Troubleshoot Expired ISE Admin Certificate

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

ISE Admin Certificate (Expired)

- Validate Admin Certificate Status
- Action Plan

Troubleshoot

- Use Case 1: Deregistered Secondary Node Stuck on Distributed State (ise-psn1)
  - Validate the Status
  - Workaround
- Use Case 2: Deregistered Secondary Node GUI Unreachable (ise-psn2)
  - Validate the Status
  - Workaround

Related Information

Introduction

This document describes how to troubleshoot and renew an expired Cisco Identity Services Engine (ISE) Admin Certificate.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- Cisco ISE Deployment.
- Certificate Management in Cisco ISE.

Components Used

The information in this document is based on these software version:

- 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document focuses on the distributed deployment; however, you can use the same troubleshooting plan on standalone node.

In ISE Distributed Deployment, the node is either Primary Admin Node (PPAN) or secondary.

This document uses ISE Admin certificate as a self-signed certificate in order to demonstrate the impact of certificate expired, but this approach is not recommended for a production system. It is better to use authority-signed certificate for admin usage.

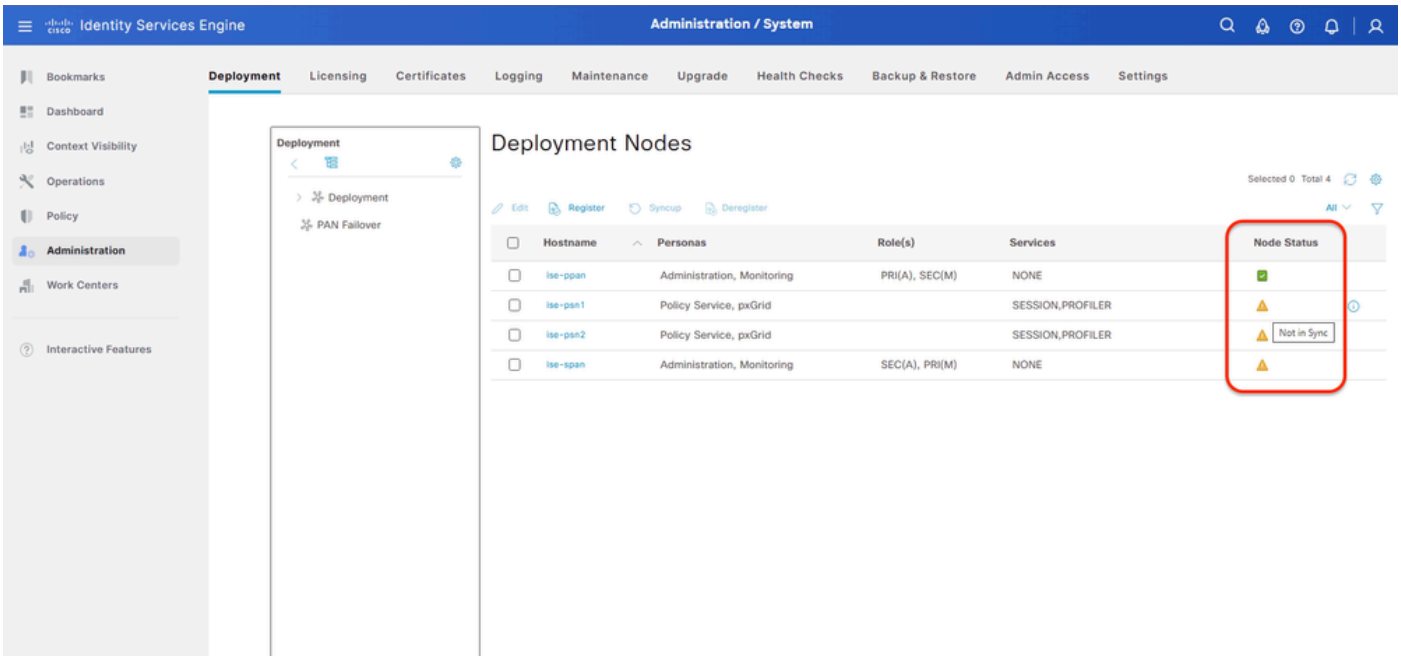
Note: Cisco recommends you to keep your Admin certificate in health state and plan the renewal in advance, find this guide to help you track and renew ISE System Certificates (Configure Certificate Renewals on ISE).

ISE Admin Certificate (Expired)

Validate Admin Certificate Status

Step 1. Check the deployment status. Navigate to **Administration > System > Deployment**.

You can check the secondary nodes status, as shown, the three secondary nodes are (**Not in Sync**).

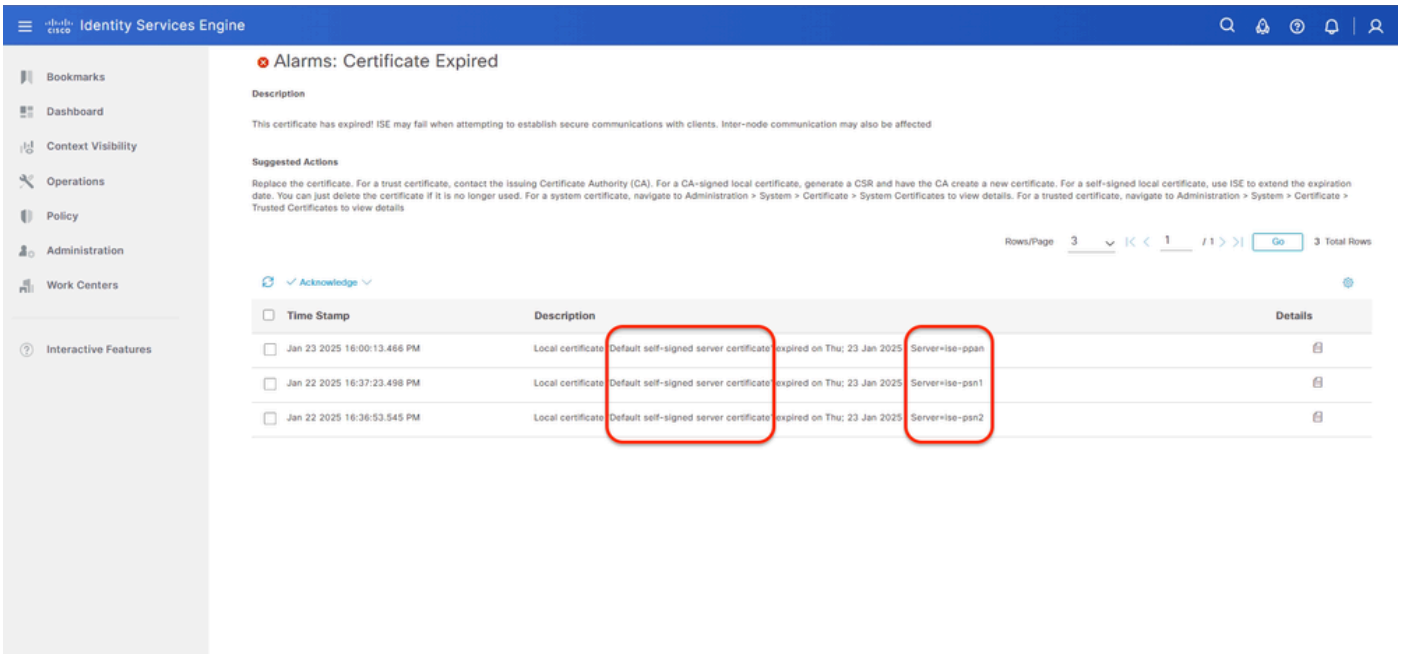


Deployment Status

Step 2. Review the **Alarms**. Navigate to **Dashboard > Alarms > (Certificate Expired)**.

To confirm which node and which certificate is expired.

Note: If the Primary Admin Node (PPAN) expired before any secondary node you can not see any alarms from that node, that is what happened for Secondary Admin Node (SPAN) in this alarm.

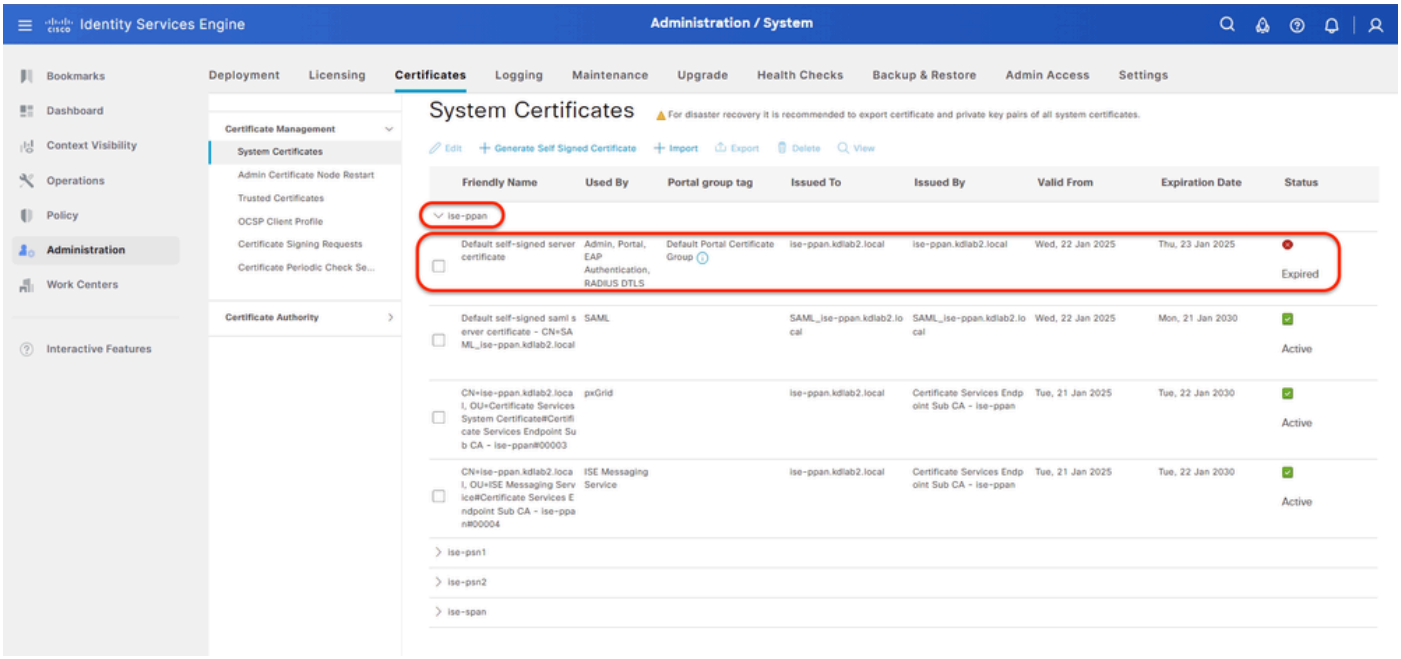


Alarms (Certificate Expired)

Step 3. Check the admin certificate status. Navigate to **Administration > System > Certificates >**

Certificate Management > System Certificates > Expand node.

