

Fehlerbehebung bei abgelaufenem ISE-Administratorzertifikat

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[ISE-Administratorzertifikat \(abgelaufen\)](#)

[Status des Administratorzertifikats überprüfen](#)

[Aktionsplan](#)

[Fehlerbehebung](#)

[Anwendungsfall 1: Deregistrierter sekundärer Knoten, der im verteilten Zustand feststeckt \(ise-psn1\)](#)

[Status überprüfen](#)

[Problemumgehung](#)

[Anwendungsfall 2: Nicht registrierte GUI des sekundären Knotens nicht erreichbar \(ise-psn2\)](#)

[Status überprüfen](#)

[Problemumgehung](#)

[Referenzen](#)

[Relevant](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung und Verlängerung eines abgelaufenen Cisco Identity Services Engine (ISE)-Administratorzertifikats beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Bereitstellung der Cisco ISE:
- Zertifikatsverwaltung in der Cisco ISE.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Softwareversion:

- Cisco Identity Services Engine (ISE) Version 3.3 Patch 4.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das vorliegende Dokument behandelt die verteilte Bereitstellung. Sie können jedoch denselben Fehlerbehebungsplan für einen eigenständigen Knoten verwenden.

Bei der verteilten ISE-Bereitstellung ist der Knoten entweder der primäre Admin-Knoten (PPAN) oder der sekundäre Knoten.

In diesem Dokument wird das ISE-Administratorzertifikat als selbstsigniertes Zertifikat verwendet, um die Auswirkungen eines abgelaufenen Zertifikats darzustellen. Für ein Produktionssystem wird dieser Ansatz jedoch nicht empfohlen. Es ist besser, ein von der Zertifizierungsstelle signiertes Zertifikat für die Verwendung durch den Administrator zu verwenden.

 Anmerkung: Cisco empfiehlt, dass Sie Ihr Administratorzertifikat im Status belassen und die Verlängerung im Voraus planen. In diesem Leitfaden finden Sie Informationen zum Nachverfolgen und Erneuern von ISE-Systemzertifikaten ([Konfigurieren der Zertifikatverlängerung auf ISE](#)).

ISE-Administratorzertifikat (abgelaufen)

Status des Administratorzertifikats überprüfen

Schritt 1: Überprüfen Sie den Bereitstellungsstatus. Navigieren Sie zu Administration > System > Deployment.

Sie können den Status der sekundären Knoten überprüfen, wie dargestellt, die drei sekundären Knoten sind (nicht synchronisiert).

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	⚠

Bereitstellungsstatus

2. Schritt: Prüfen Sie die Erinnerungen. Navigieren Sie zu Dashboard > Erinnerungen > (Zertifikat abgelaufen).

Um zu bestätigen, welcher Knoten und welches Zertifikat abgelaufen ist.

Anmerkung: Wenn der primäre Admin-Knoten (PPAN) vor einem sekundären Knoten abgelaufen ist, werden keine Alarmer von diesem Knoten angezeigt. Dies ist bei diesem Alarm für den sekundären Admin-Knoten (SPAN) der Fall.

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.

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	

Alarmer (Zertifikat abgelaufen)

Schritt 3: Überprüfen Sie den Status des Admin-Zertifikats. Navigieren Sie zu Administration > System > Certificates > Certificate Management > System Certificates > Expand node.

1. Primärer Administratorknoten (PPAN):

System Certificates

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=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#000003	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, OU=Certificate Services Endpoint Sub CA - ise-ppan#000004	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 des PPAN-Administratorzertifikats

2. Sekundäre Knoten.

Für die sekundären Knoten kann es sich um eine von zwei Optionen handeln, und in beiden Fällen müssen Sie denselben Aktionsplan anwenden:

