

Verlopen ISE-beheercertificaat voor probleemoplossing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[ISE-beheercertificaat \(verlopen\)](#)

[Status van beheercertificaat valideren](#)

[Actieplan](#)

[Problemen oplossen](#)

[Use Case 1: Gederegistreerd secundair knooppunt gekoppeld aan gedistribueerde status \(ise-psn1\)](#)

[De status valideren](#)

[Tijdelijke oplossing](#)

[Use Case 2: Gederegistreerd secundair knooppunt GUI onbereikbaar \(ise-psn2\)](#)

[De status valideren](#)

[Tijdelijke oplossing](#)

[Referenties](#)

[relevant](#)

Inleiding

Dit document beschrijft hoe u een verlopen Cisco Identity Services Engine (ISE) Admin-certificaat kunt oplossen en verlengen.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco ISE-implementatie.
- Certificaatbeheer in Cisco ISE.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversie:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document richt zich op de gedistribueerde inzet; u kunt echter hetzelfde plan voor probleemoplossing gebruiken voor zelfstandige knooppunten.

In ISE gedistribueerde implementaties is het knooppunt ofwel Primair Admin Node (PAN) of secundair.

Dit document gebruikt het ISE Admin-certificaat als een zelfondertekend certificaat om het effect van het verlopen certificaat aan te tonen, maar deze benadering wordt niet aanbevolen voor een productiesysteem. Het is beter om door de overheid ondertekend certificaat te gebruiken voor beheerdersgebruik.

 Opmerking: Cisco raadt u aan uw Admin-certificaat in de gezondheidstoestand te houden en de verlenging van te voren te plannen, deze handleiding te vinden om u te helpen de ISE-systeemcertificaten te volgen en te vernieuwen ([Certificaat verlengen op ISE configureren](#)).

ISE-beheercertificaat (verlopen)

Status van beheercertificaat valideren

Stap 1. Controleer de implementatiestatus. Navigeer naar Beheer > Systeem > Implementatie.

U kunt de status van de secundaire knooppunten controleren, zoals aangegeven, de drie secundaire knooppunten zijn (niet in sync).

Identity Services Engine Administration / System

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

Deployment Nodes

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	⚠
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	⚠

Implementatiestatus

Stap 2. Controleer het alarm. Navigeer naar Dashboard > Alarmen > (certificaat verlopen).

Om te bevestigen welk knooppunt en welk certificaat is verlopen.

 **Opmerking:** Als het Primaire Admin Node (PPAN) is verlopen voordat een secundair knooppunt wordt weergegeven, kunt u geen alarmen van dat knooppunt zien, dat is wat er in dit alarm gebeurde voor het secundaire Admin Node (SPAN).

Identity Services Engine 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 1 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-psn1	
Jan 22 2025 16:36:53.545 PM	Local certificate Default self-signed server certificate expired on Thu: 23 Jan 2025 Server=ise-psn2	

Alarmen (certificaat verlopen)

Stap 3. Controleer de status van het beheercertificaat. Navigeren naar Beheer > Systeem > Certificaten > Certificaatbeheer > Systeemcertificaten > Knooppunt uitvouwen.

1. Primair beheerknooppunt (PAN):

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate Management

System Certificates

Admin Certificate Node RestartTrusted CertificatesOCSP Client ProfileCertificate Signing RequestsCertificate Periodic Check Se...

Certificate Authority

System Certificates

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

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-ppan							
☐ 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=SA ML_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 Ica@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
> ise-psn1							
> ise-psn2							
> ise-span							

Status PAN-beheercertificaat

2. Tweede knooppunten.

Voor de secundaire knooppunten kan het 1 van 2 opties zijn en in beide gevallen moet u hetzelfde actieplan toepassen:

A. Kan het certificaat van het knoopsysteem uitbreiden en bevestigen dat het beheercertificaat is verlopen:

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate Management

System Certificates

Admin Certificate Node RestartTrusted CertificatesOCSP Client ProfileCertificate Signing RequestsCertificate Periodic Check Se...

