Configurer TACACS+ sur TLS 1.3 sur un périphérique Nexus avec ISE

Table des matières

- Introduction
  - Aperçu
  - Utilisation de ce guide
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Licences
- Configurer ISE pour l'administration des périphériques
  - Générer une demande de signature de certificat pour l'authentification du serveur TACACS+
  - Télécharger le certificat CA racine pour l'authentification du serveur TACACS+
  - Lier la demande de signature de certificat signé (CSR) à ISE
  - Activer TLS 1.3
  - Activer l'administration des périphériques sur ISE
  - Activer TACACS sur TLS
  - Périphériques réseau et groupes de périphériques réseau
  - Configurer les magasins d'identités
  - Configurer les profils Shell TACACS+
  - Administrateur NX-OS
  - Centre d'assistance NX-OS
  - Configurer les ensembles de stratégies d'administration des périphériques
- Configuration de Cisco NX-OS pour TACACS+ sur TLS
  - Configuration du serveur TACACS+
  - Configuration du point de confiance
  - Configuration de TACACS+ TLS
  - Configuration AAA
- Test et dépannage de l'accès utilisateur pour NX-OS
  - Vérification
  - Dépannage

Introduction

Ce document décrit un exemple pour TACACS+ sur TLS avec Cisco Identity Services Engine (ISE) comme serveur et un périphérique Cisco NX-OS 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 NX-OS.
· Partie 1 : configuration d'ISE pour l'administration des périphériques
· Partie 2 : configuration de Cisco NX-OS 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

L’information fournie dans ce document est basée sur les versions logicielles et matérielles suivantes :

- Appliance virtuelle ISE VMware, version 3.4, correctif 2.
- Commutateur Nexus 9000 modèle C9364D-GX2A, Cisco NX-OS version 10.5(3t).

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.

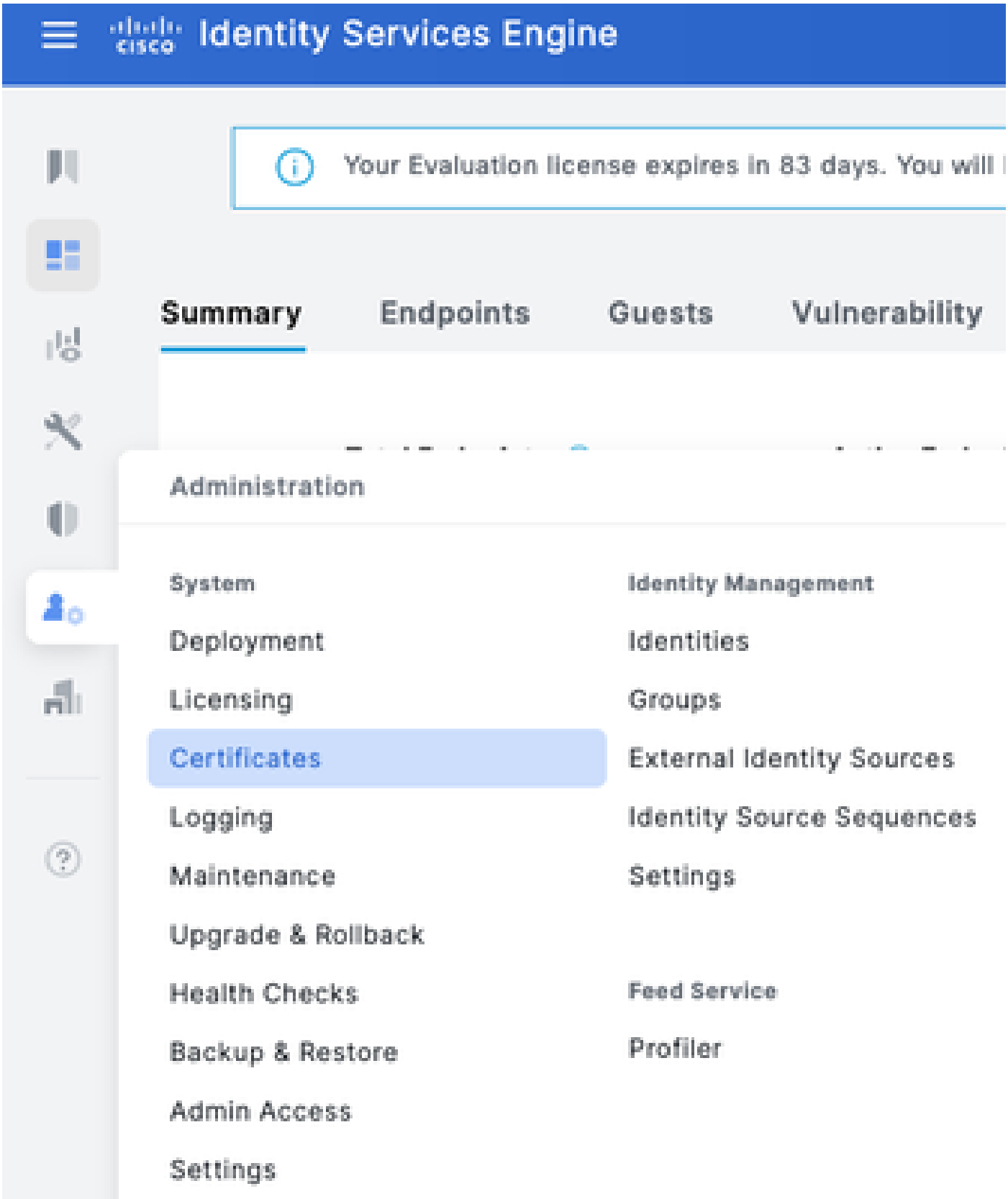
Configurer ISE pour l'administration des périphériques

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

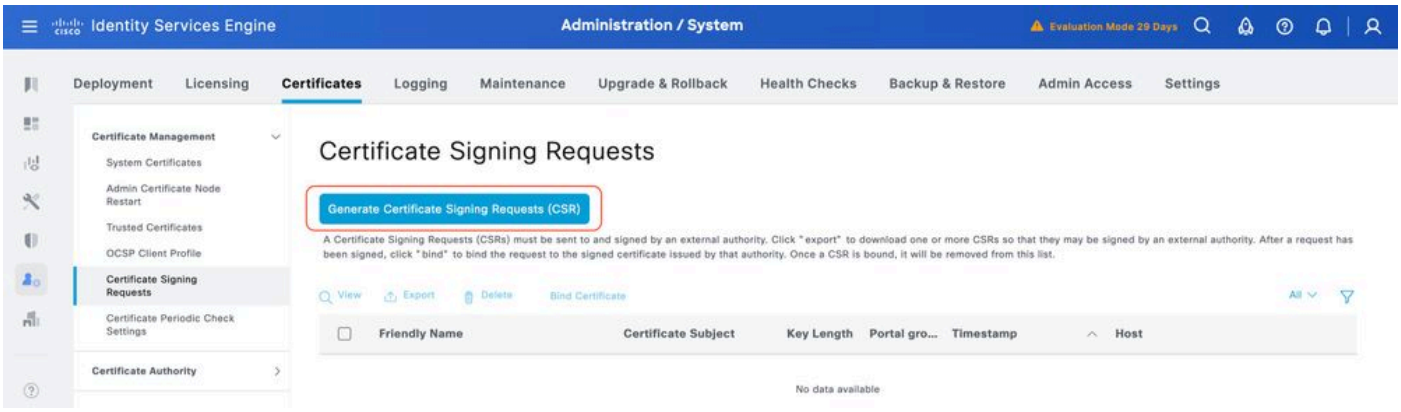
Étape 1. Connectez-vous au portail Web d’administration ISE à l’aide de l’un des navigateurs pris en charge.

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.



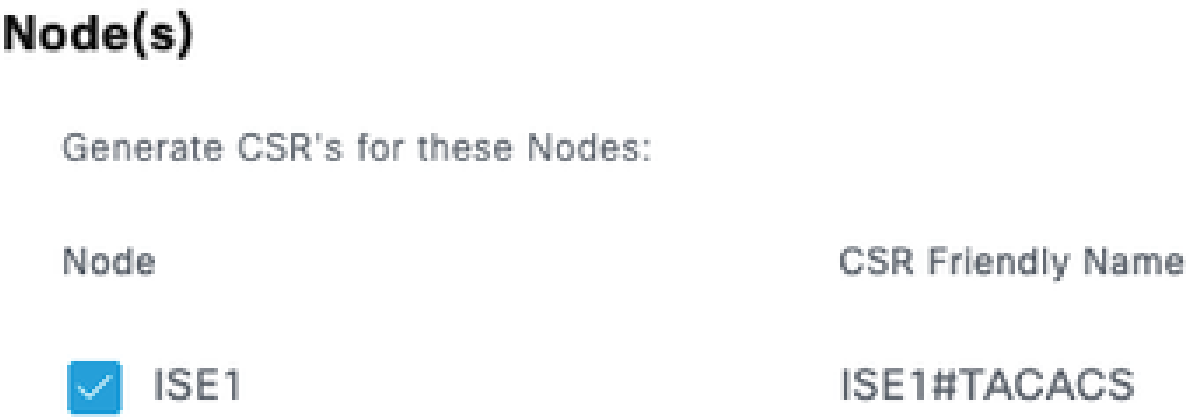
Étape 3. Sous Certificate Signing Requests, cliquez sur Generate Certificate Signing Request.



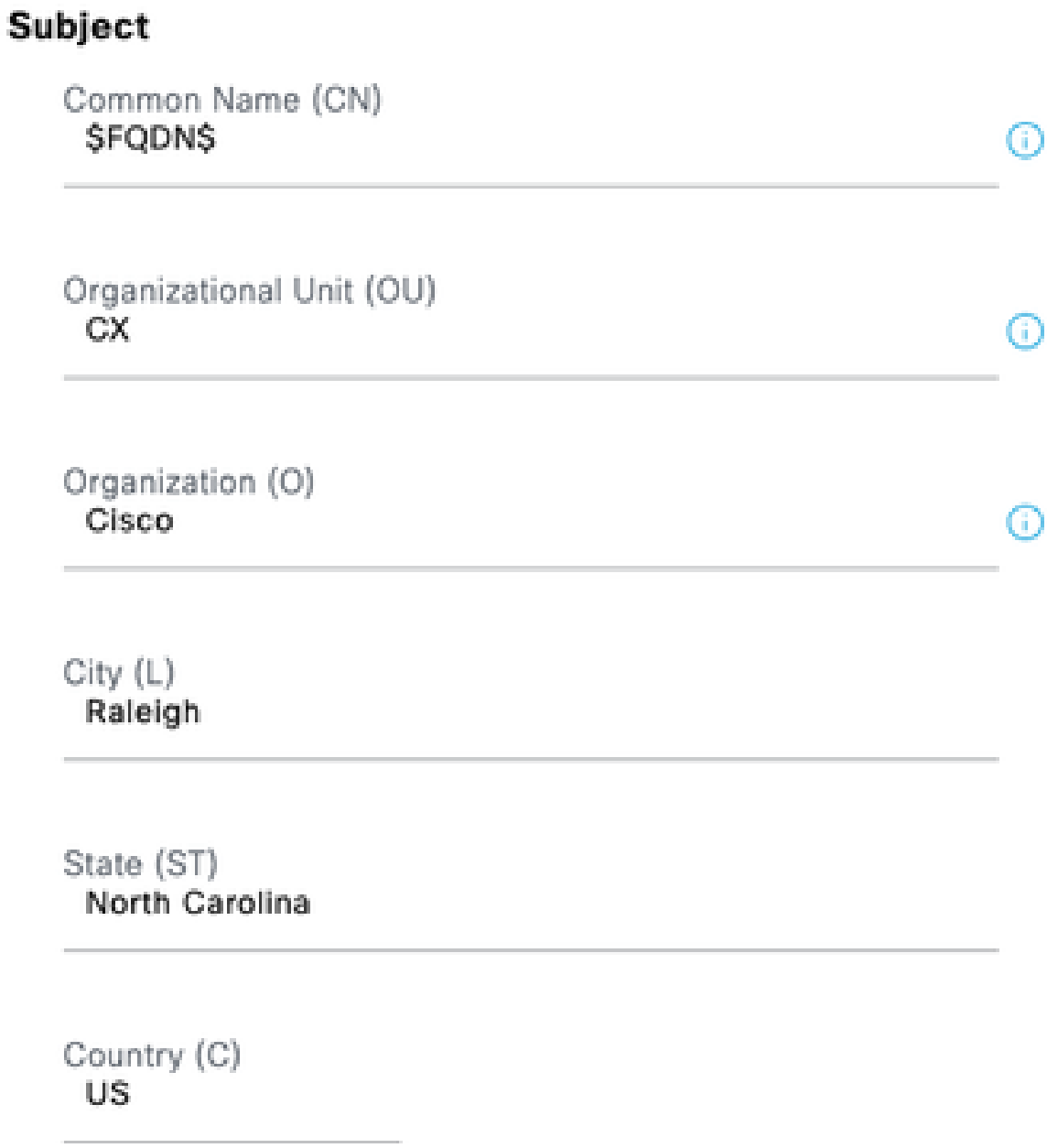
Étape 4. Sélectionnez TACACS dans Utilisation.