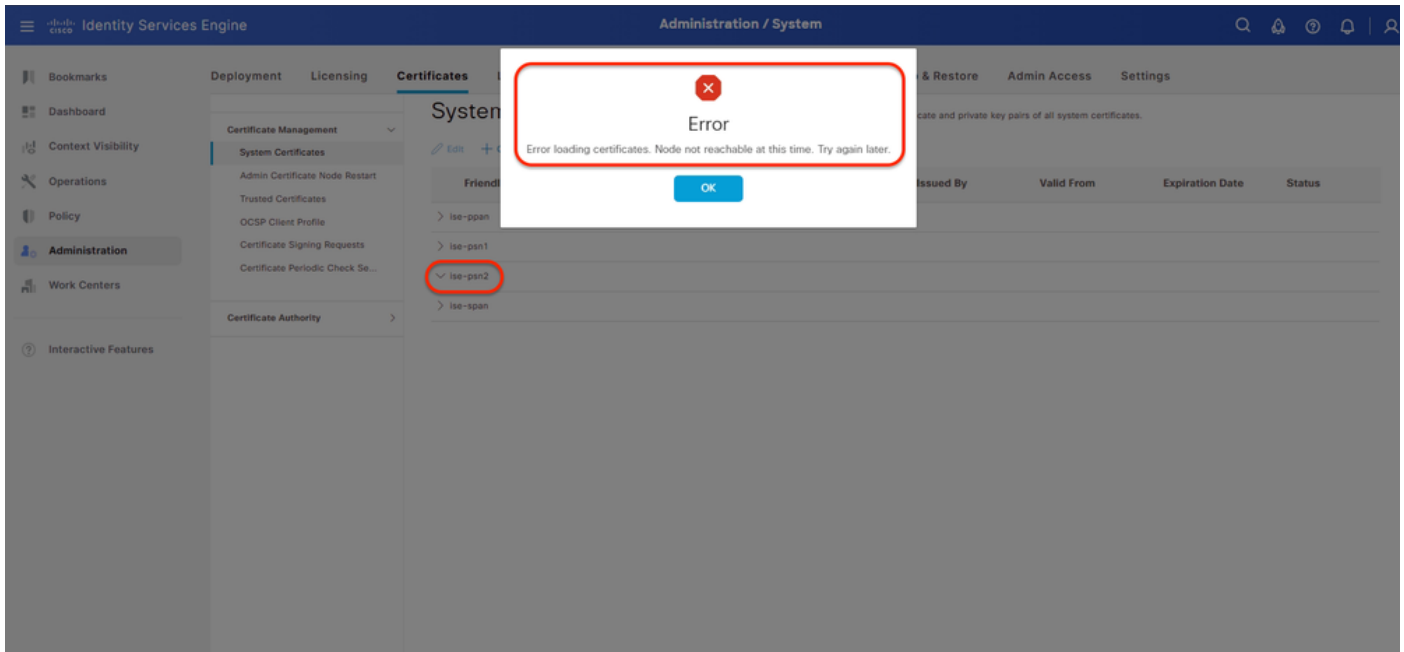
A. Kann das Knotensystemzertifikat erweitern und bestätigen, dass das Administratorzertifikat abgelaufen ist:

System Certificates

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=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-span.kdlab2.local, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ise-span#000005	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, OU=Certificate Services Endpoint Sub CA - ise-span#000006	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

Status des sekundären Knotenadministratorzertifikats

B. Fehler auslösen ("Fehler beim Laden der Zertifikate. Knoten derzeit nicht erreichbar. Versuchen Sie es später erneut."), wie für (ise-psn2



Sekundärknoten nicht erreichbar

Aktionsplan

Nachdem Sie das Ablaufende des Admin-Zertifikats für alle vier Knoten bestätigt haben, müssen Sie die folgenden Schritte durchführen:

Schritt 1: Aufheben der Registrierung aller sekundären Knoten in der verteilten Bereitstellung (nur wenn das Admin-Zertifikat abgelaufen ist)

Navigieren Sie zu Administration > System > Deployment > Check [✓] der sekundären Knoten, und klicken Sie auf Registrierung aufheben.

 Anmerkung: Die Registrierung des Knotens aufheben bedeutet, dass er in den eigenständigen Knoten verschoben wird. Anschließend können Sie das Admin-Zertifikat für diesen Knoten erneuern.

Identity Services Engine Administration / System

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

Deployment Nodes

Selected 3 Total 4

1

2

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

Sekundäre Knoten abmelden

 Anmerkung: Vergessen Sie nicht, nur die Registrierung sekundärer Knoten aufzuheben, bei denen das Administratorzertifikat bereits abgelaufen ist, und den Rest beizubehalten. In diesem Dokument sind alle sekundären Knoten abgelaufen.

Identity Services Engine Administration / System

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

Deployment Nodes

Selected 0 Total 1

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

Alle sekundären Knoten sind deregistriert

Schritt 2: Erneuern Sie das Administratorzertifikat des primären Administratorknotens (PPAN).

1. Navigieren Sie zu Administration > System > Certificates > Certificate Management > System Certificates > Click +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
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=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

Neues selbstsigniertes Administratorzertifikat generieren

2. Wählen Sie den Primären Admin-Knoten (PPAN) (ise-ppan) aus, und geben Sie die Zertifikatsinformationen ein:

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)

