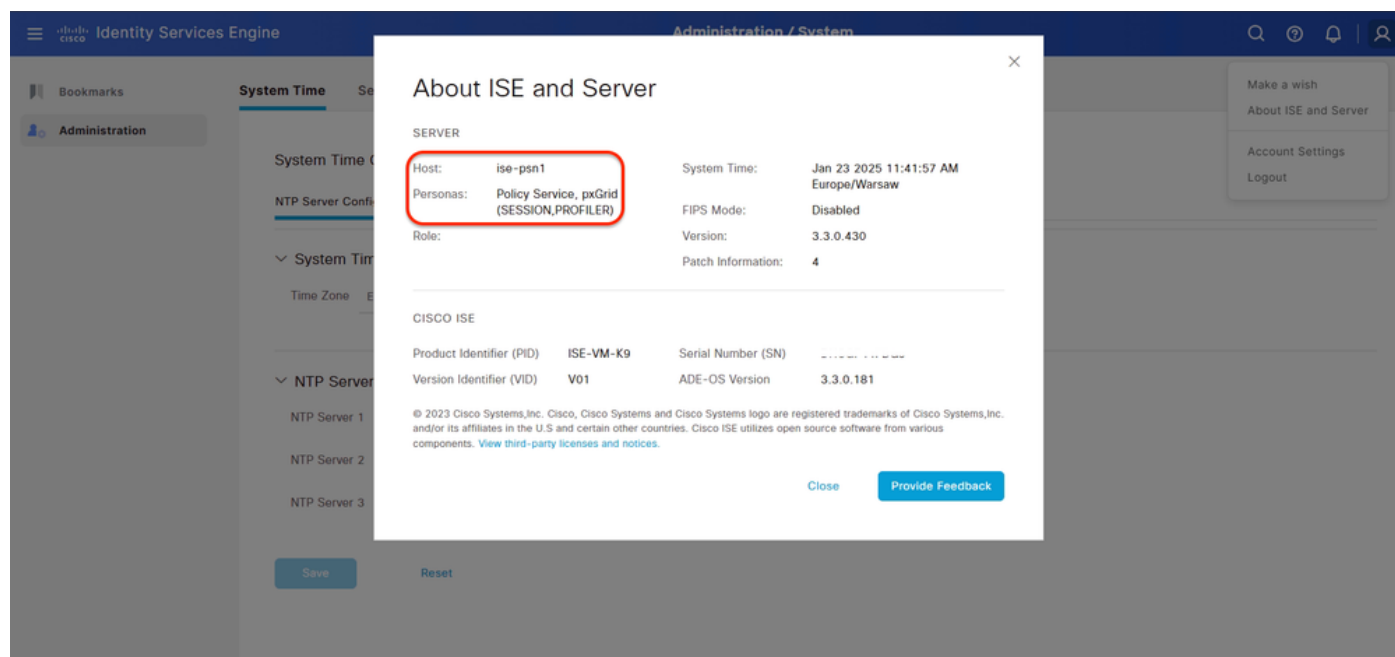
Edit Register Syncup Deregister

☐	Hostname	Personas	Role(s)	Services	Node Status
☐	ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✔
☐	ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	✔

Noeuds de déploiement (PPAN)

Étape 2 : confirmation de l'état du noeud (ise-psn1)

Parcourez le noeud secondaire via l'interface utilisateur graphique (<https://ise-psn1.kdlab.local>) et naviguez Login > About ISE and Server.