1. Primary Admin Node (PPAN):

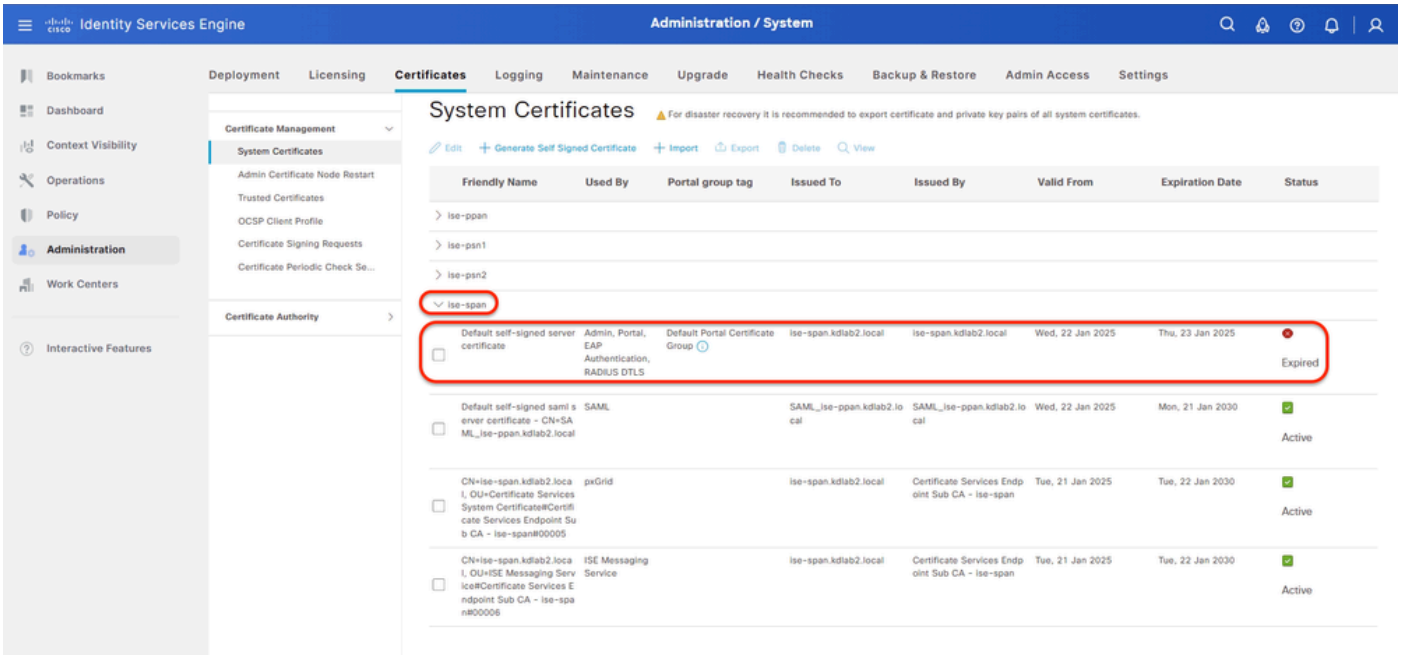


PPAN Admin Certificate Status

2. Secondary nodes.

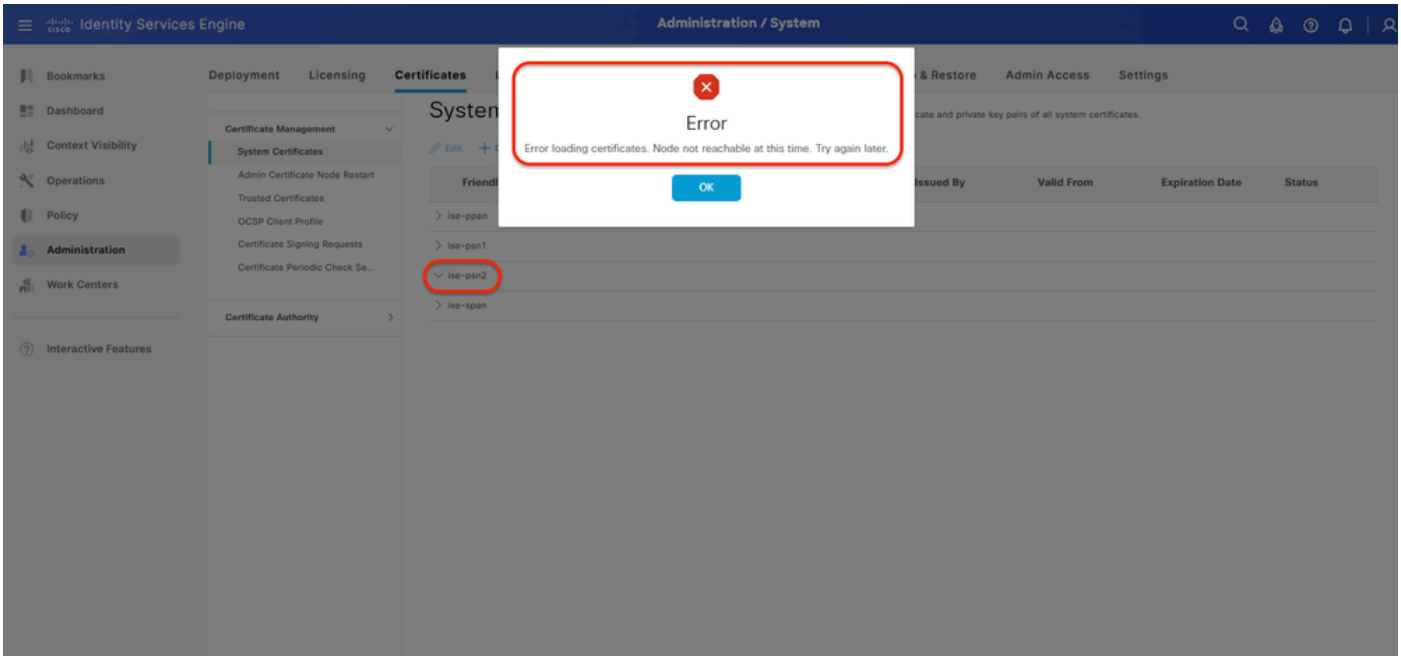
For the secondary nodes it could be 1 of 2 options and in both cases you must apply the same action plan:

A. Can Expand the node system certificate and confirm that the admin certificate is expired:



Secondary Node Admin Certificate Status

B. Throw error ("Error loading certificates. Node not reachable at this time. Try again later.") as shown for (ise-psn2).



Secondary Node Not Reachable

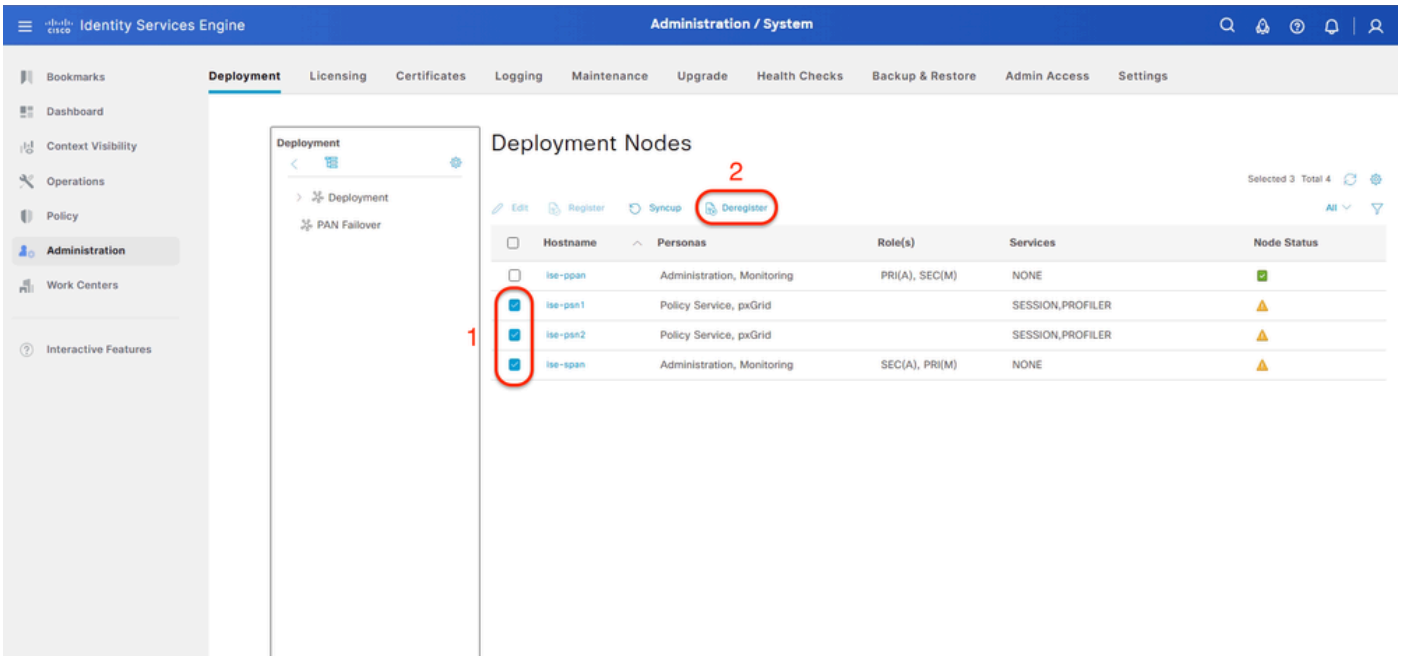
Action Plan

After you confirm the admin certificate expired for all 4 nodes, you must apply these steps:

Step 1. Deregister all secondary nodes from the distributed deployment (only if the admin certificate is expired).

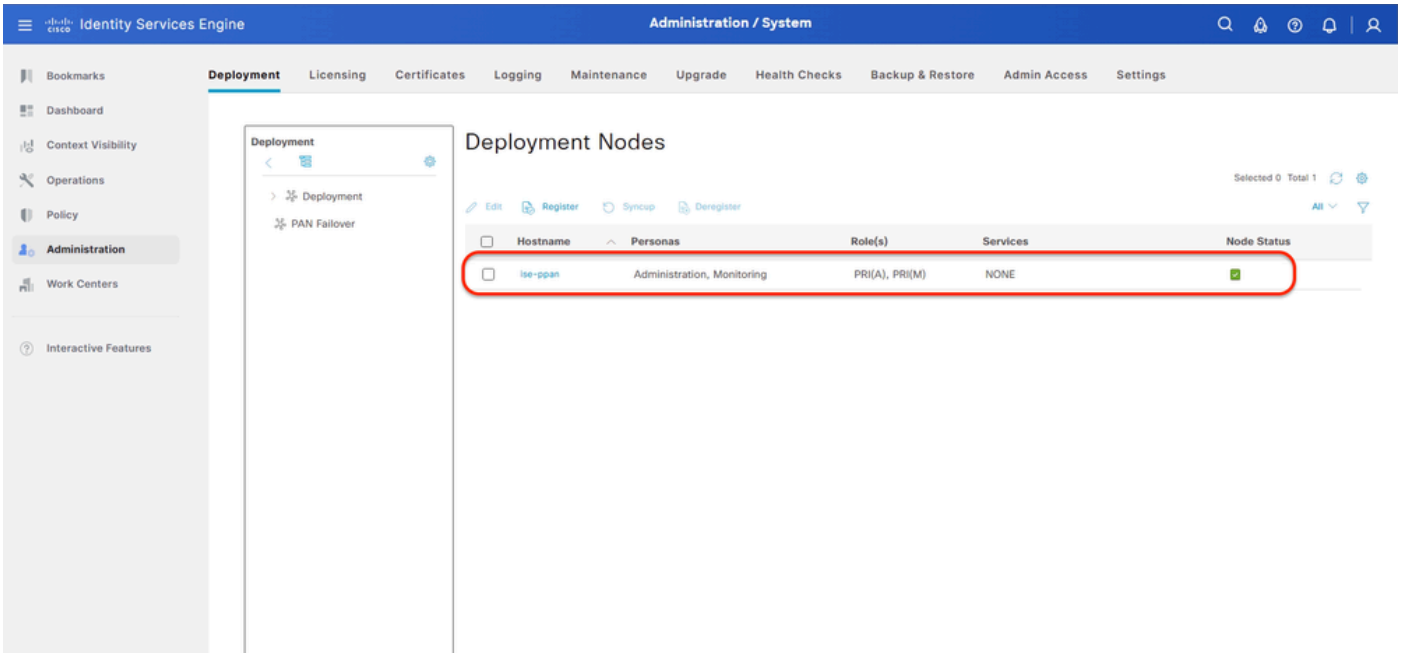
Navigate to **Administration > System > Deployment > Check** [√] of the secondary nodes and click **Deregister**.