Certificate Authority

System Certificates

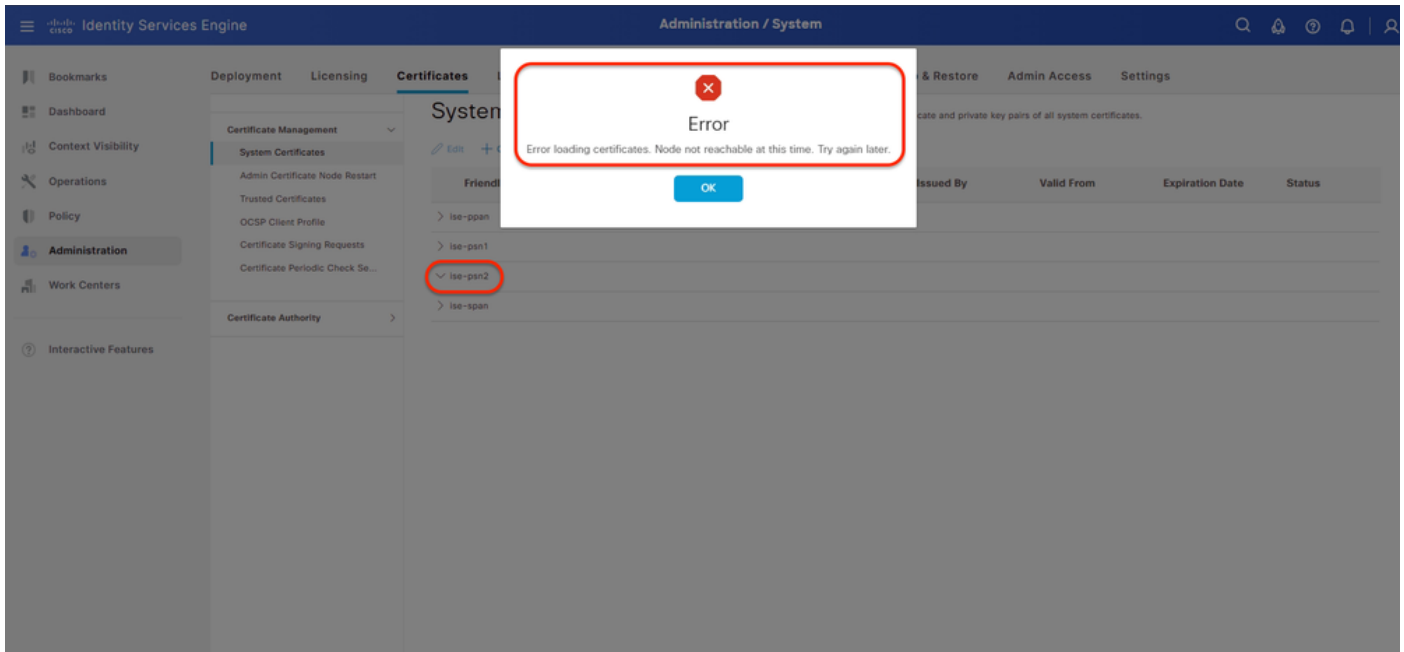
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
> ise-ppan							
> ise-psn1							
> ise-psn2							
ise-span							
☐ Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
☐ Default self-signed saml server certificate - CN=SA ML_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-span.kdlab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise-span#00005	pxGrid		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
☐ CN=ise-span.kdlab2.local, OU=ISE Messaging Service Ica@Certificate Services Endpoint Sub CA - ise-span#00006	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

Certificaatstatus secundair knooppunt

B. Gooi fout ("Fout bij laden van certificaten. Knooppunt niet bereikbaar op dit moment. Probeer het later opnieuw.") zoals getoond voor (ise-psn2



Secundair knooppunt niet bereikbaar

Actieplan

Nadat u hebt bevestigd dat het beheercertificaat voor alle vier knooppunten is verlopen, moet u de volgende stappen toepassen:

Stap 1. Registreer alle secundaire knooppunten uit de gedistribueerde implementatie (alleen als het beheercertificaat is verlopen).

Navigeer naar Beheer > Systeem > implementatie > Controleer [✓] van de secundaire knooppunten en klik op Registreren.



Opmerking: Deregistreren van het knooppunt betekent dat het wordt verplaatst naar standalone dan kunt u het beheercertificaat op dit knooppunt verlengen.

Deployment Nodes

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-pan1	Policy Service, pxGrid		SESSION, PROFILER	⚠
ise-pan2	Policy Service, pxGrid		SESSION, PROFILER	⚠
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	⚠

Secundaire knooppunten verwijderen

Opmerking: Vergeet niet om alleen secundaire knooppunten te deregistreren waar het beheercertificaat al is verlopen en de rest te bewaren. In dit document zijn alle secundaire knooppunten verlopen.