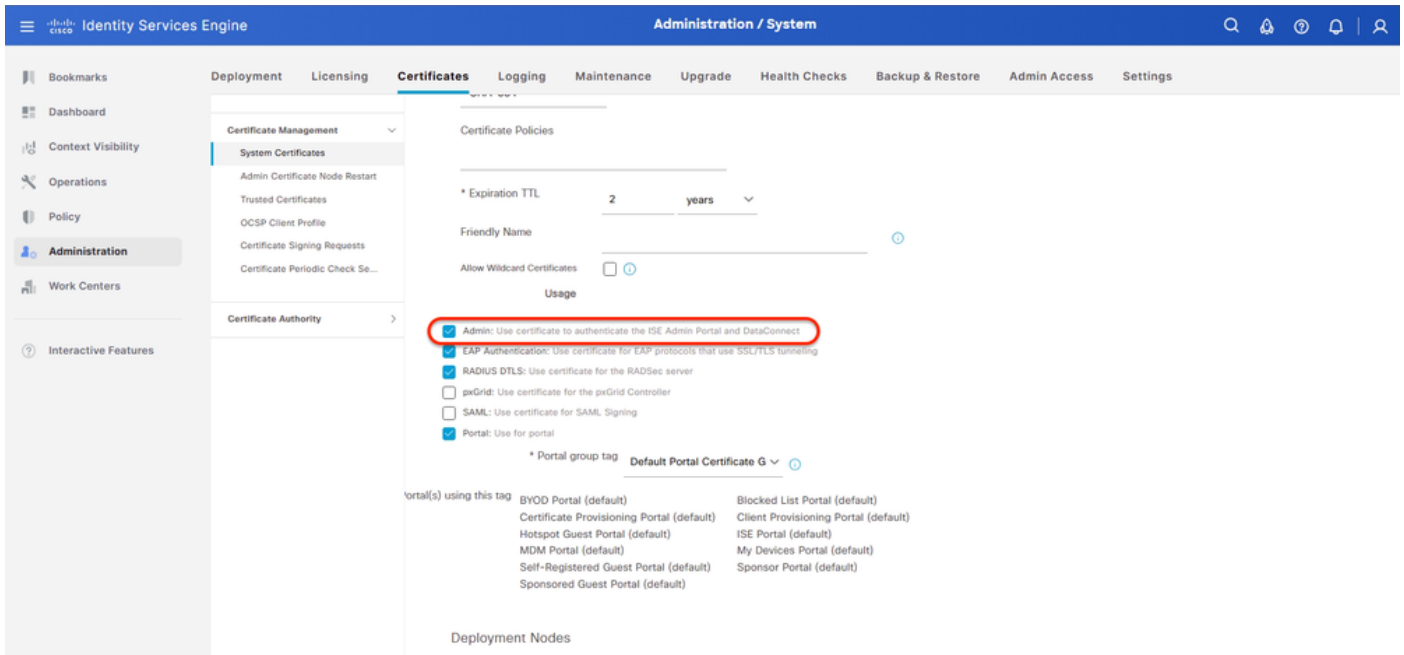
State (ST)

Country (C)

Subject Alternative Name (SAN)

Wählen Sie den primären Admin-Knoten (PPAN) aus.

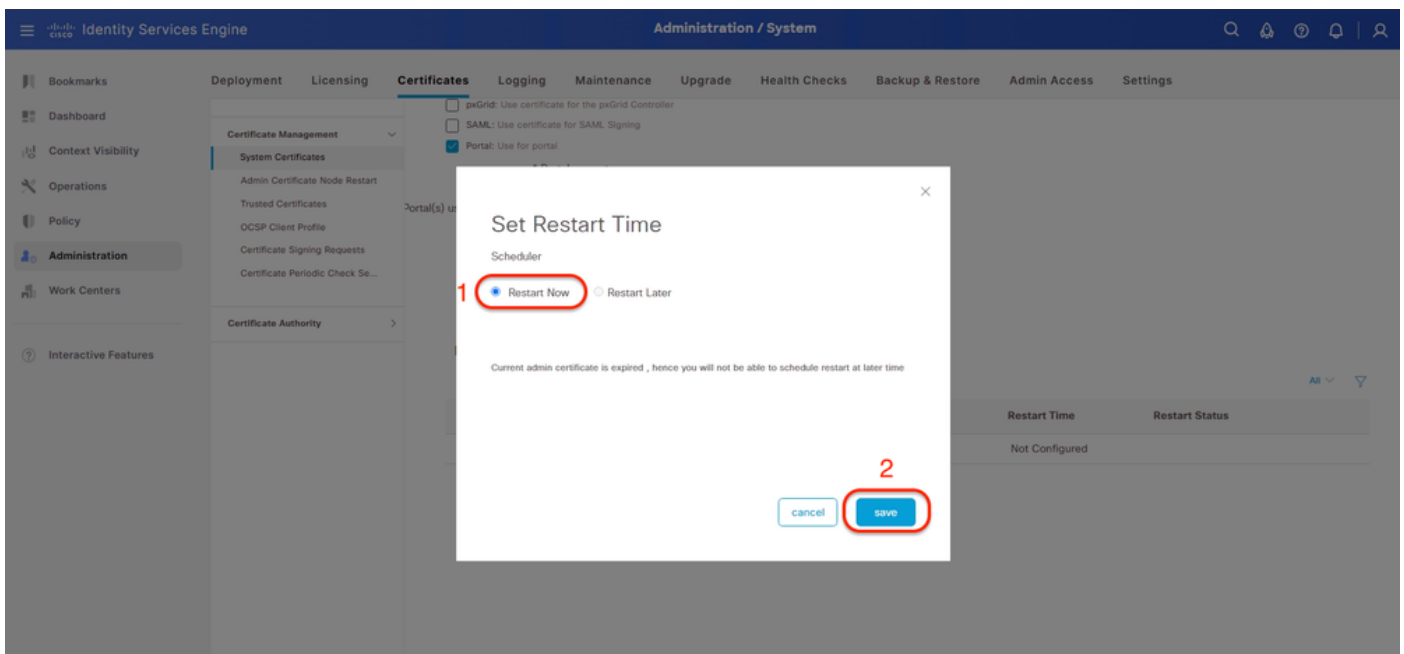
3. Aktivieren Sie [✓] die Verwendung von Admin.