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 Subject Alternative Name (SAN).



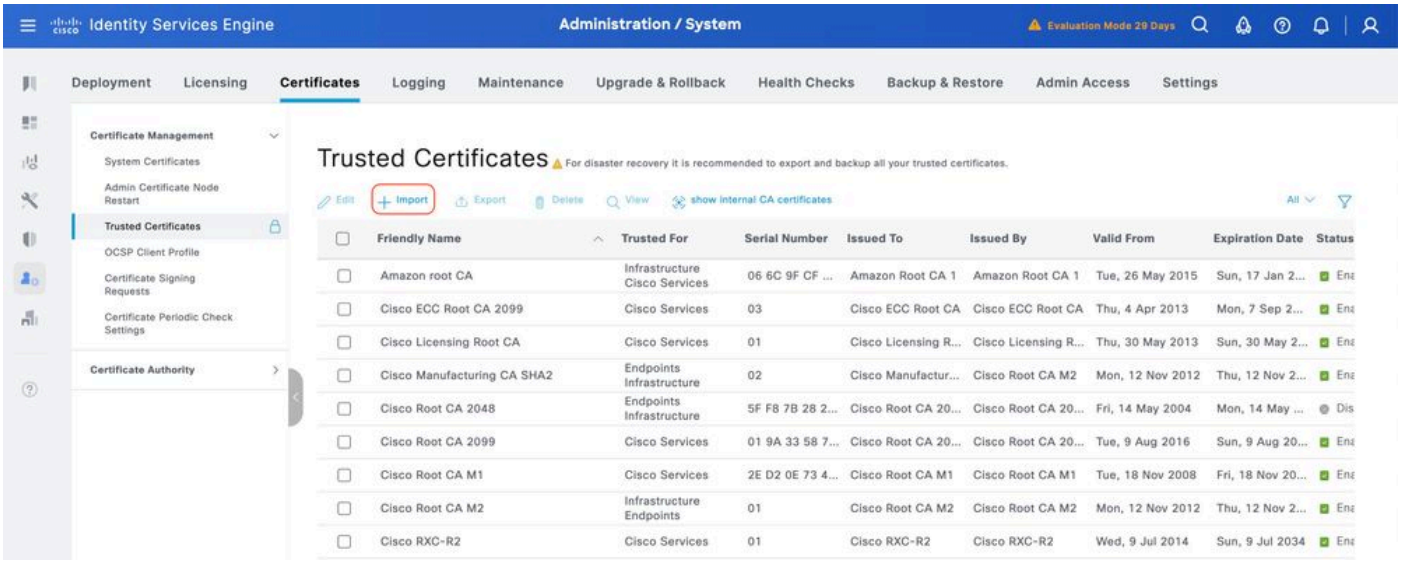
Étape 8. Cliquez sur Generate, puis sur Export.



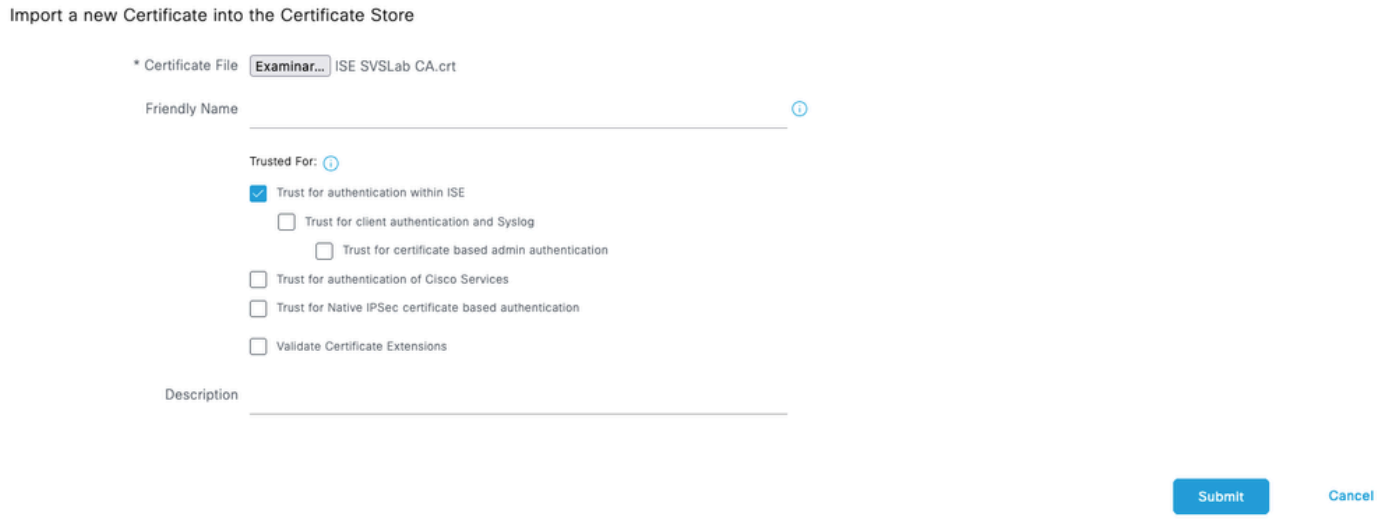
Vous pouvez maintenant faire signer le certificat (CRT) par votre autorité de certification (CA).

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

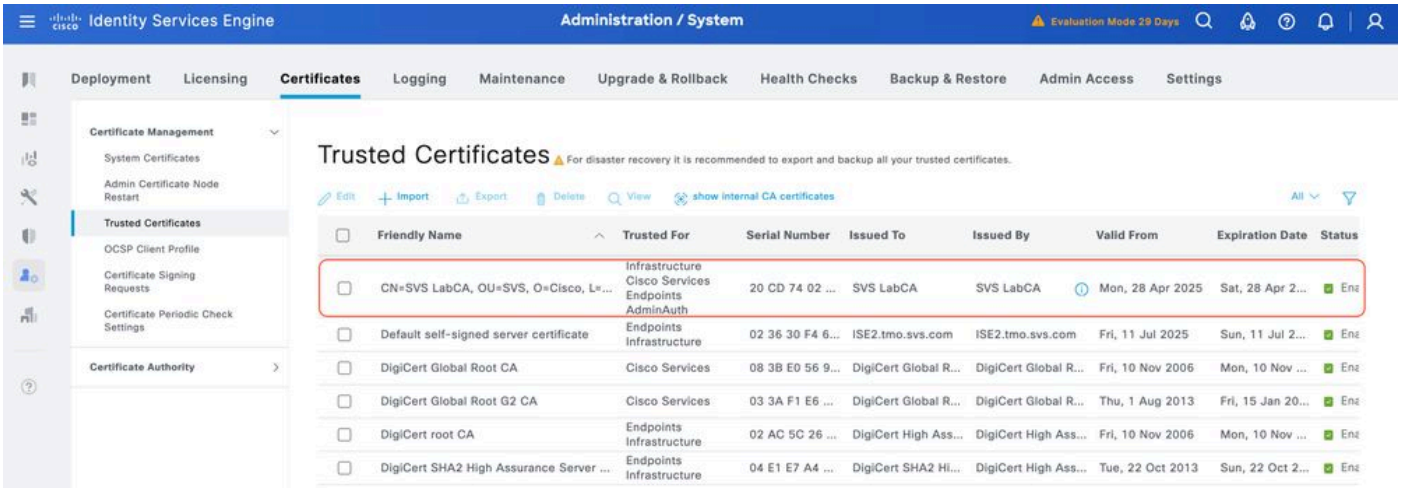
Étape 1. Accédez à Administration > System > Certificates. Sous Certificats approuvés, cliquez sur Importer.



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



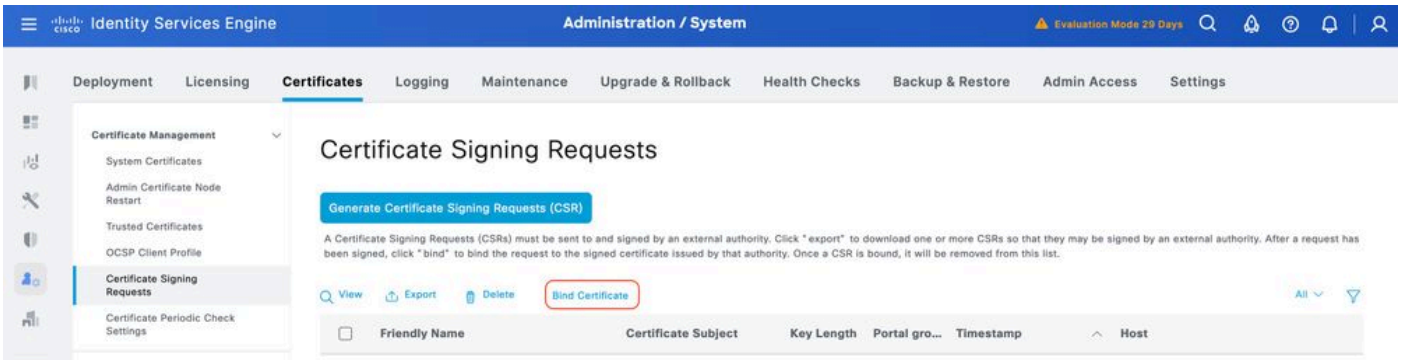
Cliquez sur Submit. Le certificat doit maintenant apparaître sous Trusted Certificates.



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

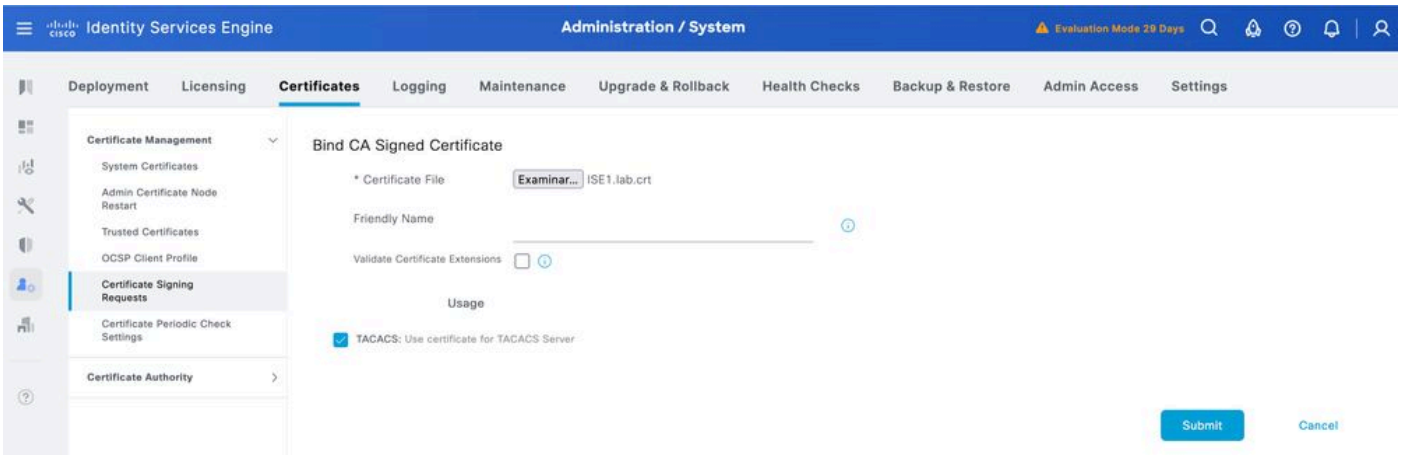
Une fois la demande de signature de certificat (CSR) signée, vous pouvez installer le certificat signé sur ISE.

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

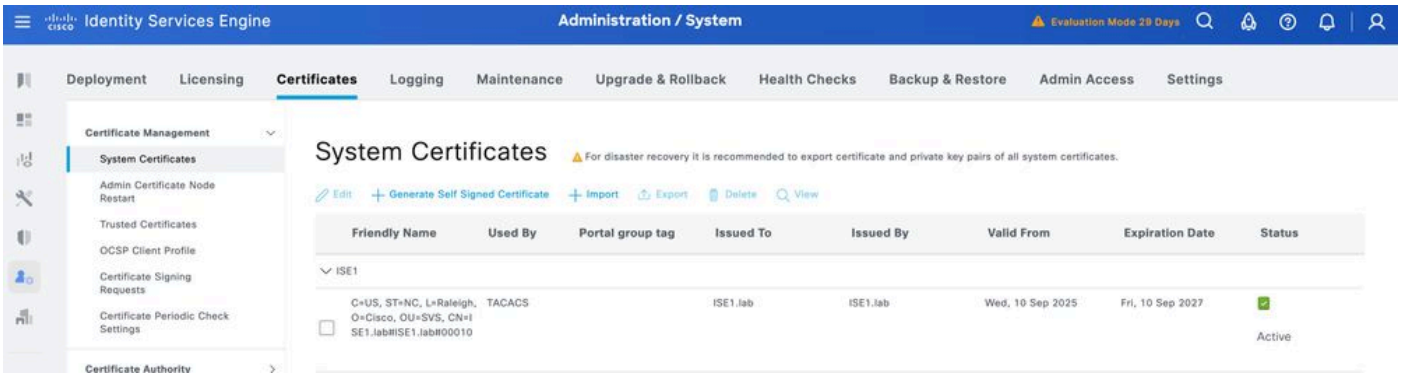
Utilisation reste sélectionnée.