Note: Deregister the node means it moved to standalone. Then, you can renew the admin certificate on this node.



Deregister Secondary Nodes

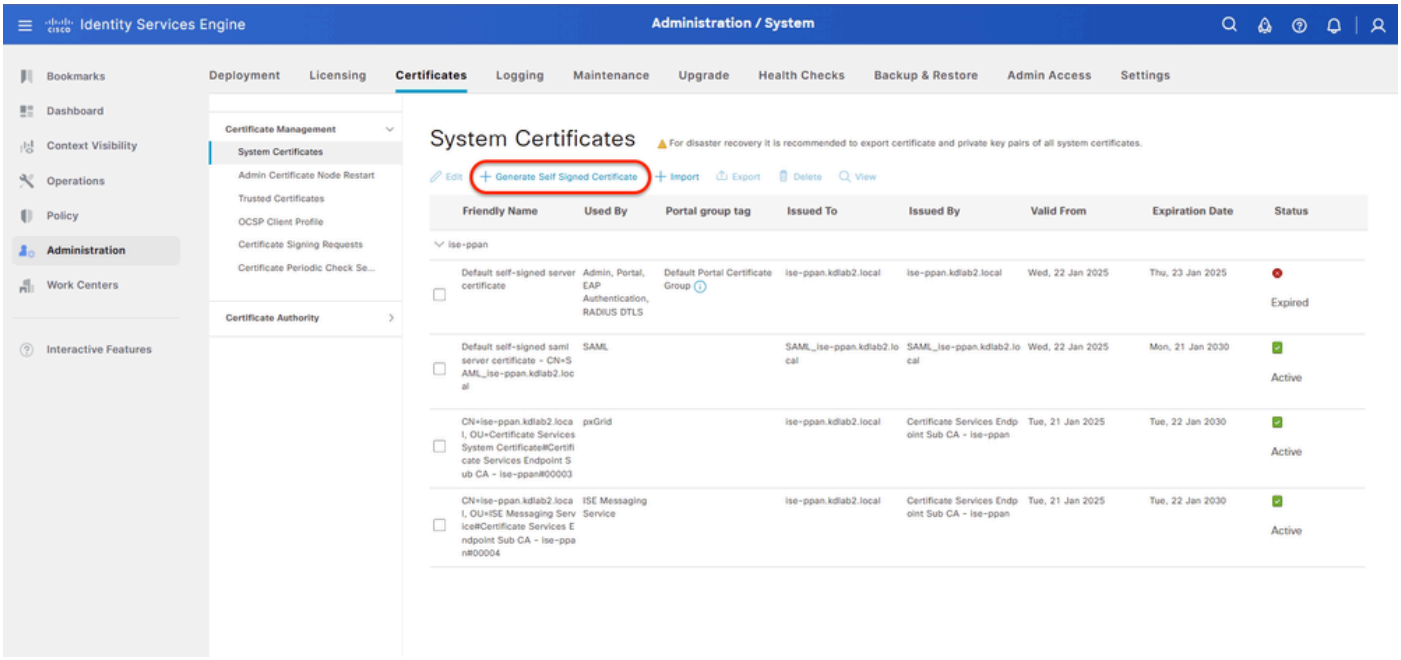
Note: Remember to deregister only secondary nodes where the admin certificate is already expired and to keep the rest. In this document, all the secondary nodes are expired.



All Secondary Nodes are Deregistered

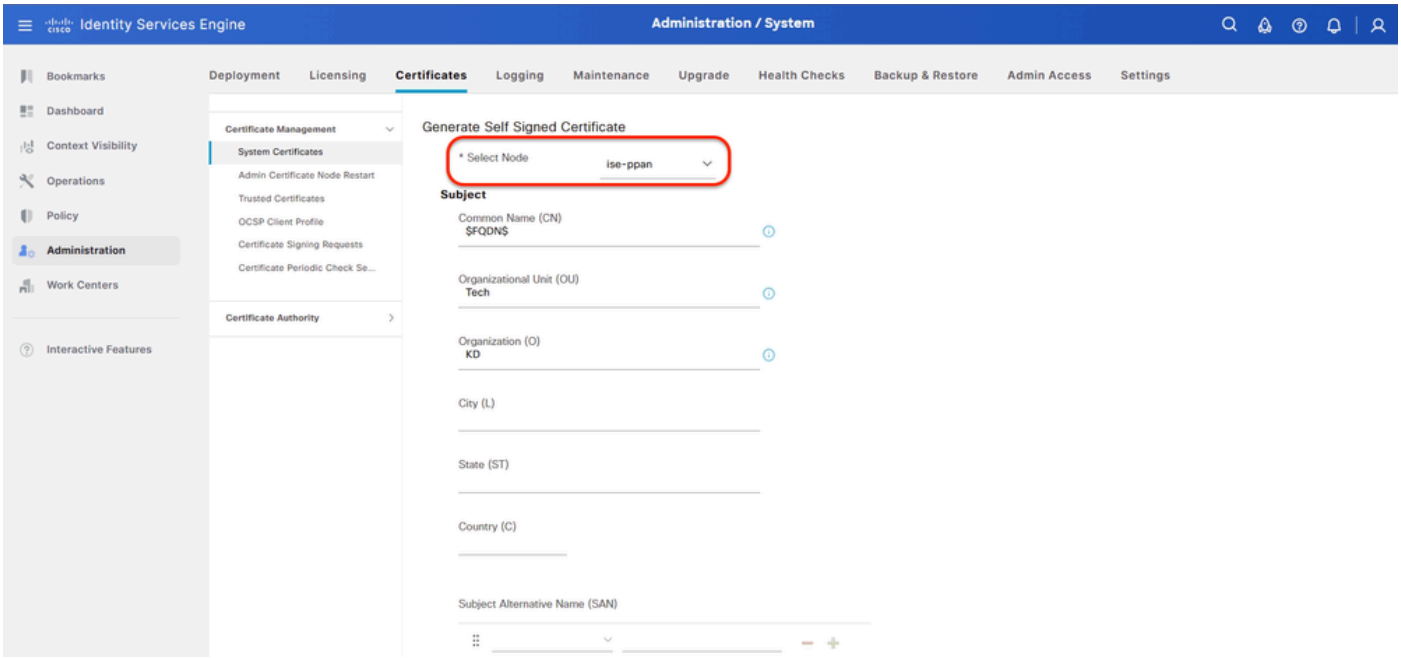
Step 2. Renew admin certificate of the Primary Admin Node (PPAN).

1. Navigate to **Administration > System > Certificates > Certificate Management > System Certificates.** Click **+Generate Self Signed Certificate**:



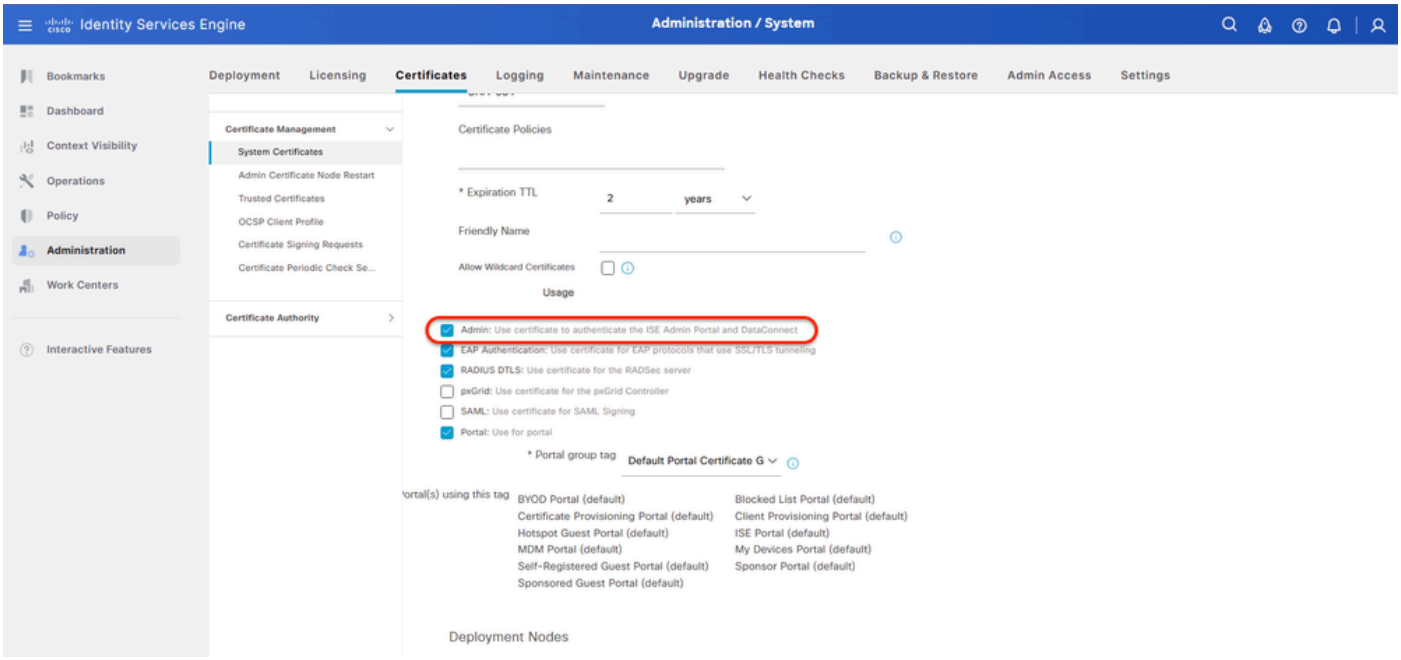
Generate new Self-Signed Admin Certificate

2. Select the **Primary Admin Node (PPAN) (ise-ppan)** and fill the **certificate information**:



Select the Primary Admin Node (PPAN)

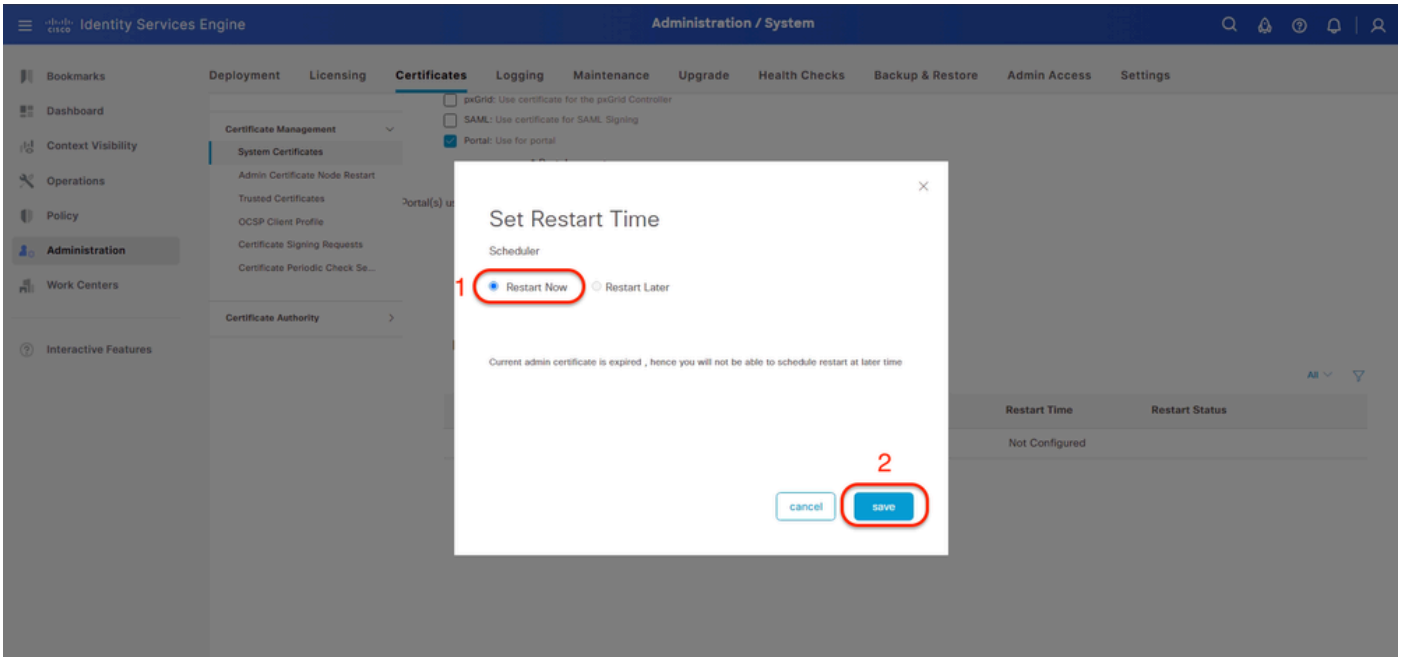
3. Check [√] the **Admin** usage.