Admin-Nutzung

4. Legen Sie die Neustartzeit für den primären Admin-Knoten (PPAN) auf Jetzt neu starten fest. Legen Sie für alle Knoten in der Bereitstellung entweder "Jetzt neu starten" oder "Später neu starten" fest.

Nachdem Sie ein Administratorzertifikat (ein für die Verwendung durch den Administrator konfiguriertes Zertifikat) auf dem primären Administratorknoten (PPAN) erneuert haben, müssen alle Knoten in Ihrer Bereitstellung neu gestartet werden.



Neustartzeit jetzt festlegen

5. Klicken Sie auf Senden.



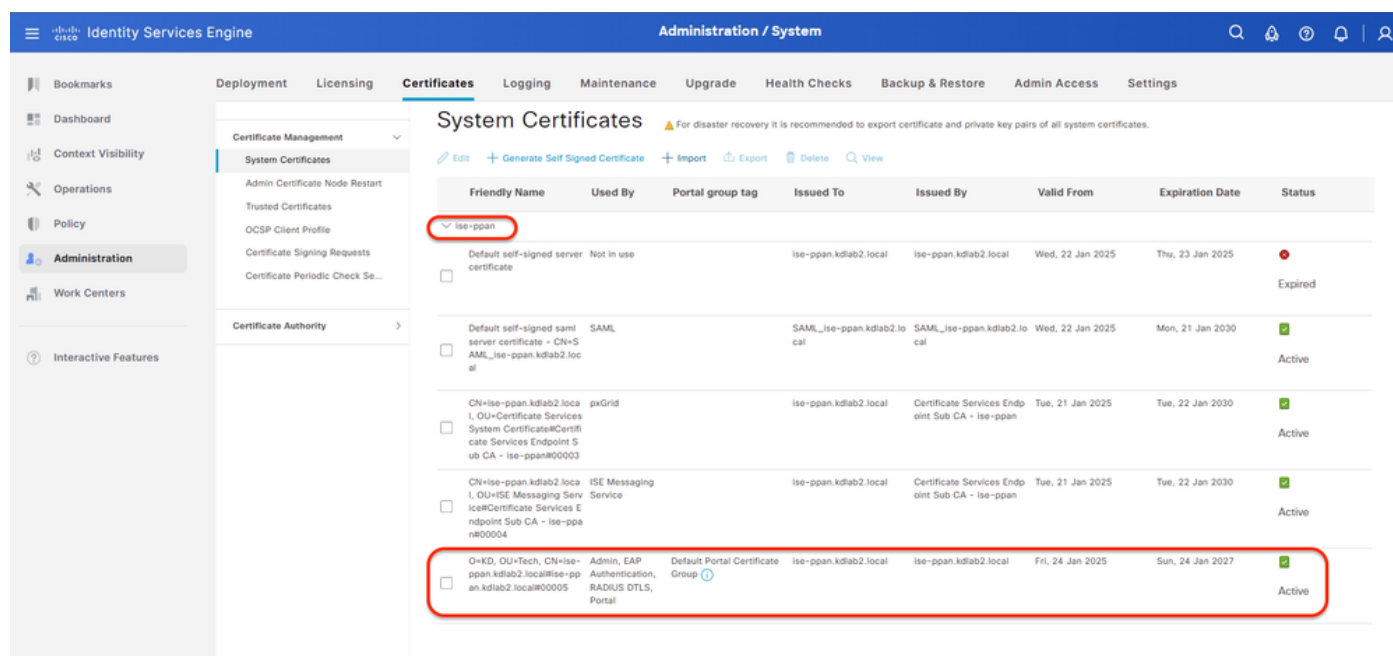
Anmerkung: Nachdem Sie ein Admin-Zertifikat (ein für die Verwendung durch den

 Administrator konfiguriertes Zertifikat) auf dem primären Admin-Knoten (PPAN) erneuert haben, müssen alle Knoten in Ihrer Bereitstellung neu gestartet werden. Sie können entweder jeden Knoten sofort neu starten oder die Neustarts zu einem späteren Zeitpunkt planen. Mit dieser Funktion können Sie sicherstellen, dass keine laufenden Prozesse durch die automatischen Neustarts unterbrochen werden, sodass Sie den Prozess besser kontrollieren können.

Sie können die geplanten Neustarts im Fenster Administration > System > Certificates > Admin Certificate Node Restart (Verwaltung > Zertifikatsknoten-Neustart) anzeigen und bearbeiten, das in Cisco ISE Version 3.3 zur Verfügung steht.