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



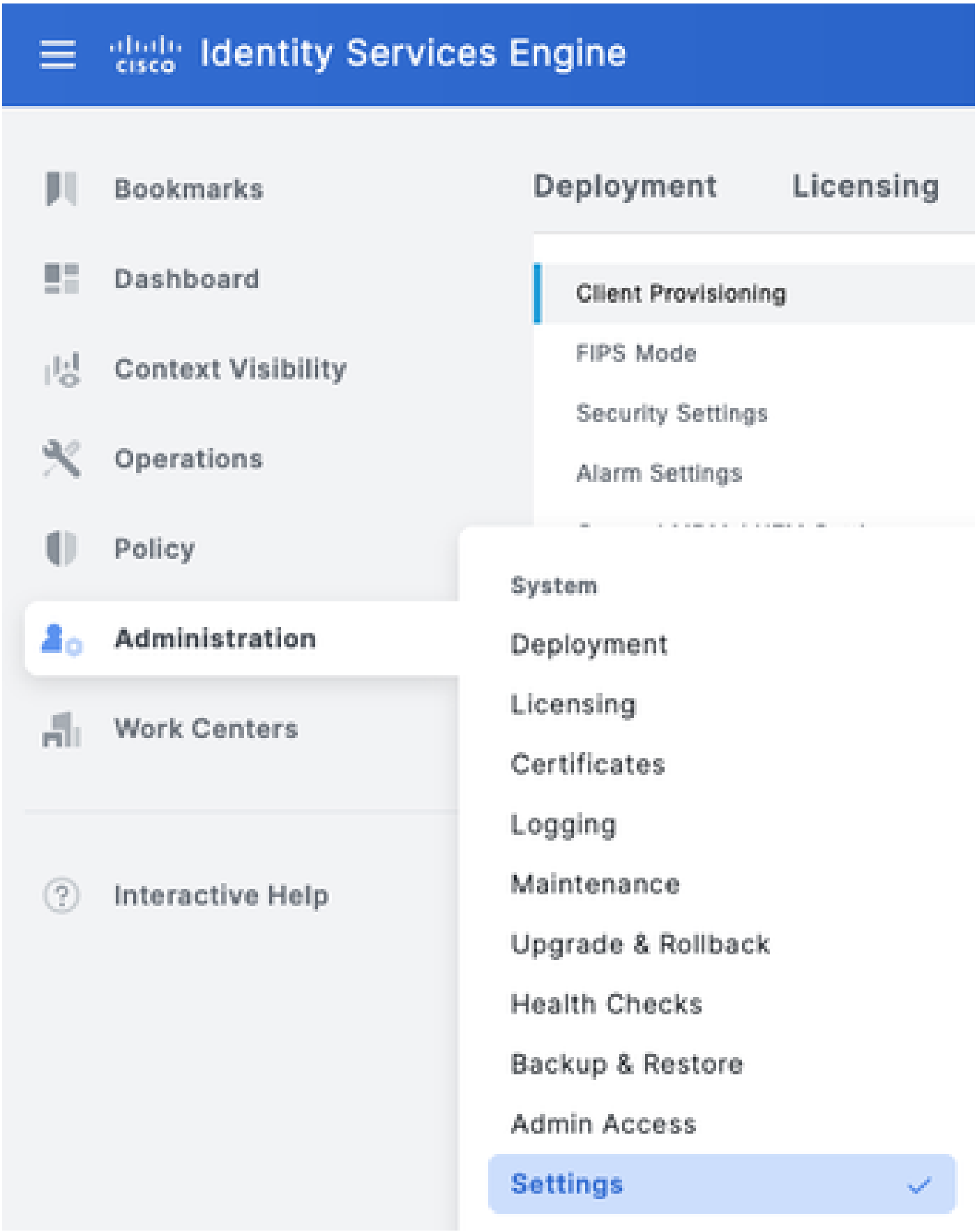
Le certificat doit maintenant être correctement installé. Vous pouvez le vérifier sous Certificats système.



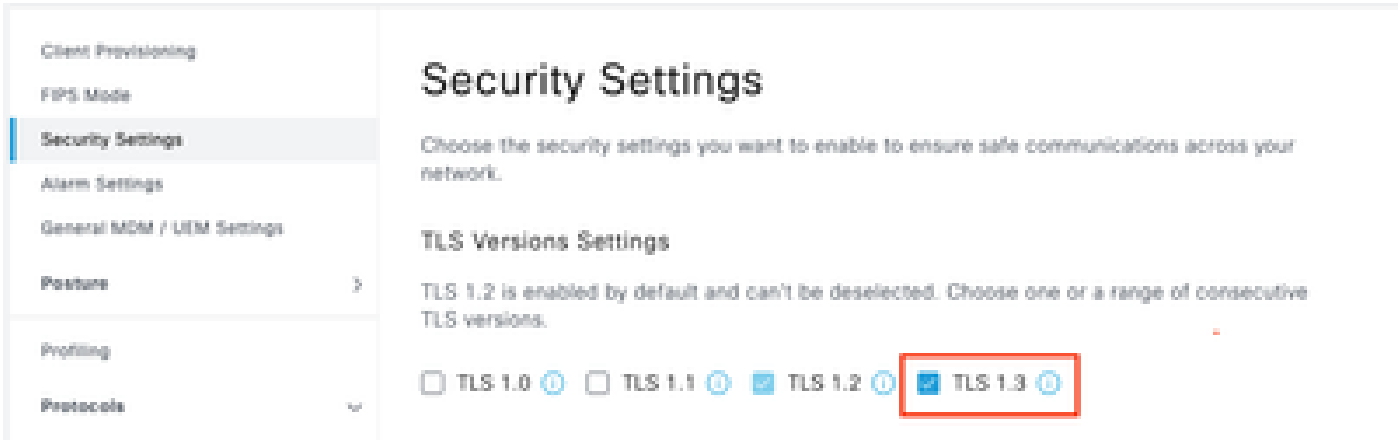
Activer TLS 1.3

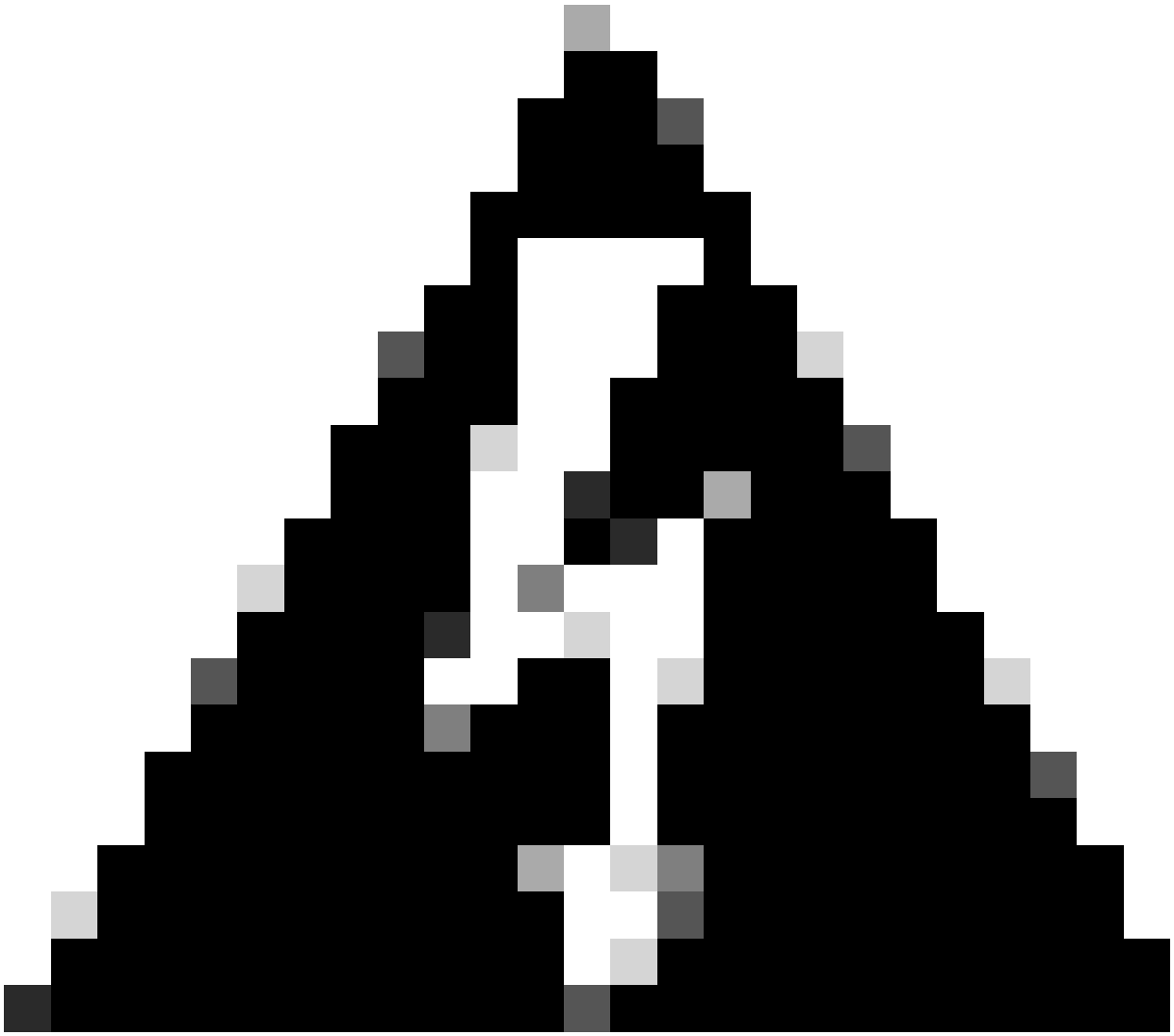
TLS 1.3 n'est pas activé par défaut dans ISE 3.4.x. Il doit être activé manuellement.

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.



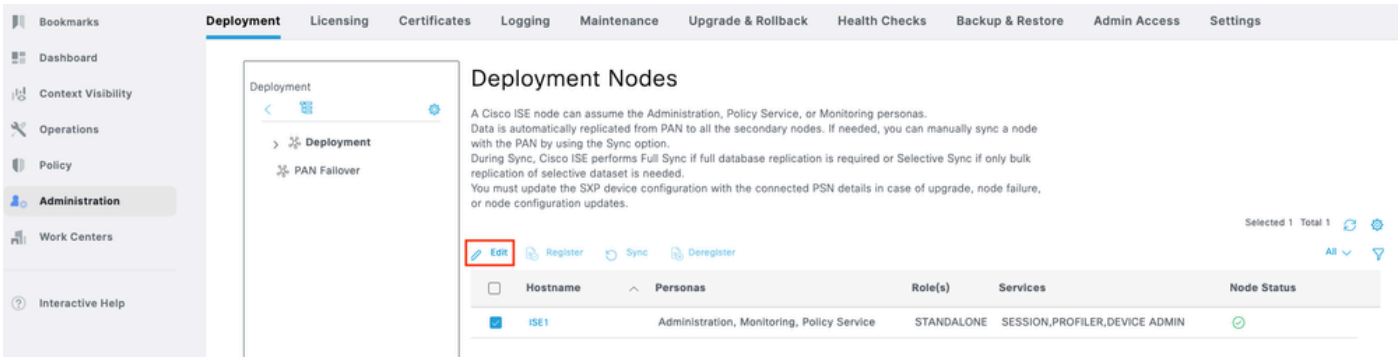


Avertissement : Lorsque vous modifiez la version TLS, le serveur d'applications Cisco ISE redémarre sur toutes les machines de déploiement Cisco ISE.