Admin Usage

4. Set the **Restart Time** to **Restart Now** for the Primary Admin Node (PPAN). Set all nodes on the deployment either to **Restart Now** or **Restart Later**.

After you renew an admin certificate (a certificate configured for admin usage) on the Primary Admin Node (PPAN), all the nodes in your deployment must be restarted.



Set Restart Time to Now

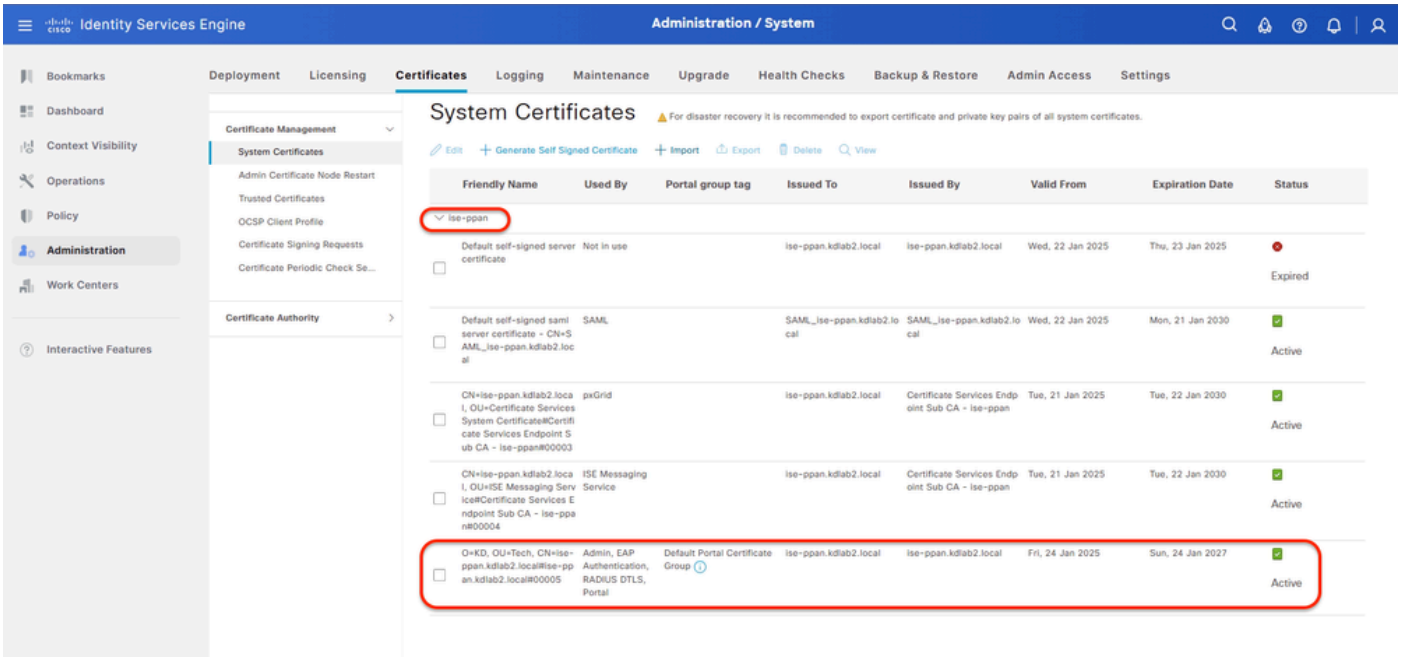
5. Click **Submit**.

Note: After you renew an admin certificate (a certificate configured for admin usage) on the Primary Admin Node (PPAN) all the nodes in your deployment must be restarted. You can either restart each node immediately or schedule the restarts later. This feature allows you to ensure that no running processes are disrupted by the automatic restarts, giving you greater control over the process.

You can view and edit the scheduled restarts in the **Administration > System > Certificates > Admin Certificate Node Restart** window, which is available from Cisco ISE Release 3.3.

6. Verify the new admin certificate of the Primary Admin Node (PPAN).

Navigate to **Administration > System > Certificates > Certificate Management > System Certificates > Expand** (**ise-ppan**).

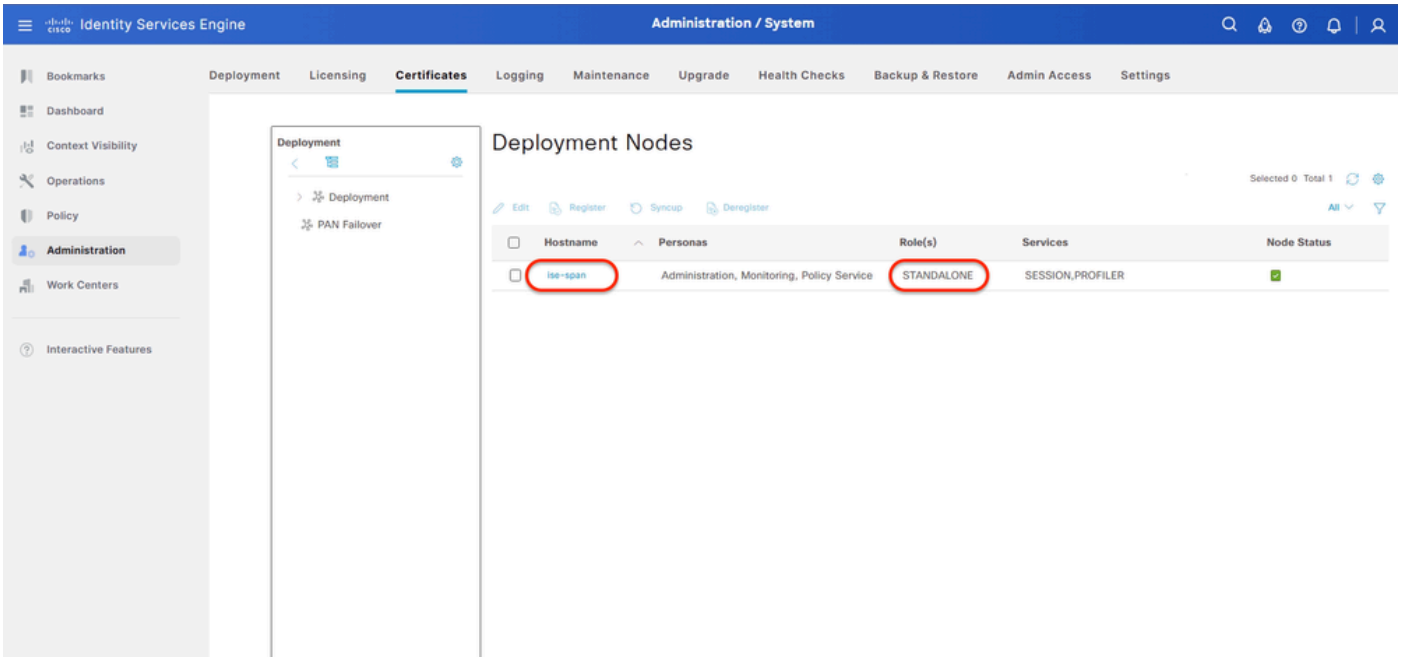


New Admin Certificate (ise-ppan)

Step 3. Renew admin certificate of the secondary nodes.

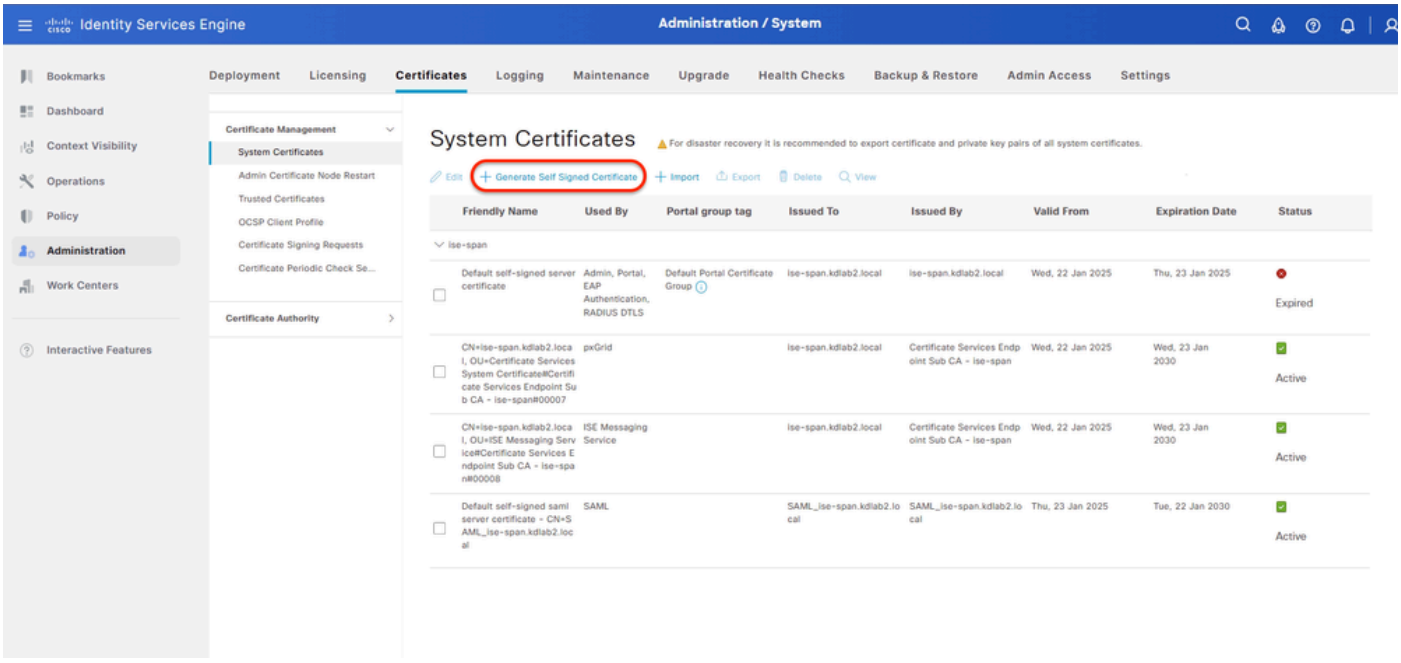
1. Confirm the secondary node on standalone deployment after deregistered from the distributed deployment.

Browse the node via GUI (**https://<FQDN/IP>**) and navigate to **Administration > System > Deployment**.