6. Überprüfen Sie das neue Administratorzertifikat des primären Administratorknotens (PPAN).

Navigieren Sie zu Administration > System > Certificates > Certificate Management > System Certificates > Expand (ise-span).



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

Neues Administratorzertifikat (ise-ppan)

Schritt 3: Erneuern Sie das Administratorzertifikat der sekundären Knoten.

1. Bestätigen Sie den sekundären Knoten bei einer eigenständigen Bereitstellung, nachdem Sie die Registrierung bei der verteilten Bereitstellung aufgehoben haben.

Navigieren Sie über die GUI (<https://<FQDN/IP>>) zum Knoten, und navigieren Sie zu Administration > System > Deployment.

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 and 'STANDALONE' as the Role(s). Both are circled in red. The Node Status is 'Active' (green checkmark).

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

(ise-span) bei Standalone-Bereitstellung

2. Navigieren Sie zu Administration > System > Certificates > Certificate Management > System Certificates > Click +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

Neues selbstsigniertes Administratorzertifikat generieren

3. Wählen Sie die (ise-span) und füllen Sie die Zertifikatinformationen.

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)

Wählen Sie den Knoten

4. Aktivieren Sie [✓] die Verwendung von 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)	

Admin-Nutzung



Anmerkung: Wenn Sie das Zertifikat des Admin-Rollenzertifikats auf dem ISE-Knoten ändern, werden die Dienste neu gestartet.

5. Klicken Sie auf Senden.

6. Überprüfen Sie das neue Admin-Zertifikat auf (ise-span).

Navigieren Sie zu Verwaltung > System > Zertifikate > Zertifikatsverwaltung > Systemzertifikate > Erweitern (Spannweite).

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							Expired
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=KED, 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 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, 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

Neues Administratorzertifikat (ise-span)

Schritt 4: Registrieren der sekundären Knoten für die verteilte Bereitstellung

Richten Sie Ihre Bereitstellungspersonen und -rollen wie zuvor ein (Admin, MNT, PSN usw.).

1. Navigieren Sie von der PPAN-GUI (Primary Admin Node) zu Administration > System > Deployment > Click 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

Primäre Administrationsknoten-GUI (PPAN)

2. Geben Sie den FQDN und die Zugangsdaten des sekundären Knotens (Benutzername/Passwort) ein.

Geben Sie den DNS-auflösbaren vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des eigenständigen Knotens ein, den Sie registrieren möchten. Der FQDN des (PPAN)

und des registrierten Knotens müssen voneinander auflösbar sein.

Zugriff auf sekundären Knoten eingeben

3. Aktivieren Sie die richtigen Personen und Dienste.

Sekundären Knoten registrieren (ise-span)

Schritt 5: Überprüfen des Bereitstellungsstatus

Navigieren Sie zu Administration > System > Deployment.

Identity Services Engine Administration / System

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

Deployment

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) Zur Bereitstellung hinzugefügt

Fehlerbehebung

Anwendungsfall 1: Deregistrierter sekundärer Knoten, der im verteilten Zustand feststeckt (ise-psn1)

Status überprüfen

Schritt 1: Bestätigen Sie den Status der verteilten Bereitstellung.

Von der primären Administrationsknoten-GUI (PPAN) aus. Navigieren Sie zu Administration > System > Deployment. Sie können bestätigen, dass dieser Knoten (ise-psn1) bereits deregistriert ist.

