Configurer TACACS+ sur TLS 1.3 sur un périphérique IOS XR avec ISE

Table des matières

Introduction

Ce document décrit un exemple pour TACACS+ sur TLS avec Cisco Identity Services Engine (ISE) comme serveur et un périphérique Cisco IOS® XR comme client.

Aperçu

Le protocole TACACS+ (Terminal Access Controller Access-Control System Plus) [RFC8907] permet une administration centralisée des périphériques pour les routeurs, les serveurs d'accès réseau et les autres périphériques réseau via un ou plusieurs serveurs TACACS+. Il fournit des services d'authentification, d'autorisation et de comptabilité (AAA), spécialement conçus pour les cas d'utilisation d'administration de périphériques.

TACACS+ sur TLS 1.3 [RFC8446] améliore le protocole en introduisant une couche de transport sécurisée, protégeant les données hautement sensibles. Cette intégration garantit la confidentialité, l'intégrité et l'authentification de la connexion et du trafic réseau entre les clients et les serveurs TACACS+.

Utilisation de ce guide

Ce guide divise les activités en deux parties pour permettre à ISE de gérer l'accès administratif pour les périphériques réseau basés sur Cisco IOS XR.
· Partie 1 : configuration d'ISE pour l'administration des périphériques
· Partie 2 : configuration de Cisco IOS XR pour TACACS+ sur TLS

Conditions préalables

Exigences

Conditions requises pour configurer TACACS+ sur TLS :

- Une autorité de certification (CA) pour signer le certificat utilisé par TACACS+ sur TLS pour signer les certificats d'ISE et de périphériques réseau.
- Le certificat racine de l'autorité de certification (CA).
- Les périphériques réseau et ISE sont accessibles via DNS et peuvent résoudre les noms d'hôte.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance virtuelle ISE VMware, version 3.4, correctif 2
- Routeur Cisco 8201, version 25.3.1

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.

Licences

Une licence Device Administration vous permet d'utiliser les services TACACS+ sur un noeud Policy Service. Dans un déploiement autonome haute disponibilité (HA), une licence d'administration de périphériques vous permet d'utiliser les services TACACS+ sur un noeud Policy Service unique dans la paire HA.

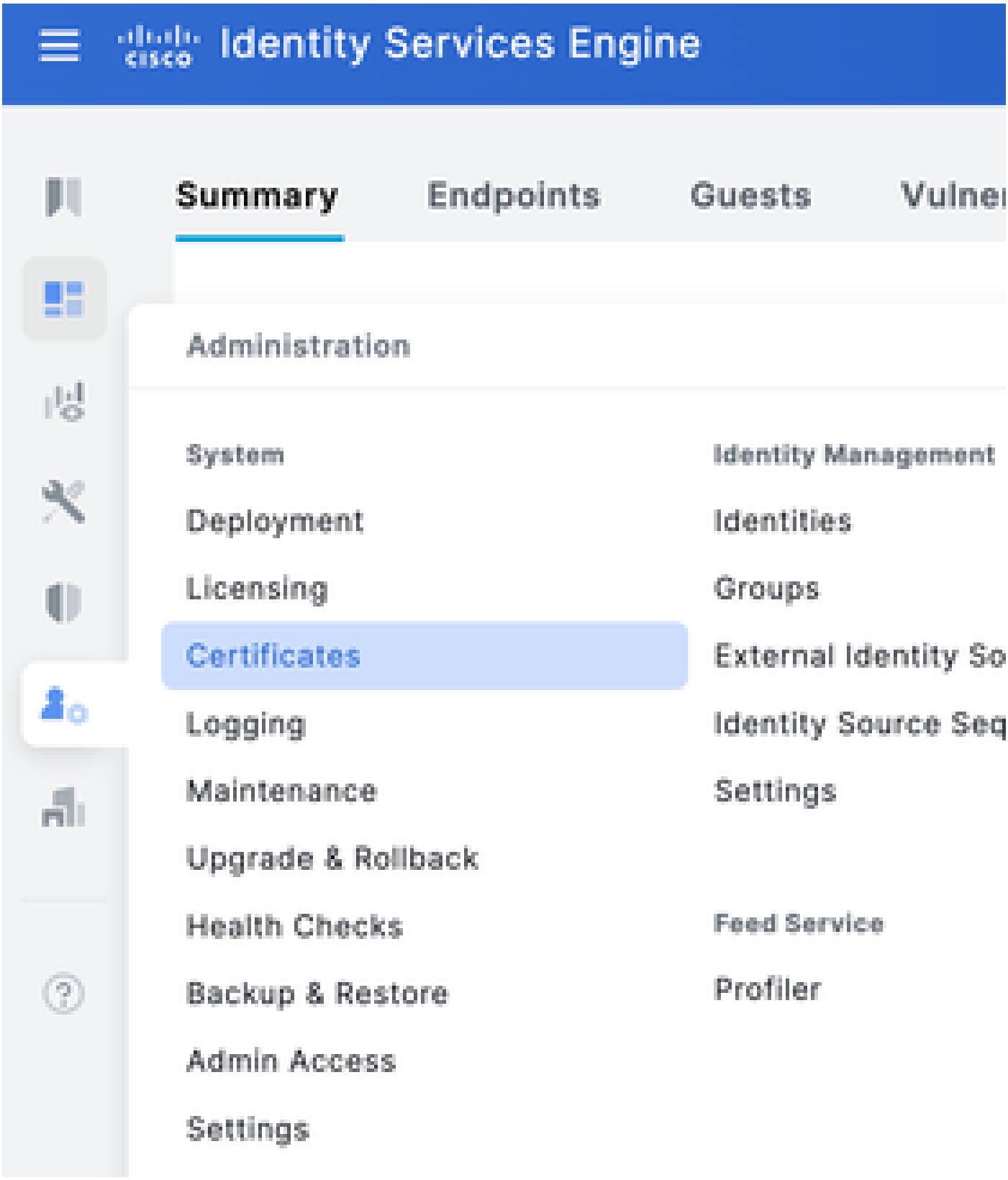
Partie 1 - Configuration ISE pour l'administration des périphériques

Générer une demande de signature de certificat pour l'authentification du serveur TACACS+

Étape 1. Connectez-vous au portail Web d’administration ISE à l’aide de l’un des navigateurs pris en charge.

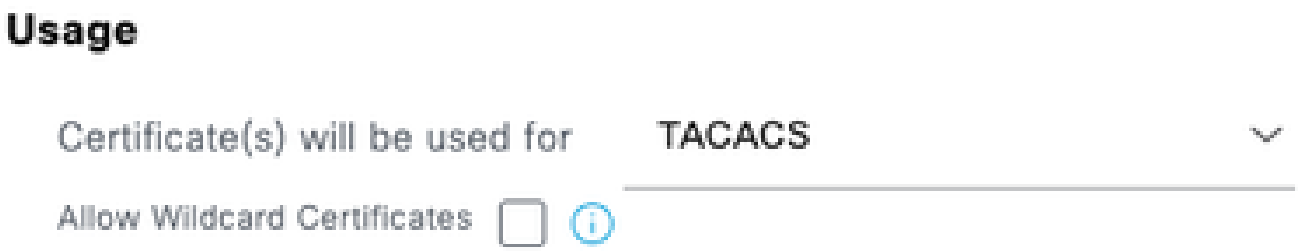
Par défaut, ISE utilise un certificat auto-signé pour tous les services. La première étape consiste à générer une demande de signature de certificat (CSR) pour la faire signer par notre autorité de certification (CA).

Étape 2. Accédez à Administration > System > Certificates.

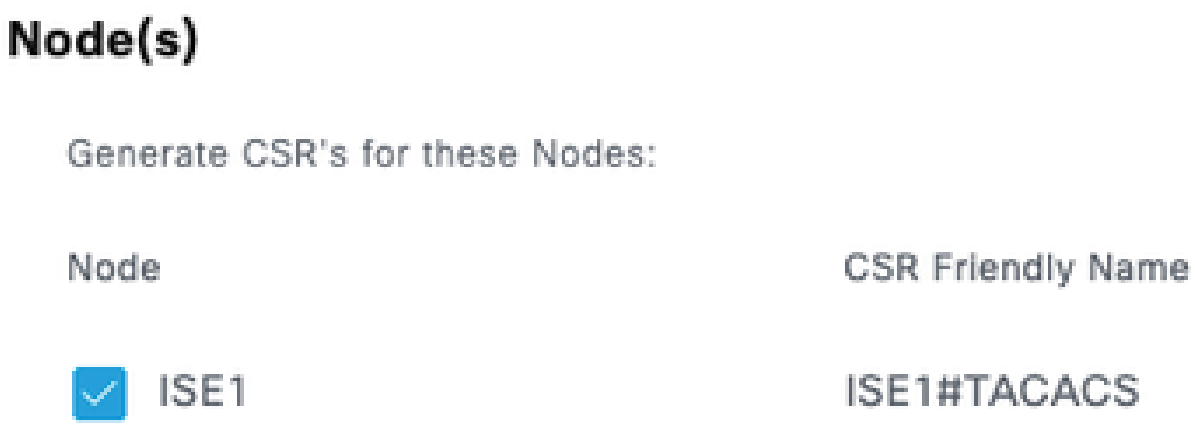


Étape 3. Sous Certificate Signing Requests, cliquez sur Generate Certificate Signing Request.

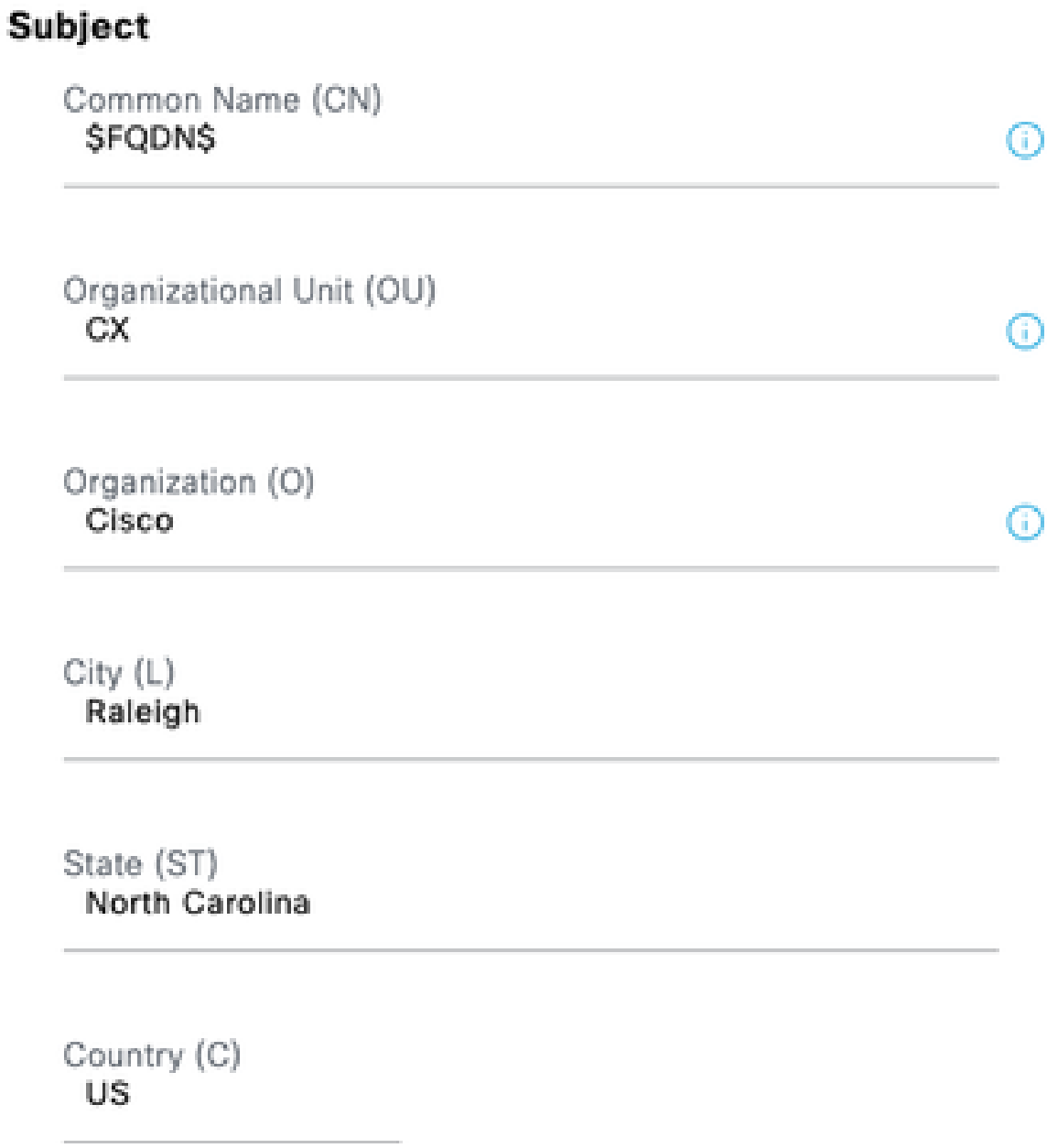
Étape 4. Sélectionnez TACACS dans Utilisation.



Étape 5. Sélectionnez les PSN sur lesquels TACACS+ est activé.

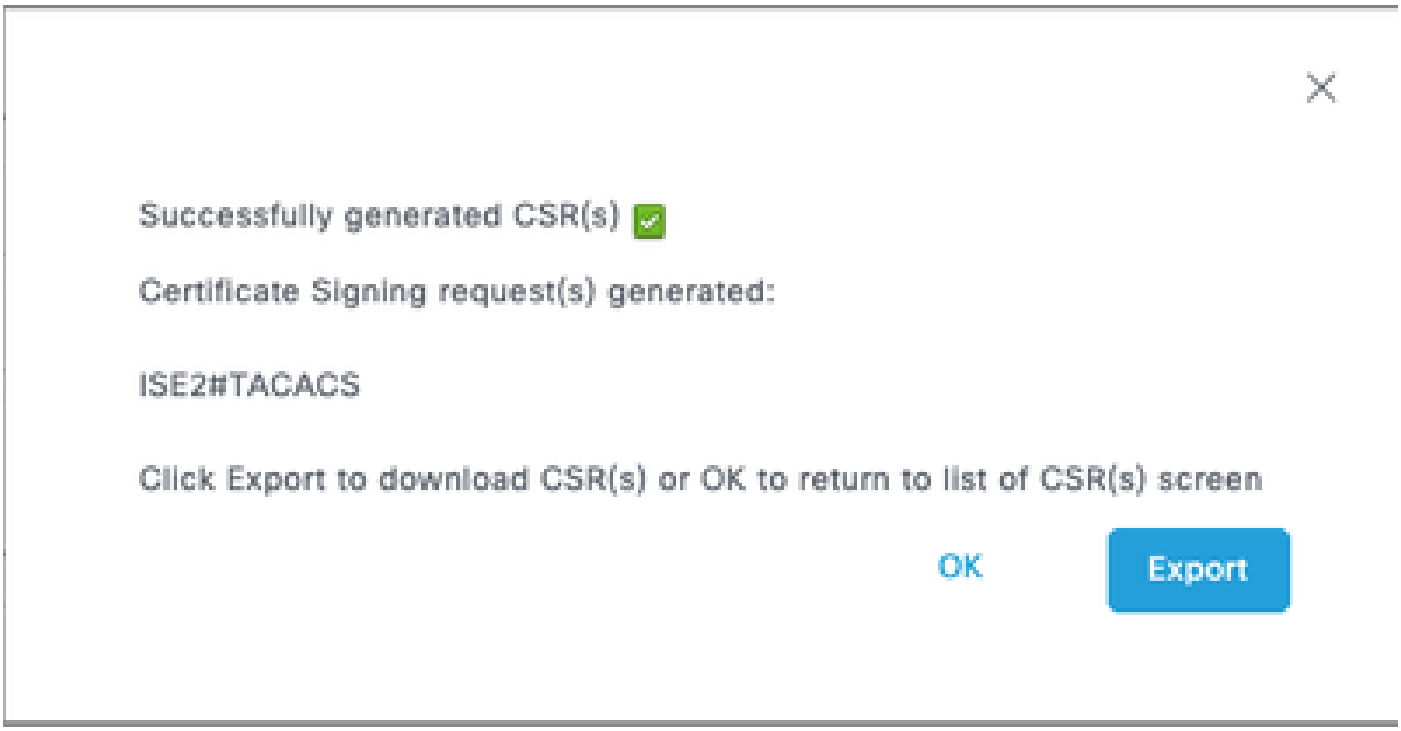


Étape 6. Remplissez les champs Subject avec les informations appropriées.



Étape 7. Ajoutez le nom DNS et l'adresse IP sous le nom alternatif du sujet (SAN).

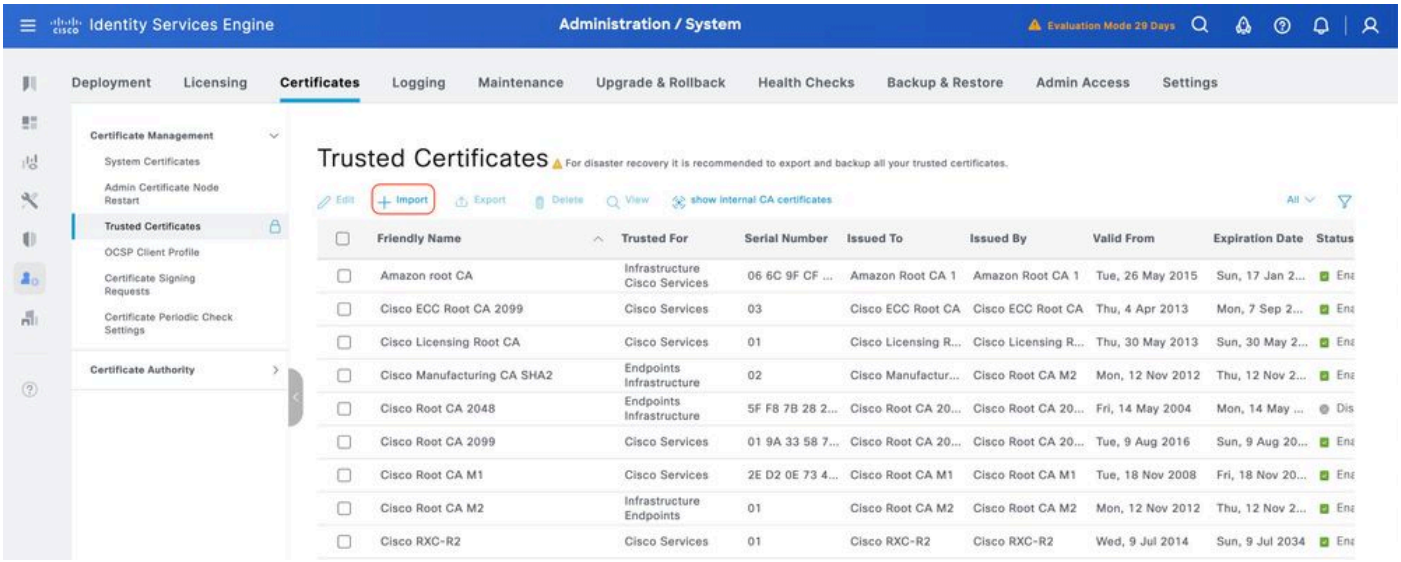
Étape 8. Cliquez sur Generate, puis sur Export.