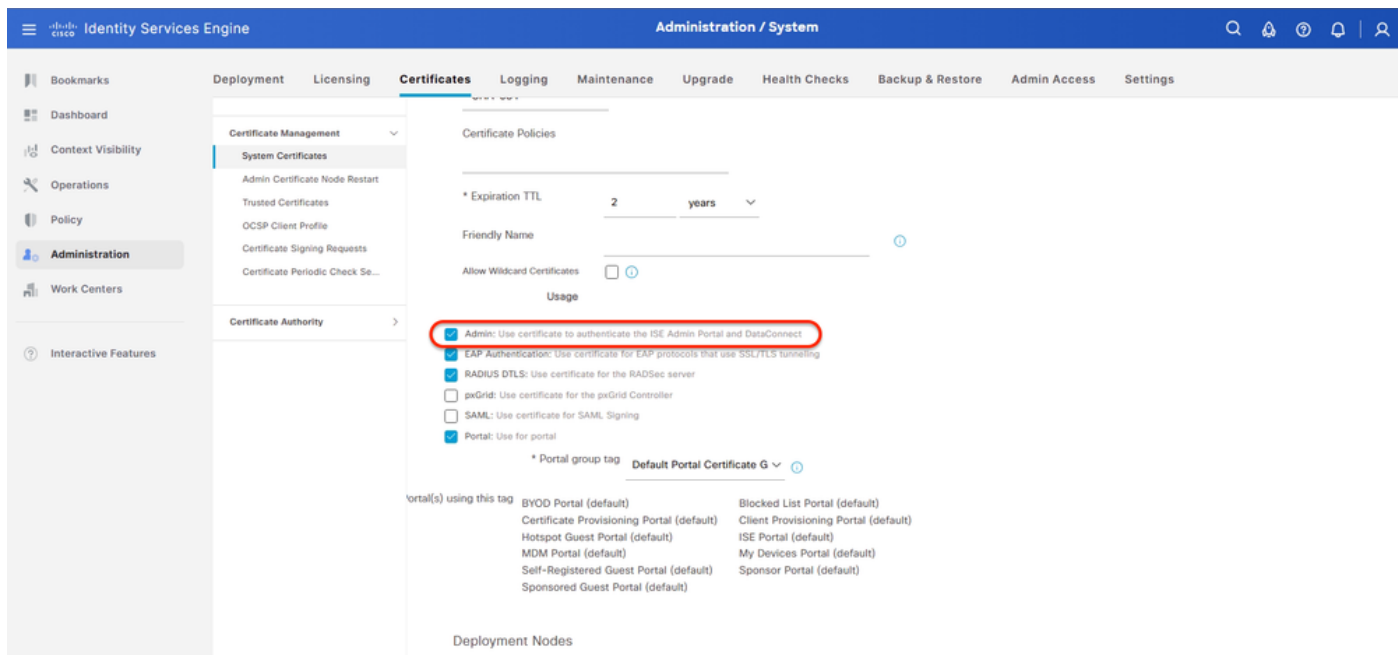
Deployment Nodes

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

Alle secundaire knooppunten zijn gedereguleerd

Stap 2. Verleng het beheercertificaat van het primaire beheerknooppunt (PAN).

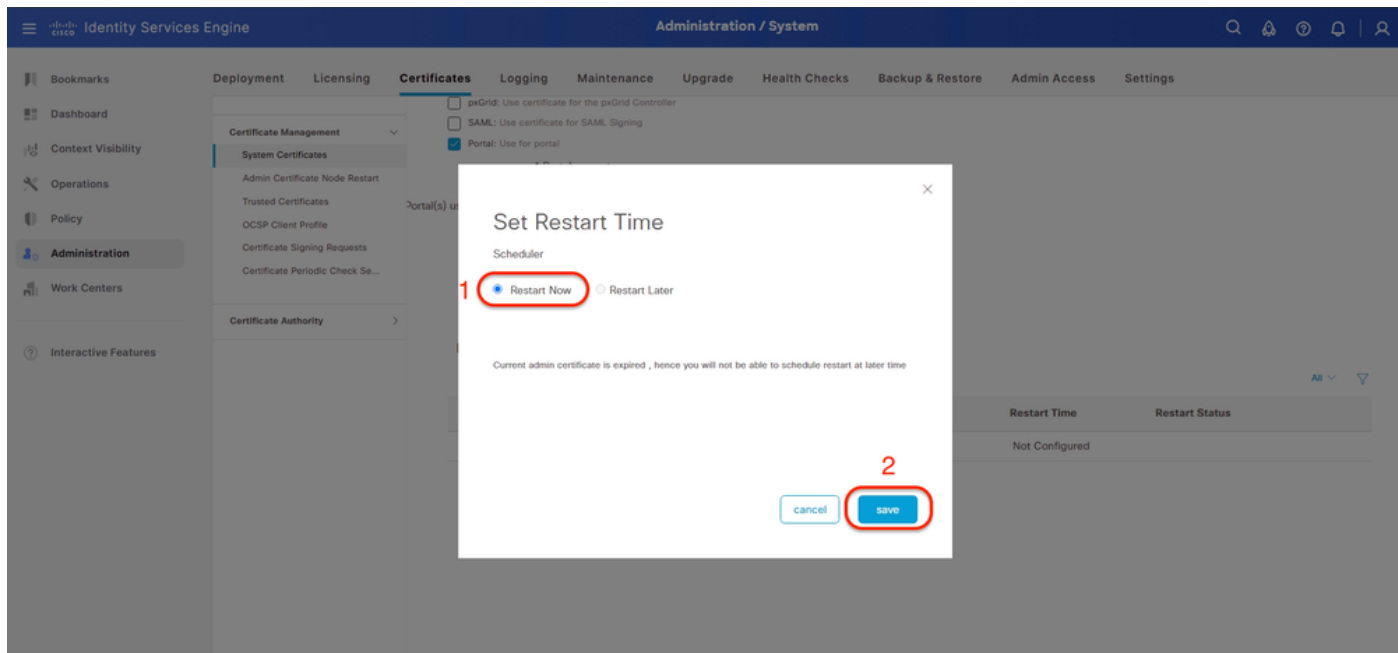
1. Navigeren naar Beheer > Systeem > Certificaten > Certificaatbeheer > Systeemcertificaten > Klik op +Generate Self Signed Certificate:



Admin-gebruik

4. Stel de herstarttijd in om nu opnieuw te starten voor het primaire beheerknooppunt (PAN). Stel alle knooppunten op de implementatie in om nu opnieuw te starten of later opnieuw te starten.

Nadat u een beheercertificaat hebt verlengd (een certificaat dat is geconfigureerd voor beheerdersgebruik) op het primaire beheerknooppunt (PAN), moeten alle knooppunten in uw implementatie opnieuw worden gestart.