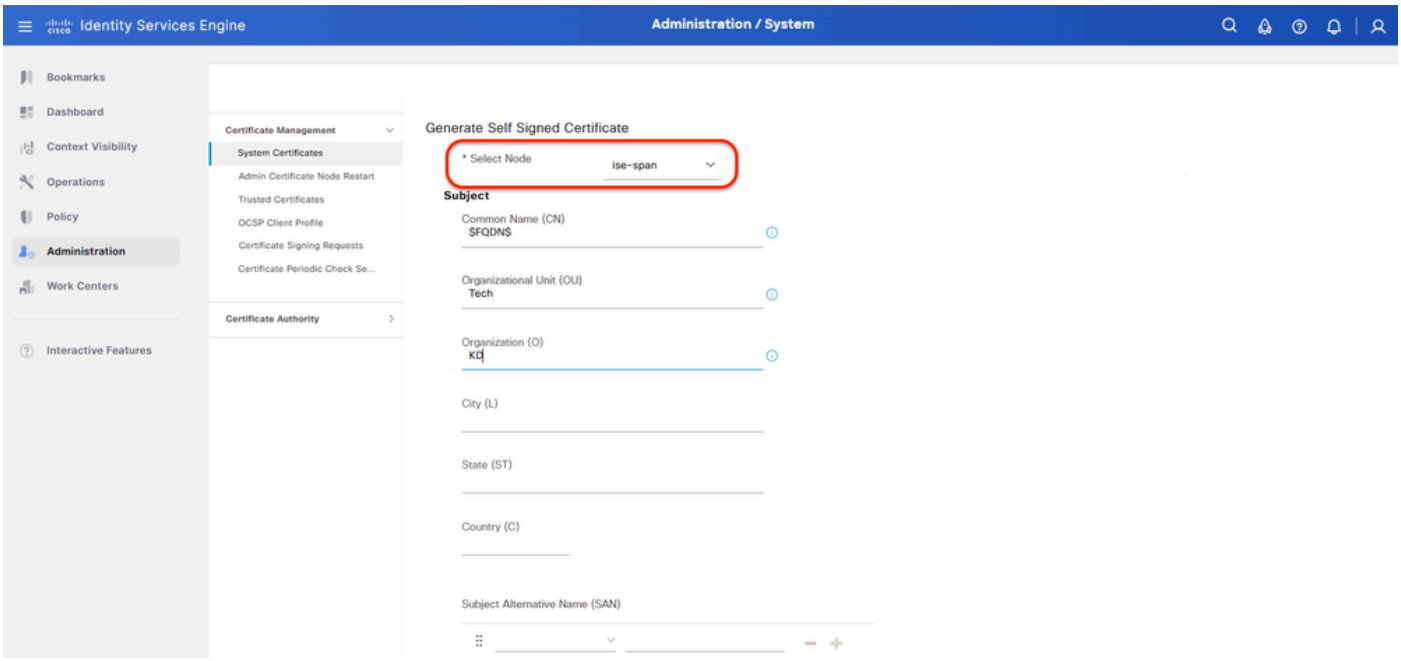
(ise-span) on Standalone Deployment

2. Navigate to **Administration > System > Certificates > Certificate Management > System Certificates**. Click **+Generate Self Signed Certificate**.



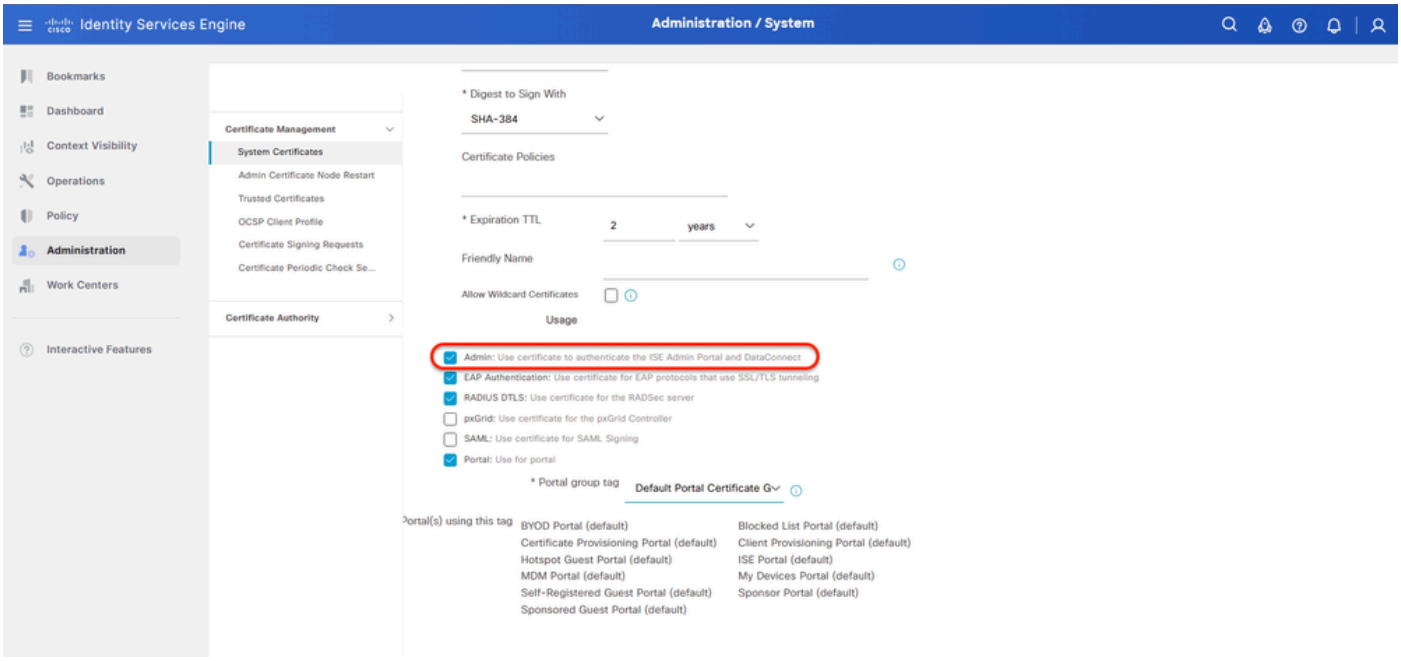
Generate new Self-Signed Admin Certificate

3. **Select** the (**ise-span**) and fill the **certificate information**.



Select the Node

4. Check [√] the **Admin** usage.



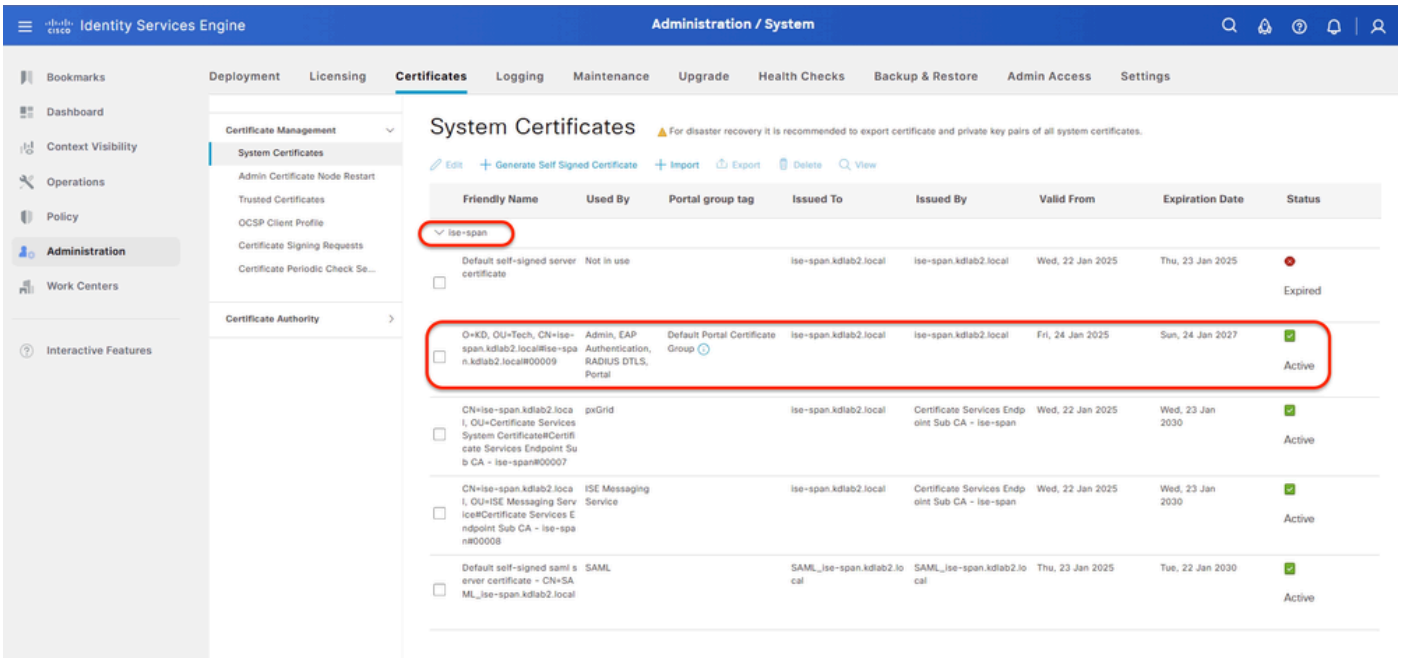
Admin Usage

Note: Changing the certificate of the admin role certificate on ISE node restarts services.

5. Click **Submit**.

6. Verify the new admin certificate on (**ise-span**).

Navigate to **Administration > System > Certificates > Certificate Management > System Certificates > Expand** (**ise-span**).

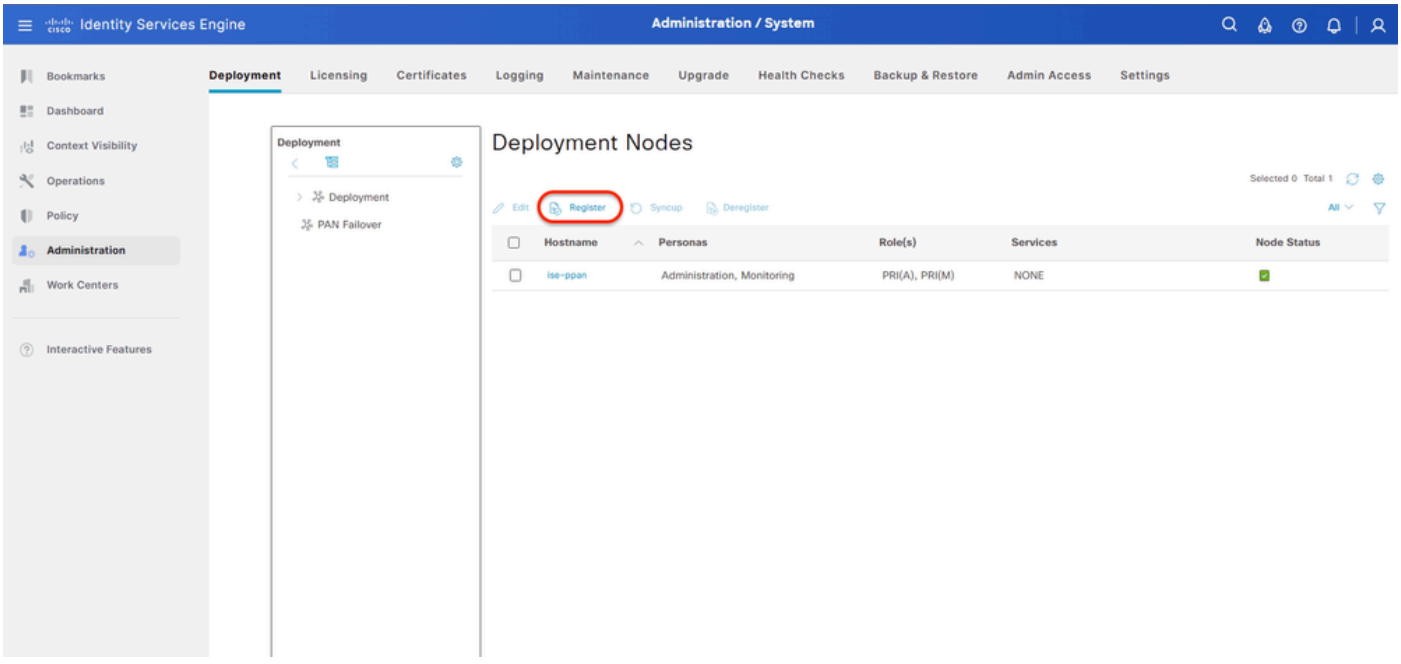


New Admin Certificate (ise-span)

Step 4. Register the **secondary nodes** to the distributed deployment.