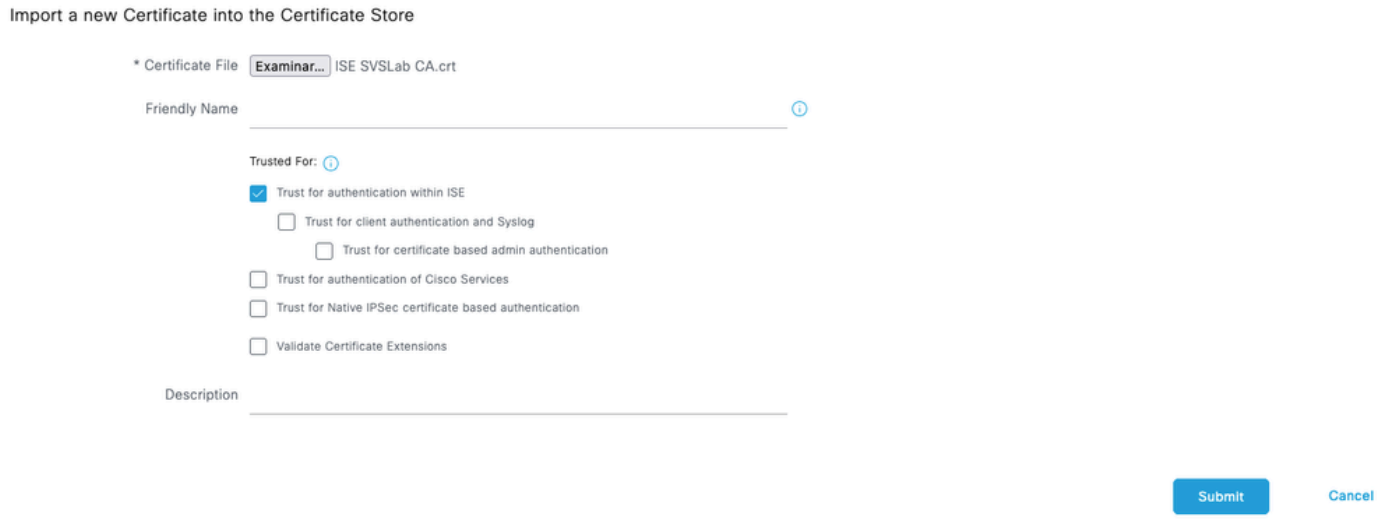
Vous pouvez maintenant faire signer le certificat (CRT) par votre autorité de certification (CA).

Télécharger le certificat CA racine pour l'authentification du serveur TACACS+

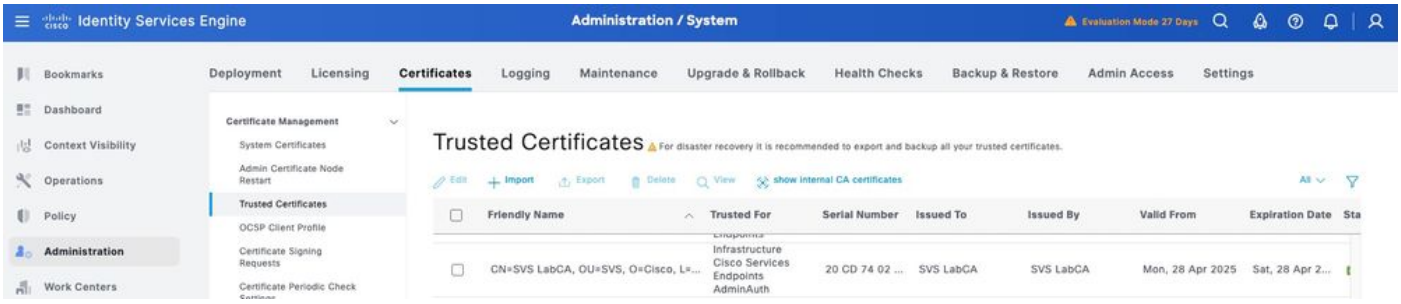
Étape 1.Accédez à Administration > System > Certificates. Sous Certificats approuvés, cliquez sur Importer.



Étape 2. Sélectionnez le certificat émis par l'autorité de certification (AC) qui a signé votre demande de signature de certificat (CSR) TACACS. Assurez-vous que le Confiance pour l'authentification dans ISE est activée.



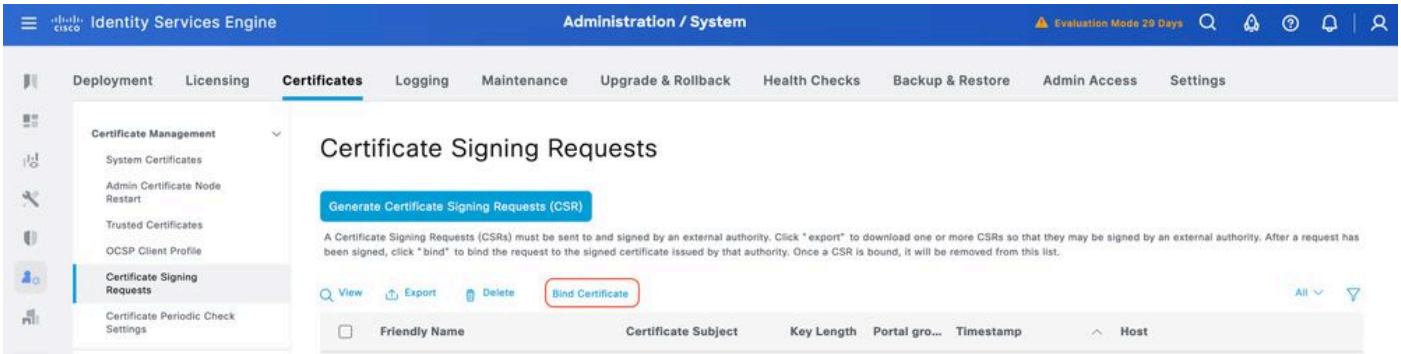
Cliquez sur Envoyer. Le certificat doit maintenant apparaître sous Certificats approuvés.



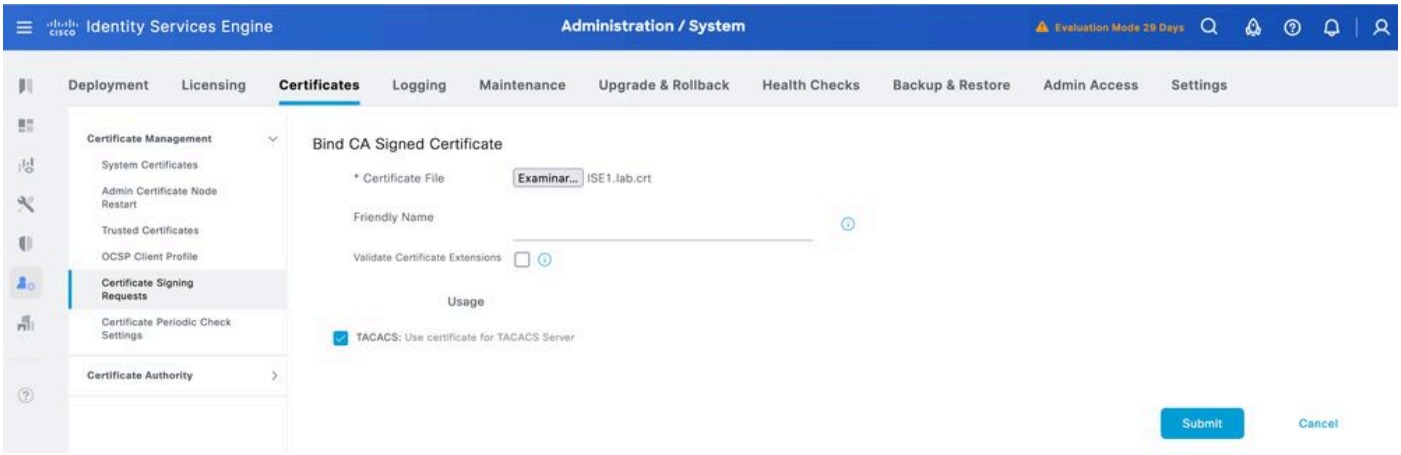
Lier la demande de signature de certificat signé (CSR) à ISE

Une fois la demande de signature de certificat (CSR) signée, vous pouvez installer le certificat signé sur ISE.

Étape 1. Accédez à Administration > System > Certificates. Sous Certificate Signing Requests, sélectionnez le CSR TACACS généré à l'étape précédente et cliquez sur Bind Certificate.

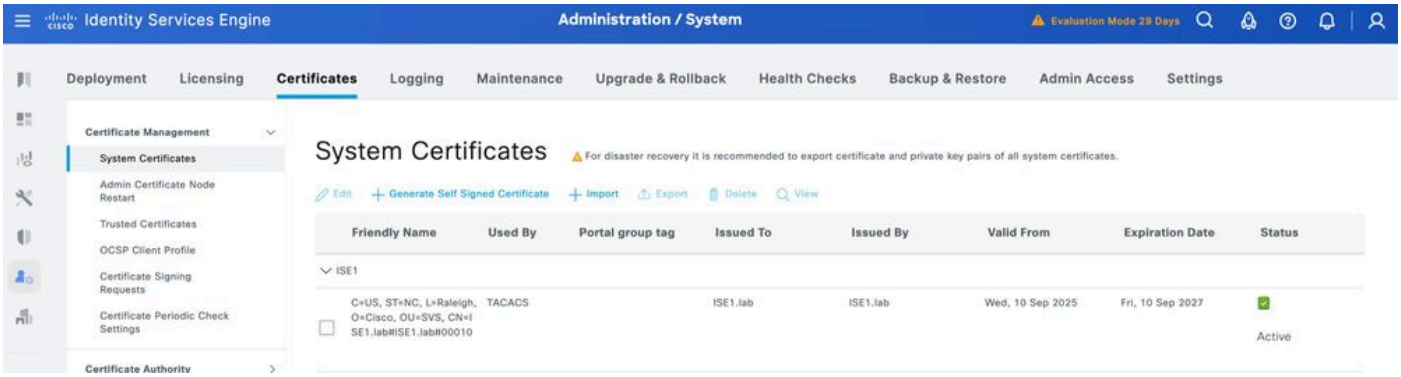


Étape 2. Sélectionnez le certificat signé et assurez-vous que la case à cocher TACACS sous Usage reste sélectionnée.



Étape 3. Cliquez sur Envoyer. Si vous recevez un avertissement concernant le remplacement du certificat existant, cliquez sur Yes pour continuer.

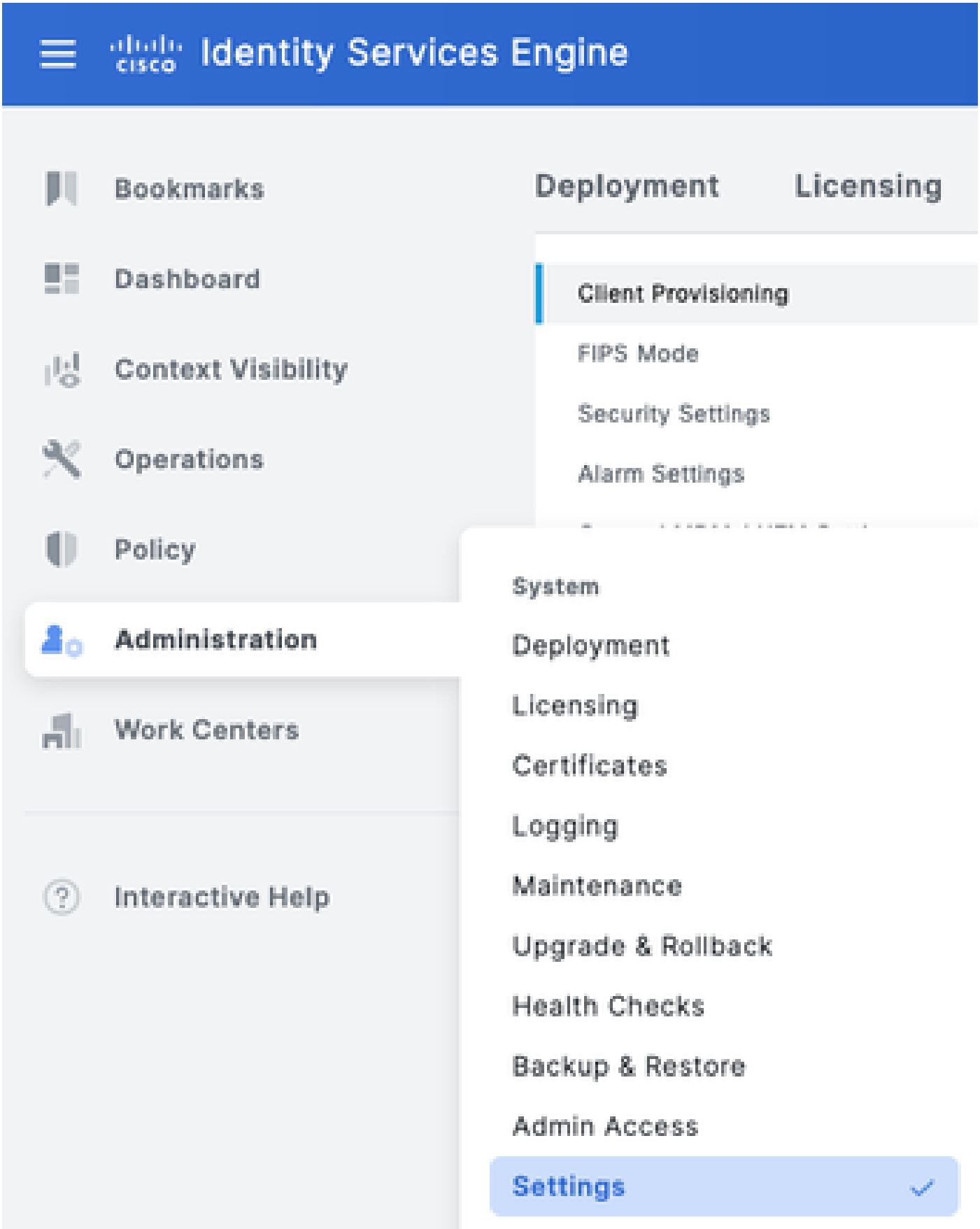
Le certificat doit maintenant être correctement installé. Vous pouvez le vérifier sous Certificats système.



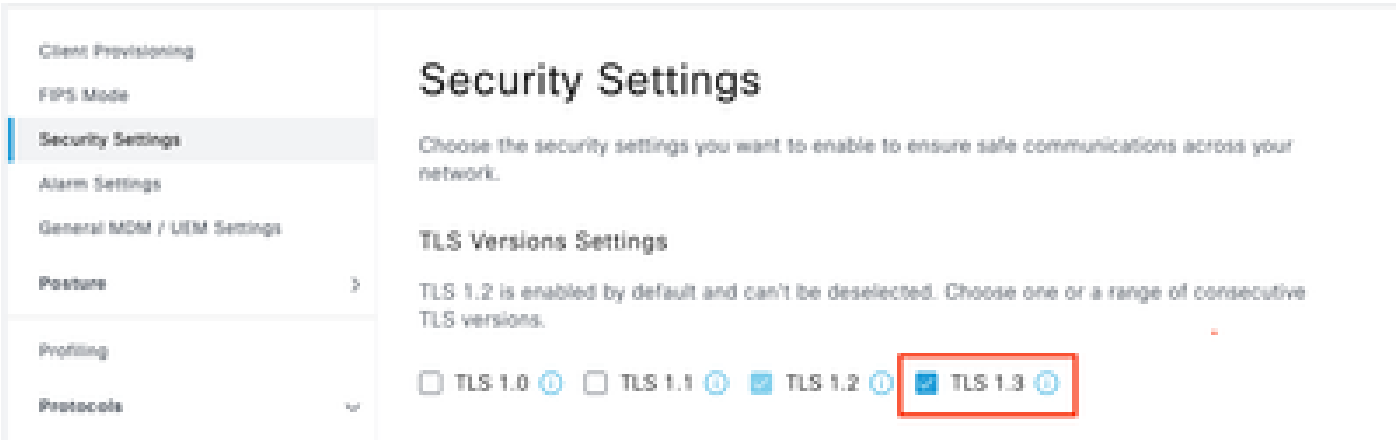
Activer TLS 1.3

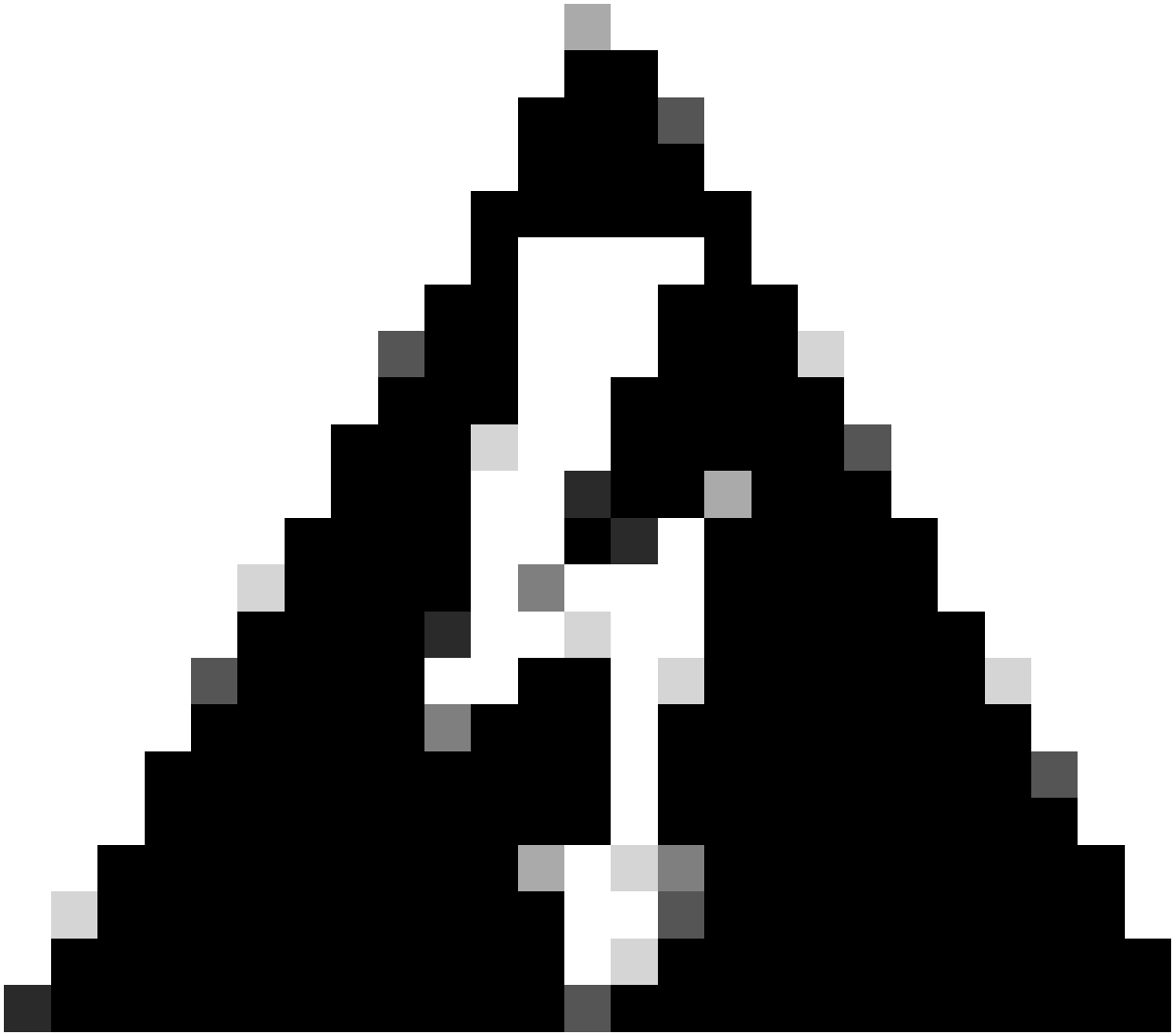
TLS 1.3 n'est pas activé par défaut dans ISE 3.4.x. Il doit être activé manuellement.