Stel herstarttijd in op nu

5. Klik op Indienen.

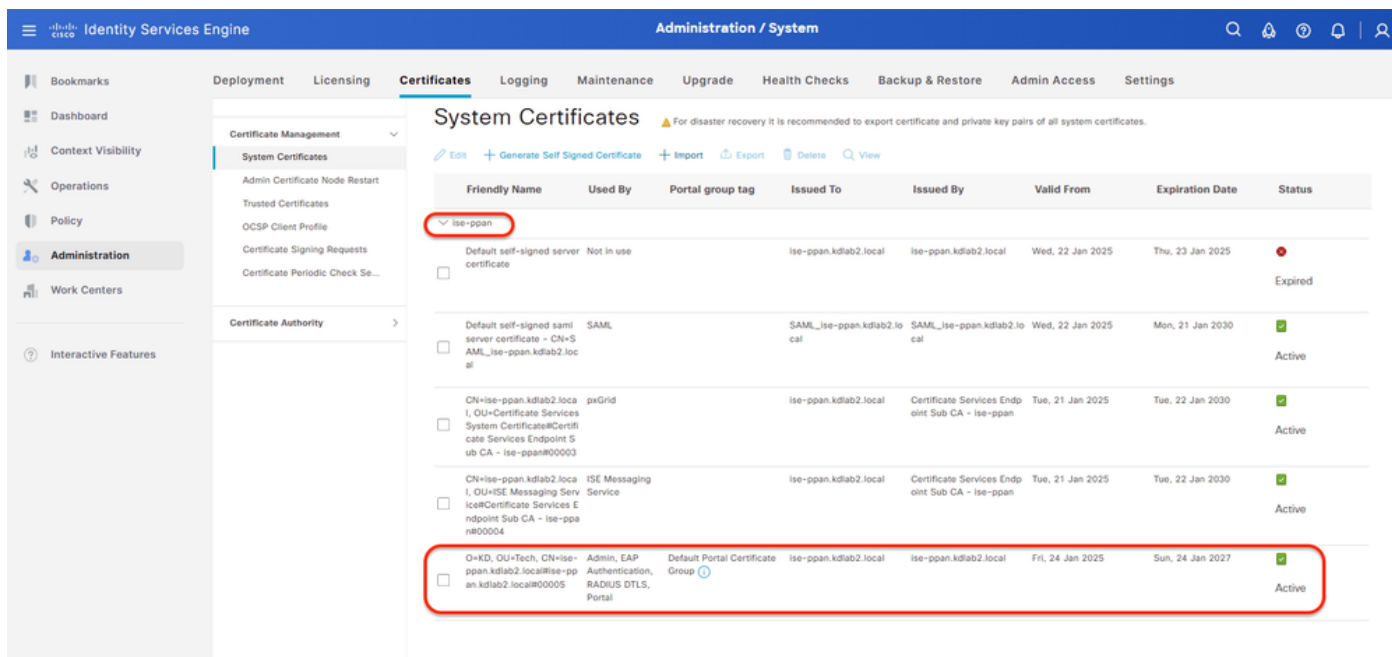
 **Opmerking:** Nadat u een beheercertificaat hebt verlengd (een certificaat dat is geconfigureerd voor beheerdersgebruik) op het primaire beheerknooppunt (PAN) moeten

 alle knooppunten in uw implementatie opnieuw worden gestart. U kunt elk knooppunt direct opnieuw opstarten of de herstart later plannen. Met deze functie kunt u ervoor zorgen dat geen actieve processen worden verstoord door de automatische herstart, waardoor u meer controle over het proces.

U kunt de geplande herstart bekijken en bewerken in het venster Beheer > Systeem > Certificaten > Admin Certificate Node Herstart, dat beschikbaar is via Cisco ISE-software release 3.3.

6. Controleer het nieuwe beheercertificaat van het primaire beheerknooppunt (PAN).

Navigeer naar Beheer > Systeem > Certificaten > Certificaatbeheer > Systeemcertificaten > Uitvouwen (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	peGrid		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
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

Nieuw Admin-certificaat (ISE-ppan)

Stap 3. Verleng het beheercertificaat van de secundaire knooppunten.

1. Bevestig het secundaire knooppunt van standalone implementatie na uitschrijving van de gedistribueerde implementatie.

Blader door de knooppunt via GUI (<https://<FQDN/IP>>) en navigeer naar Beheer > Systeem > implementatie.

The screenshot shows the 'Deployment Nodes' table in the Identity Services Engine Administration / System interface. The table has columns: Hostname, Personas, Role(s), Services, and Node Status. One row is visible with 'ise-span' as the Hostname, 'Administration, Monitoring, Policy Service' as the Personas, 'STANDALONE' as the Role(s), 'SESSION_PROFILER' as the Services, and a green checkmark as the Node Status. The 'ise-span' and 'STANDALONE' are circled in red.

Hostname	Personas	Role(s)	Services	Node Status
ise-span	Administration, Monitoring, Policy Service	STANDALONE	SESSION_PROFILER	✓

(ise-span) bij standalone implementatie

2. Navigeer naar Beheer > Systeem > Certificaten > Certificaatbeheer > Systeemcertificaten > Klik op +Generate Self Signed Certificate.

The screenshot shows the 'System Certificates' section in the Identity Services Engine Administration / System interface. The '+ Generate Self Signed Certificate' button is highlighted with a red circle. Below the button is a table listing system certificates.