Set up your deployment personas and roles as it was before (Admin, MNT, PSN, etc).

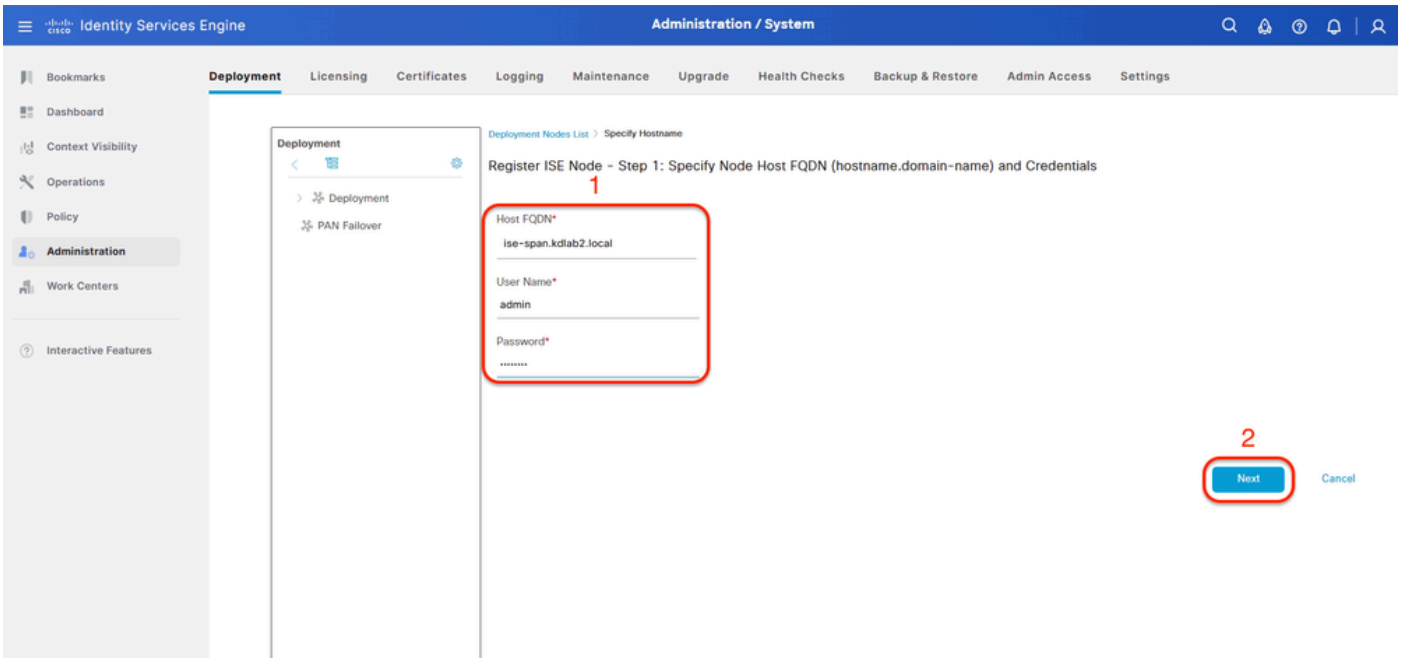
1. From Primary Admin Node (PPAN) GUI. Navigate to **Administration > System > Deployment**. Click **Register**.



Primary Admin Node (PPAN) GUI

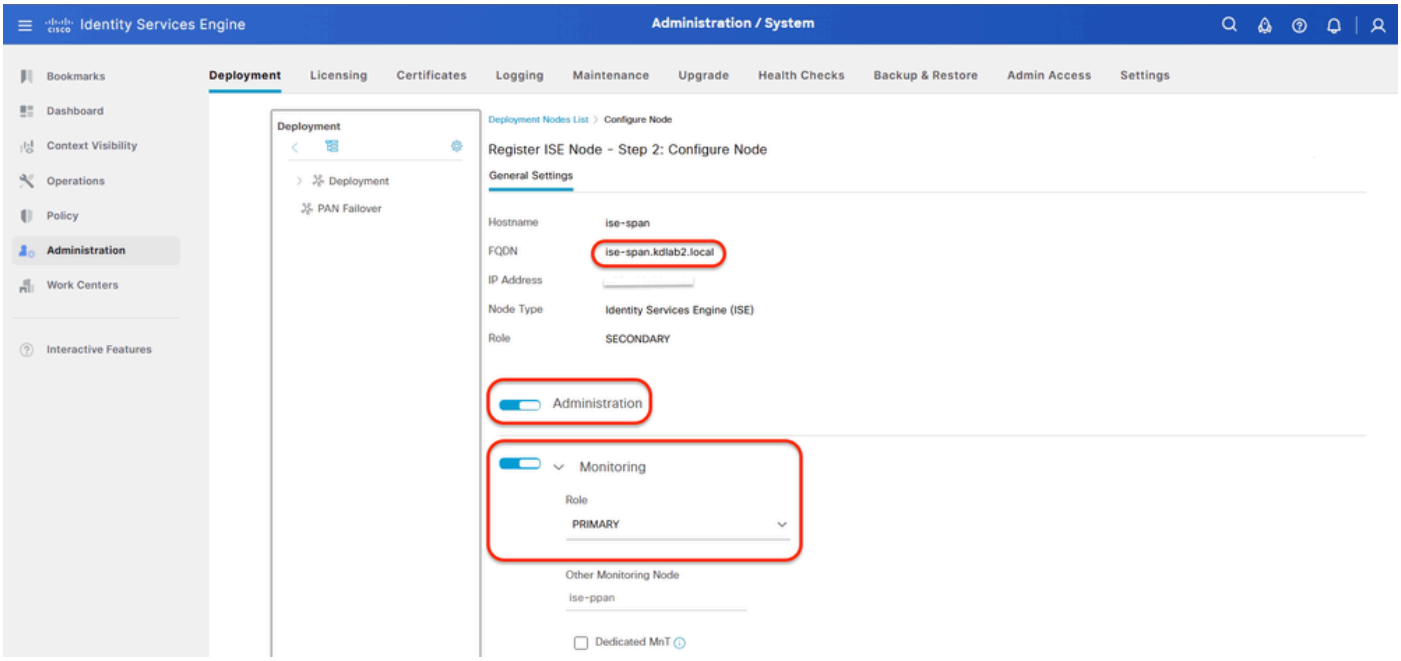
2. Enter the **FQDN** and credentials of the secondary node (**User Name/Password**).

Enter the DNS-resolvable fully qualified domain name (FQDN) of the standalone node that you are going to register. The FQDN of the (PPAN) and the node being registered must be resolvable from each other.



Enter Secondary Node Access

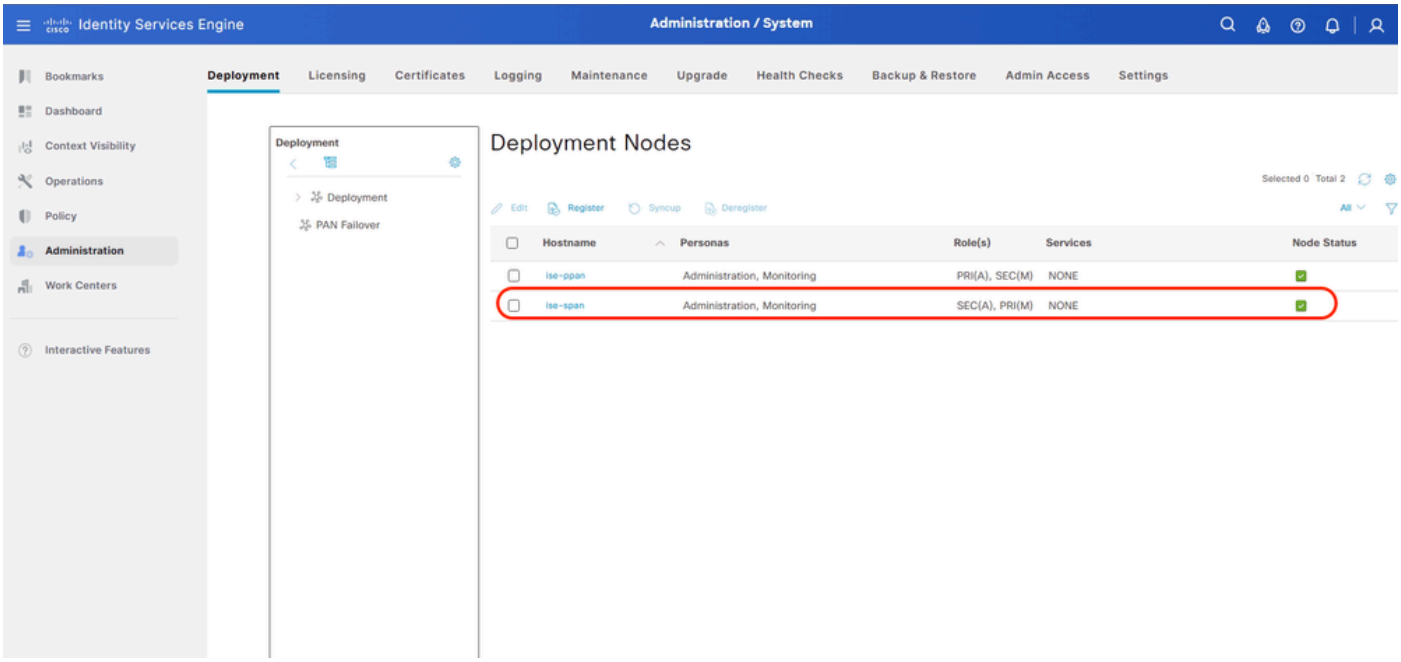
3. Enable the **correct persona** and **services**.



Register Secondary Node (ise-span)

Step 5. Verify the deployment status.

Navigate to **Administration > System > Deployment**.