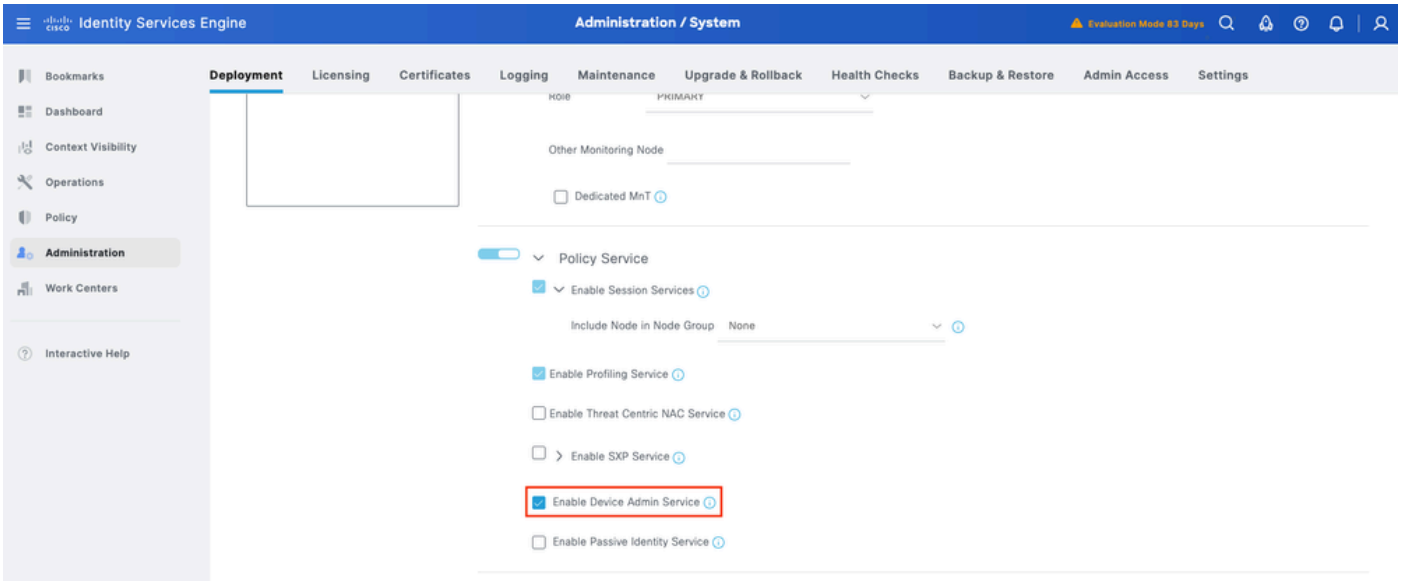
Activer l'administration des périphériques sur ISE

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

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



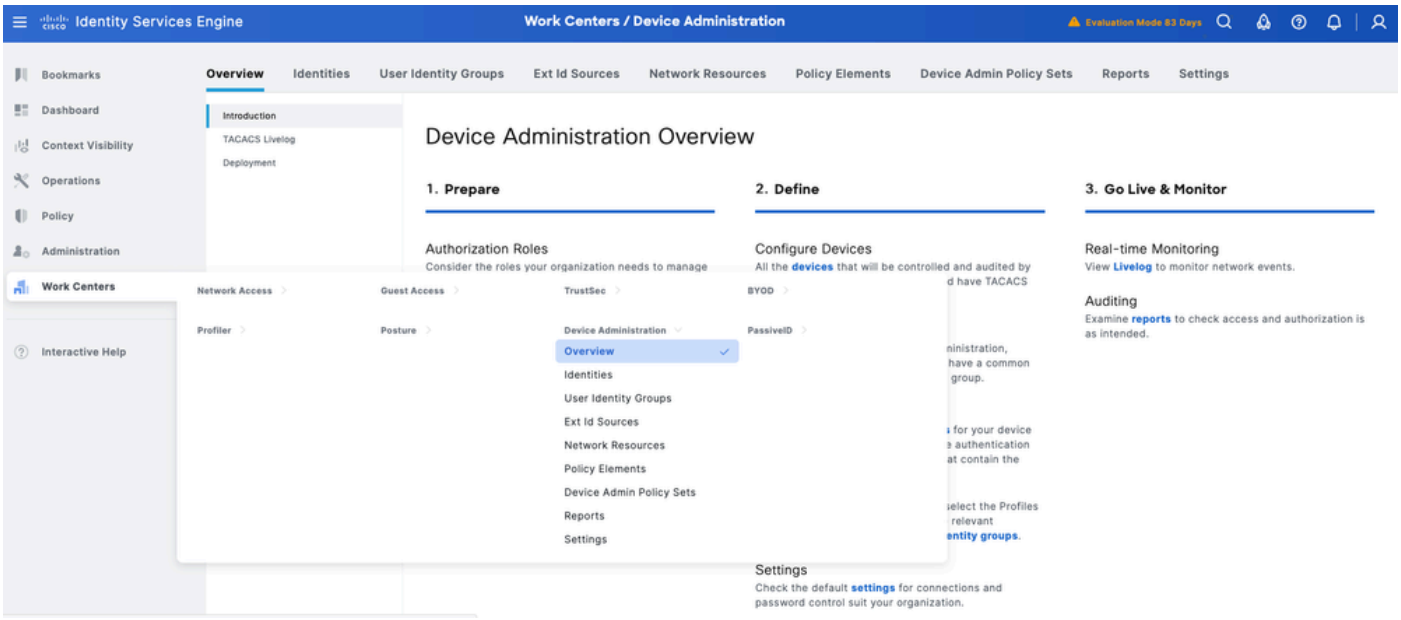
Étape 2. Sous General Settings, faites défiler la page vers le bas et activez la case à cocher en regard de Enable Device Admin Service.



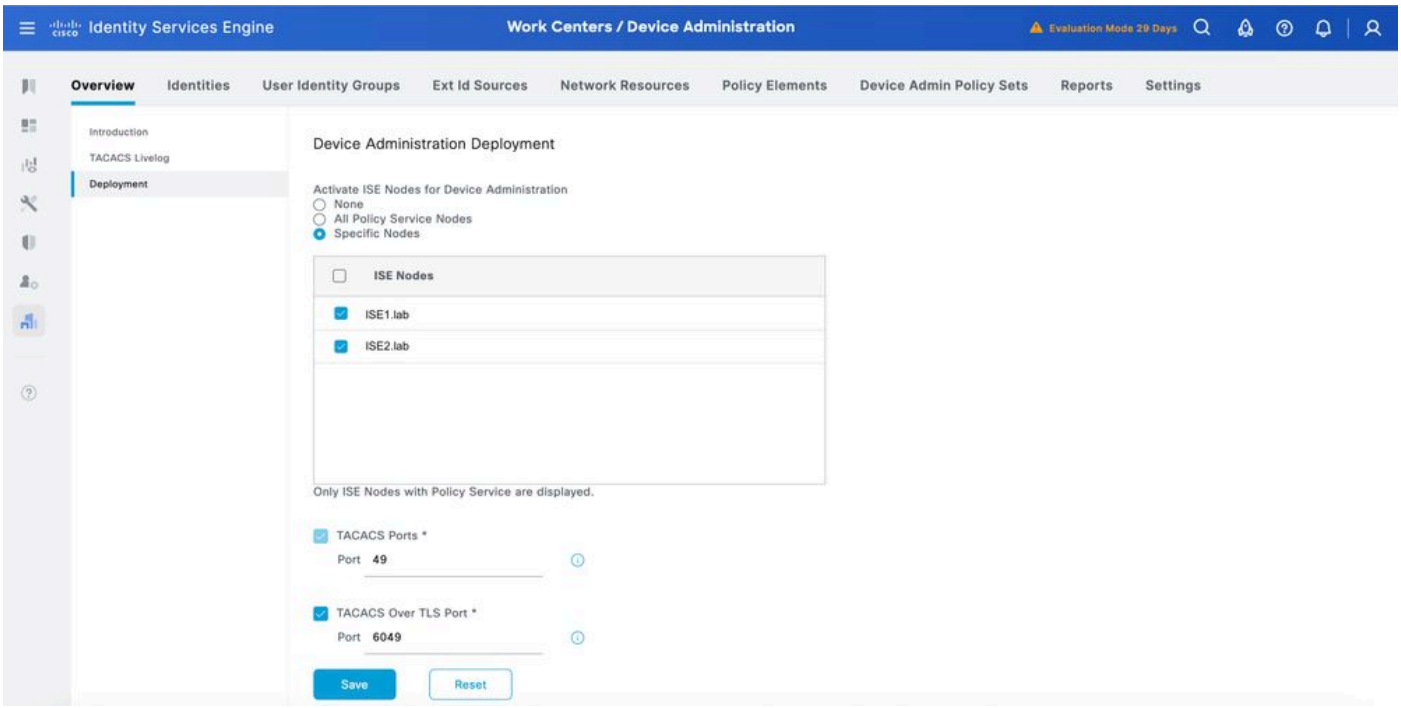
Étape 3 : enregistrement de la configuration Le service d'administration des périphériques est désormais activé sur ISE.

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.

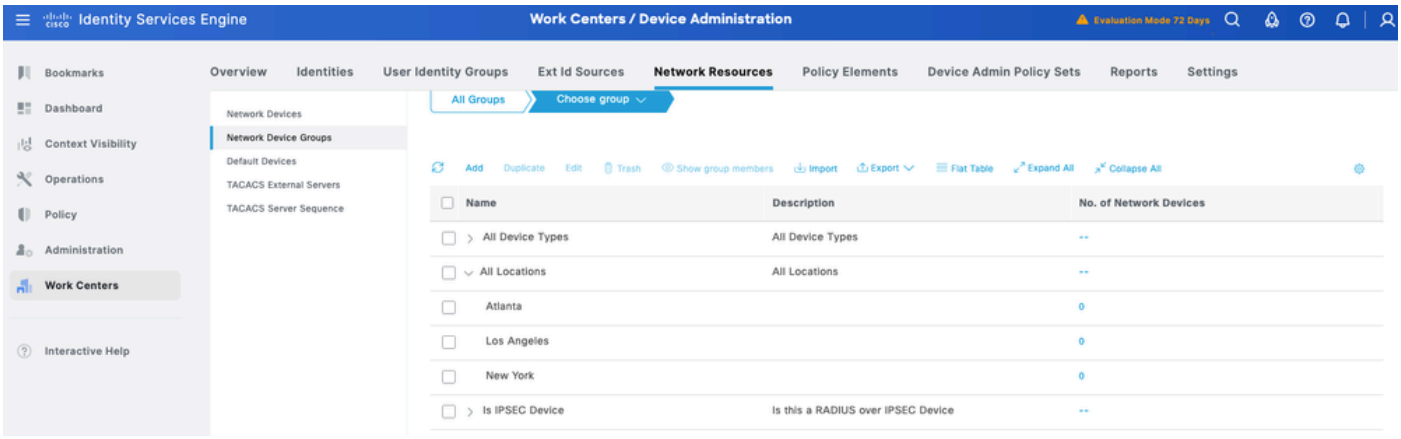


Étape 3. Conservez le port par défaut 6049 ou spécifiez un autre port TCP pour TACACS sur TLS, puis cliquez sur Save.

Périphériques réseau et groupes de périphériques réseau

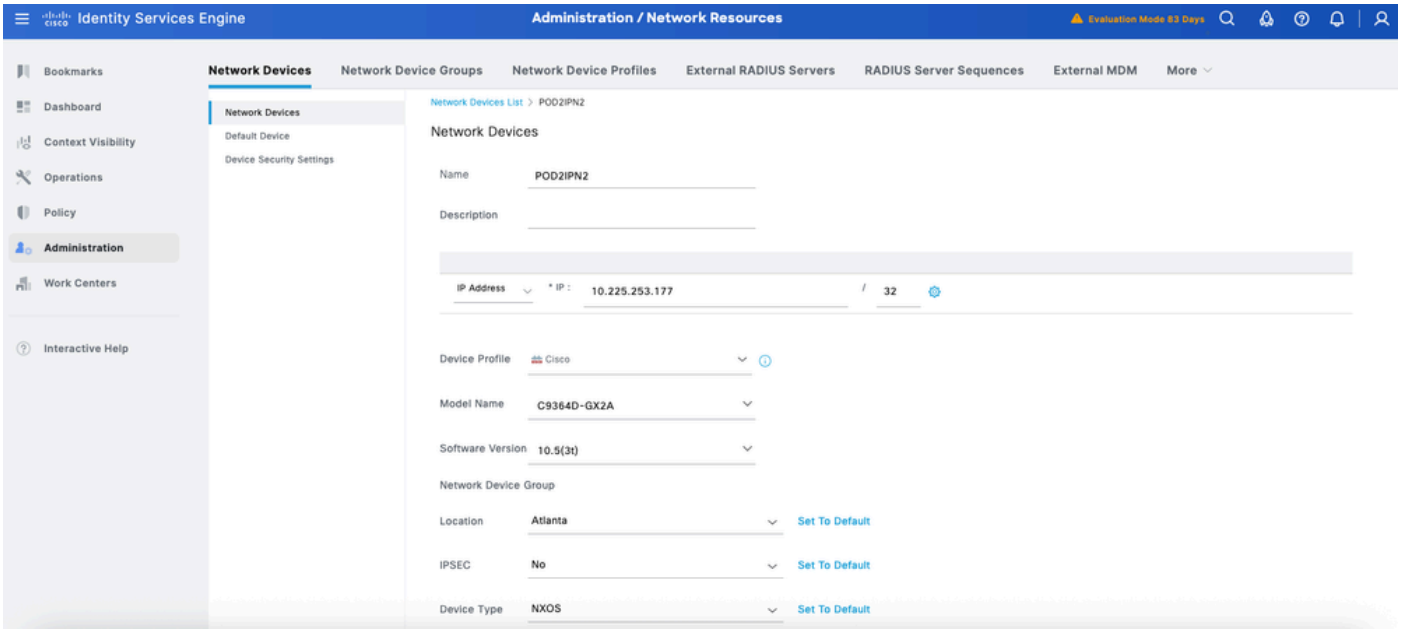
ISE fournit un regroupement de périphériques puissant avec plusieurs hiérarchies de groupes de périphériques. Chaque hiérarchie représente une classification distincte et indépendante des périphériques réseau.

Étape 1. Accédez à Work Centers > Device Administration > Network Resource. Cliquez sur Network Device Groups.