Identity Services Engine Administration / System

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

Deployment

Deployment Nodes

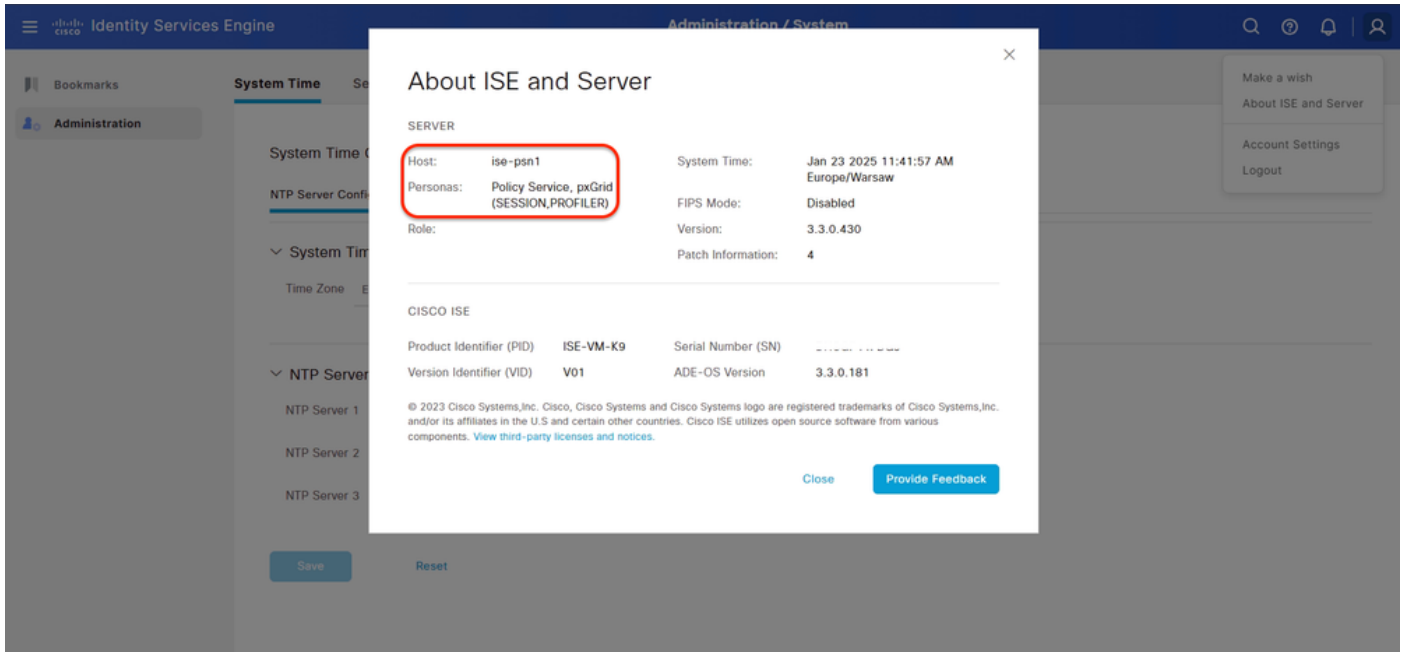
Selected 0 Total 2

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	✓

(PPAN) Bereitstellungsknoten

Schritt 2: Bestätigen Sie den Status des Knotens (ise-psn1).

Durchsuchen Sie den sekundären Knoten über die GUI (<https://ise-psn1.kdlab.local>), und navigieren Sie zu Login > About ISE and Server.