(ise-span) Added to the Deployment

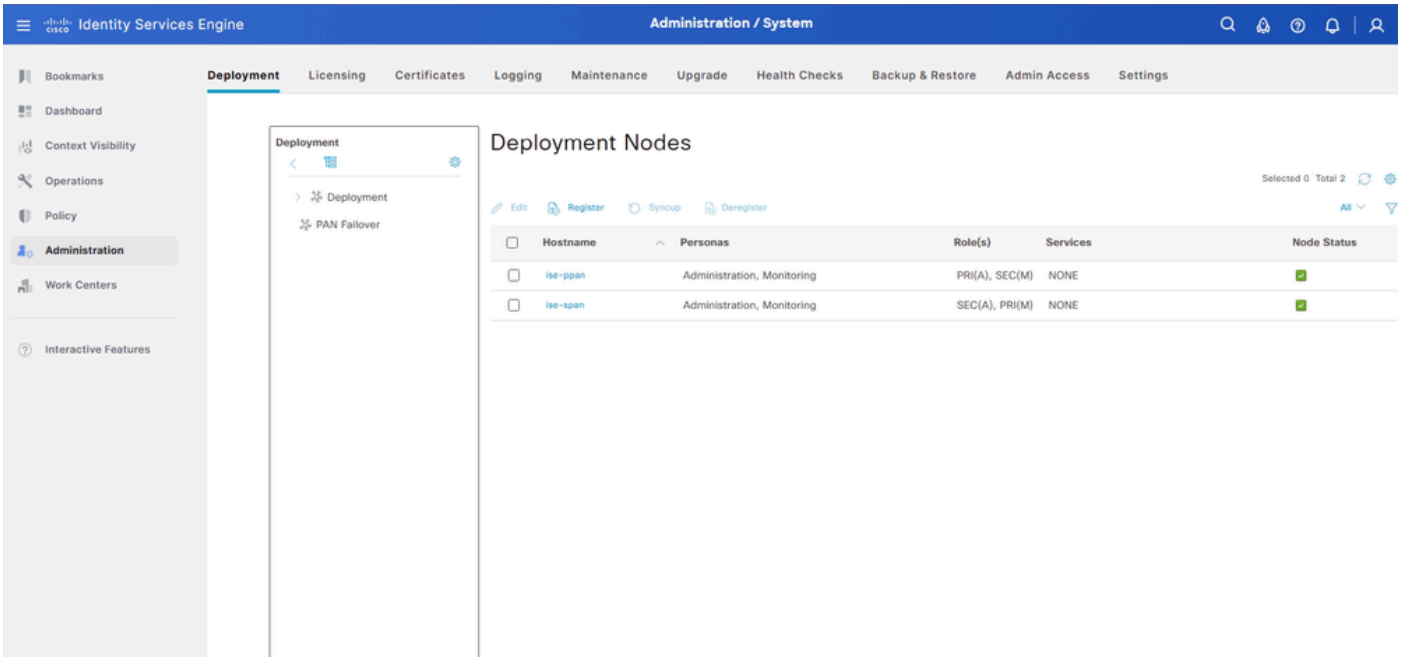
Troubleshoot

Use Case 1: Deregistered Secondary Node Stuck on Distributed State (ise-psn1)

Validate the Status

Step 1. Confirm the distributed deployment status.

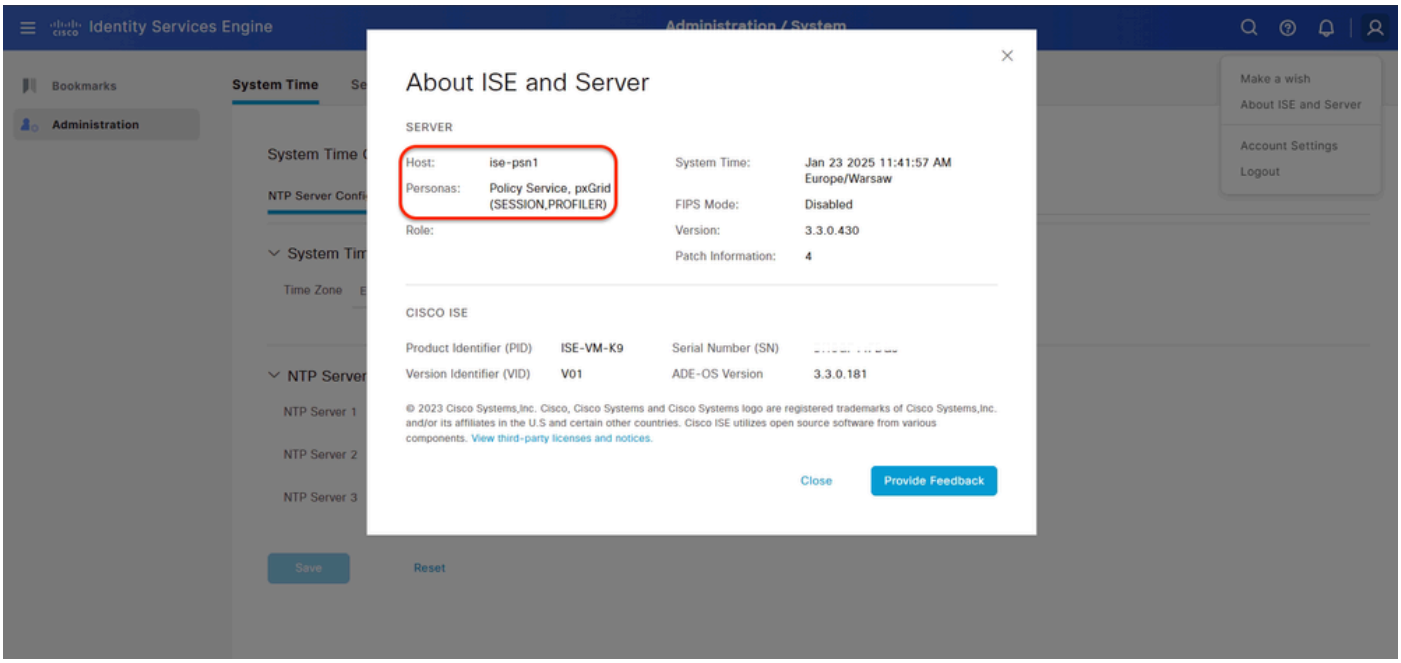
From Primary Admin Node (PPAN) GUI. Navigate to **Administration > System > Deployment**. You can confirm this node (**ise-psn1**) is already deregisted.



(PPAN) Deployment Nodes

Step 2. Confirm the (**ise-psn1**) node status.

Browse the secondary node via GUI (**KD lab local**) and navigate **Log in > About ISE and Server**.

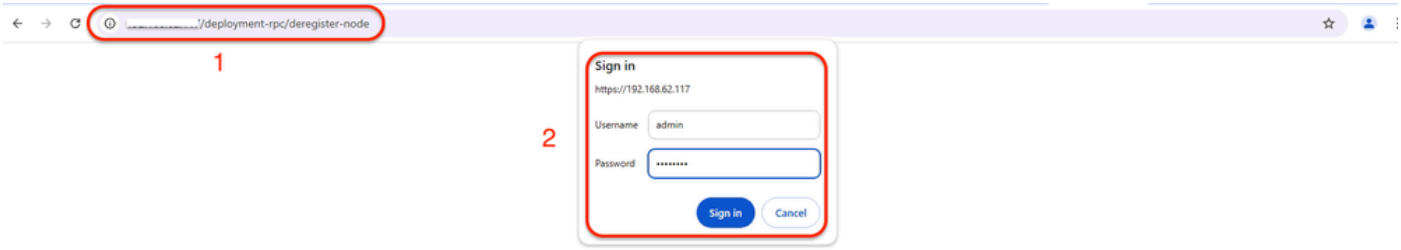


Secondary Node (ise-psn1) Stuck on Distributed Deployment Status

Workaround

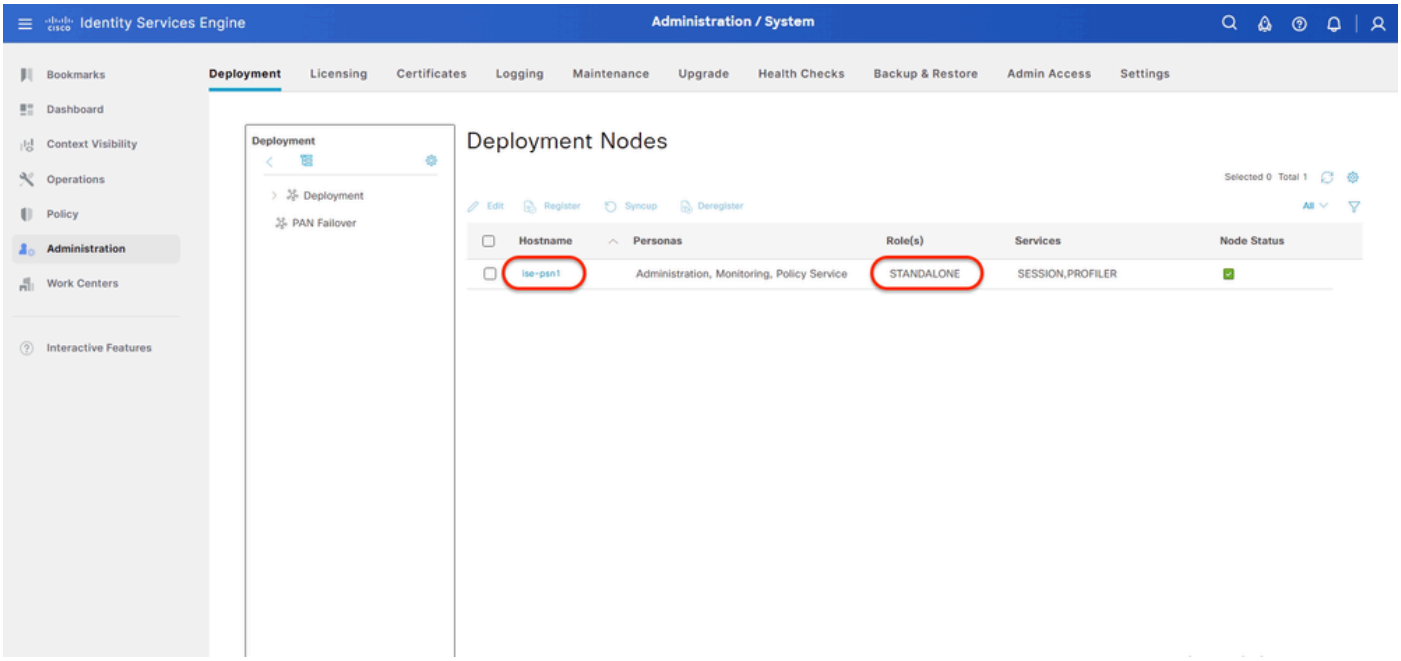
Step 1. Deregister the (**ise-psn1**) node manually.

Enforce the (**ise-psn1**) node to standalone deployment via GUI (**Deregister Node**).



Deregister the Node Manually - GUI

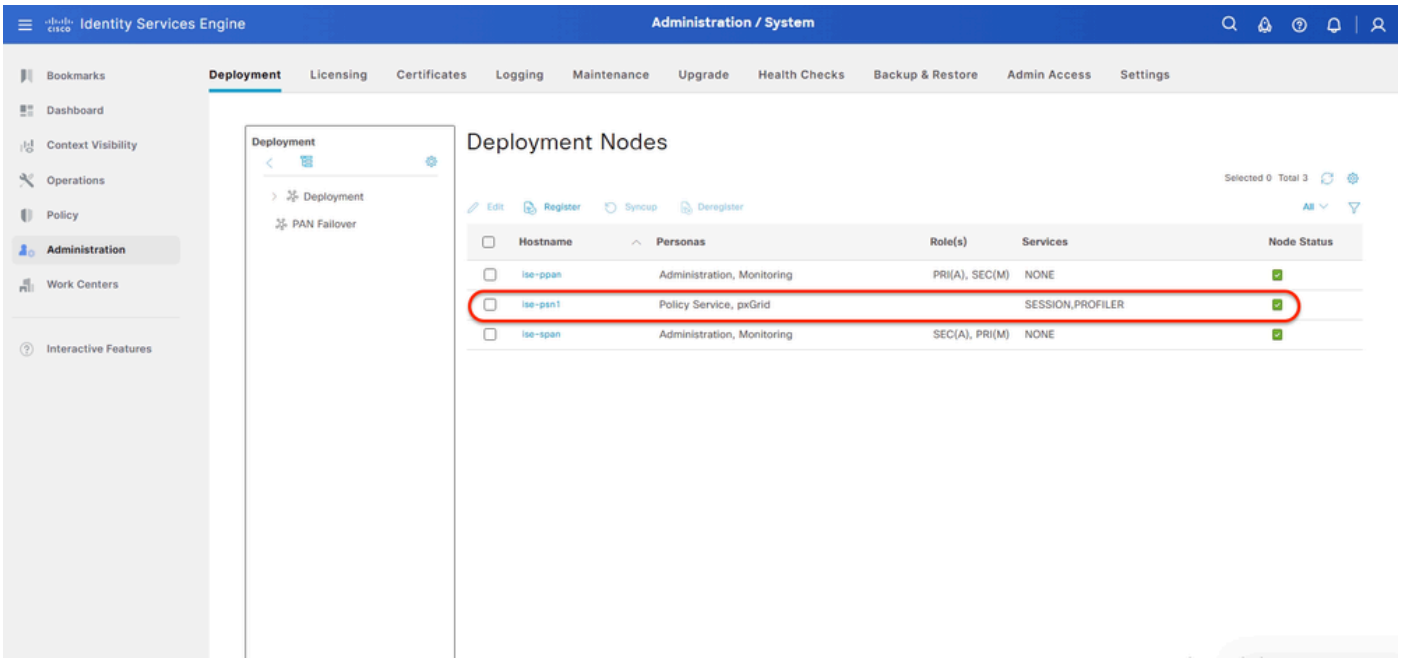
Step 2. Verify the (**ise-psn1**) now on standalone deployment.