Étape 1.Accédez à Administration > System > Settings.



Étape 2. Cliquez sur Security Settings, activez la case à cocher en regard de TLS1.3 sous TLS Version Settings, puis cliquez sur Save.



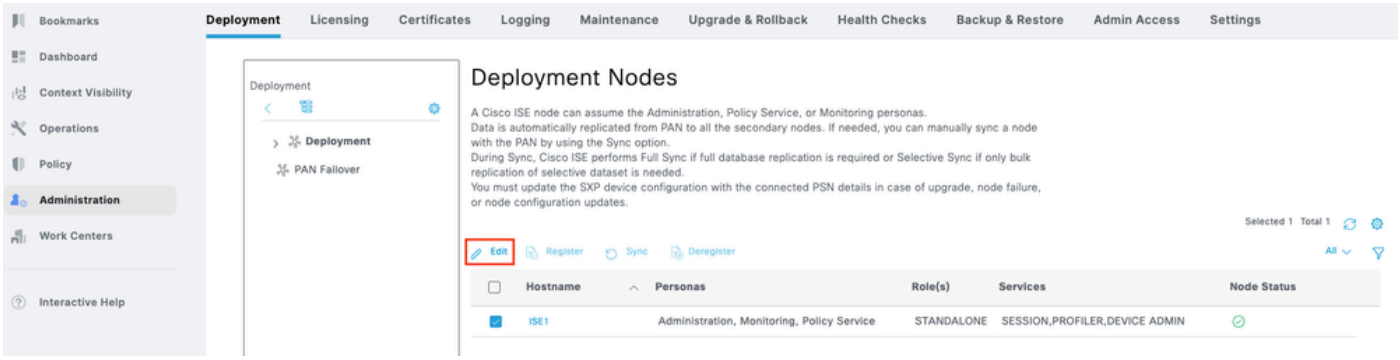


Avertissement : Lorsque vous modifiez la version TLS, le serveur d'applications Cisco ISE redémarre sur toutes les machines de déploiement Cisco ISE.

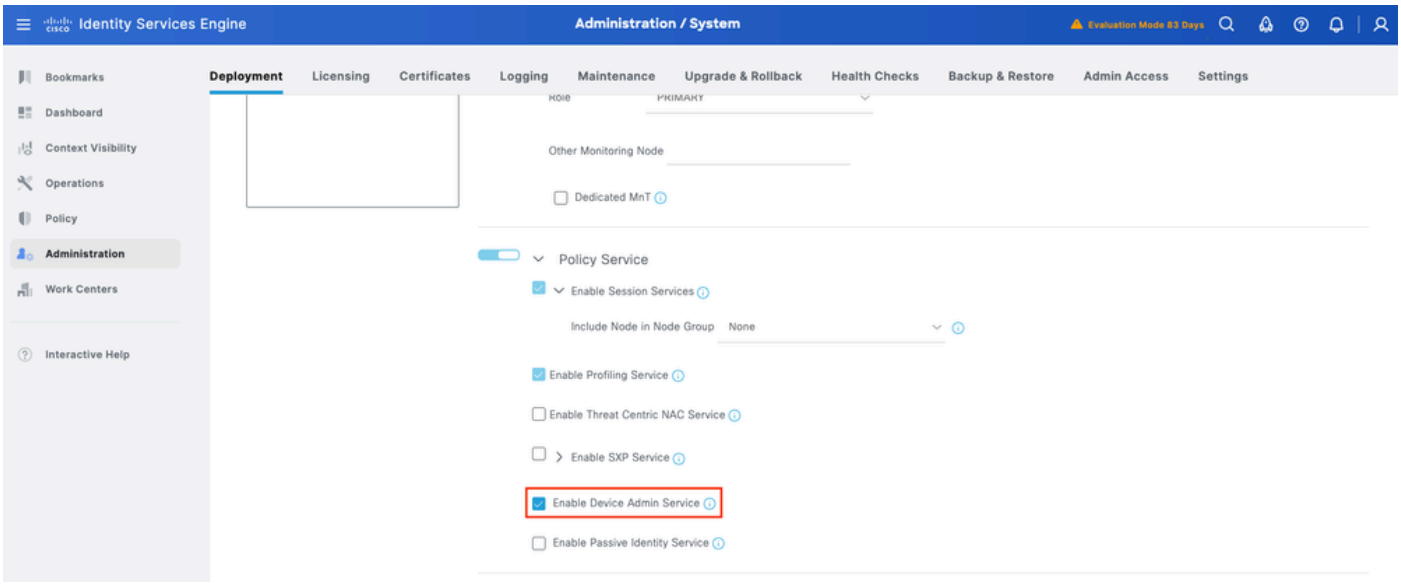
Activer l'administration des périphériques sur ISE

Le service d'administration des périphériques (TACACS+) n'est pas activé par défaut sur un noeud ISE. Pour activer TACACS+ sur un noeud PSN :

Étape 1. Accédez à Administration > System > Deployment. Cochez la case en regard du noeud ISE et cliquez sur Edit.



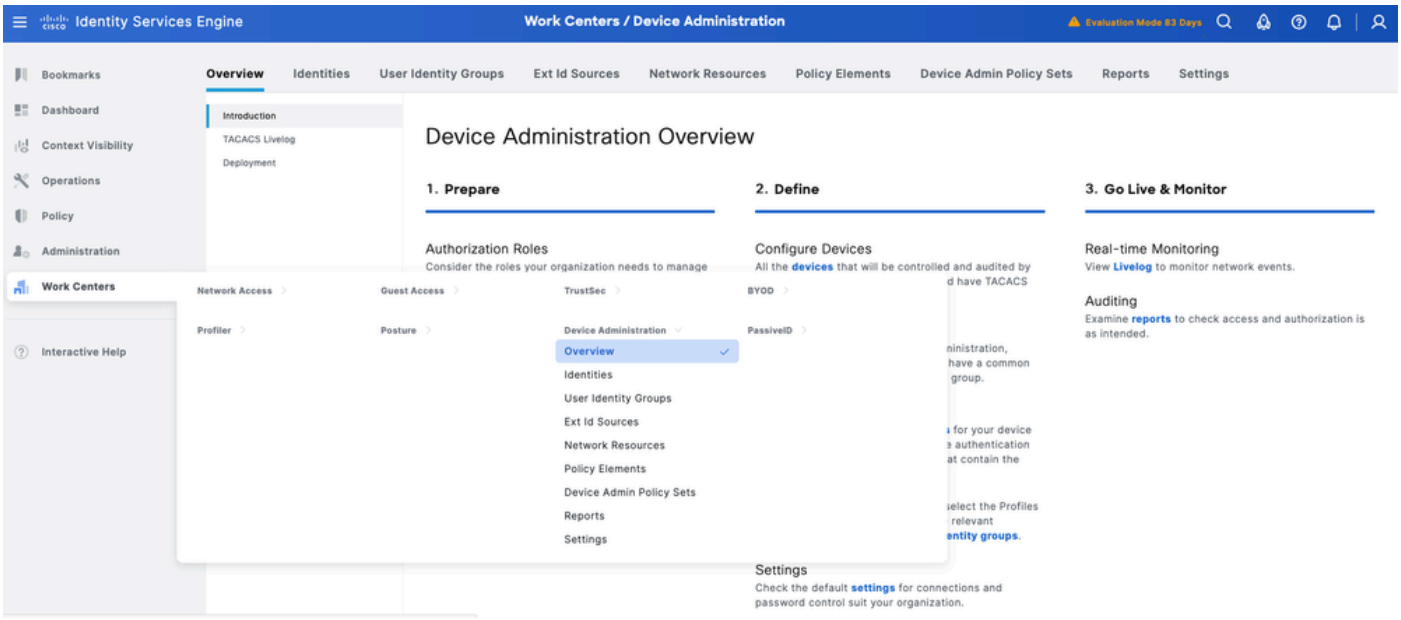
Étape 2.Sous GeneralSettings, faites défiler la page vers le bas et activez la case à cocher en regard de Enable Device Admin Service.



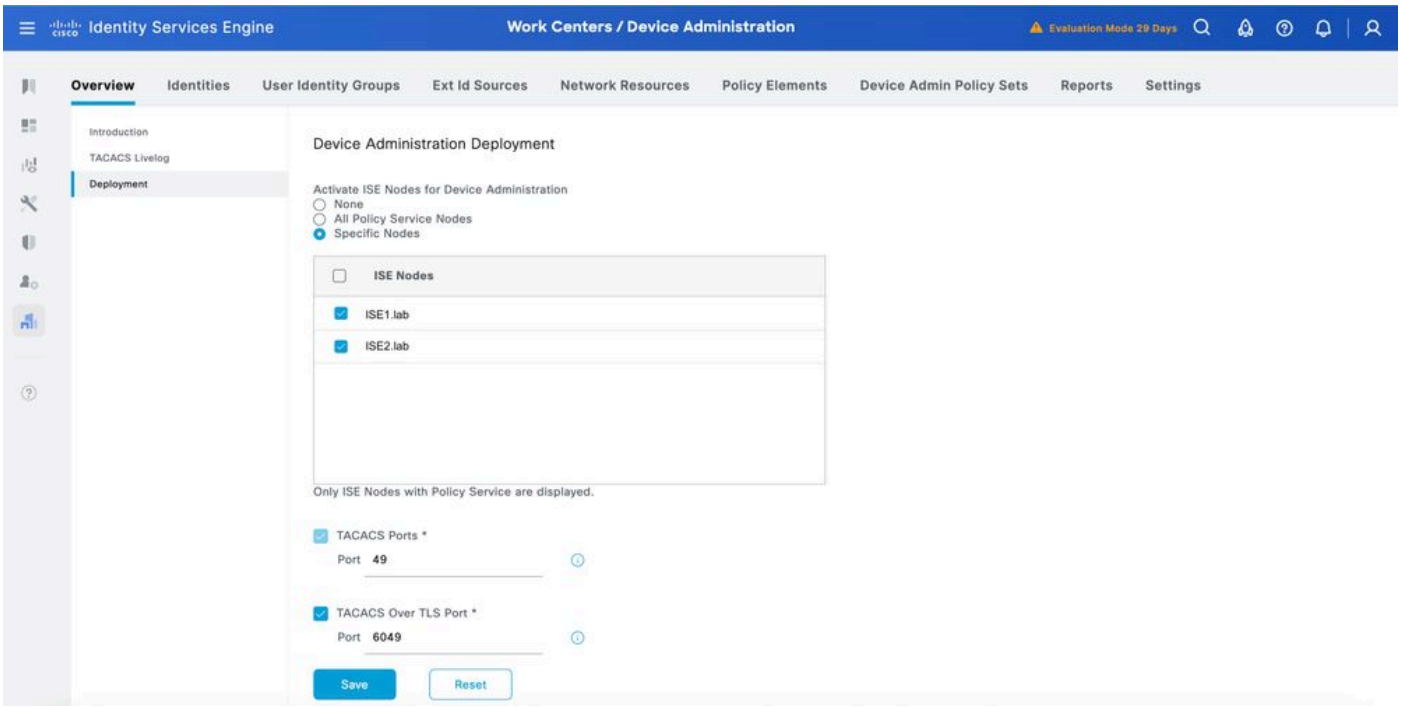
Étape 3 : enregistrement de la configuration Le service d'administration des périphériques est désormais activé sur ISE.

Activer TACACS sur TLS

Étape 1.Accédez à Work Centers > Device Administration > Overview.



Étape 2. Cliquez sur Deployment. Sélectionnez les noeuds PSN où vous souhaitez activer TACACS sur TLS.

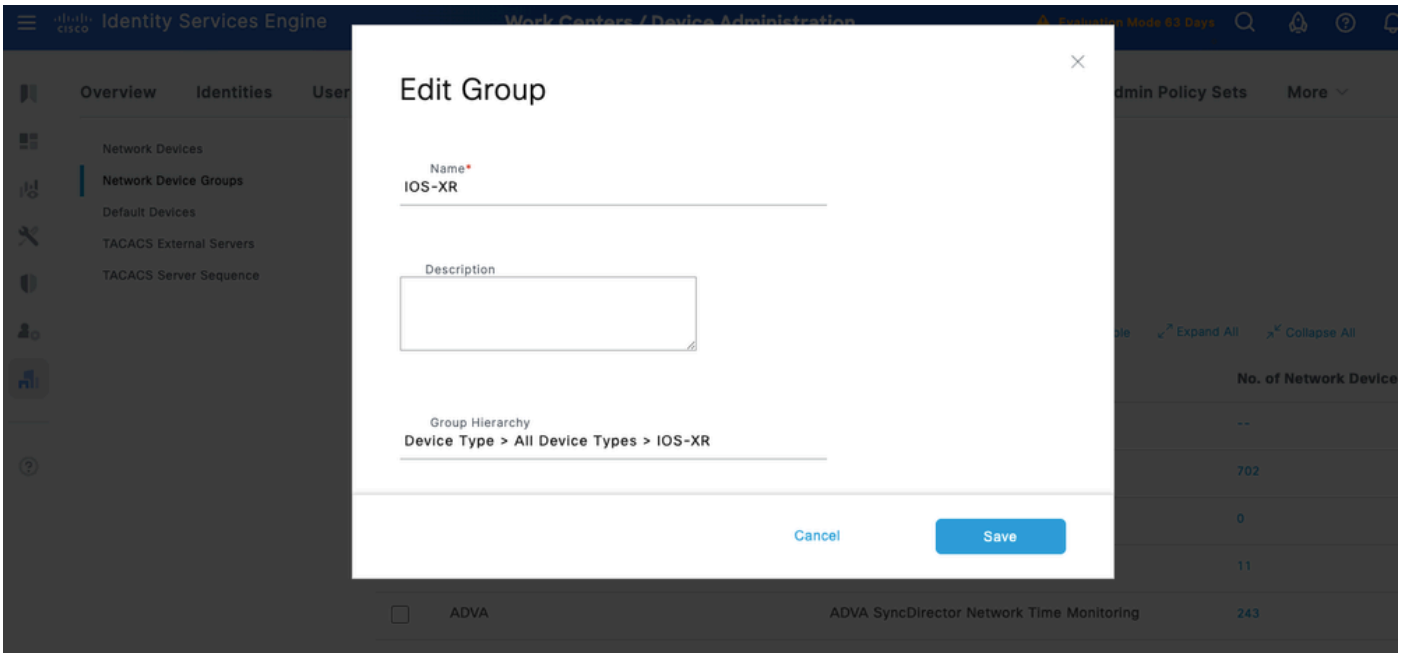


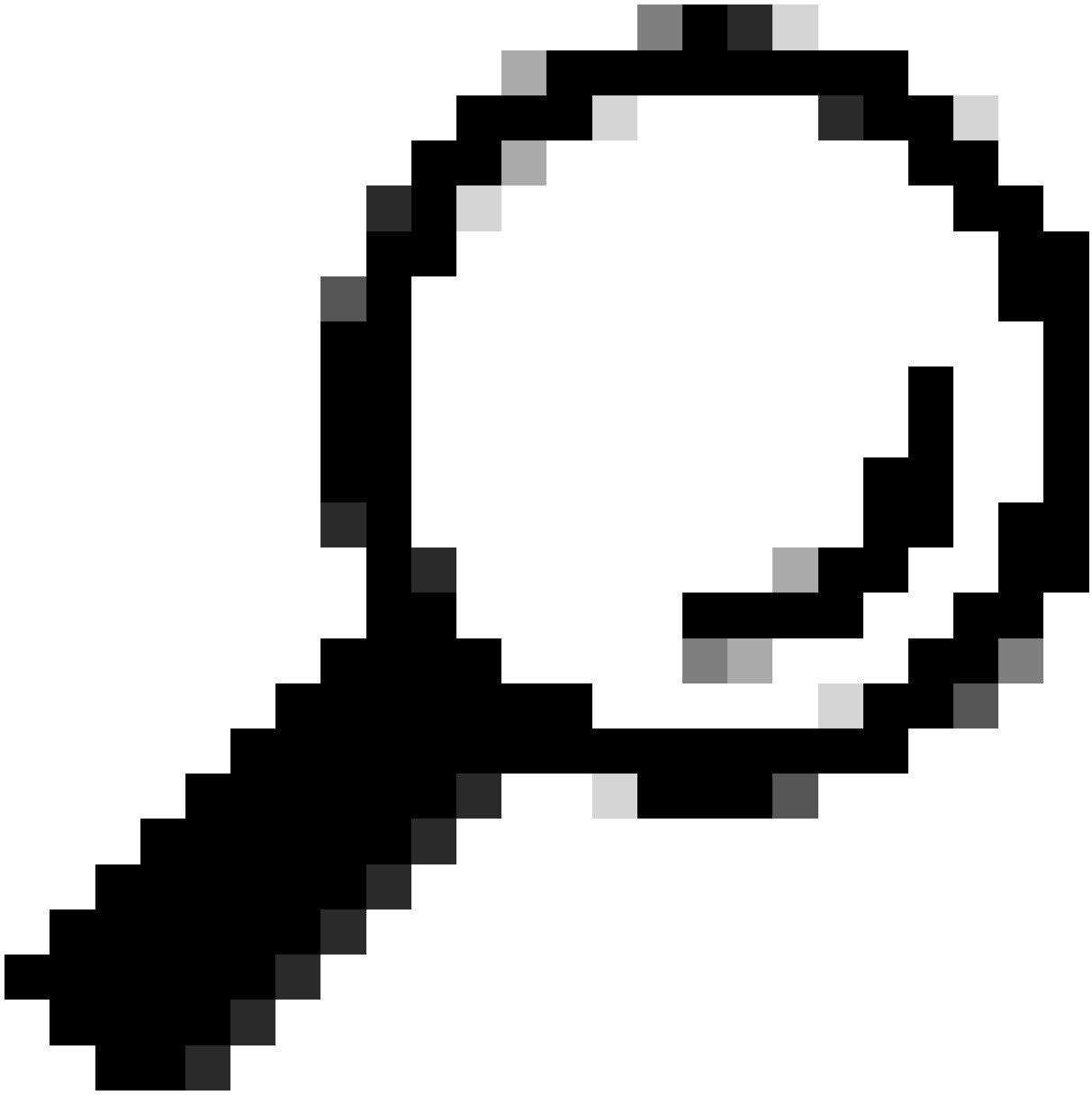
Étape 3.Conservez le port par défaut 6049 ou spécifiez un autre port TCP pour TACACS sur TLS, puis cliquez sur Save.