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-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
CN=ise-span.kdlab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint 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 Ice@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

Nieuw zelfondertekend beheercertificaat genereren

3. Selecteer de (ise-span) en vul de certificaatinformatie in.

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) SFQDN\$

Organizational Unit (OU) Tech

Organization (O) KQ

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

Selecteer het knooppunt

4. Controleer [✓] het gebruik van de beheerder.

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

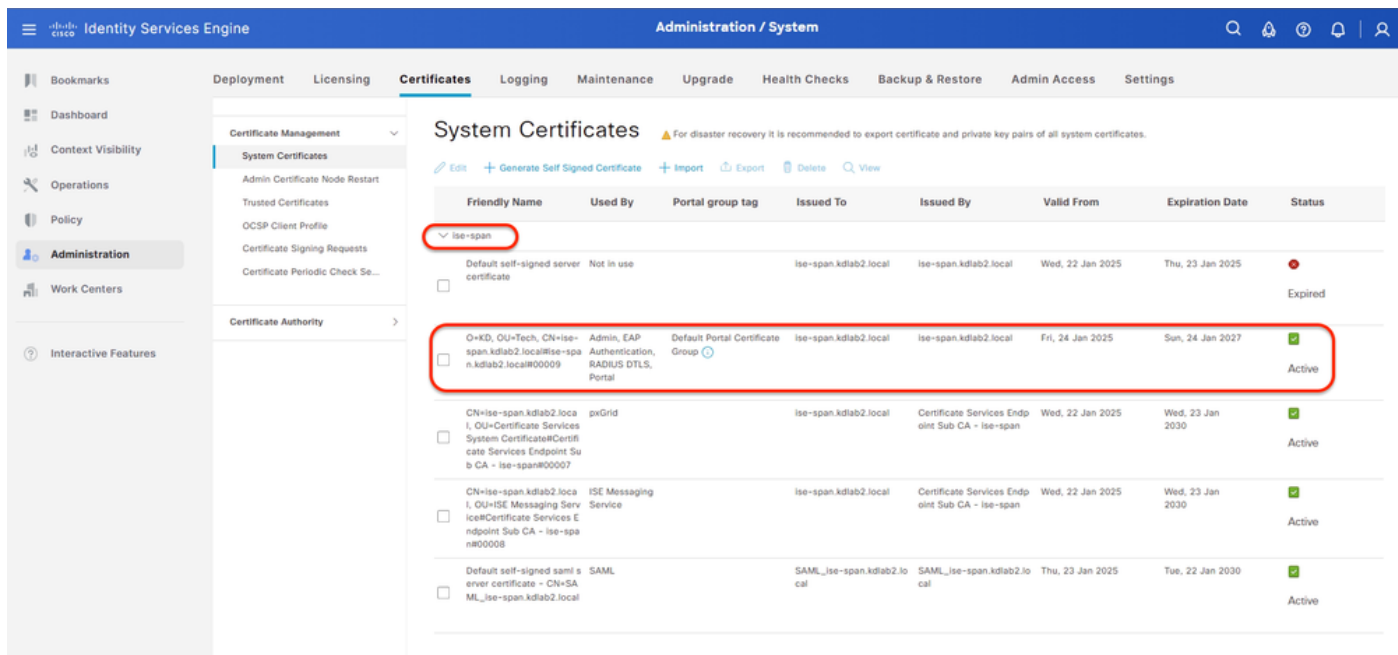
Admin-gebruik

Opmerking: Het wijzigen van het certificaat van de admin rol certificaat op ISE knooppunt herstart services.

5. Klik op Indienen.

6. Controleer het nieuwe beheercertificaat op (ise-span).

Naar navigeren Beheer > Systeem > Certificaten > Certificaatbeheer > Systeemcertificaten > Uitvouwen (ise-span).



System Certificates

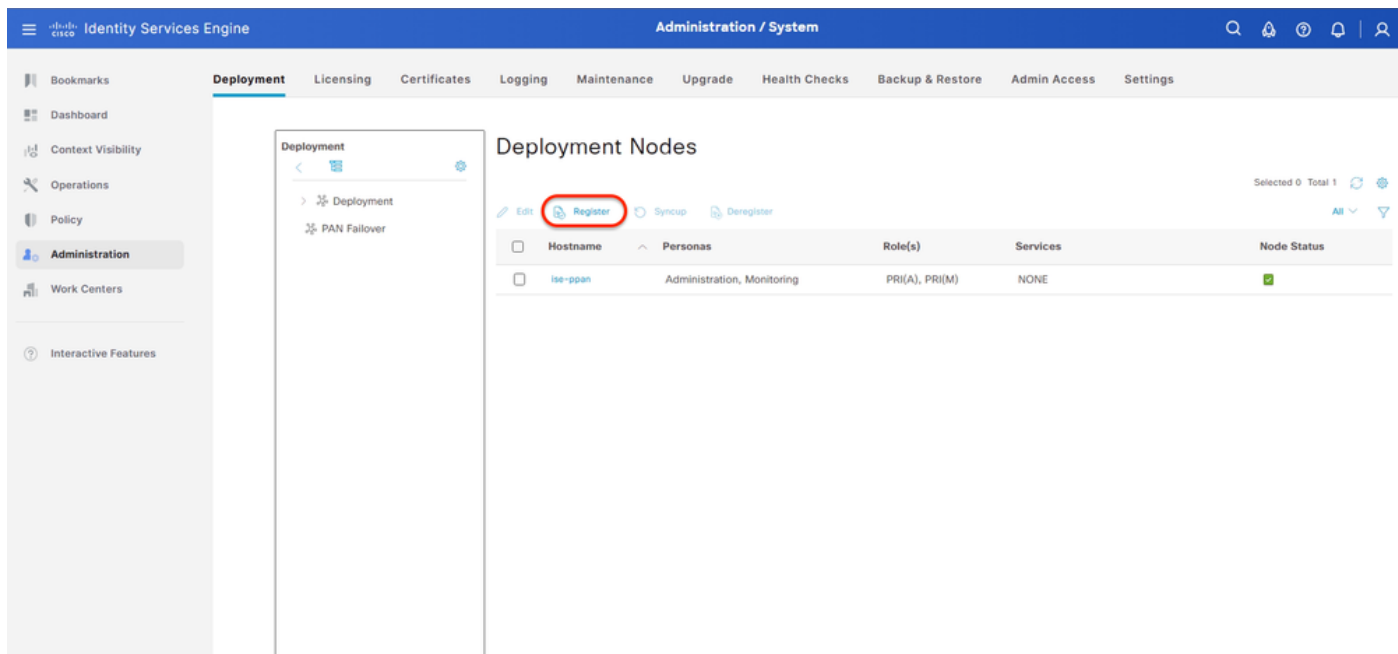
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Not in use		Ise-span.kdlab2.local	Ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Ise-span	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal 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 Certificates, Certificate Services Endpoint 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, Ise-span.kdlab2.local#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=Ise-span.kdlab2.local	SAML		SAML_Ise-span.kdlab2.local	SAML_Ise-span.kdlab2.local	Thu, 23 Jan 2025	Tue, 22 Jan 2030	Active