(ise-psn1) on Standalone Deployment

Step 3. Once you can confirm the node on standalone status, proceed with the same steps in **Action Plan** section:

1. Renew admin certificate of the (**ise-psn1**) Node.
2. Register the(**ise-psn1**) node to the distributed deployment.
3. Verify the deployment status.



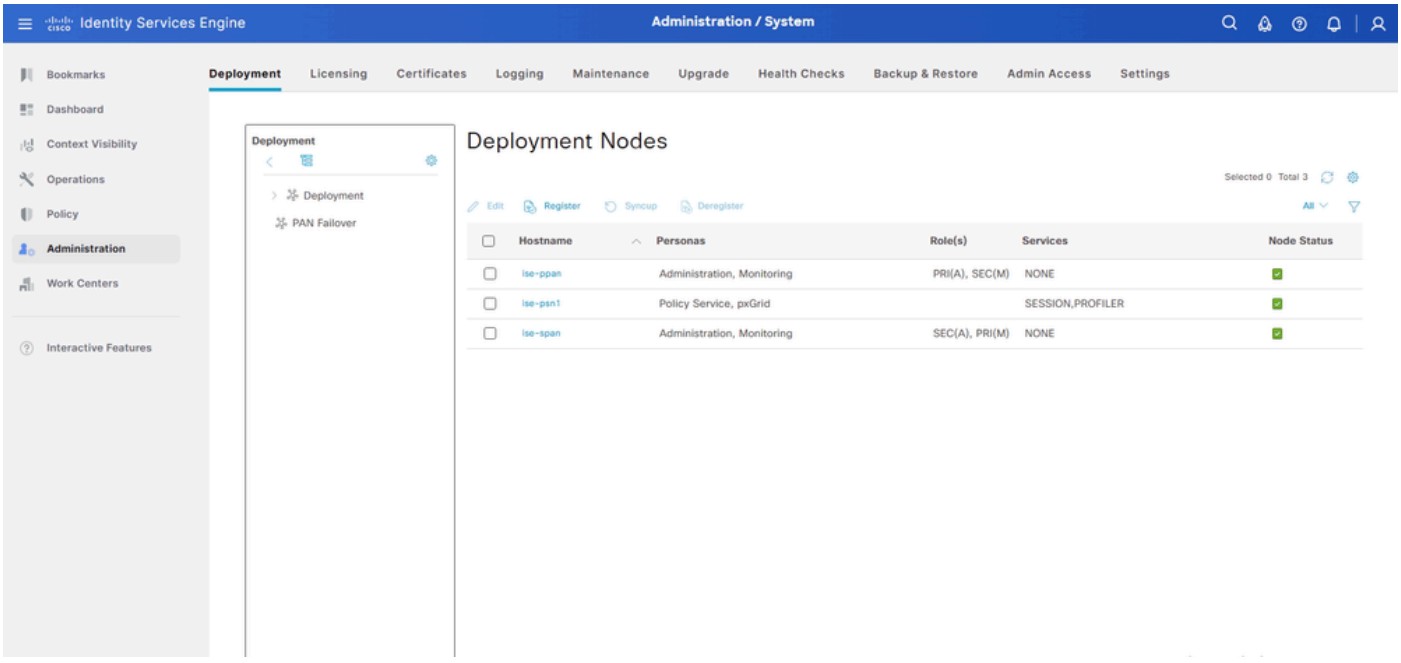
(ise-psn1) Added to the Deployment

Use Case 2: Deregistered Secondary Node GUI Unreachable (ise-psn2)

Validate the Status

Step 1. Confirm the distributed deployment status.

From Primary Admin Node (PPAN) GUI. Navigate to **Administration > System > Deployment**. You can confirm this node (**ise-psn2**) is already deregisted.



(PPAN) Deployment Nodes

Step 2. Confirm the (**ise-psn2**) node status.

Due to the admin certificate is expired in some cases you can hit these symptoms:

- (**ise-psn2**) GUI unreachable.
- (**ise-psn2**) CLI (**show application status ise**) ISE application is stuck on (**initializing** or **not running**).
- (**ise-psn2**) CLI (**show tech**) the node already on standalone deployment.

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

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

(ise-psn2) on Standalone Deployment

Workaround

Step 1. Renew admin certificate of the (**ise-psn2**) Node.

1. Log in to (**ise-psn2**) via CLI.
2. Enter **application configure ise**.
3. Enter **31** ([31] Generate Self-Signed Admin Certificate)).
4. Do you want to continue? y/[n]: **y**
5. Do you want to replace existing certificate after generation? y/[n]: **y**

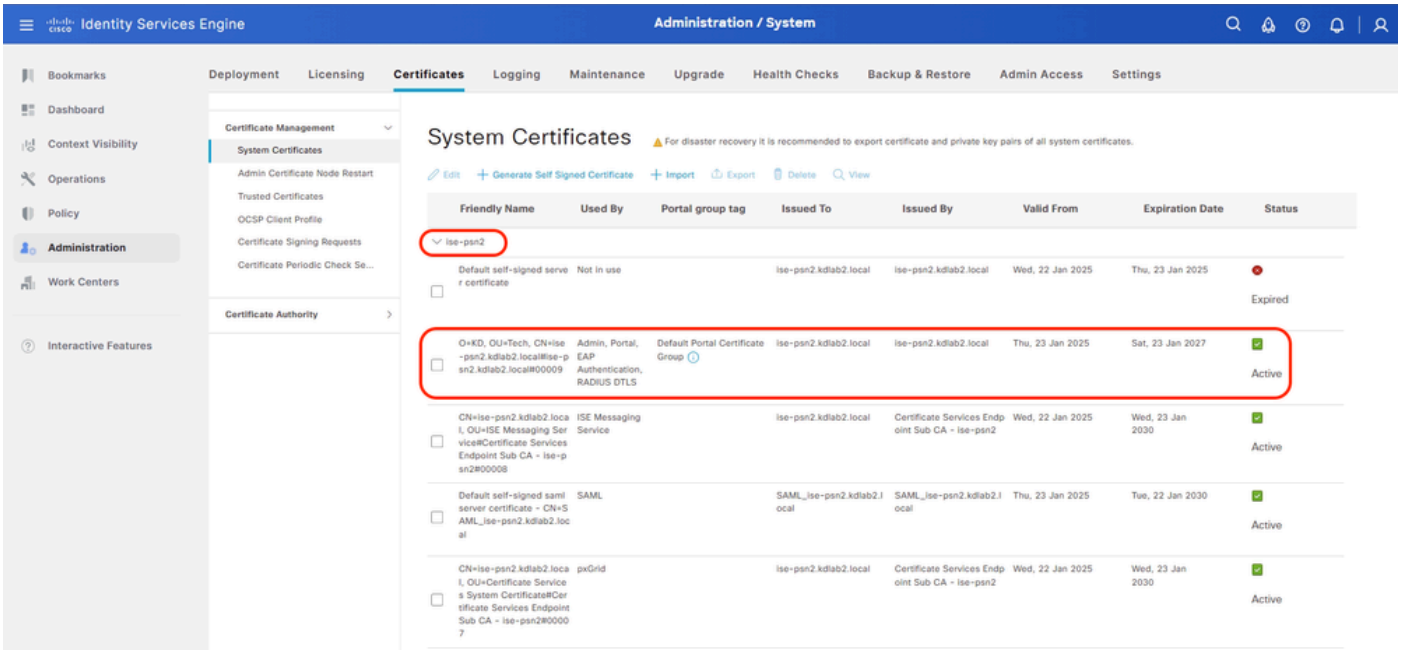
```
ise-psn2/admin#application configure ise

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
[31]Generate Self-Signed Admin Certificate
[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
```

Renew (ise-psn1) Admin Certificate

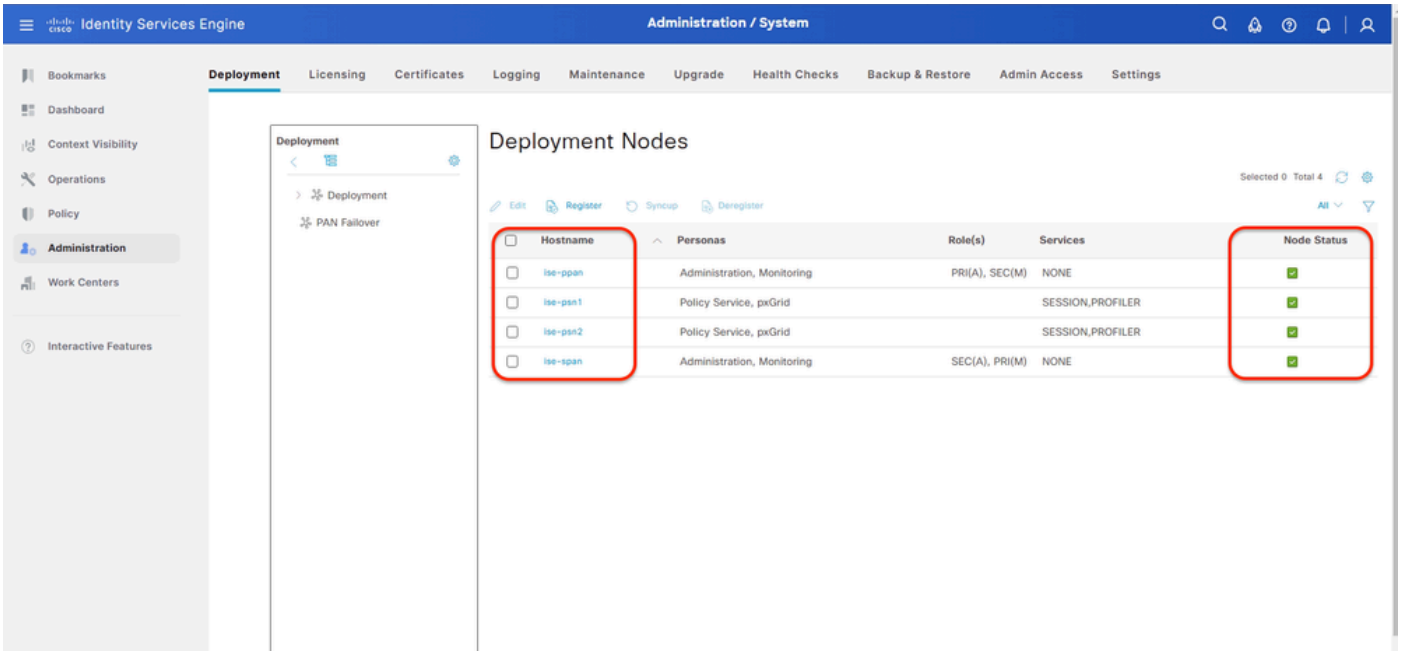
6. Verify the new admin certificate on (**ise-psn2**).



New Admin Certificate (ise-psn2)

Step 2. Register the (**ise-psn2**) node to the distributed deployment.

Step 3. Verify the deployment status.



The Deployment in Sync Again!

Related Information

- Deployment of Cisco ISE
- Certificate Management in Cisco ISE

- Configure Certificate Renewals on ISE