Création de périphériques réseau et de groupes de périphériques réseau

ISE fournit un regroupement de périphériques puissant avec plusieurs hiérarchies de groupes de périphériques. Chaque hiérarchie représente une classification distincte et indépendante des périphériques réseau.

Étape 1.Accédez à Work Centers > Device Administration > Network Resources.Cliquez sur Network Device Groups et créez un groupe avec le nom IOS XR.

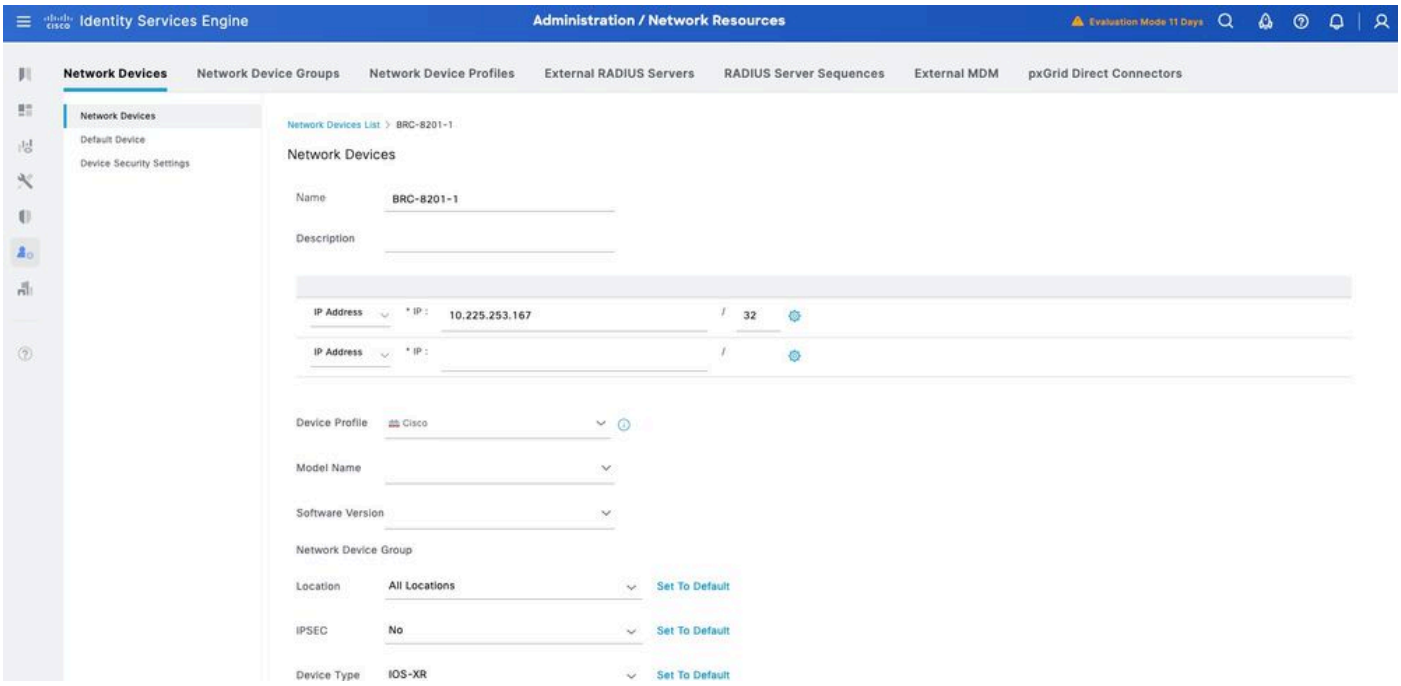

Identity Services Engine
Work Centers / Device Administration
Overview
Identities
User
Admin Policy Sets
More
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Expand All
Collapse All
No. of Network Device
Edit Group
Name*
IOS-XR
Description
Group Hierarchy
Device Type > All Device Types > IOS-XR
Cancel
Save
ADVA
ADVA SyncDirector Network Time Monitoring
243



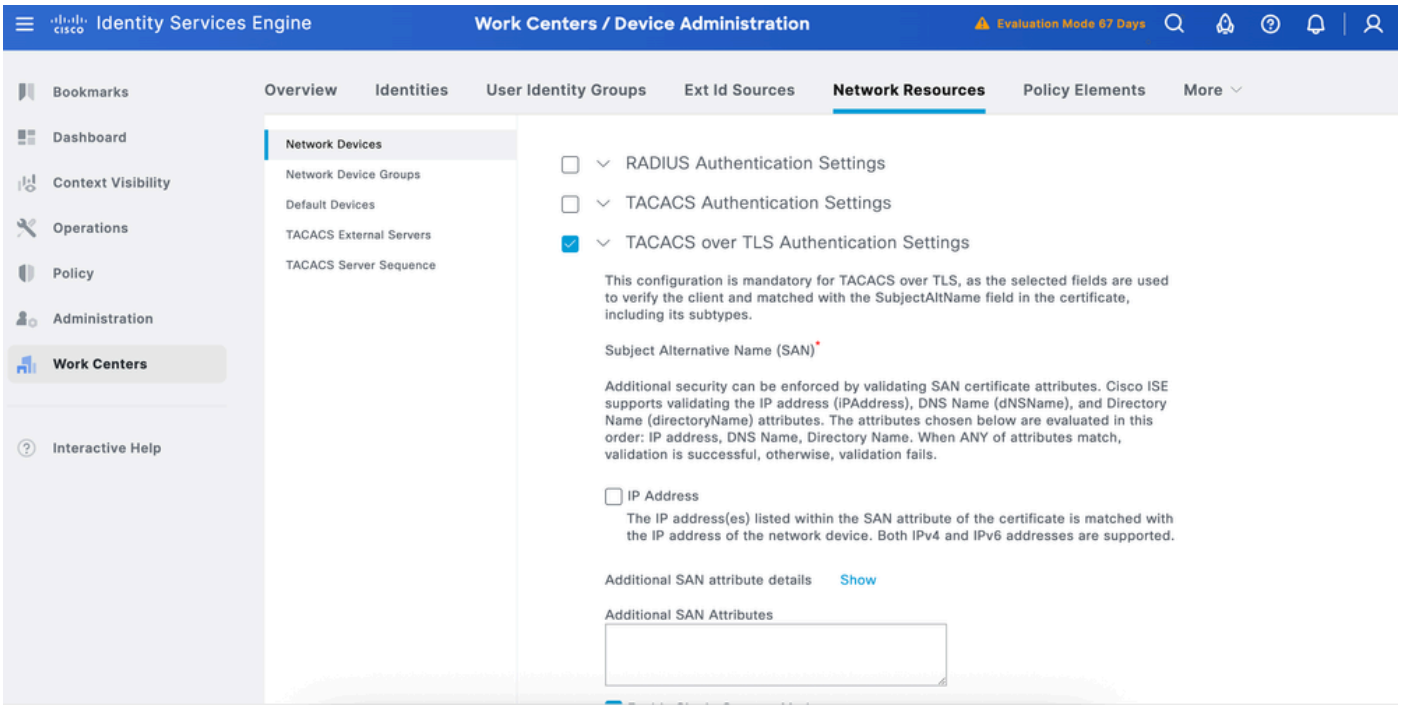
Conseil : Tous les types de périphériques et tous les emplacements sont des hiérarchies par défaut fournies par ISE. Vous pouvez ajouter vos propres hiérarchies et définir les différents composants pour identifier un périphérique réseau qui pourra être utilisé ultérieurement dans la condition de stratégie

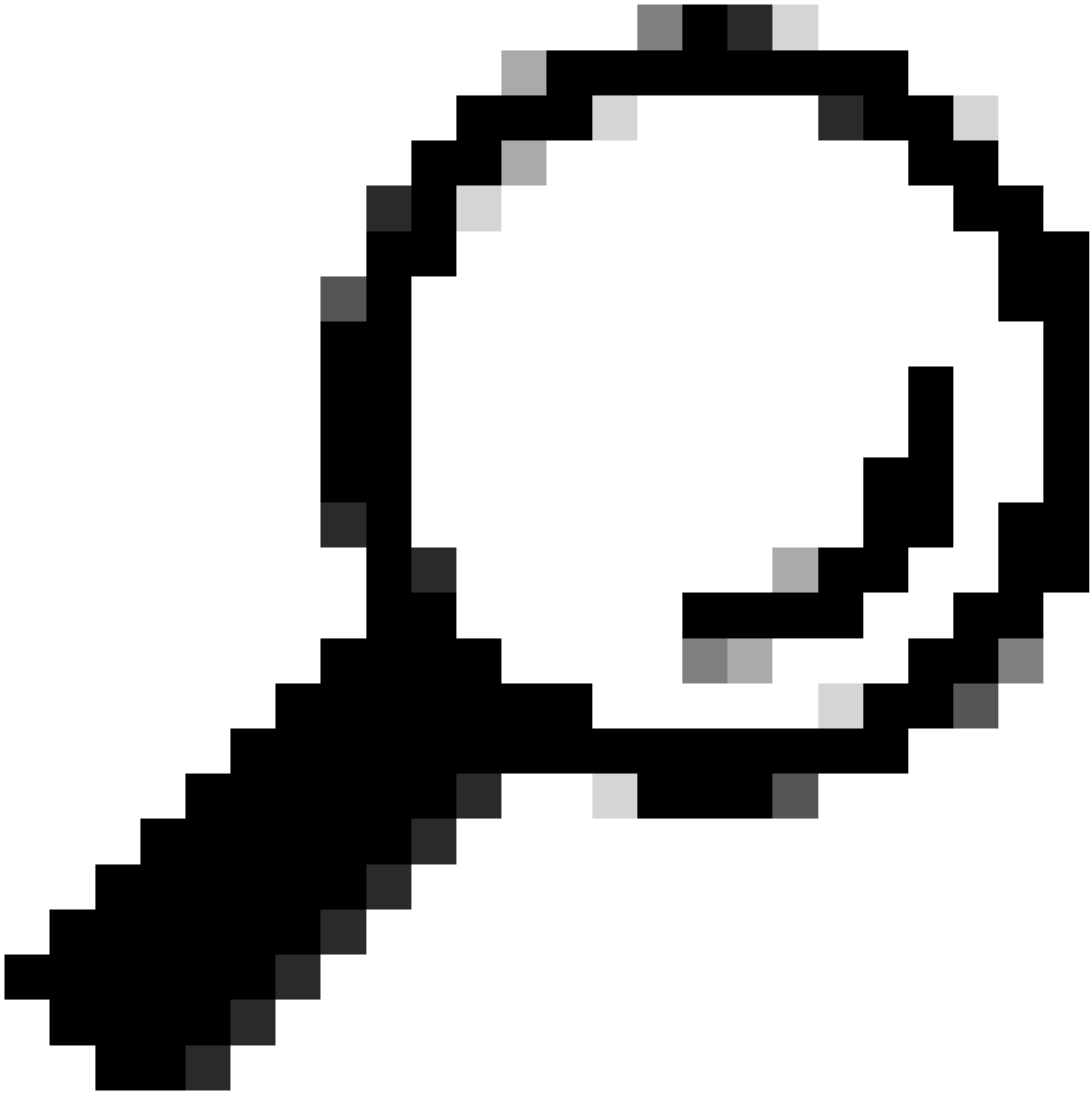
---

Étape 2. À présent, ajoutez un périphérique Cisco IOS XR en tant que périphérique réseau. Accédez à Work Centers > Device Administration > Network Resources > Network Devices. Cliquez sur Add pour ajouter un nouveau périphérique réseau.



Étape 3. Entrez l'adresse IP du périphérique et assurez-vous de mapper l'emplacement et le type de périphérique (IOS XR) pour le périphérique. Enfin, activez les paramètres d'authentification TACACS+ sur TLS.



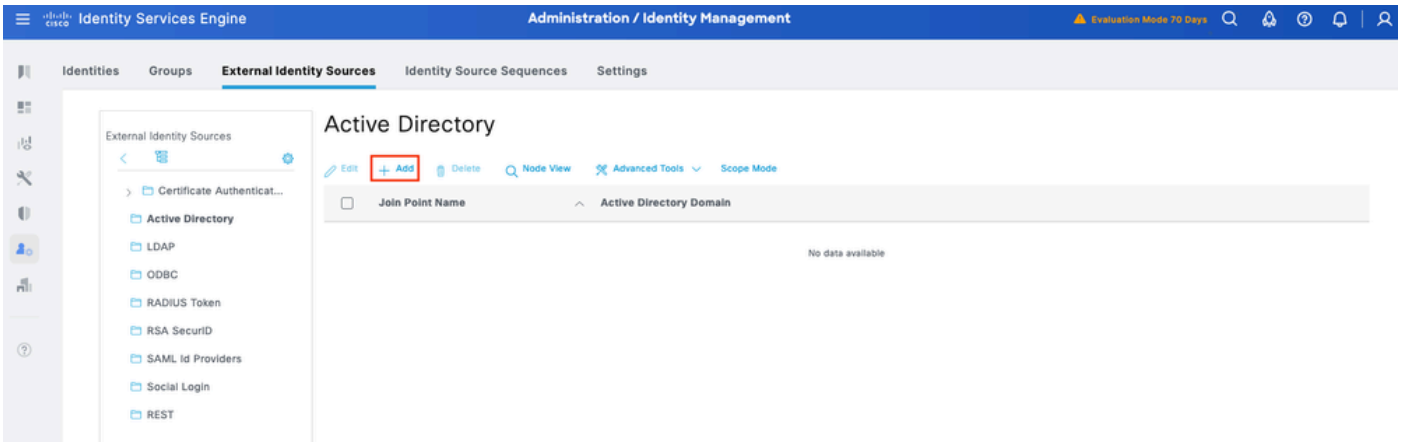


Conseil : Il est recommandé d'activer le mode de connexion unique pour éviter de redémarrer la session TCP chaque fois qu'une commande est envoyée au périphérique.

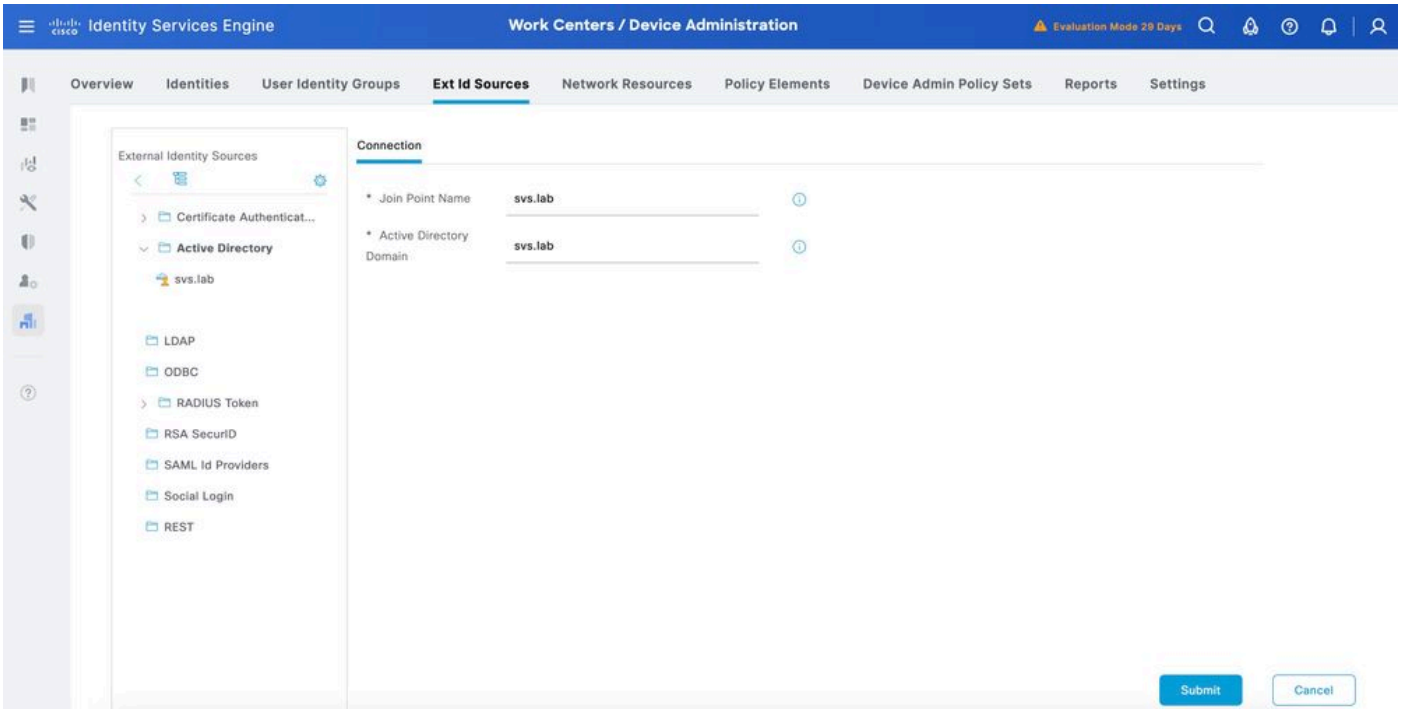
Configurer les magasins d'identités

Cette section définit un magasin d'identités pour les administrateurs de périphériques, qui peut être les utilisateurs internes ISE et toutes les sources d'identités externes prises en charge. Utilise ici Active Directory (AD), une source d'identité externe.

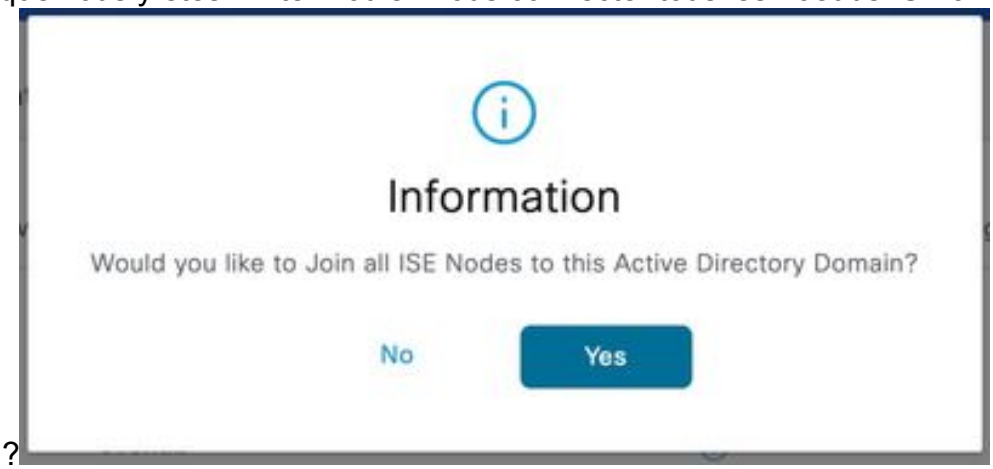
Étape 1. Accédez à Administration > Identity Management > External Identity Stores > Active Directory. Cliquez sur Add pour définir un nouveau point de jonction AD.