Nieuw beheercertificaat (Ise-span)

Stap 4. Registreer de secundaire knooppunten voor de gedistribueerde implementatie.

Stel uw implementatiepersona's en rollen in zoals deze voorheen waren (Admin, MNT, PSN, enzovoort).

1. Van primaire Admin Node (PAN) GUI. Navigeer naar Beheer > Systeem > Implementatie > Klik op Registreren.



Deployment Nodes

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

Primaire beheerder, knooppunt (PAN) GUI

2. Voer de FQDN en referenties van het secundaire knooppunt in (gebruikersnaam/wachtwoord).

Voer de DNS-oplosbare, volledig gekwalificeerde domeinnaam (FQDN) in van de standalone knooppunt dat u gaat registreren. FQDN (PPAN) en het knooppunt dat wordt geregistreerd,

moeten onderling oplosbaar zijn.

Identity Services Engine Administration / System

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

Deployment Nodes List > Specify Hostname

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

Host FQDN*
ise-span.kdlab2.local

User Name*
admin

Password*

Next Cancel

Toegang tot secundair knooppunt

3. Schakel de juiste persoon en diensten in.

Identity Services Engine Administration / System

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

Deployment Nodes List > Configure Node

Register ISE Node - Step 2: Configure Node

General Settings

Hostname ise-span

FQDN ise-span.kdlab2.local

IP Address

Node Type Identity Services Engine (ISE)

Role SECONDARY

Administration

Monitoring

Role PRIMARY

Other Monitoring Node ise-ppan

Dedicated MnT

Secundair knooppunt registreren (ISE-span)

Stap 5. Controleer de implementatiestatus.

Ga naar Beheer > Systeem > Implementatie.

Identity Services Engine Administration / System

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

Deployment Nodes

Selected 0 Total 2

Hostnames	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) toegevoegd aan de implementatie

Problemen oplossen

Use Case 1: Gederegistreerd secundair knooppunt gekoppeld aan gedistribueerde status (ise-psn1)

De status valideren

Stap 1. Bevestig de status van de gedistribueerde implementatie.

Van primaire Admin Node (PAN) GUI. Navigeer naar Beheer > Systeem > Implementatie. U kunt controleren of dit knooppunt (ise-psn1) al uit het register is verwijderd.