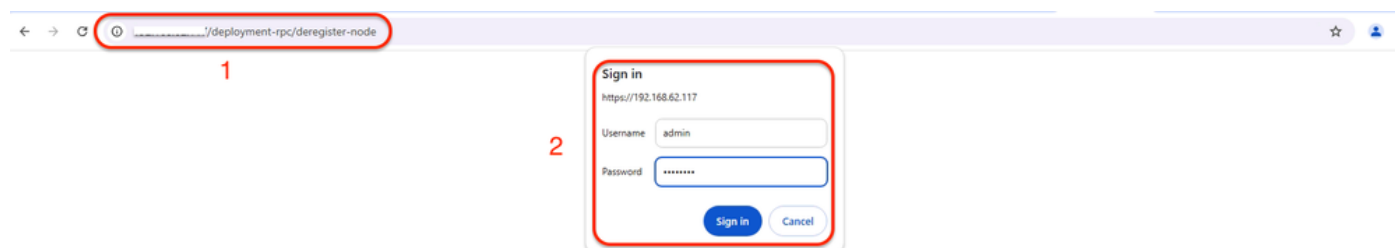


Noeud secondaire (ise-psn1) bloqué sur l'état de déploiement distribué

Solution de contournement

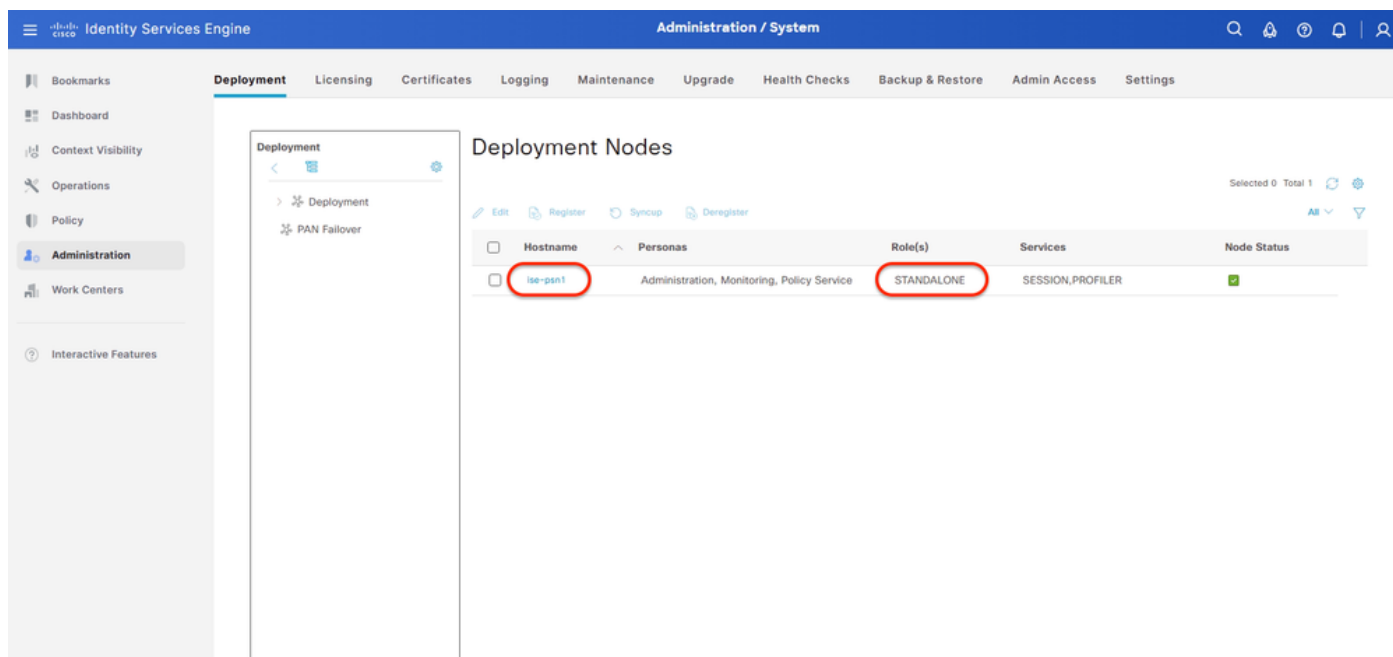
Étape 1 : annulation de l'enregistrement du noeud (ise-psn1) manuellement

Appliquer le noeud (ise-psn1) au déploiement autonome via l'interface utilisateur graphique (<https://<ise-psn1 IP>/deployment-rpc/deregister-node>).