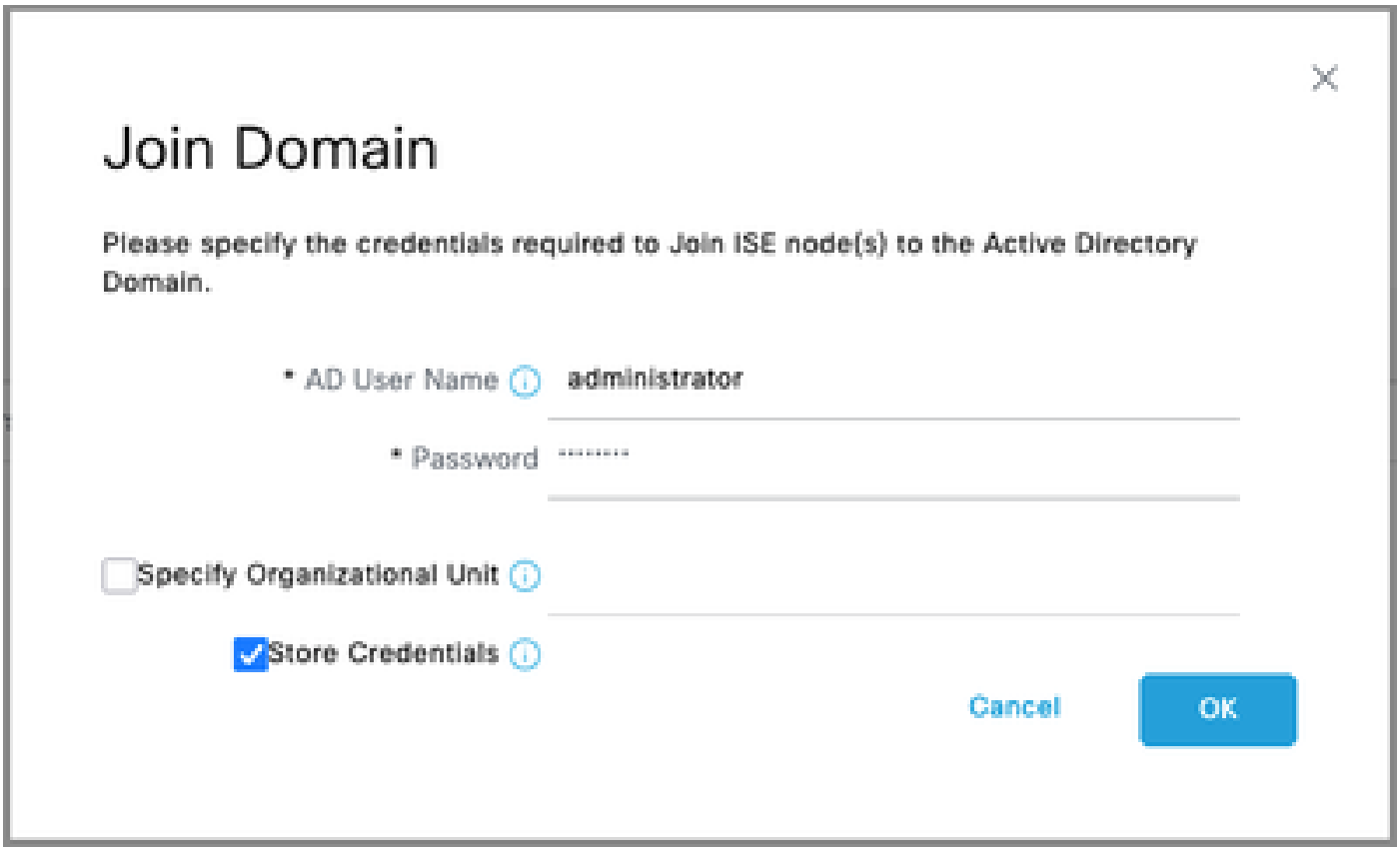
Étape 2. Spécifiez le nom du point de jonction et le nom de domaine AD, puis cliquez sur Submit.

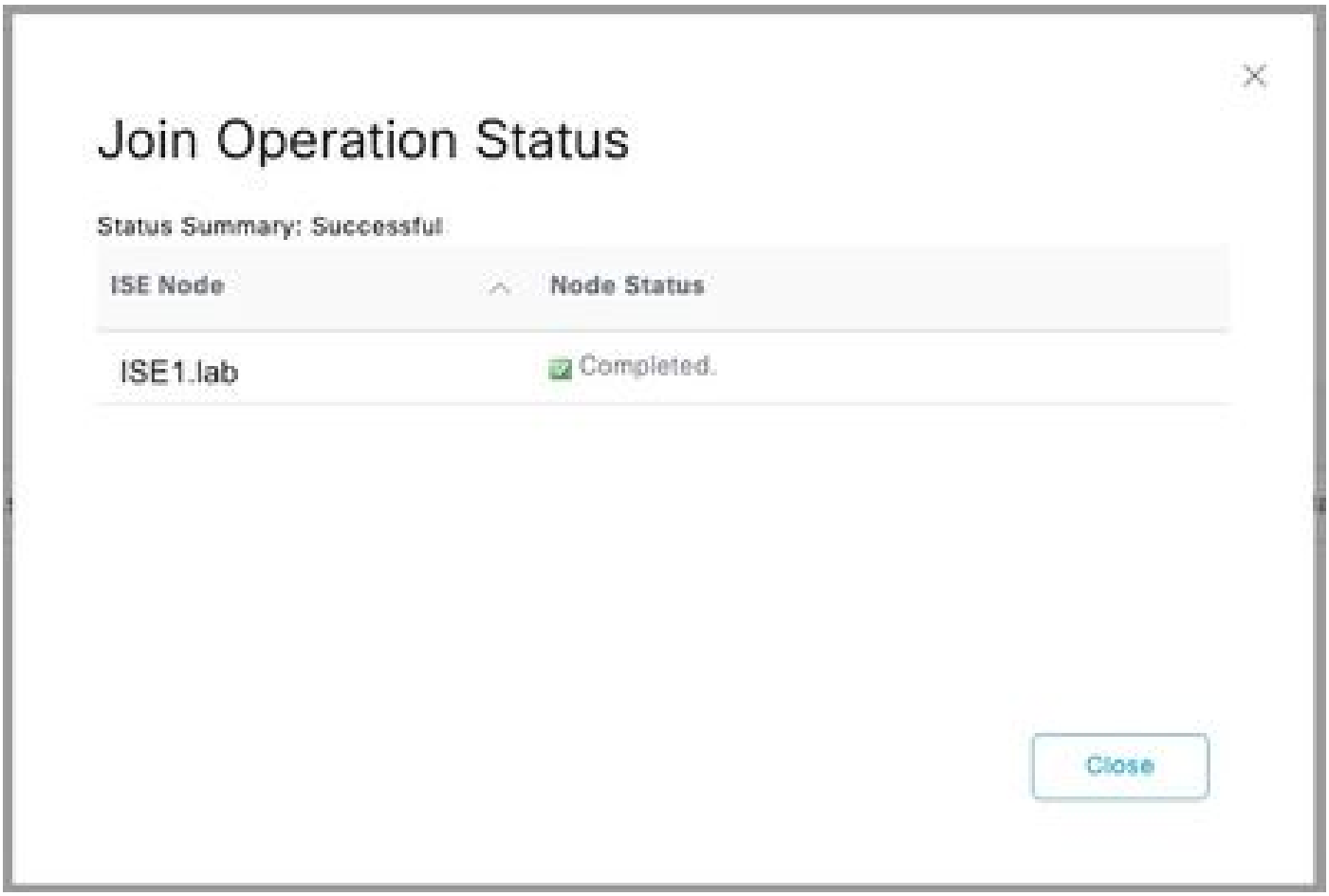


Étape 3.Cliquez sur Yes lorsque vous y êtes invité. Voulez-vous connecter tous les noeuds ISE à ce domaine Active Directory ?

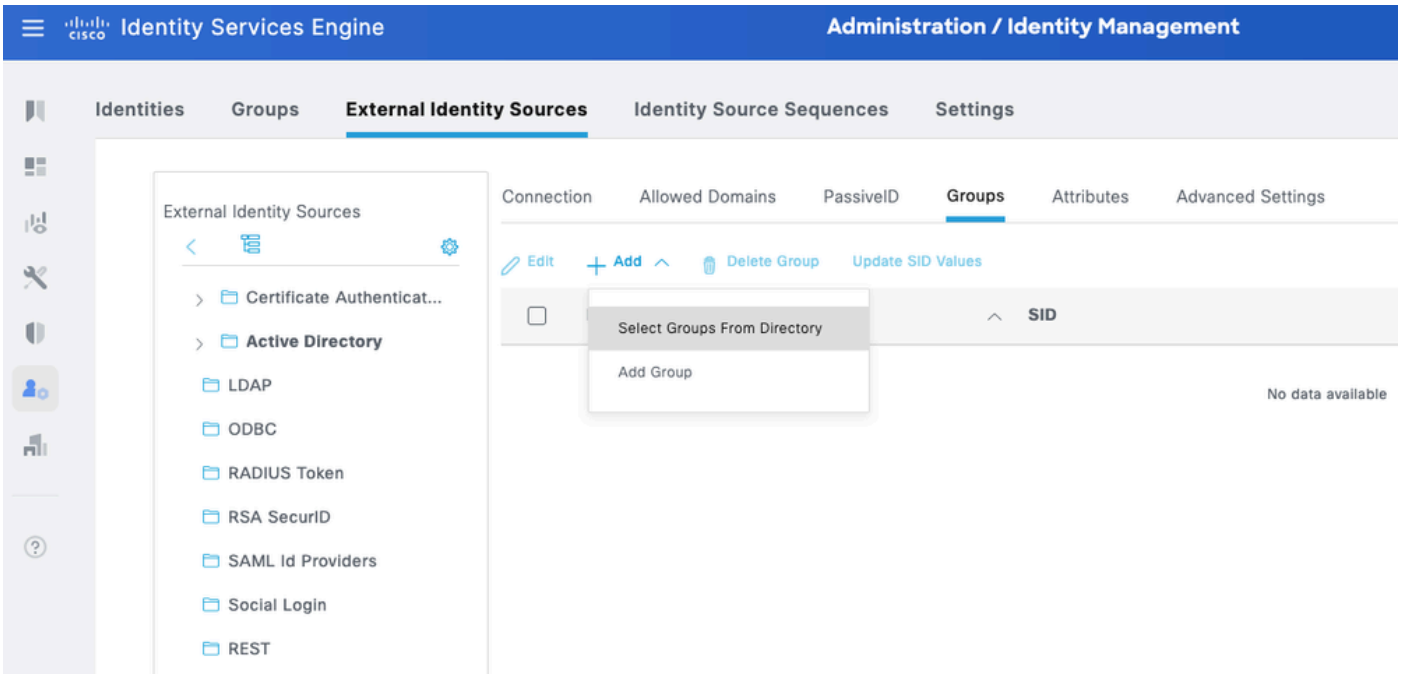


Étape 4. Entrez les informations d'identification avec les privilèges de jointure AD et joignez ISE à AD. Vérifiez l'état pour vous assurer qu'il est opérationnel.





Étape 5.Accédez à l'onglet Groups, et cliquez sur Add pour obtenir tous les groupes nécessaires en fonction des utilisateurs autorisés pour l'accès au périphérique. Cet exemple montre les groupes utilisés dans la stratégie d'autorisation.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain svs.lab

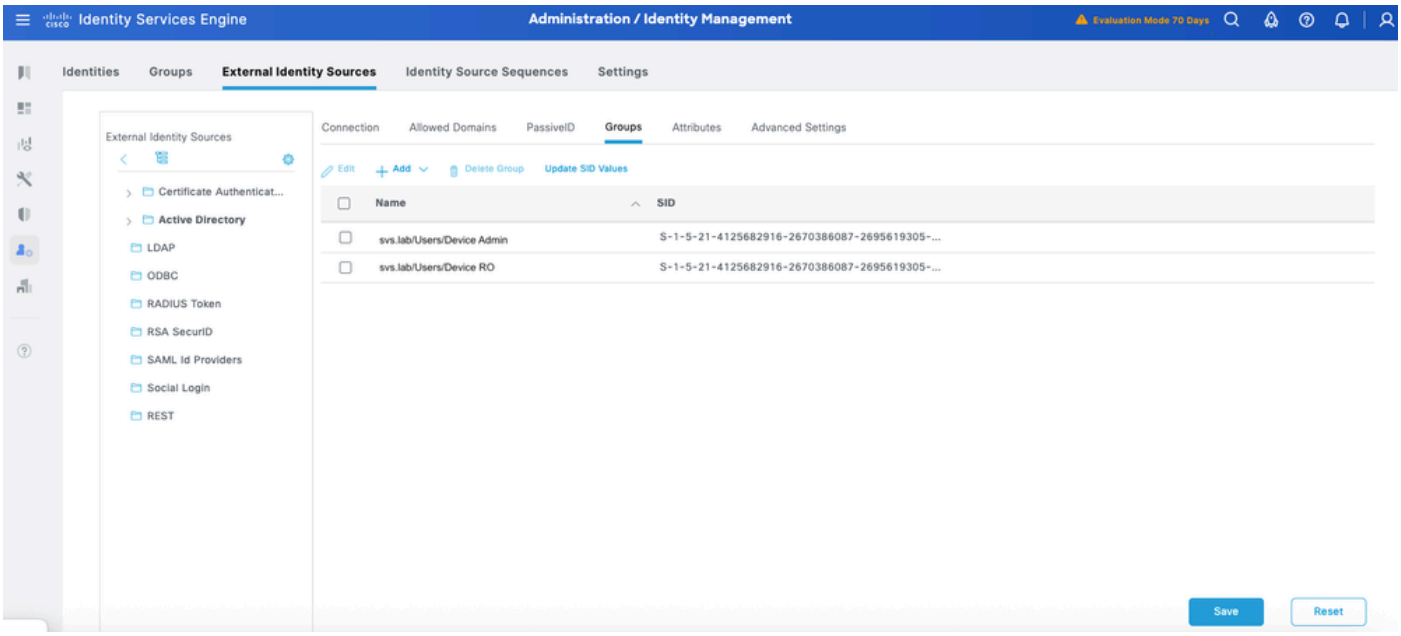
Name Filter Device *

SID Filter *

Type Filter ALL

Retrieve Groups... 2 Groups Retrieved.

Name	Group SID	Group Type
svs.lab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
svs.lab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



Configuration des profils TACACS+

Mappez les profils TACACS+ aux rôles utilisateur sur les périphériques Cisco IOS XR. Dans cet exemple, ils sont définis comme suit :

- Administrateur du système racine : il s'agit du rôle le plus privilégié dans le périphérique. L'utilisateur doté du rôle d'administrateur système racine dispose d'un accès administratif complet à toutes les commandes système et à toutes les fonctionnalités de configuration.
- Opérateur - Ce rôle est destiné aux utilisateurs qui ont besoin d'un accès en lecture seule au système à des fins de surveillance et de dépannage.

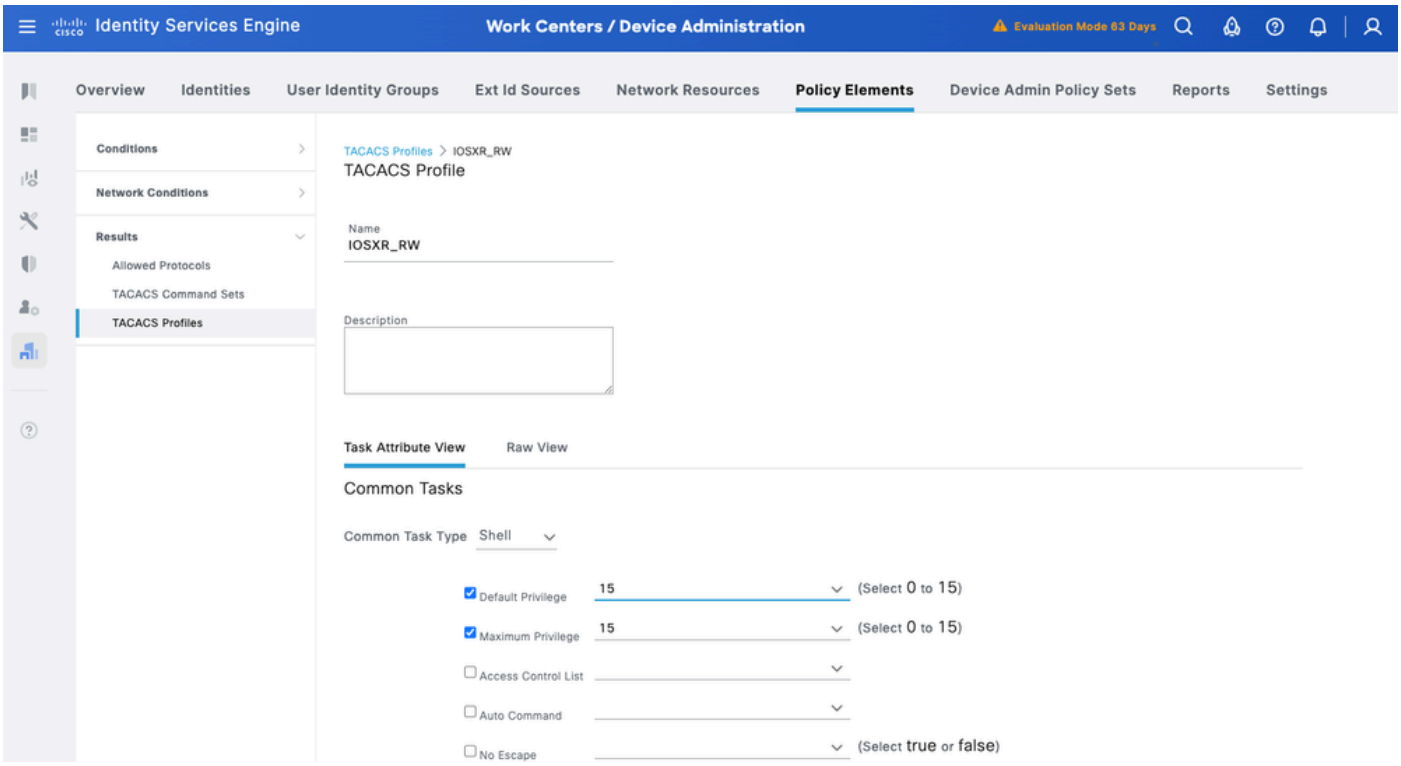
Définissez deux profils TACACS+ : IOSXR_RW et IOSXR_RO.

IOS XR_RW - Profil d'administrateur

Étape 1. Accédez à Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Ajoutez un nouveau profil TACACS et nommez-le IOSXR_RW.

Étape 2. Vérifiez et définissez le privilège par défaut et le privilège maximal sur 15.

Étape 3 : confirmation de la configuration et enregistrement.