Identity Services Engine Administration / System

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

Deployment Nodes

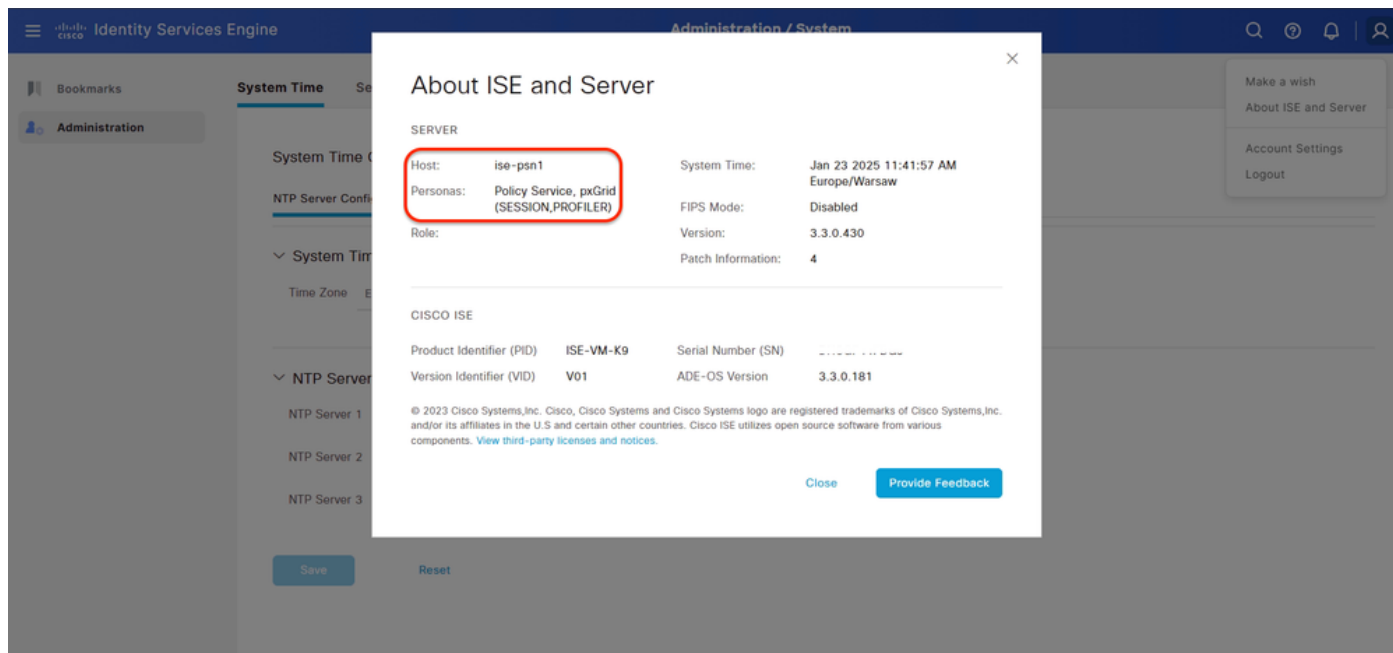
Selected 0 Total 2

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

(PAN) implementatieknooppunten

Stap 2. Bevestig de status van het (ise-psn1) knooppunt.

Blader door het secundaire knooppunt via GUI (<https://ise-psn1.kdlab.local>) en navigeer Login > Info over ISE en server.

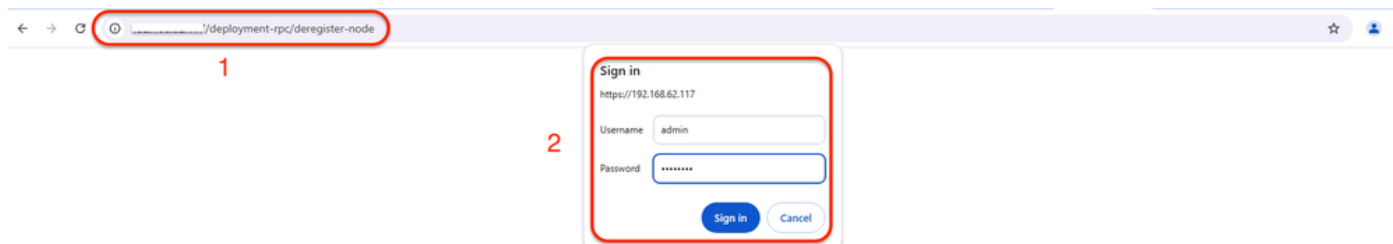


Secundair knooppunt (ise-psn1) gekoppeld aan gedistribueerde implementatiestatus

Tijdelijke oplossing

Stap 1. Registreer handmatig het knooppunt (ise-psn1).

Versterk de standalone implementatie van het (ise-psn1) knooppunt via GUI (<https://<ise-psn1 IP>/implementation-rpc/deregister-node>).



Registreer het knooppunt handmatig - GUI

Stap 2. Controleer de (ise-psn1) nu op standalone implementatie.

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 'Deployment Nodes' and shows a table with the following columns: Hostname, Personas, Role(s), Services, and Node Status. The table contains one row for 'ise-psn1' with the role 'STANDALONE' and status 'OK'. The 'ise-psn1' hostname and 'STANDALONE' role are circled in red.

Hostname	Personas	Role(s)	Services	Node Status
ise-psn1	Administration, Monitoring, Policy Service	STANDALONE	SESSION, PROFILER	OK

(ise-psn1) op standalone implementatie

Stap 3. Zodra u het knooppunt over de status van de standalone kunt bevestigen, gaat u verder met dezelfde stappen in de sectie Actieplan:

1. Verleng beheercertificaat van het knooppunt (ise-psn1).
2. Registreer het knooppunt (ise-psn1) naar de gedistribueerde implementatie.
3. Controleer de implementatiestatus.

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 'Deployment Nodes' and shows a table with the following columns: Hostname, Personas, Role(s), Services, and Node Status. The table contains three rows: 'ise-ppan', 'ise-psn1', and 'ise-span'. The 'ise-psn1' row is highlighted with a red circle. The 'ise-psn1' hostname and 'STANDALONE' role are circled in red.