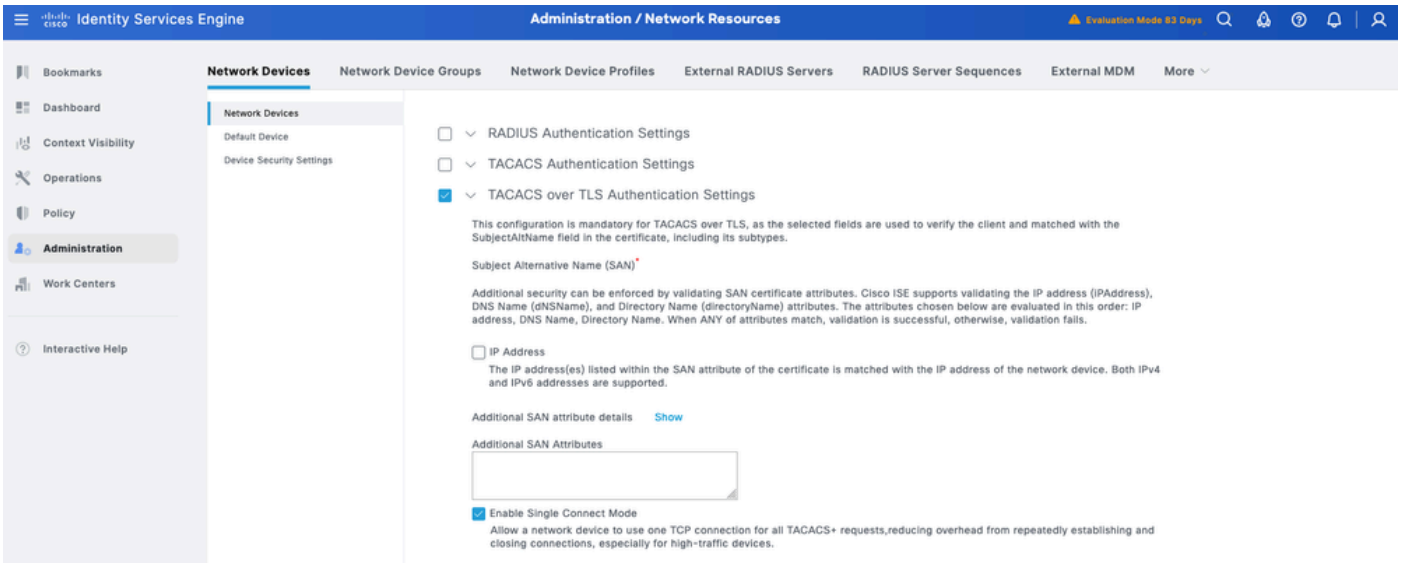


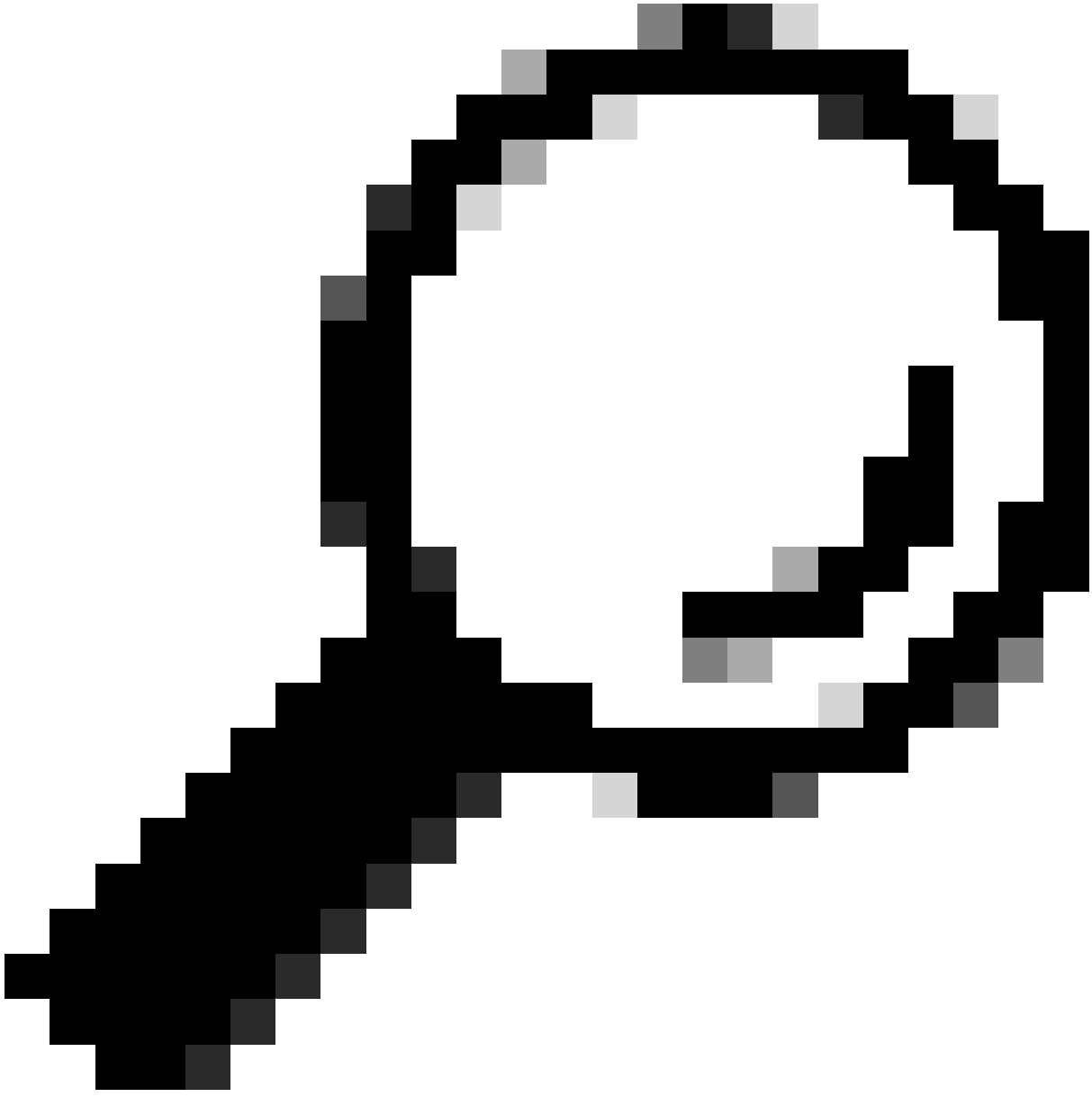
Tous les types de périphériques et tous les emplacements sont des hiérarchies par défaut fournies par ISE. Vous ajoutez vos propres hiérarchies et définissez les différents composants pour identifier un périphérique réseau qui peut être utilisé ultérieurement dans la condition de stratégie.

Étape 2. À présent, ajoutez un périphérique NS-OX en tant que périphérique réseau. Accédez à Work Centers > Device Administration > Network Resources. Cliquez sur Add pour ajouter un nouveau périphérique réseau POD2IPN2.



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


Identity Services Engine
Administration / Network Resources
Evaluation Mode 83 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
External MDM
More
Network Devices
Default Device
Device Security Settings
RADIUS Authentication Settings
TACACS Authentication Settings
TACACS over TLS Authentication Settings
This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.
Subject Alternative Name (SAN)*
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.
IP Address
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.
Additional SAN attribute details
Show
Additional SAN Attributes
Enable Single Connect Mode
Allow a network device to use one TCP connection for all TACACS+ requests,reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

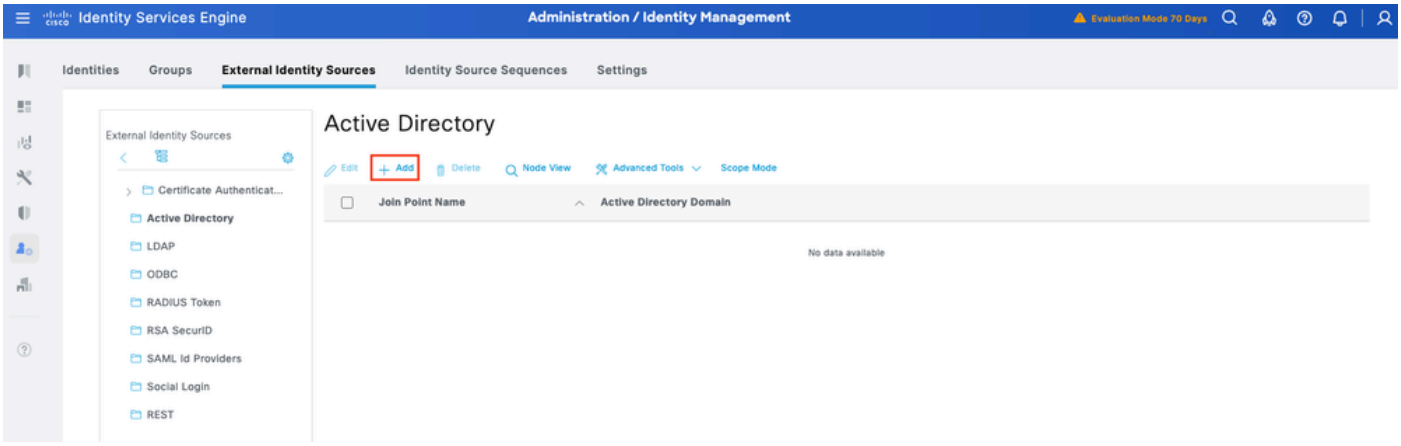


Conseil : Il est recommandé d'activer le mode de connexion unique pour éviter de redémarrer la session TCP chaque fois qu'une commande est envoyée au périphérique.

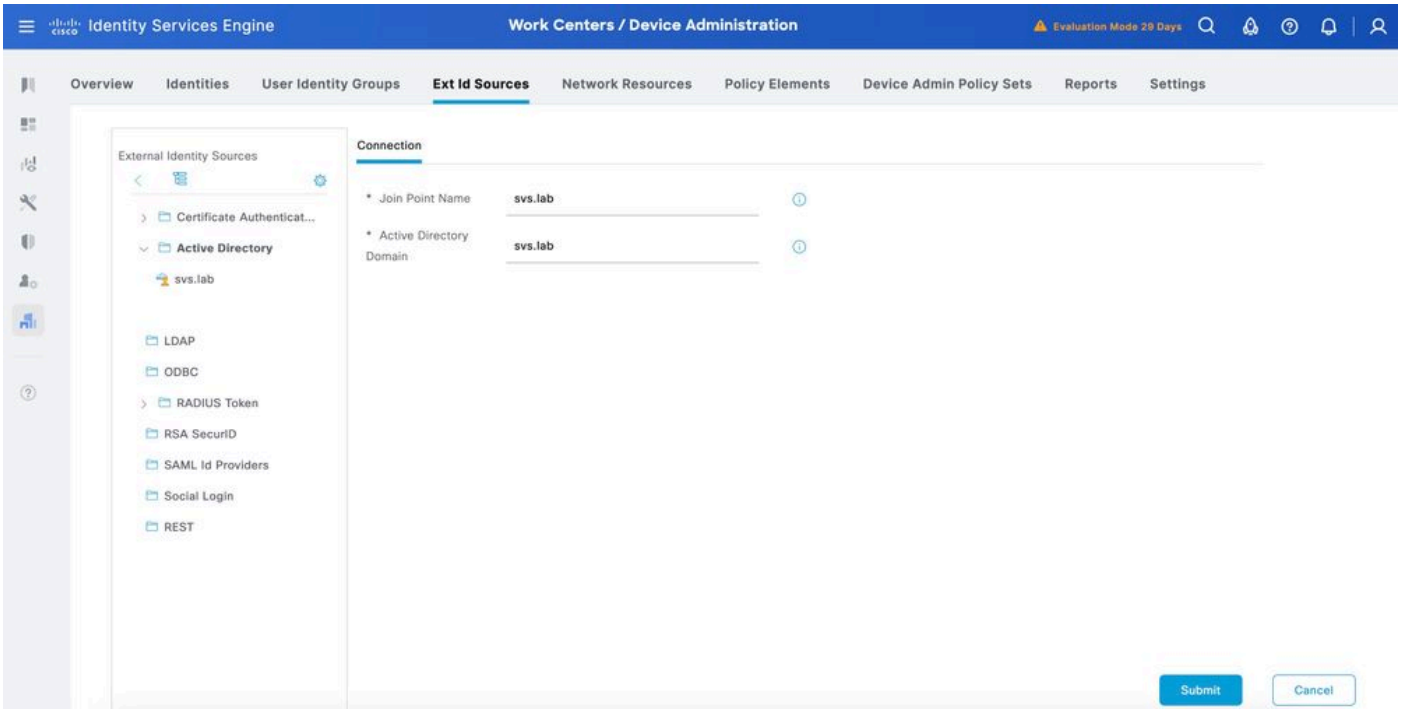
Configurer les magasins d'identités

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.