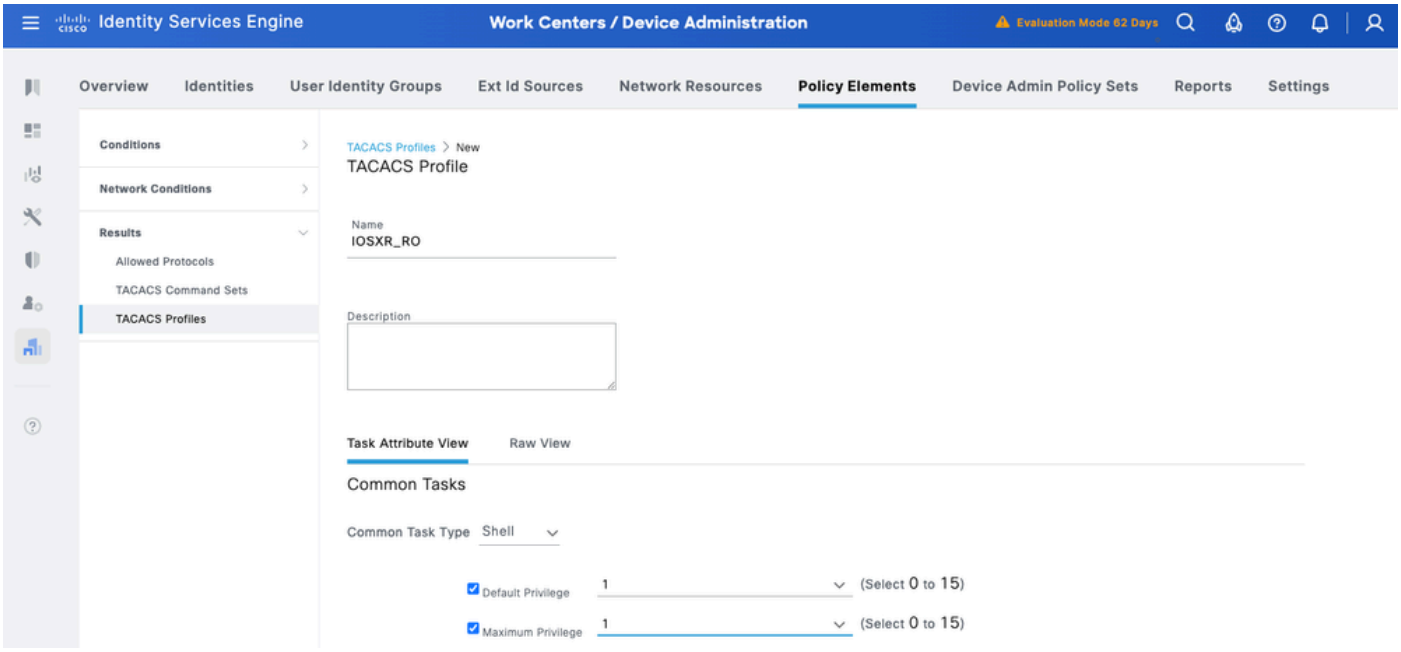


IOS XR_RO - Profil d'opérateur

Étape 1. Accédez à Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Ajoutez un nouveau profil TACACS et nommez-le IOSXR_RO.

Étape 2. Vérifiez et définissez le privilège par défaut et le privilège maximal sur 1.

Étape 3 : confirmation de la configuration et enregistrement.



Configurer les jeux de commandes TACACS+

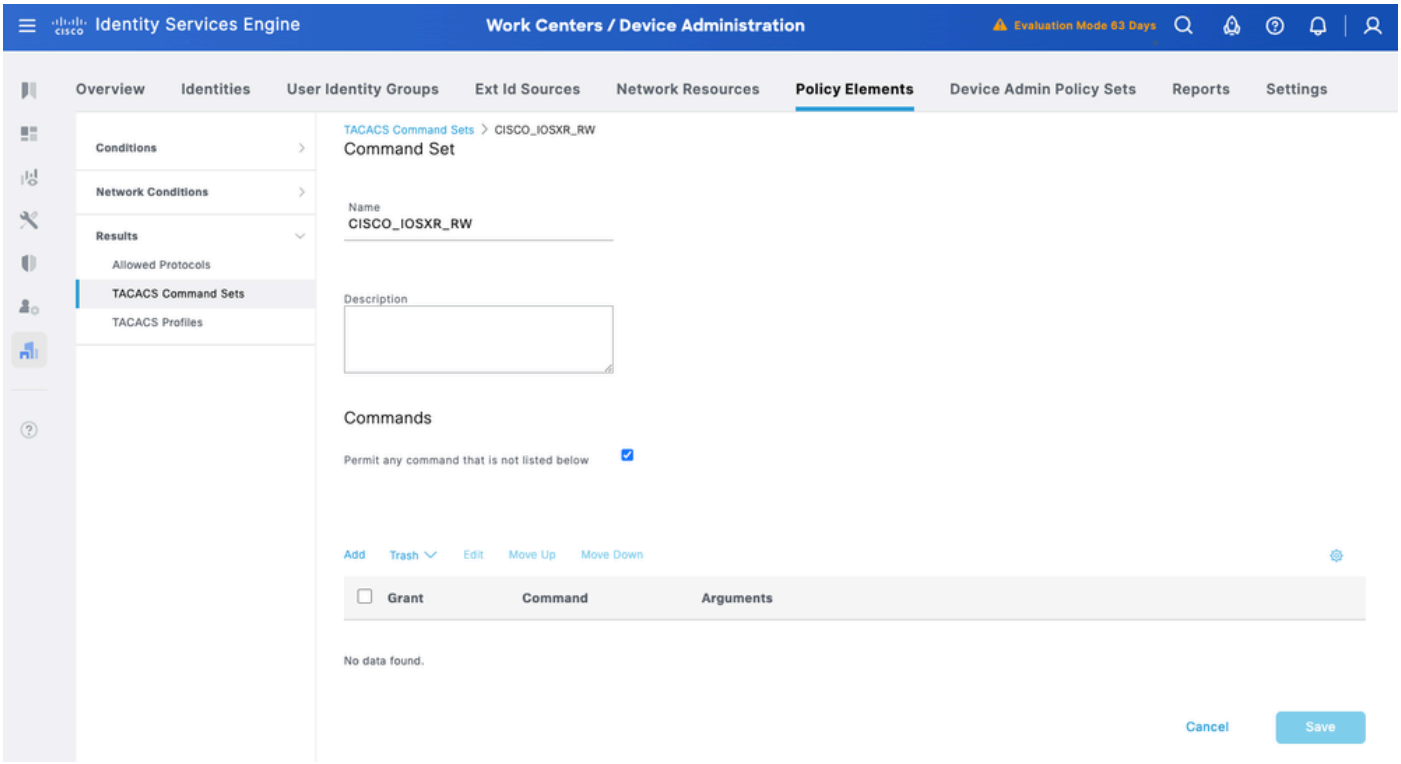
Définissez les jeux de commandes TACACS+ : Dans cet exemple, ils sont définis par

CISCO_IOSXR_RW et CISCO_IOSXR_RO.

CISCO IOS XR RW - Ensemble de commandes de l'administrateur

Étape 1. Accédez à Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. Ajoutez un nouvel ensemble de commandes TACACS et nommez-le CISCO_IOSXR_RW.

Étape 2. Cochez la case Autoriser toute commande qui n'est pas répertoriée ci-dessous (cela autorise toute commande pour le rôle d'administrateur) et cliquez sur Enregistrer.



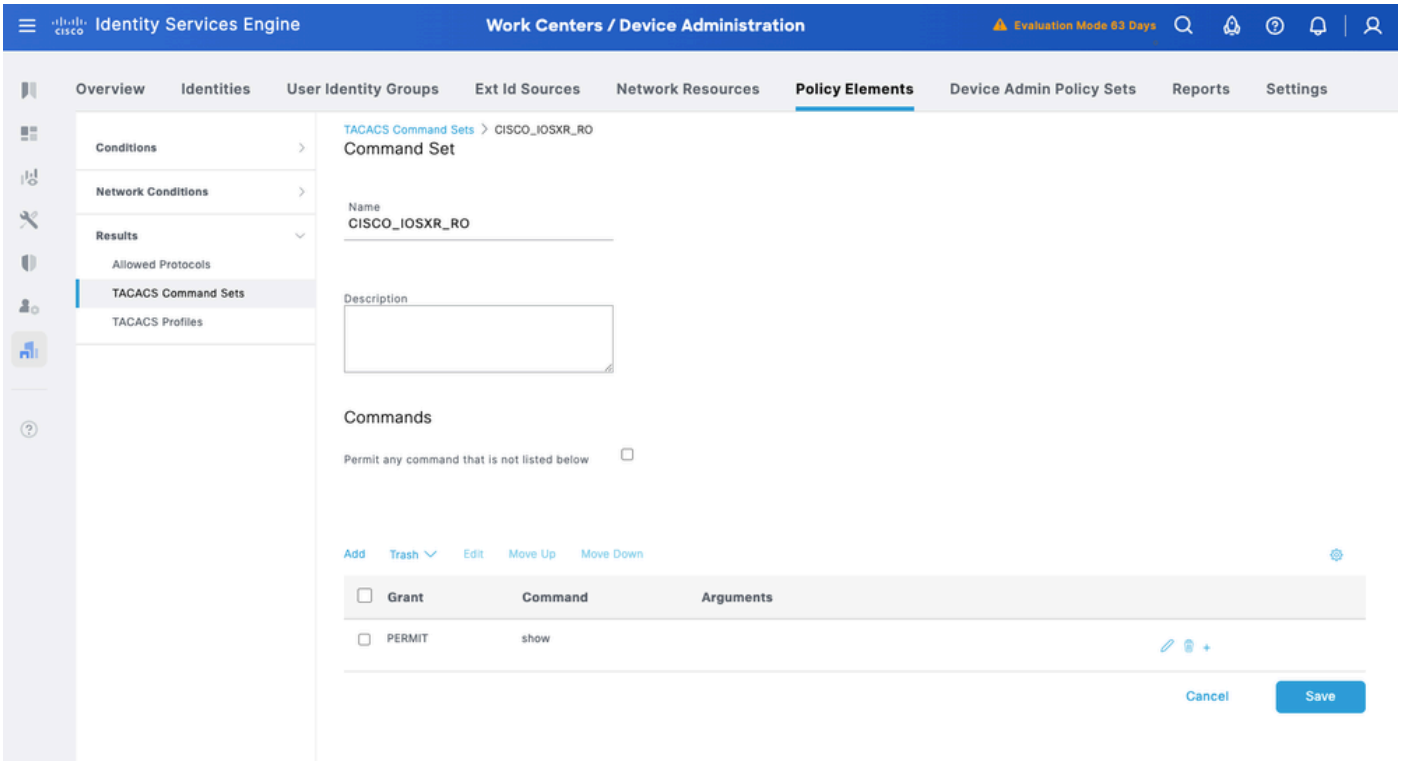
CISCO IOS XR RO - Jeu de commandes opérateur

Étape 1. Dans l'interface utilisateur d'ISE, accédez à Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. Ajoutez un nouvel ensemble de commandes TACACS et nommez-le CISCO_IOSXR_RO.

Étape 2. Dans la section Commands, ajoutez une nouvelle commande.

Étape 3. Sélectionnez Permit dans la liste déroulante pour la colonne Grant et entrez show dans la colonne Command ; et cliquez sur la flèche de vérification.

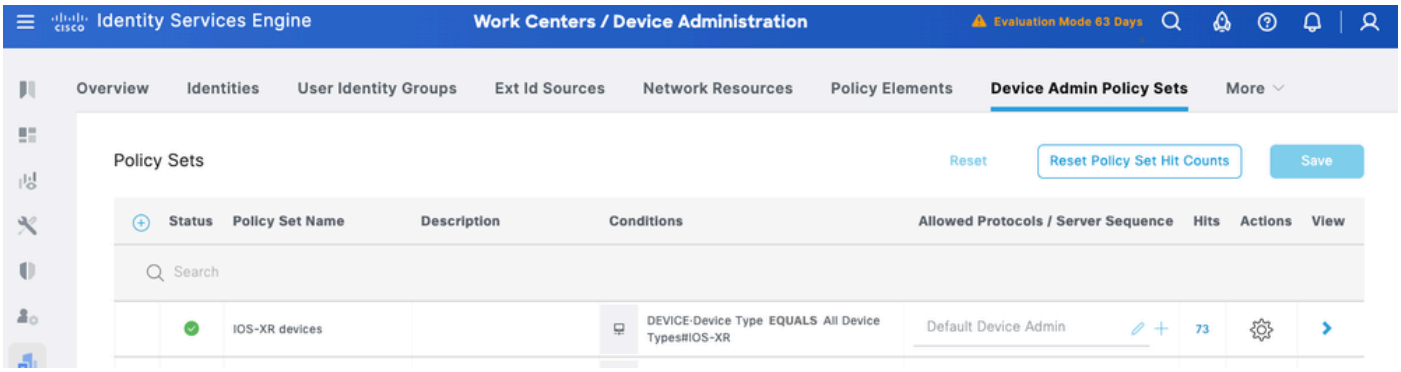
Étape 4. Confirmez les données et cliquez sur Save.



Configurer les ensembles de stratégies d'administration des périphériques

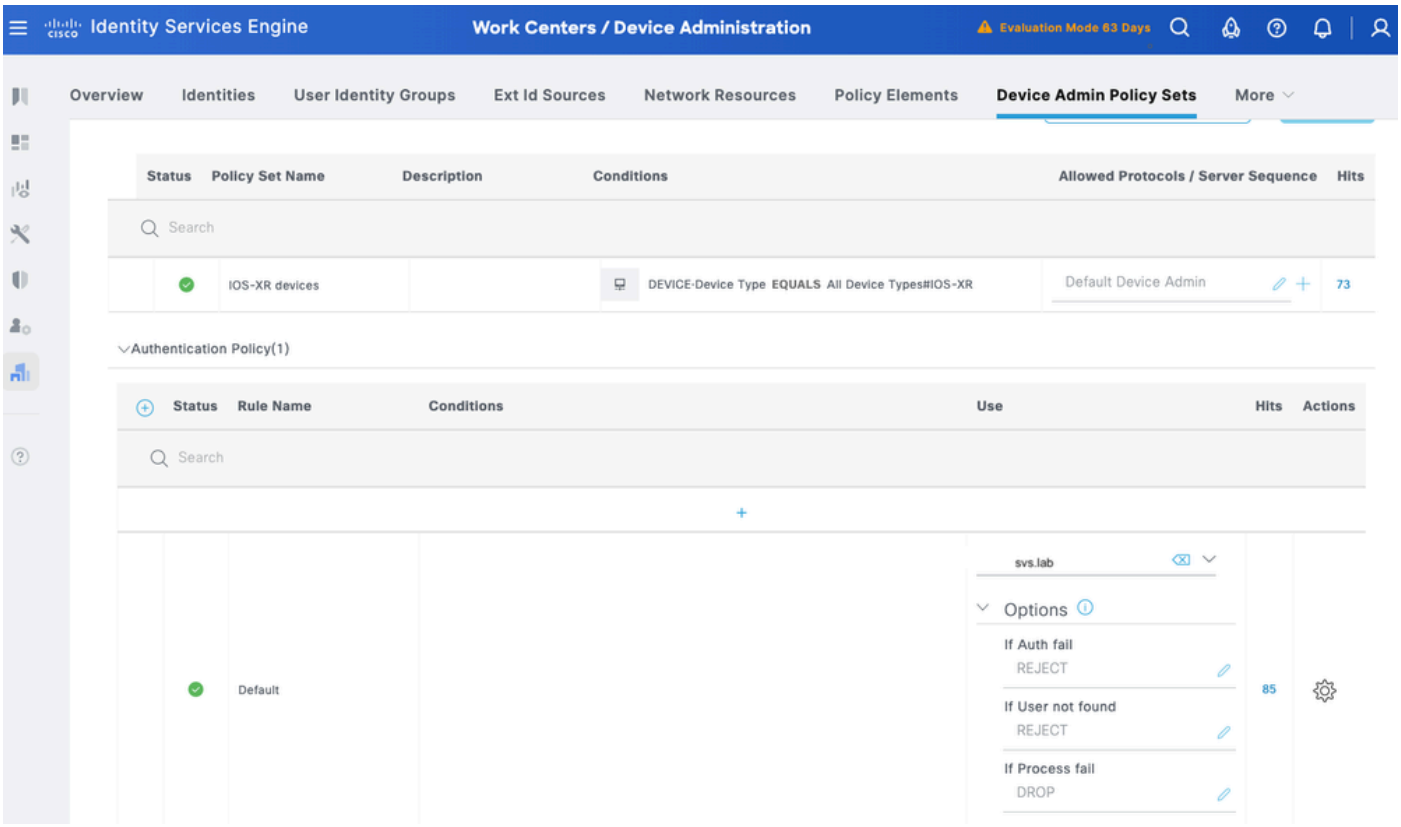
Les jeux de stratégies sont activés par défaut pour l'administration des périphériques. Les ensembles de politiques peuvent diviser les politiques en fonction des types de périphériques afin de faciliter l'application des profils TACACS.

Étape 1.Accédez à Work Centers > Device Administration > Device Admin Policy Sets. Ajouter un nouvel ensemble de stratégies Périphériques IOS XR. Dans cette condition, spécifiez DEVICE:Device Type EQUALS All Device Types#IOS XR. Sous Allowed Protocols, sélectionnez Default Device Admin.



Étape 2. Cliquez sur Enregistrer et cliquez sur la flèche droite pour configurer ce jeu de stratégies.

Étape 3 : création de la stratégie d'authentification. Pour l'authentification, vous utilisez AD comme magasin d'ID. Conservez les options par défaut sous If Auth fail, If User not found et If Process fail.

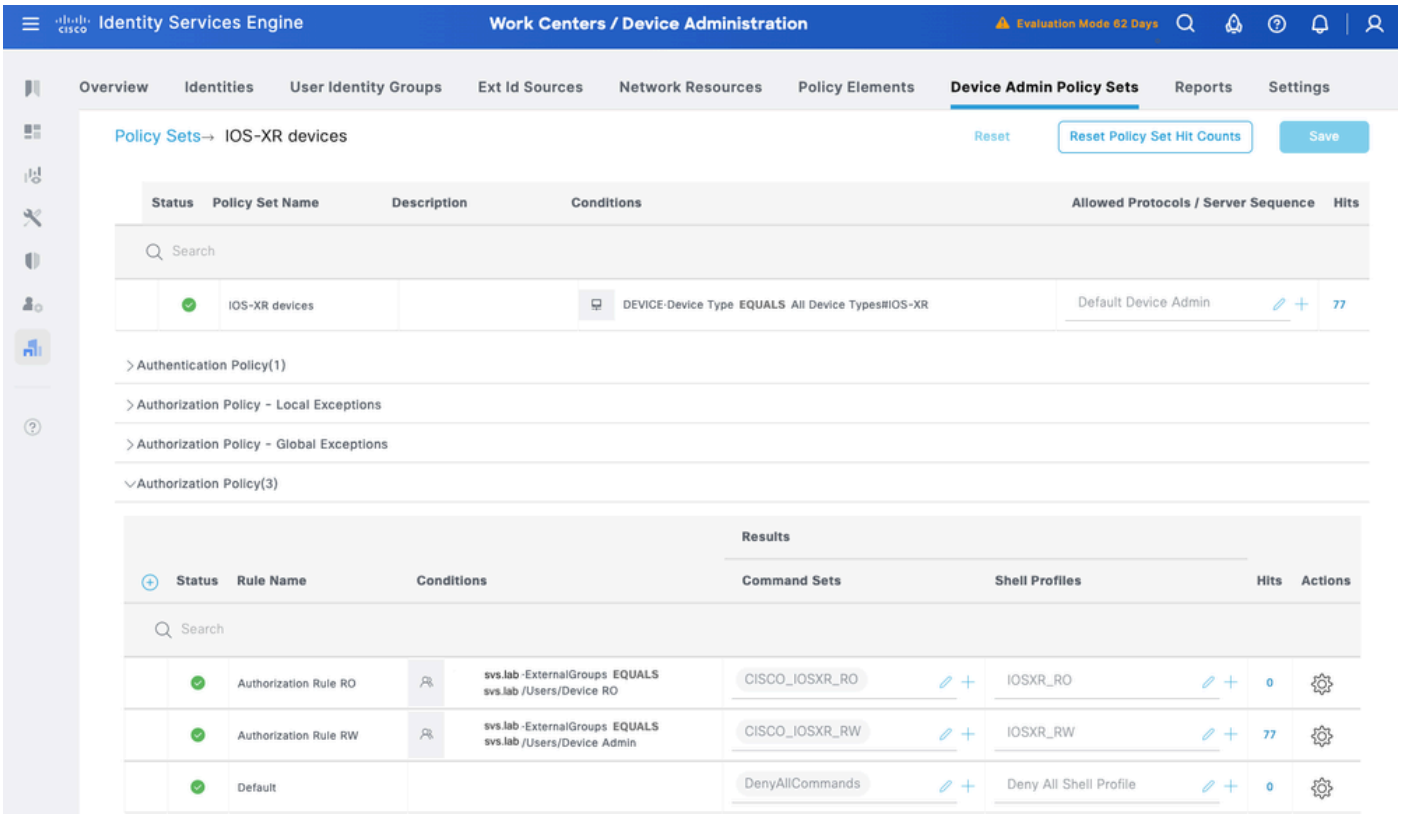


Étape 4. Définissez la stratégie d’autorisation.