Désinscription manuelle du noeud - GUI

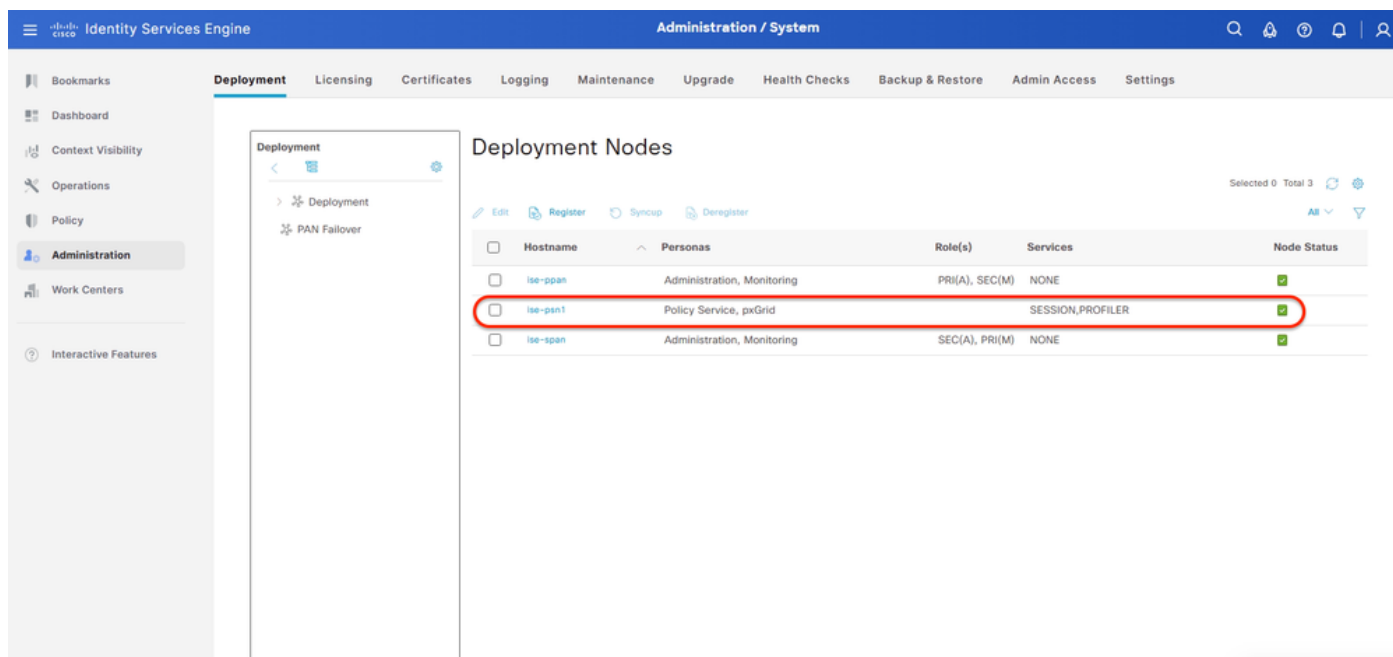
Étape 2 : vérification du (ise-psn1) lors du déploiement autonome



(ise-psn1) sur le déploiement autonome

Étape 3. Une fois que vous avez confirmé le statut autonome du noeud, suivez les mêmes étapes dans la section Plan d'action :

1. Renouvelez le certificat d'administration du noeud (ise-psn1).
2. Enregistrez le noeud (ise-psn1) dans le déploiement distribué.
3. Vérifiez l'état du déploiement.