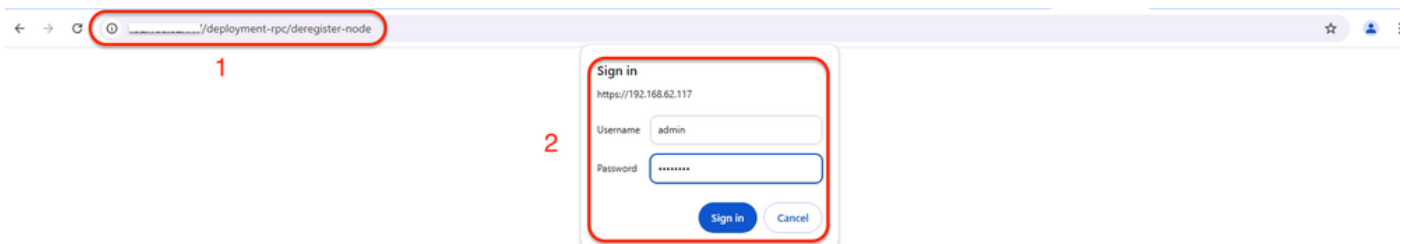


Sekundärknoten (ise-psn1) mit festem Status für verteilte Bereitstellung

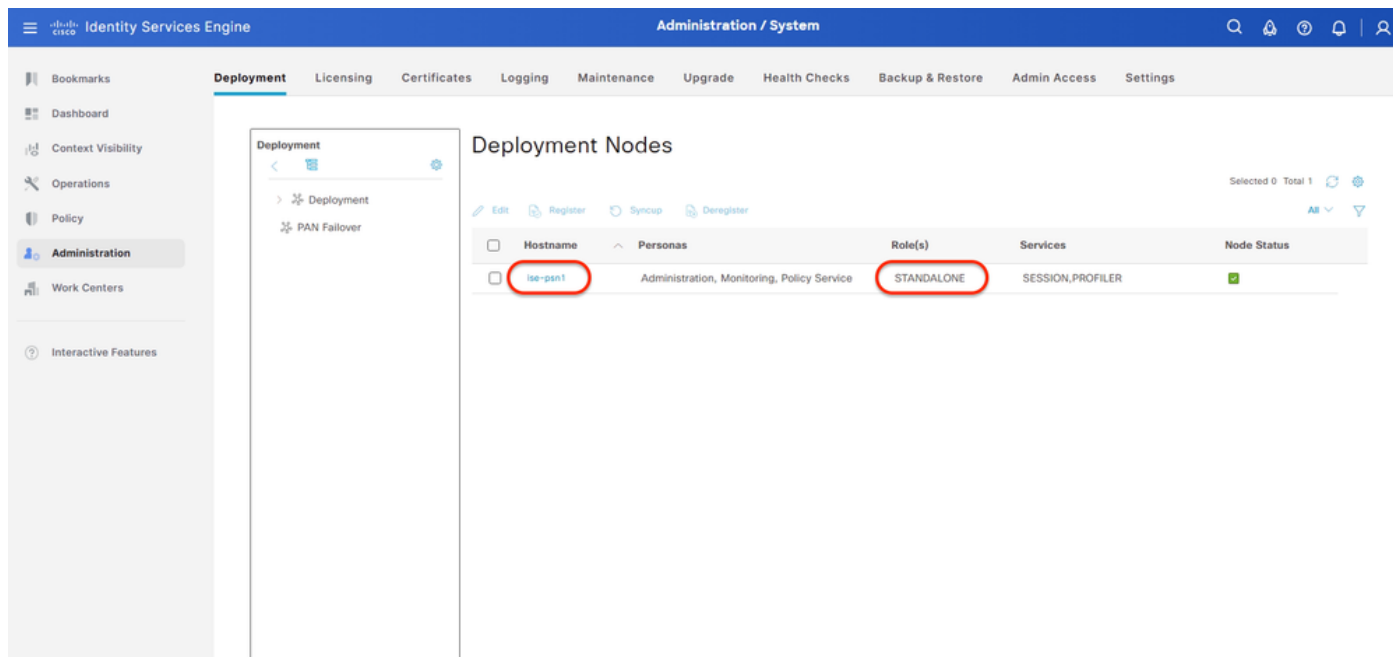
Problemumgehung

Schritt 1: Deaktivieren Sie den (ise-psn1)-Knoten manuell.

Setzen Sie den (ise-psn1)-Knoten über die GUI (<https://<ise-psn1 IP>/deployment-rpc/deregister-node>) in eine Standalone-Bereitstellung um.



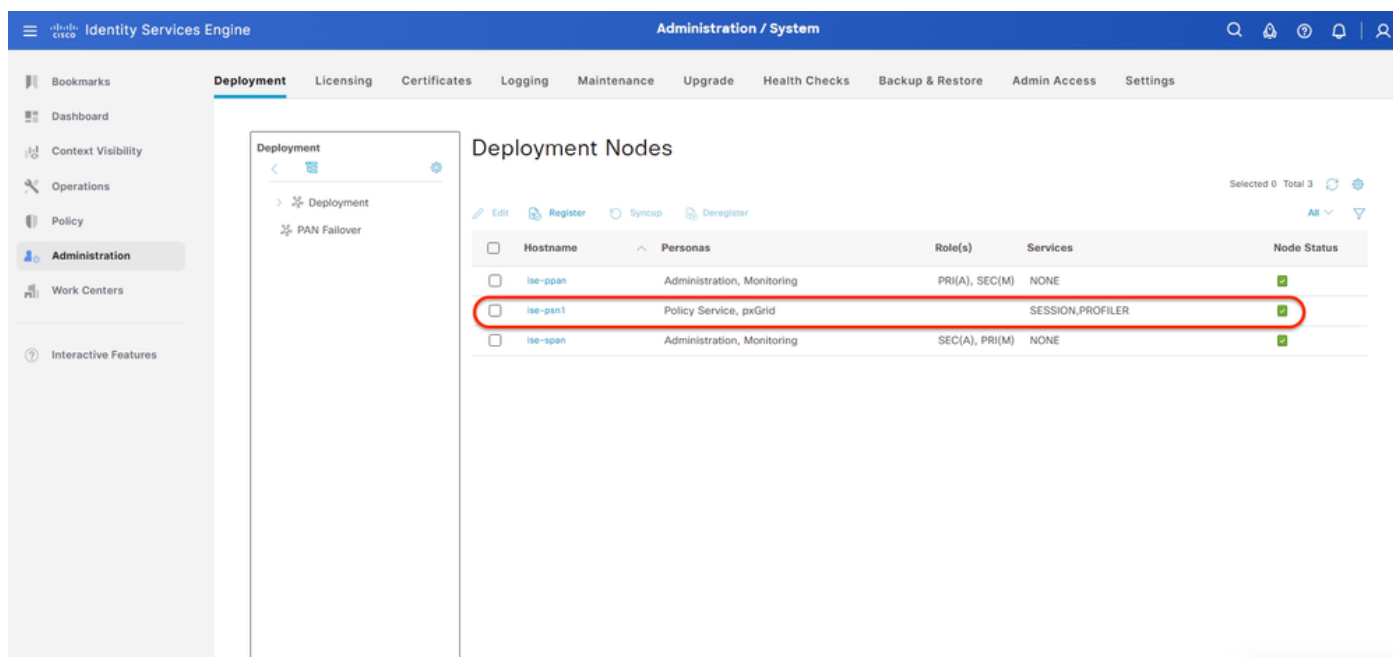
Schritt 2: Überprüfen Sie die (ise-psn1) jetzt bei Standalone-Bereitstellung.