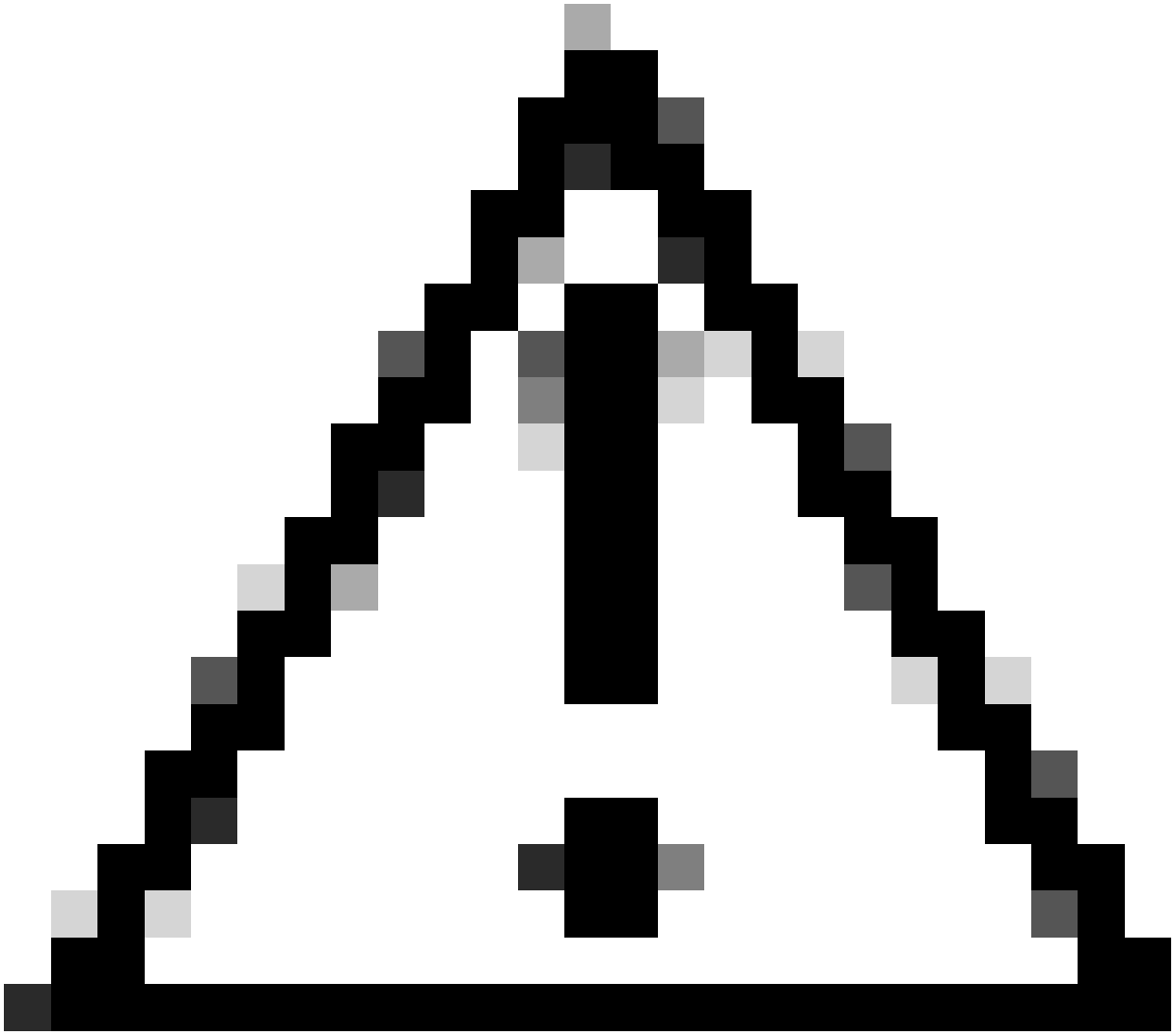
Créez la stratégie d'autorisation en fonction des groupes d'utilisateurs dans Active Directory (AD).

Exemple :

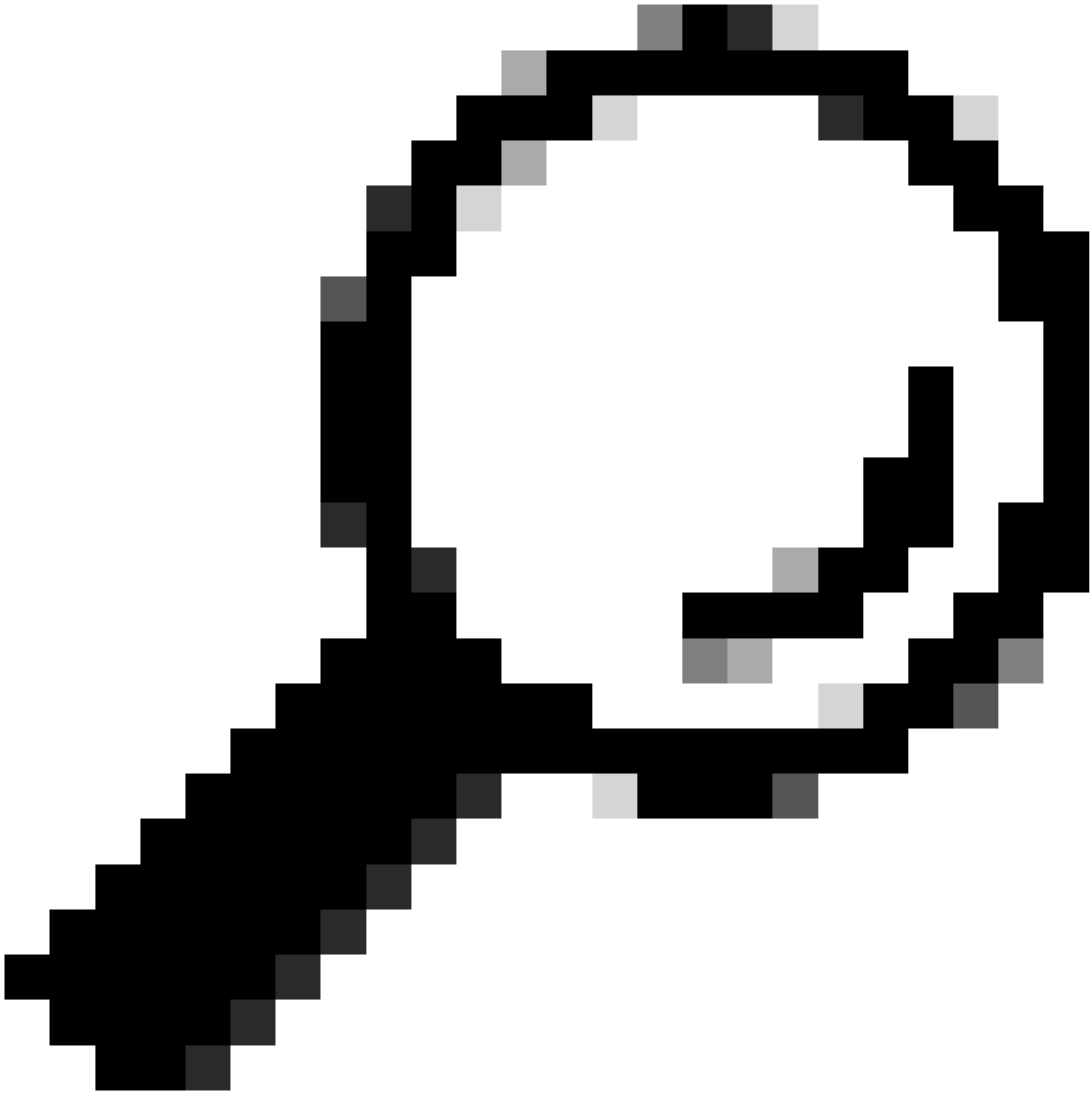
- Les utilisateurs du périphérique du groupe AD se voient attribuer le jeu de commandes CISCO_IOSXR_RO et le profil d'environnement de ligne de commande IOSXR_RO.
- Les utilisateurs du groupe AD Device Admin sont affectés à l'ensemble de commandes CISCO_IOSXR_RW et au profil d'environnement de ligne de commande IOSXR_RW.



Partie 2 : configuration de Cisco IOS XR pour TACACS+ sur TLS 1.3



Mise en garde : Assurez-vous que la connexion console est accessible et qu'elle fonctionne correctement.



Conseil : Il est recommandé de configurer un utilisateur temporaire et de modifier les méthodes d'authentification et d'autorisation AAA afin d'utiliser des informations d'identification locales au lieu de TACACS lors des modifications de configuration, afin d'éviter d'être verrouillé hors du périphérique.

Paramètres de configuration initiaux

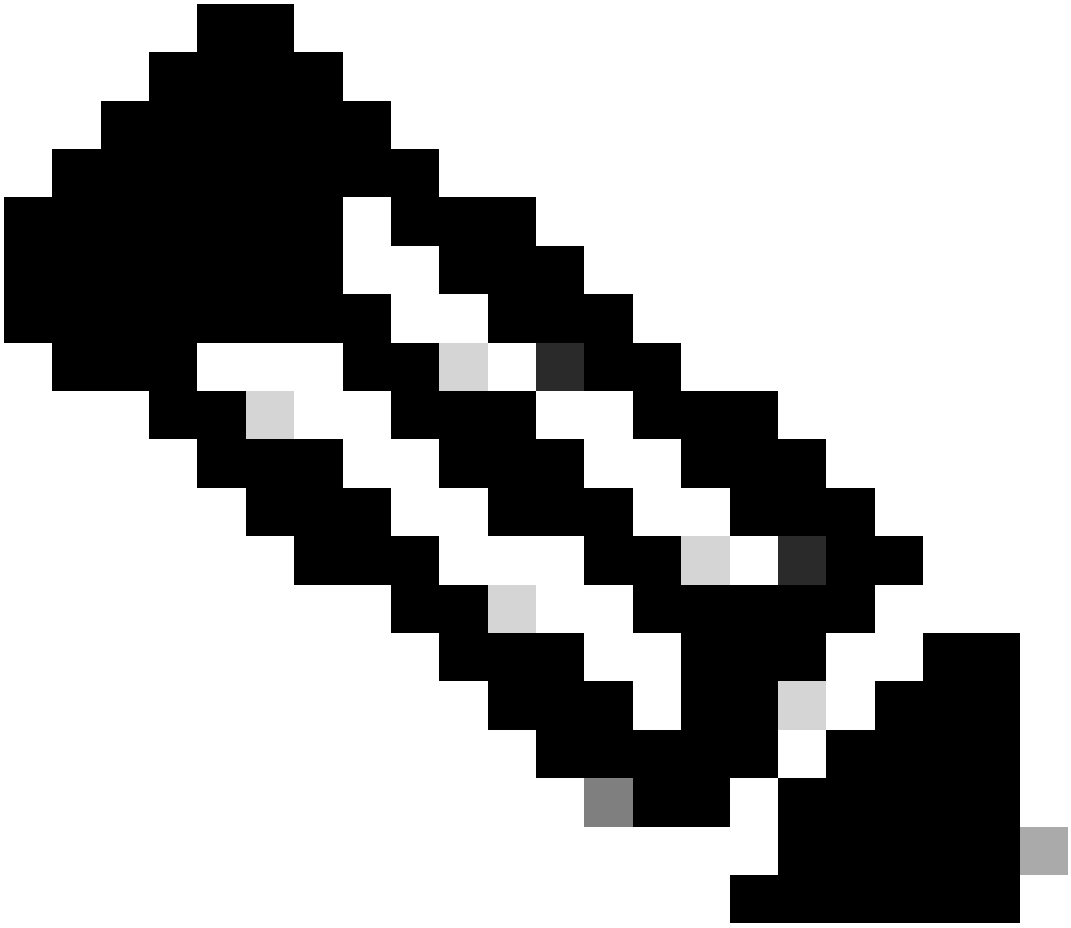
Étape 1 : vérification de la configuration du serveur de noms (DNS) et de la capacité du routeur à résoudre les noms de domaine fréquemment qualifiés (FQDN), en particulier le nom de domaine complet du serveur ISE

```
domain vrf mgmt name svs.lab
domain vrf mgmt name-server 10.225.253.247
```

```
no domain vrf mgmt lookup disable

RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Étape 2. Effacez tous les certificats et points de confiance anciens/inutilisés. Assurez-vous qu'aucun certificat ou point de confiance ancien n'est présent. Si vous voyez d'anciennes entrées, supprimez-les.

```
show crypto ca trustpoint
show crypto ca certificates

(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



Remarque : Vous pouvez créer manuellement une nouvelle paire de clés RSA et l'attacher sous trustpoint. Si vous n'en créez pas, la paire de clés par défaut est utilisée. La définition de la paire de clés ECC sous trustpoint n'est pas prise en charge actuellement.

Configurer le point de confiance

Étape 1 : configuration de la paire de clés (facultatif)

<#root>

RP/0/RP0/CPU0:BRC-8201-1(config)#

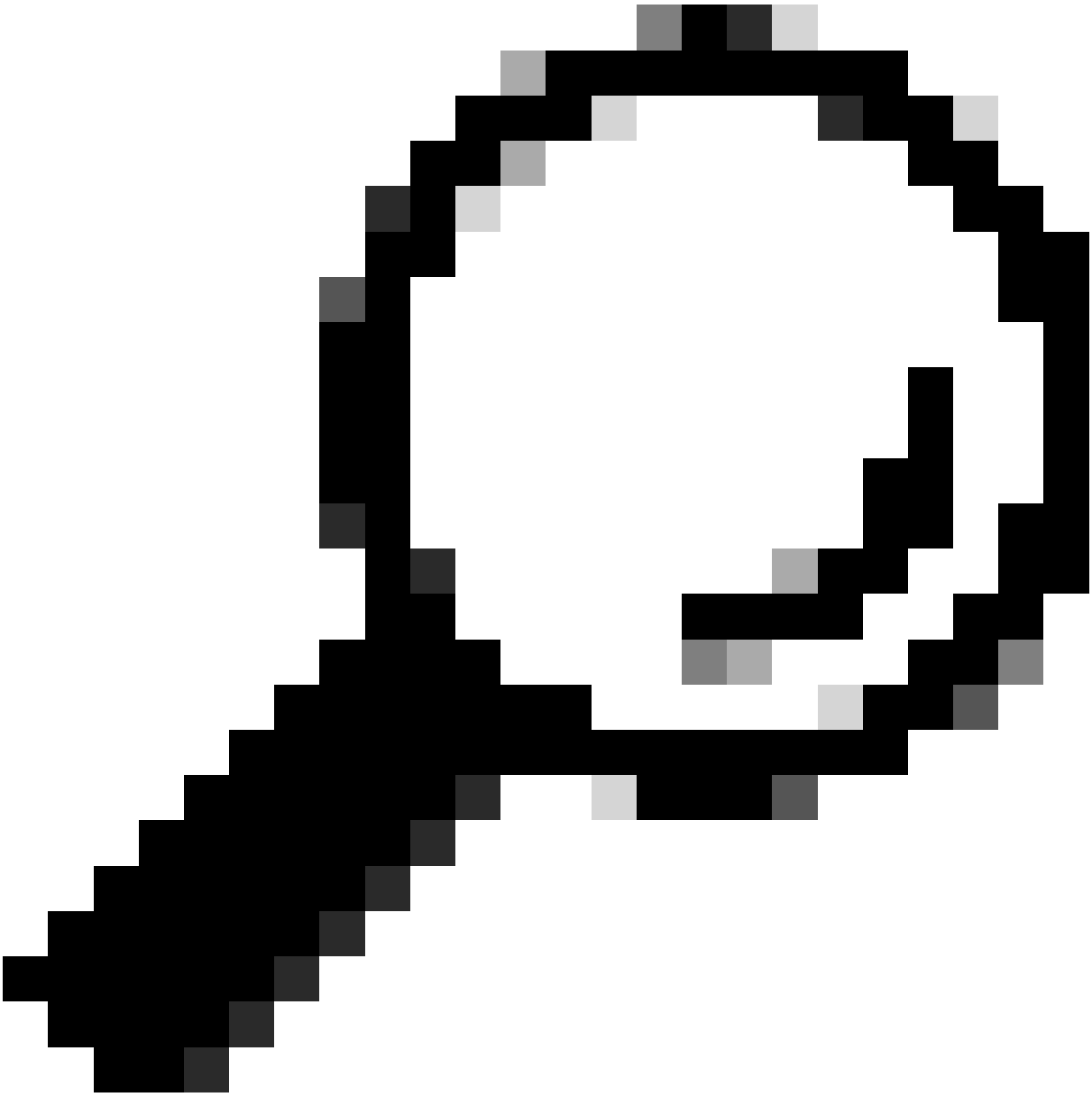
crypto key generate rsa

```
          4096
```

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair
```

Étape 2 : création du point de confiance.

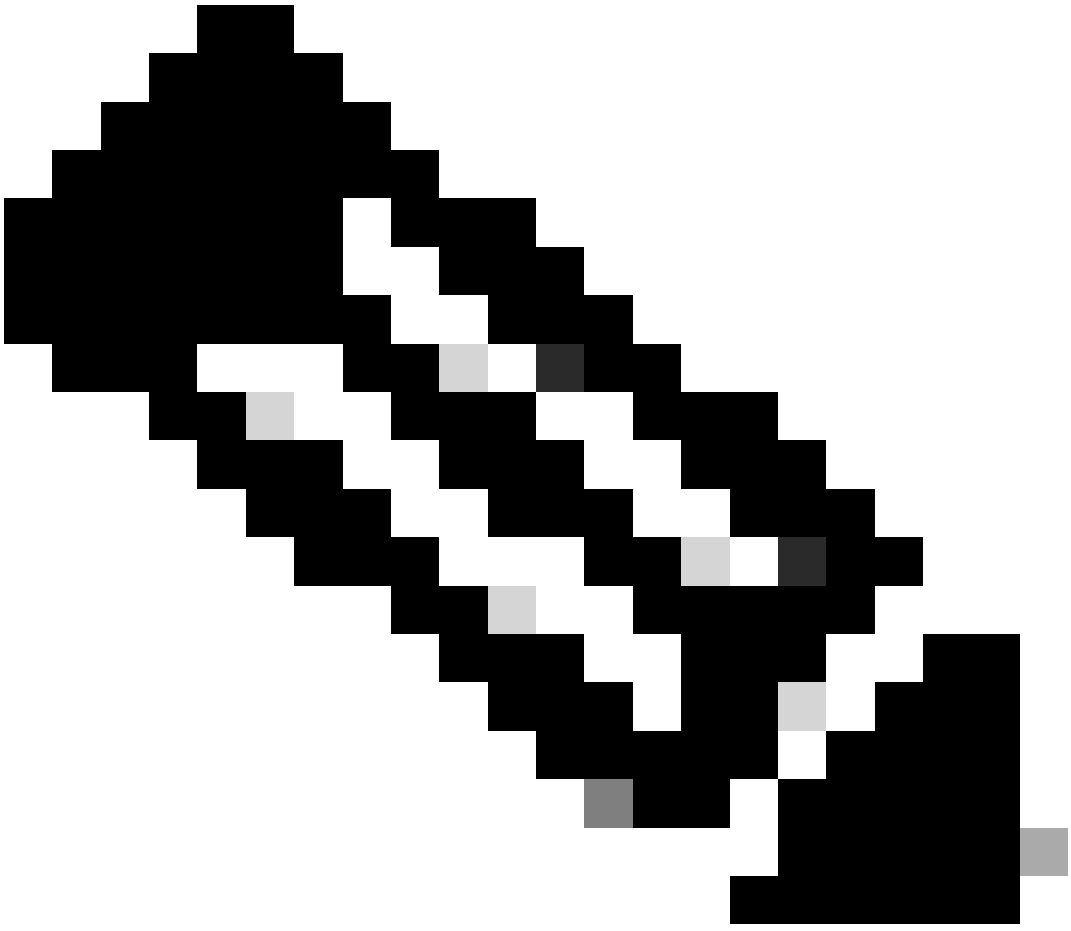


Conseil : La configuration DNS pour le nom alternatif du sujet est facultative (si elle est activée sur ISE), mais recommandée.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint svs

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
vrf mgmt

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
crl optional
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
enrollment url terminal
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair svs-4096

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
commit
```



Remarque : Si vous devez utiliser une virgule dans O ou OU, vous pouvez utiliser une barre oblique inverse (\) avant la virgule. Exemple : O=Cisco Systems\, Inc.