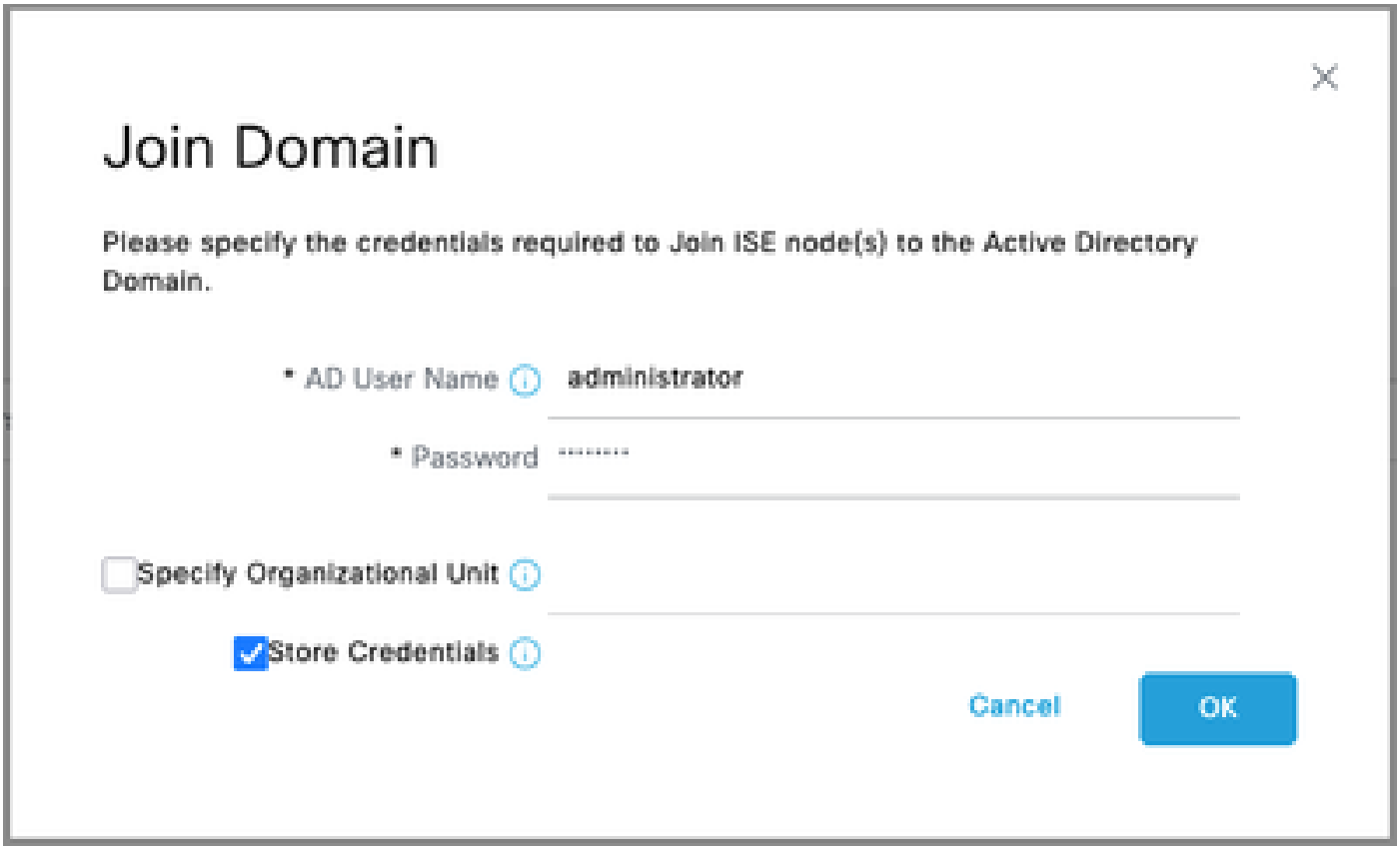
Étape 2. Spécifiez le nom du point de jonction et le nom du domaine Active Directory, puis cliquez sur Envoyer.

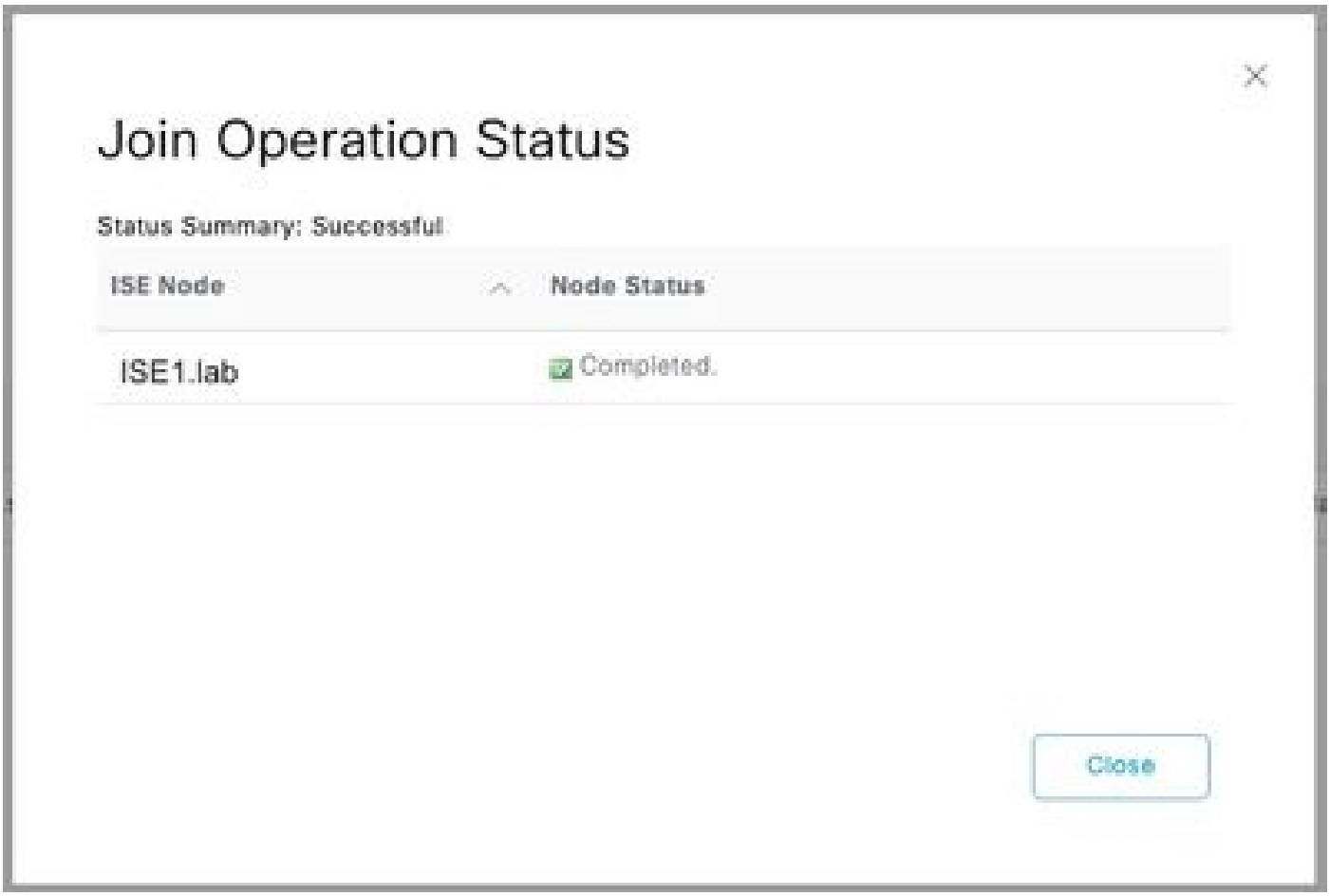


Étape 3. Cliquez sur Yes lorsque le message « Would you like to Join all ISE Nodes to this Active Directory Domain ? » s'affiche

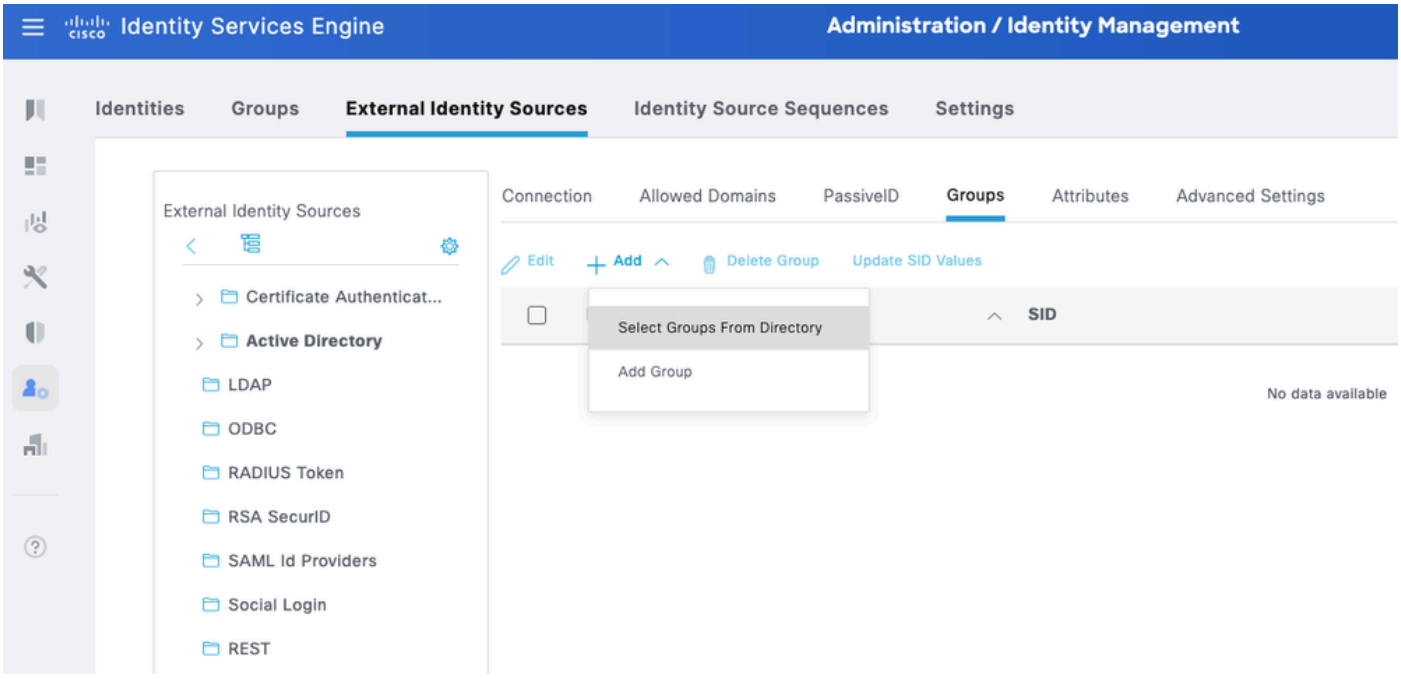


Étape 4. Entrez les informations d'identification avec les privilèges de jointure AD et Joignez ISE à AD. Vérifiez l'état pour vous assurer qu'il est opérationnel.

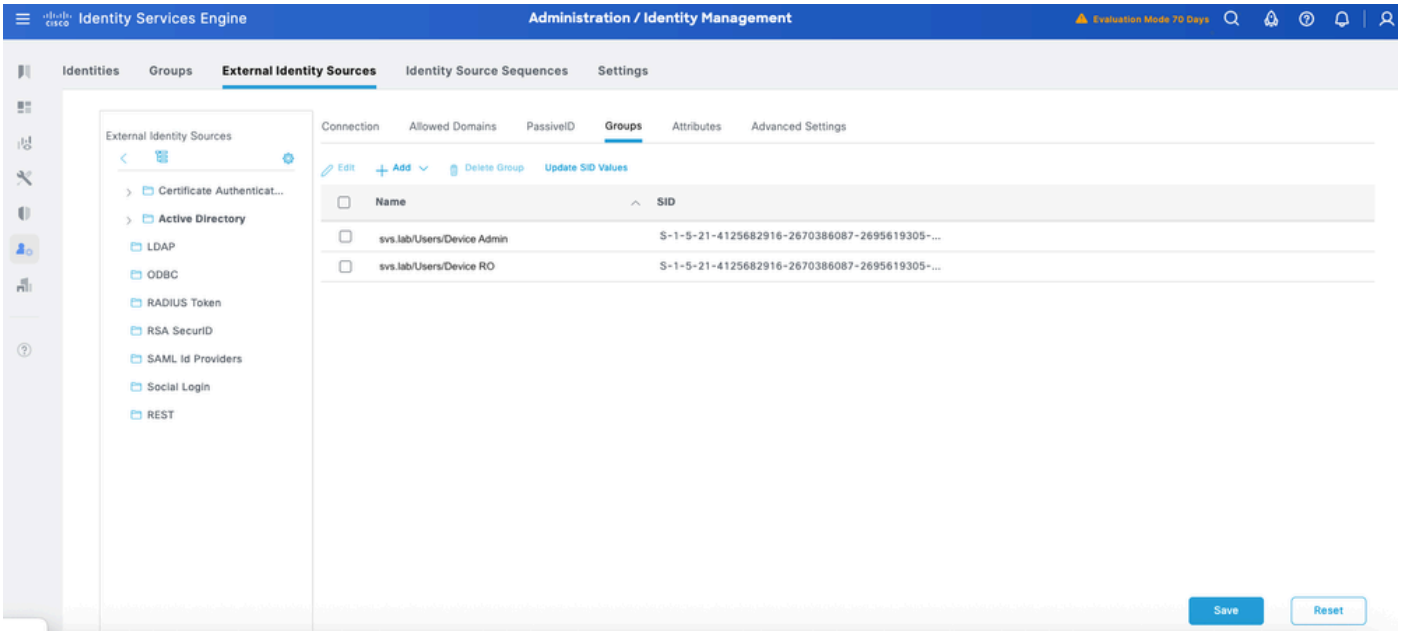




Étape 5. Accédez à l'onglet Groups, et cliquez sur Add pour obtenir tous les groupes nécessaires en fonction des utilisateurs autorisés à accéder au périphérique. Cet exemple montre les groupes utilisés dans la stratégie d'autorisation de ce guide.