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

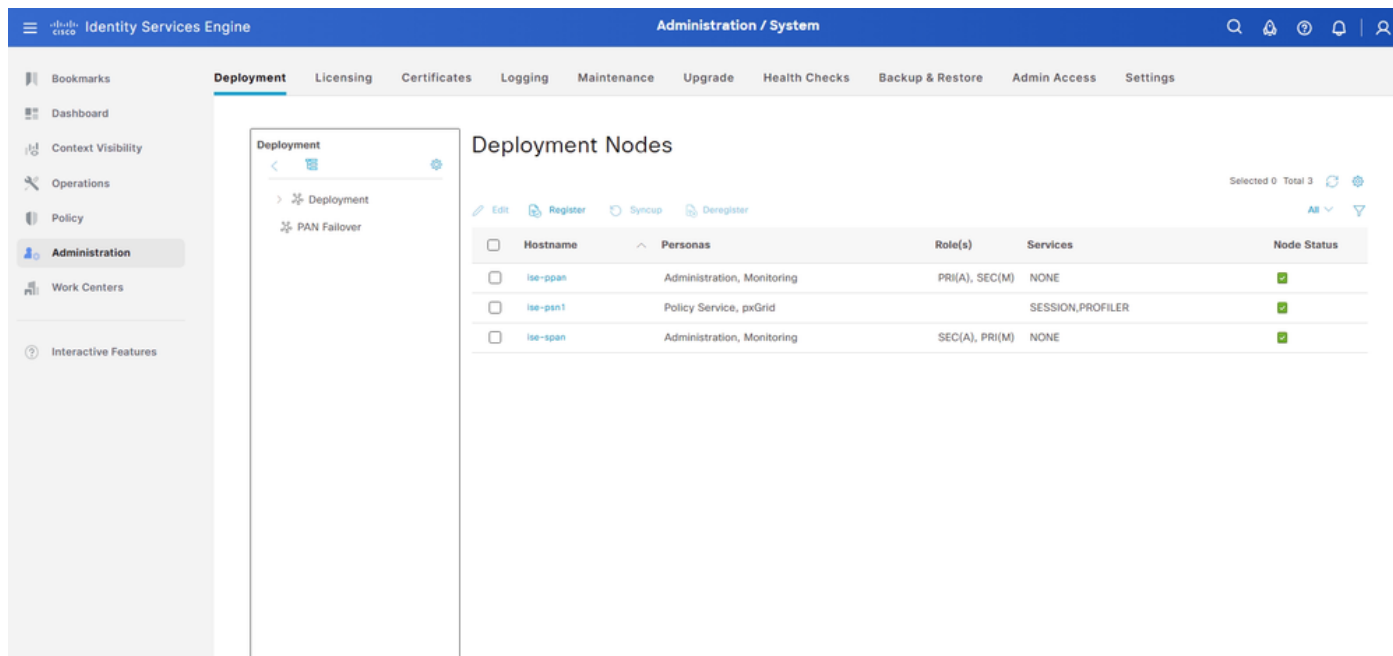
(ise-psn1) Toegevoegd aan de implementatie

Use Case 2: Gederegistreerd secundair knooppunt GUI onbereikbaar (ise-psn2)

De status valideren

Stap 1. Bevestig de status van de gedistribueerde implementatie.

Van primaire Admin Node (PAN) GUI. Navigeer naar Beheer > Systeem > Implementatie. U kunt controleren of dit knooppunt (ise-psn2) al uit het register is verwijderd.

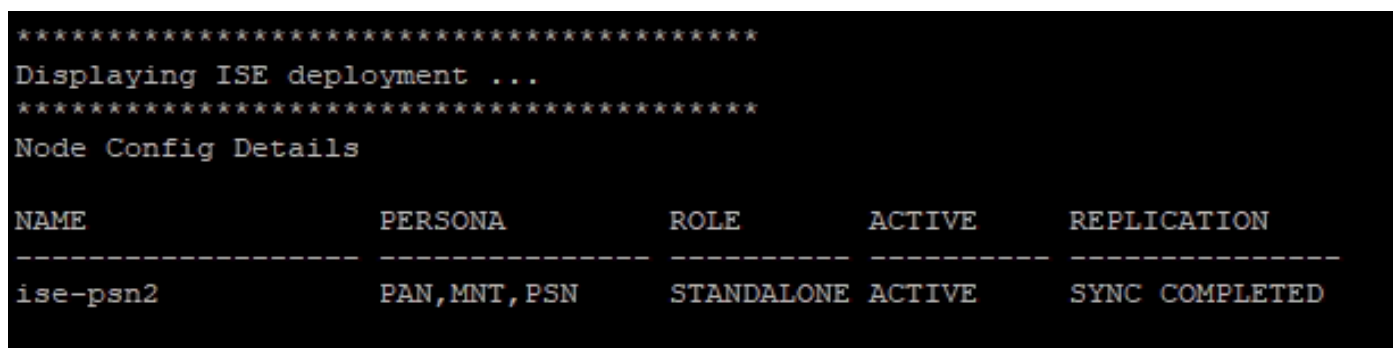


(PAN) implementatieknooppunten

Stap 2. Bevestig de (Sise-psn2).

Vanwege het admin certificaat is in sommige gevallen verlopen kunt u deze symptomen:

- (ise-psn2) GUI onbereikbaar.
- (ise-psn2) CLI (toon de status van de toepassing) ISE-applicatie is ingeschakeld (initialiseren of niet actief).
- (ise-psn2) CLI (show tech) het knooppunt bevindt zich al op een standalone implementatie.



(ise-psn2) op standalone implementatie

Tijdelijke oplossing

Stap 1. Verleng het beheercertificaat van het knooppunt (ISE-pst2).

1. Login bij (ise-psn2) via CLI.
2. Voer applicatie configuratie ise in.
3. Voer 31 in ([31] Generate Self-Signed Admin Certificate).
4. Wilt u doorgaan? y/[n]: y
5. Wilt u het bestaande certificaat na generatie vervangen? y/[n]: y

```

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

```


Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.