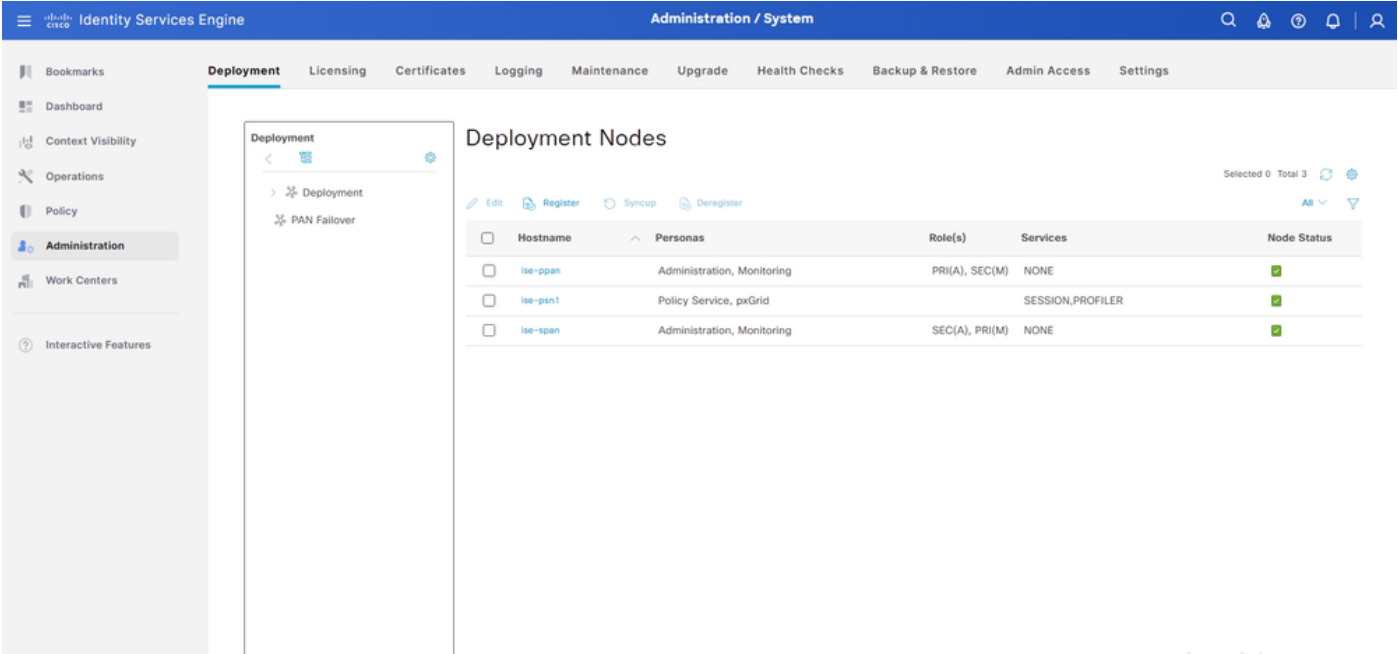
(ise-psn1) Ajouté au déploiement

Cas d'utilisation 2 : Interface utilisateur graphique du noeud secondaire désinscrit inaccessible (ise-psn2)

Valider l'état

Étape 1 : confirmation de l'état du déploiement distribué

Dans l'interface graphique du noeud d'administration principal (PPAN), accédez à Administration > System > Deployment. Vous pouvez confirmer que ce noeud (ise-psn2) est déjà désinscrit.



Noeuds de déploiement (PPAN)

Étape 2. Confirmez le (ise-psn2) état du noeud.

En raison de l'expiration du certificat d'administration dans certains cas, vous pouvez rencontrer ces symptômes :

- (ise-psn2) GUI inaccessible.
- (ise-psn2) CLI (show application status ise) L'application ISE est bloquée (en cours d'initialisation ou non en cours d'exécution).
- (ise-psn2) CLI (show tech) le noeud déjà en déploiement autonome.

```
*****
Displaying ISE deployment ...
*****
Node Config Details

NAME                PERSONA                ROLE                ACTIVE                REPLICATION
-----
ise-psn2            PAN,MNT,PSN           STANDALONE ACTIVE           SYNC COMPLETED
```

(ise-psn2) sur le déploiement autonome

Solution de contournement

Étape 1 : renouvellement du certificat d'administration du noeud (ise-psn2)

1. Connectez-vous à (ise-psn2) via CLI.
2. Entrez application configure ise.
3. Entrez 31 ([31] Generate Self-Signed Admin Certificate).
4. Voulez-vous continuer ? y/[n] : o
5. Voulez-vous remplacer le certificat existant après la génération ? y/[n] : o

```

ise-psn2/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Reset Upgrade Tables
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[30]Fetch SGA/PGA Memory usage
[31]Generate Self-Signed Admin Certificate
[32]View Certificates in NSSDB or CA_NSSDB
[33]Recreate REPLOGNS tablespace
[34]View Native IPsec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
[38]Localised ISE Install
[39]Reset System 360 Monitoring Page
[40]Enable/Disable Explicit EC Check
[41]Gather Diagnostic data for Certificates
[42]Enable/Disable Parse SAN DirName Extension
[0]Exit

31
After this operation, the ISE node will restart
Do you want to continue? y/[n]: y
Certificate Subject
  *Common Name (CN) : ise-psn2.kdlab2.local
  Enter Organization Unit (OU) : Tech
  Enter Organization (O) : KD
Do you want to replace existing certificate after generation? y/[n]: y
Old Memory Size : 32639004

```


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.