Configuration des profils Shell TACACS+

Contrairement aux périphériques Cisco IOS, qui utilisent des niveaux de privilège pour l'autorisation, les périphériques Cisco NX-OS mettent en oeuvre un contrôle d'accès basé sur les rôles (RBAC). Dans ISE, vous pouvez mapper des profils TACACS+ à des rôles d'utilisateur sur des périphériques Cisco NX-OS à l'aide des tâches communes de type Nexus.

Les rôles prédéfinis sur les périphériques NX-OS diffèrent selon les plates-formes NX-OS. Les deux plus courantes sont :

- network-admin : le rôle d'administrateur réseau prédéfini dispose d'un accès complet en lecture et en écriture à toutes les commandes du commutateur ; disponible dans le contexte de périphérique virtuel (VDC) par défaut uniquement si les périphériques (par exemple, Nexus 7000) ont plusieurs VDC. Utilisez la commande CLI NX-OS show cli syntaxe roles

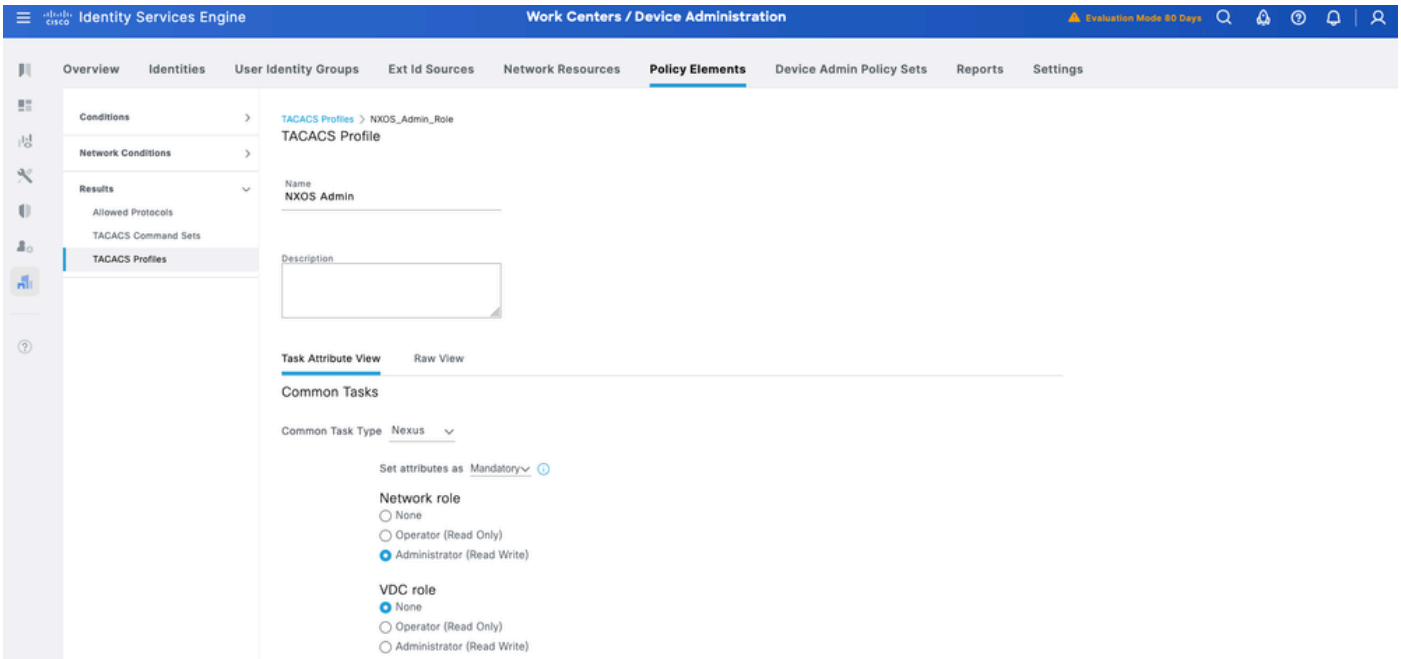
network-admin pour afficher la liste complète des commandes disponibles pour ce rôle.
- network-operator : le rôle d'administrateur réseau prédéfini dispose d'un accès en lecture complet à toutes les commandes du commutateur ; disponible dans le VDC par défaut uniquement si les périphériques (par exemple, Nexus 7000) ont plusieurs VDC. Utilisez la commande CLI NX-OS show cli syntaxe roles network-operator pour afficher la liste complète des commandes disponibles pour ce rôle.

Ensuite, deux profils TACACS sont définis : NXOS Admin et NXOS HelpDesk.

Administrateur NX-OS

Étape 1. Ajouter un autre profil et le nommer Admin NX-OS.

Étape 2. Sélectionnez Obligatoire dans la liste déroulante Définir les attributs. Sélectionnez Administrateur dans l'option Rôle réseau sous Tâches communes.



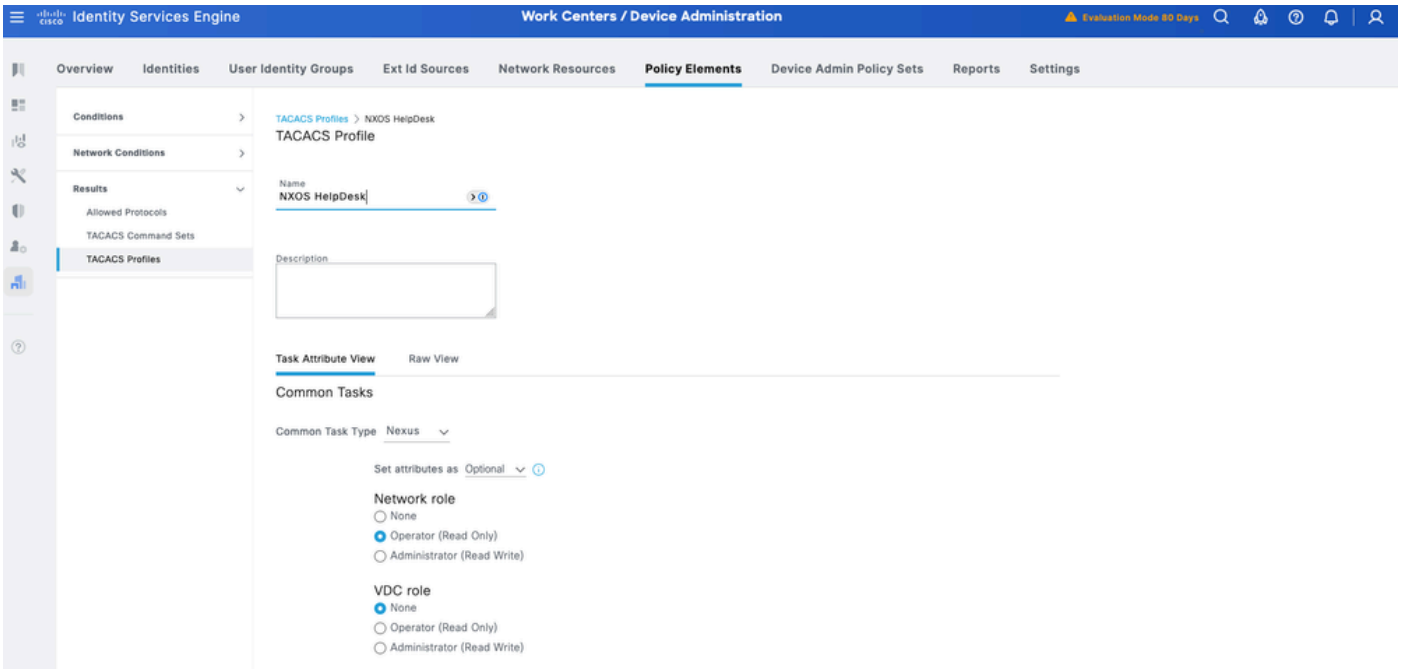
Étape 3. Cliquez sur Submit pour enregistrer le profil.

Centre d'assistance NX-OS

Étape 1. Dans l'interface utilisateur d'ISE, accédez à Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Ajoutez un nouveau profil TACACS et nommez-le NXOS HelpDesk. Accédez à la liste déroulante Type de tâche commun et sélectionnez Nexus.

Vous pouvez voir les modifications du modèle spécifiques au rôle d'utilisateur. Vous pouvez sélectionner ces options en fonction du rôle d'utilisateur que vous souhaitez configurer.

Étape 2. Sélectionnez Obligatoire dans la liste déroulante Définir les attributs. Sélectionnez Opérateur dans l'option Rôle réseau sous Tâches communes.

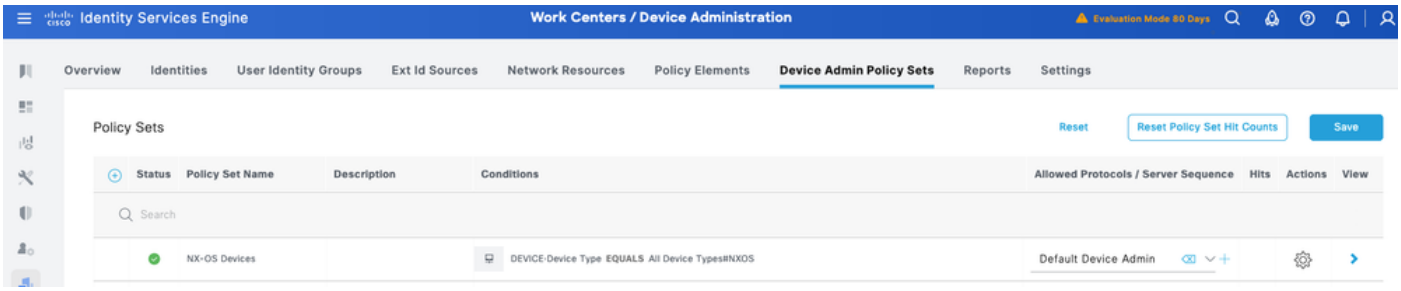


Étape 3. Cliquez sur Save pour enregistrer le profil.

Configurer les ensembles de stratégies d'administration des périphériques

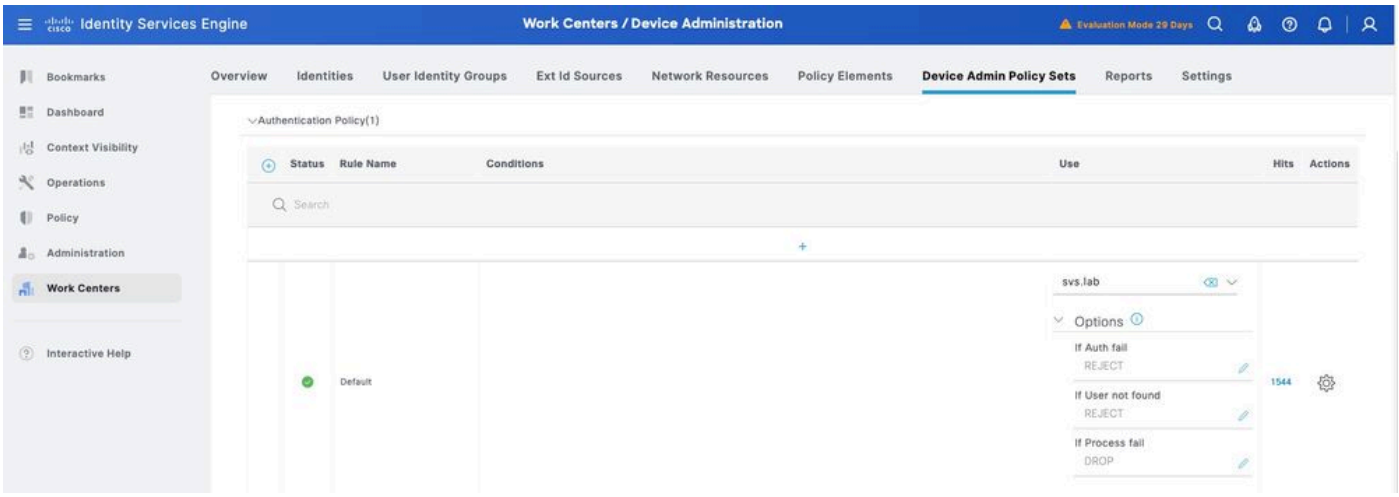
Les jeux de stratégies sont activés par défaut pour l'administration des périphériques. Les ensembles de politiques peuvent diviser les politiques en fonction des types de périphériques afin de faciliter l'application des profils TACACS. Par exemple, les périphériques Cisco IOS utilisent des niveaux de privilège et/ou des jeux de commandes, tandis que les périphériques Cisco NX-OS utilisent des attributs personnalisés.