Étape 3 : authentification du point de confiance en installant le certificat CA.

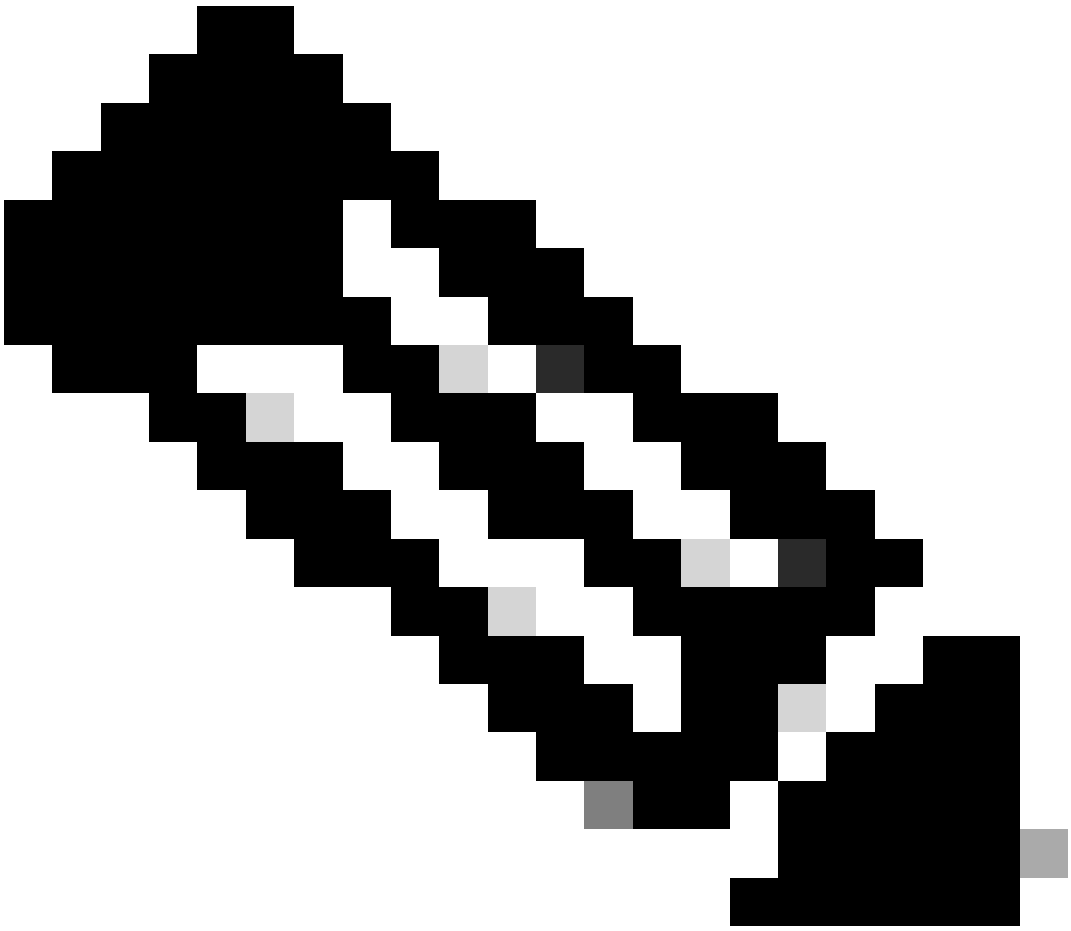
<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#

crypto ca authenticate svs



Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----


quit


   Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5
   Subject:
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
   Issued By :
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
   Validity Start : 17:05:00 UTC Mon Apr 28 2025
   Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
   SHA1 Fingerprint:
      0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
```

yes

```
RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated
```



Remarque : Si vous disposez d'un système d'autorité de certification subordonnée, vous devez importer les certificats d'autorité de certification racine et d'autorité de certification secondaire. Utilisez la même commande avec Sub CA en haut et Root CA en bas.

Étape 4. Génération d’une demande de signature de certificat (CSR).

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca enroll svs

```
Fri May 9 14:52:44.030 UTC
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
```

Password:

Re-enter Password:

```
% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167
% The subject name in the certificate will include: BRC-8201-1.svs.lab
% Include the router serial number in the subject name? [yes/no]:
```

yes

```
% The serial number in the certificate will be: 4090843b
% Include an IP address in the subject name? [yes/no]:
```

yes

```
Enter IP Address[]
```

10.225.253.167

```
Fingerprint: 36354532 38324335 43434136 42333545
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANTVlMxFzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQclZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaiMGqETnO0LKpwmtx10IqXL7UYMHHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkWkwI0cb1X2HgtbVQdCXTAwJDmr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAaCBiTAYBgkqhkiG
9w0BCQcxCxMJQzFzY28uMTIzMG0GCSqGSIb3DQEJDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBBXOeWF5ZUz7O1GFjuQHBBDgYb+3lhFOxbYm9psIWfv1uwjkKoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswjlYpO+IxkUM971Ejwg2rj+jABDR7I8SU
O6YO6mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTIljdgVxB+XyzOFJMckIO5US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f9OA+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4lizO5Zj2NJbUKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZNOO
```

```
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

Étape 5. Importez le certificat signé par l'autorité de certification.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca import svs certificate

```
Fri May 9 15:00:35.426 UTC

Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA5MTQ1NzAwWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEOMAwGA1UECgwFQ2lzY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOdO2uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7ispmoBnXEOGJ
qIwaoROc7QsqnCa3HXQipcvtRgwcfAX29EgjnbOiaRYDxrrdbHrpSQTFpeh5dp/k
eQuioO7rxfzdTss+8x7WwzC+artGbLYMC7fQcH8l9iVAIeZNUXPczl8G3zrHHi3W
fFMVT/iVFYwLvdROvlhOokuMykFPaOOTemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTAjRxvVfYeC1tVBOJdMDAkOavY73N3ZkJrl6dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJOaWZpY2FO
ZTAOBgNVHQ8BAf8EBAMCBaAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMAkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjI1LjI1My4xNjeHBArh/acw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+ojO121O6WxedDQ8VduObBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8YOO7HR/2jf7gfhoRvwcR5QNOEHv4o6l
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV8lRGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr5lM4Ysvoltx1k9AeLjzb2syv5/fG6QuOZdWwTaaQhOY2h/cVDiV97wg
ODlmEfdSv6QrxQSujZr22RzVyKKHltuiV2B74pthUuGRBtfHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDplrf1ZIrPmv3ZPP7woTB22yWzydOuse+5IalbOw7OtwN4t/IIw
8CJu6HfnDXLDPZOjsC8steffrSlopwGccp3j6aZKPFz+I/Purb44a9WxEWa2TA7H
+rloynBcGMetOHxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF537Ow+uNHoK8Bdt8mqadUT4OoUSqY8ArVOBomO5tzbemreVPmQAZ/IahZ7TqKo
3dGNonTAfFTESM1iujQ81iRKsikDHySnwcCM2nilCKZrhVq5IB8NK6jKRJZOeQAX
vMt1
-----END CERTIFICATE-----
```

quit

```
Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792
```

Vérifiez que le certificat d'identité du routeur est inscrit.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

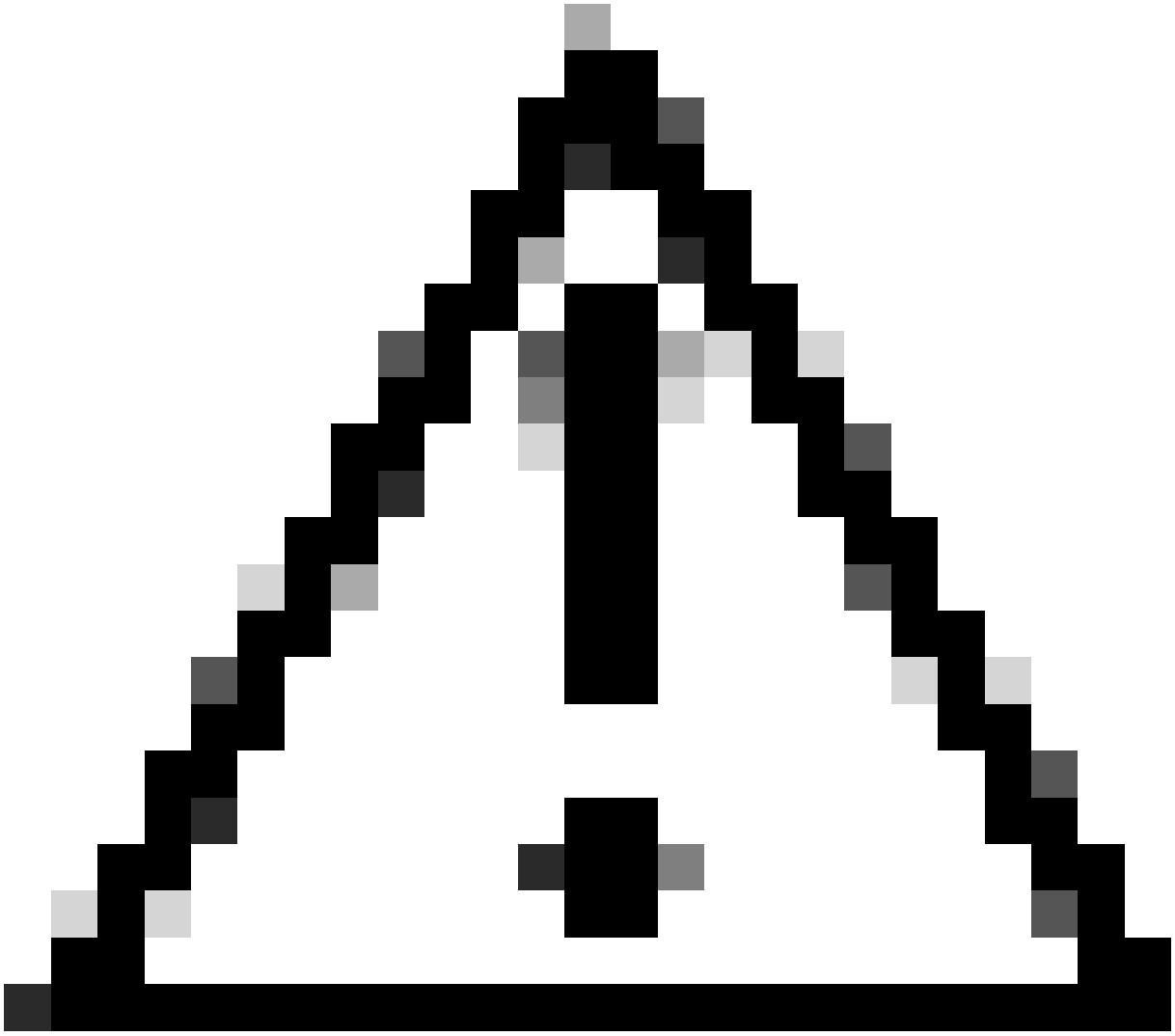
show crypto ca trustpoint svs detail

```
Trustpoint        :svs-new
================================================================
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1#
```

show crypto ca certificates svs

```
Wed May 14 14:55:58.173 UTC

Trustpoint       : svs-new
================================================
CA certificate
  Serial Number  : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
         0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
        serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
         AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs
```

Configuration de TACACS et AAA avec TLS



Mise en garde : Effectuez les modifications de configuration via la console avec les informations d'identification locales.

Étape 1 : configuration du serveur TACACS+.

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
  key 7 072C705F4D0648574453

aaa group server tacacs+ tacacs2
 server 10.225.253.209
 vrf mgmt
```

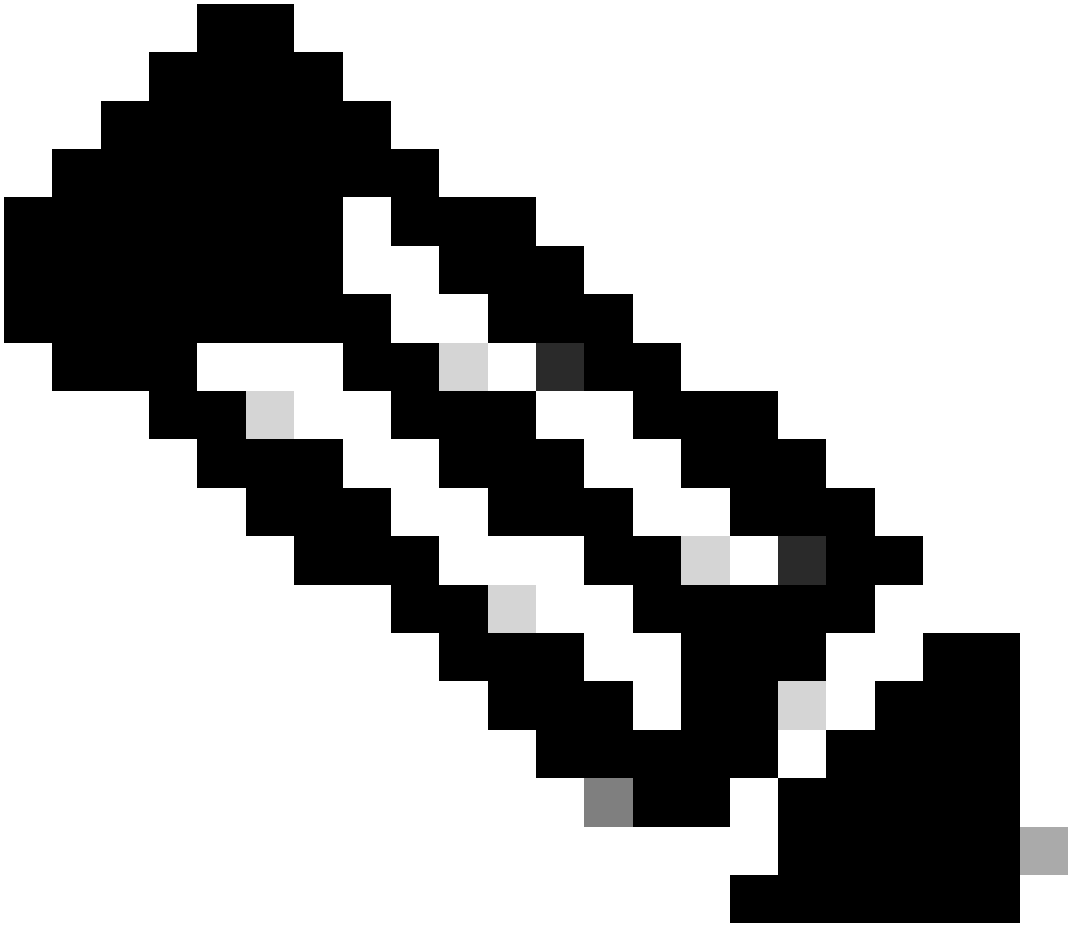
Étape 2 : configuration du groupe AAA.

```
aaa group server tacacs+ tac_tls_sc
 vrf mgmt
 server-private 10.225.253.209 port 6049
  timeout 10
  tls
   trustpoint svs
  !
  single-connection
```

Étape 2 : configuration de AAA.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

Renouvellement du certificat



Remarque : Il n'est pas nécessaire de supprimer le point de confiance de la configuration TACACS+ lors du renouvellement.

Étape 1. Vérifier les dates de validité actuelles des certificats

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svs-new
Thu Aug 14 15:13:37.465 UTC

Trustpoint : svs-new
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030
```

```
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5GvOAZM

  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 16:38:36 UTC Wed Jul 30 2025
  Validity End : 16:38:35 UTC Thu Jul 30 2026
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svs-new
```

Étape 2 : suppression du certificat trustpoint existant

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database update
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

Étape 3. Réauthentifiez et inscrivez le point de confiance comme décrit dans les étapes sous Configuration du point de confiance.

Étape 4. Vérification de la mise à jour des dates de validité des certificats

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC
```

```
Trustpoint : KF_TP
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5GvOAZM
  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 15:17:29 UTC Thu Aug 14 2025
  Validity End : 15:17:28 UTC Fri Aug 14 2026

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP
```

Vérification

Vérifier la configuration

```
show crypto ca certificates [detail]
show crypto ca trustpoint detail
show tacacs details
```

Débogage pour TACACS+

```
debug tacacs tls
```

Debug TLS

```
debug ssl error
debug ssl events
```

Testez l'utilisateur distant avant de configurer l'authentification AAA.

<#root>

test aaa group tacacs2

```
user has been authenticated
```

Dépannage

Effacement des certificats (tous les certificats associés à un point de confiance sont supprimés).

```
clear crypto ca certificate <trustpoint name>
```

Redémarrage du processus TACACS (si nécessaire)

```
process restart tacacsd
```

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.