(ise-psn1) bei Standalone-Bereitstellung

Schritt 3: Nachdem Sie den Status des Knotens als eigenständiger Knoten bestätigt haben, fahren Sie mit den gleichen Schritten im Abschnitt "Aktionsplan" fort:

1. Erneuern Sie das Administratorzertifikat des (ise-psn1)-Knotens.
2. Registrieren Sie den (ise-psn1)-Knoten für die verteilte Bereitstellung.
3. Überprüfen des Bereitstellungsstatus



(ise-psn1) Zur Bereitstellung hinzugefügt

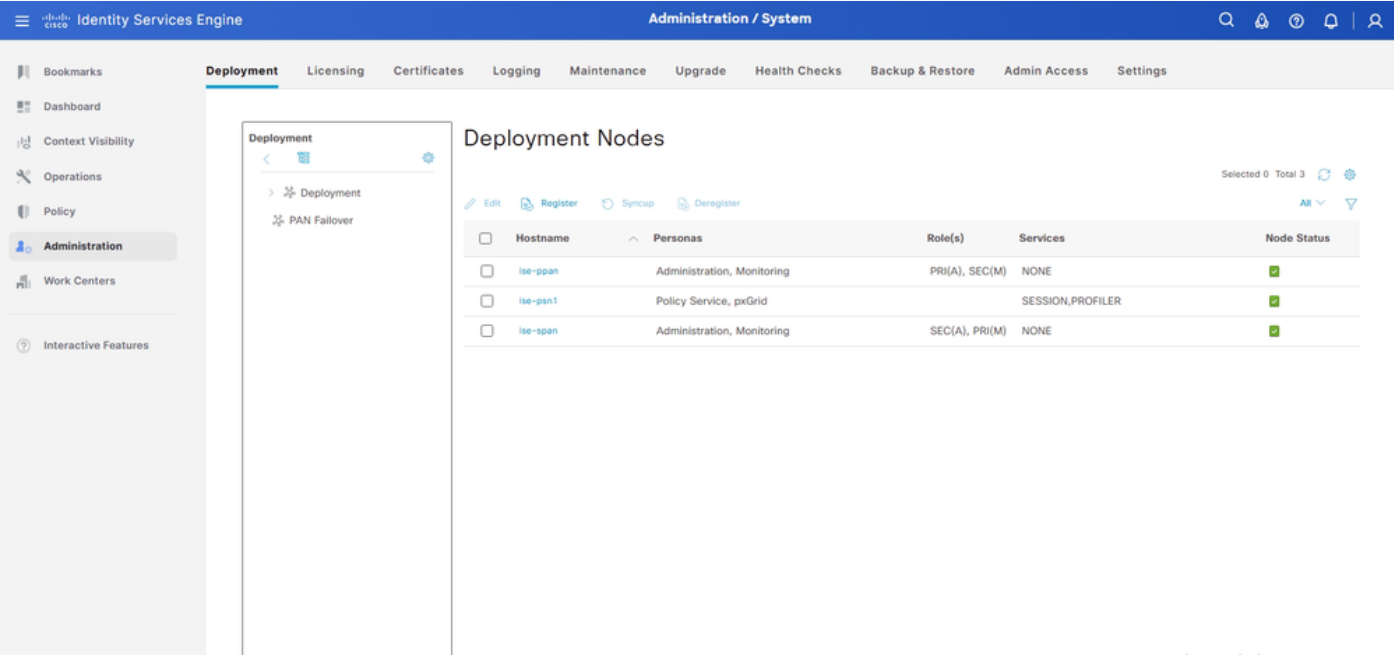
Anwendungsfall 2: Nicht registrierte GUI des sekundären Knotens nicht erreichbar

(ise-psn2)

Status überprüfen

Schritt 1: Bestätigen Sie den Status der verteilten Bereitstellung.

Von der primären Administrationsknoten-GUI (PPAN) aus. Navigieren Sie zu Administration > System > Deployment. Sie können bestätigen, dass dieser Knoten (ise-psn2) bereits deregistriert ist.



(PPAN) Bereitstellungsknoten

Schritt 2: Bestätigen Sie das (ise-psn2) Knotenstatus.

Da das Administratorzertifikat in einigen Fällen abgelaufen ist, können Sie die folgenden Symptome feststellen:

- (ise-psn2) GUI nicht erreichbar.
- (ise-psn2) CLI (show application status ise) ISE-Anwendung hängt fest (wird initialisiert oder wird nicht ausgeführt).
- (ise-psn2) CLI (show tech) des Knotens, der sich bereits in einer Standalone-Bereitstellung befindet

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

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

Problemumgehung

Schritt 1: Erneuern Sie das Administratorzertifikat des (ise-psn2)-Knotens.

1. Melden Sie sich bei (ise-psn2) über die CLI an.
2. Geben Sie `application configure ise` ein.
3. Geben Sie `31` ein ([31] Erstellen Sie ein selbstsigniertes Administratorzertifikat).
4. Möchten Sie fortfahren? `y/[n]: y`
5. Möchten Sie das vorhandene Zertifikat nach der Generierung ersetzen? `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
```


Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.