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



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

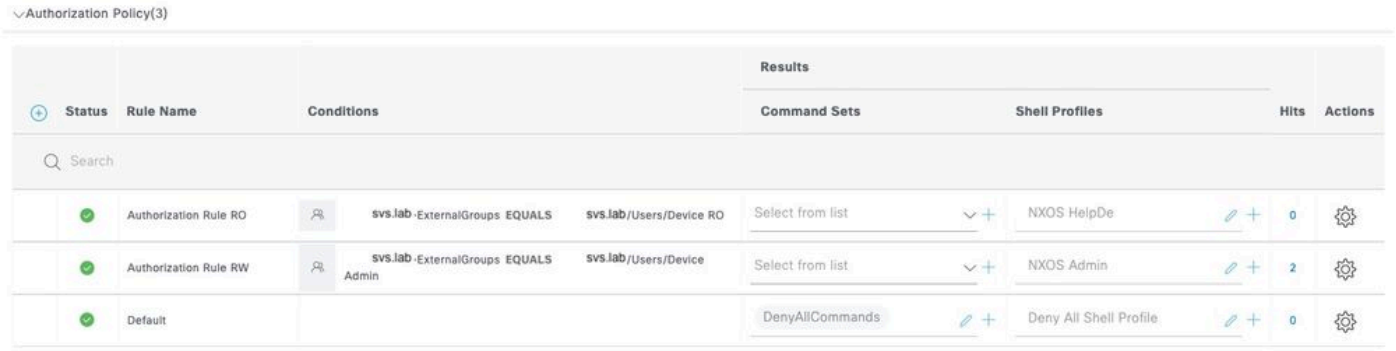
Étape 3 : création de la stratégie d'authentification. Pour l'authentification, vous utilisez AD comme magasin d'ID. Conservez les options par défaut sous If Auth fail, If User not found et If Process fail.



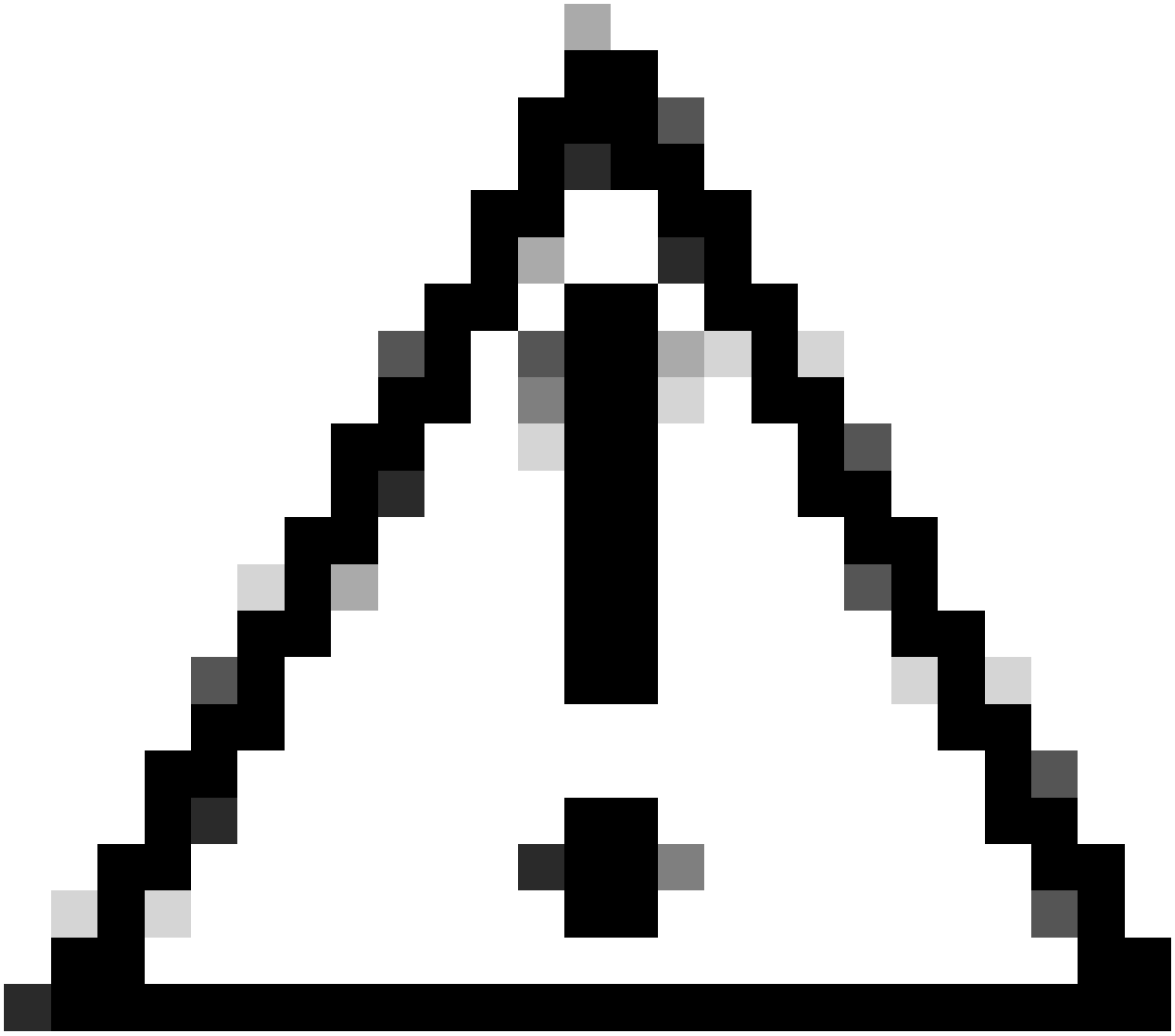
Étape 4 : définition de la politique d’autorisation

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

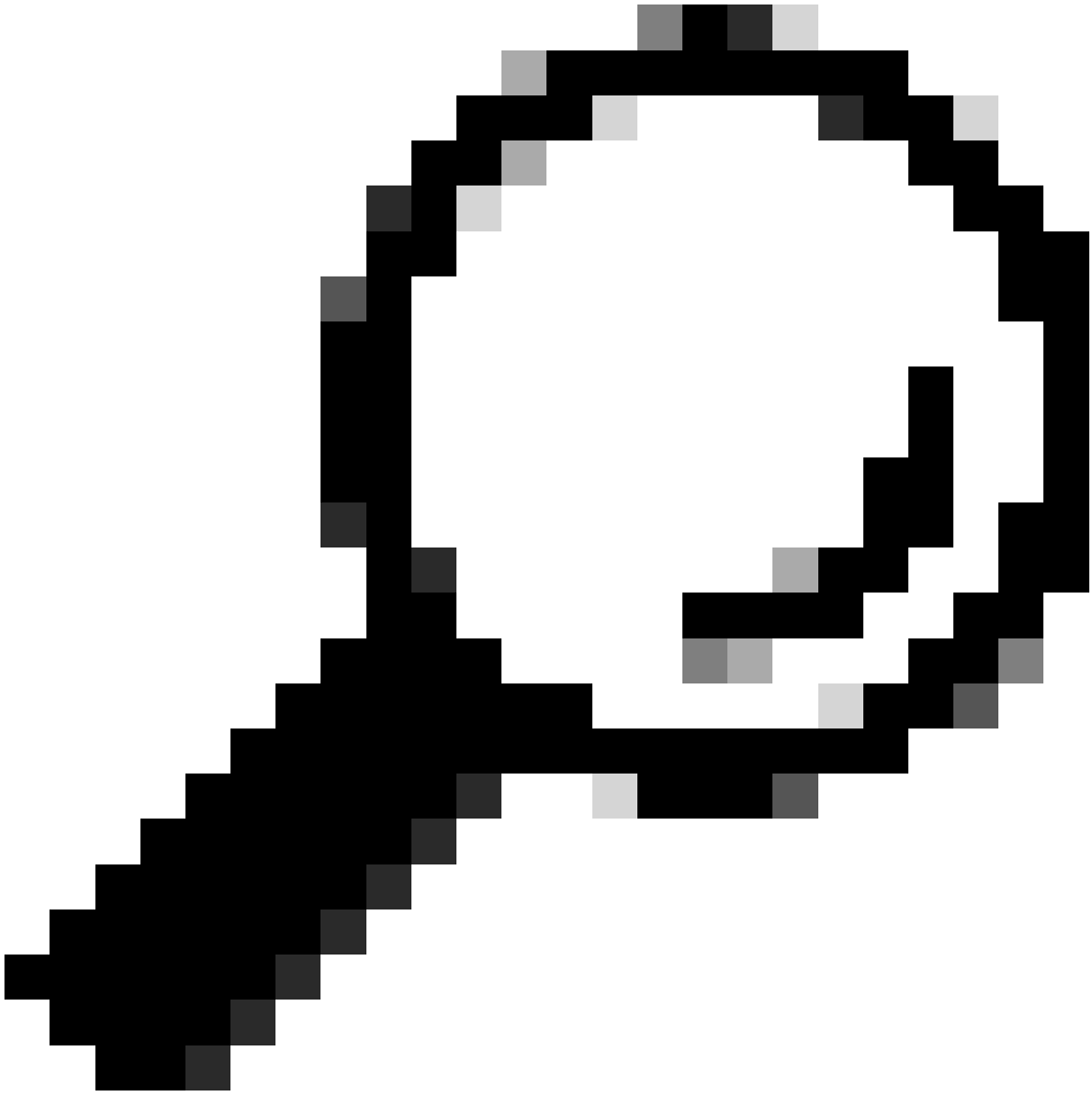
Exemple :
· Les utilisateurs du groupe AD Device Admin se voient attribuer le profil TACACS Admin NXOS.
· Les utilisateurs du groupe AD Device RO se voient attribuer le profil TACACS NXOS HelpDesk.



Configuration de Cisco NX-OS pour TACACS+ sur TLS



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.

Configuration du serveur TACACS+

Étape 1 : configuration initiale

```
POD2IPN2# sho run tacacs

feature tacacs+

tacacs-server host 10.225.253.209 key 7 "F1whg.123"
```

```
aaa group server tacacs+ tacacs2
  server 10.225.253.209
  use-vrf management
```

Configuration du point de confiance

Étape 1. Créez une étiquette de clé, dans votre cas, utilisez la paire de clés ecc.

<#root>

```
POD2IPN2(config)#
```

crypto key generate ecc label ec521-label exportable modulus 521

Étape 2. Associez-le à un point de confiance.

<#root>

```
POD2IPN2(config)#
```

crypto ca trustpoint ec521-tp

```
POD2IPN2(config-trustpoint)#
```

ecckeypair ec521-label

Étape 3 : installation de la clé publique CA.

<#root>

```
POD2IPN2(config)#
```

crypto ca authenticate ec521-tp

```
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
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
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKVOARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
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
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

```
Fingerprint(s): SHA1
Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

Do you accept this certificate? [yes/no]:yes
POD2IPN2(config)#
POD2IPN2(config)#
```

show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient
POD2IPN2(config)#
```

Étape 4. Générer une demande de certificat d’identité de commutateur.

<#root>

```
POD2IPN2(config)#
```

crypto ca enroll ec521-tp

```
 Create the certificate request ..
 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:C1sco.123
 The subject name in the certificate will be the name of the switch.
```

```
 Include the switch serial number in the subject name? [yes/no]:
```

yes

```
 The serial number in the certificate will be: FDO2649OP4T
 Include an IP address in the subject name [yes/no]:
```

yes

```
ip address:10.225.253.177
 Include the Alternate Subject Name ? [yes/no]:
```

no

```
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwwIUE9EMklQTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6LzpkOhPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q42OmCe8Mef+bqJBdJ9wzpyEjhI2lIIoXt4814nBxObkIWWyR5cZN
IiXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMklQTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/44lul
+3H1y52vn4Rm4CGU3wkzXU3qGO3YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt3OhpaDDOTWzzvZY7qFflCOl5p6pvUpHigqoZNg5
9xhNdM1CQSykOg==
-----END CERTIFICATE REQUEST-----
```

Étape 5. Importez le certificat d'identité du commutateur signé par l'autorité de certification.

<#root>

```
POD2IPN2(config)#
```

crypto ca import ec521-tp certificate

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA3MTkxMDAwWhcNMjYwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjYOOTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokFOn3DOn
ISOEjaUgihe3jzXicHE5uQhZbJHlxk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAcBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZO1PUXNTyZidXpGd/yTrdQAl5JzpW4pEudrbCJMZEEYtqoP
wD+4OE8vKoYEgyWlDrpRZOZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
liToeYy2Q0cTesSZCKvRBv6Ewj5JuSLemURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61LnlVxhXombiS6
INoa0GvQONrl+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MWtkK1wVO16Hv7vGpSMYonD6
a271im+tJPyKnnezQ6OykzlGqsL/Ta6JOdip/fEYp8UmRq9InDh23gDjqrojWL7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJTlnuk5KCqFx//4P7mAoyZYiTIDp1pkYS
```

```
VK65fJKD+pYxIhSP9wN8rnwtzSCWbOZ78sgOO6Y6wIXyTPOUB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
lfKuuebdZkbwz72r7OyyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

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

<#root>

```
POD2IPN2(config)#
```

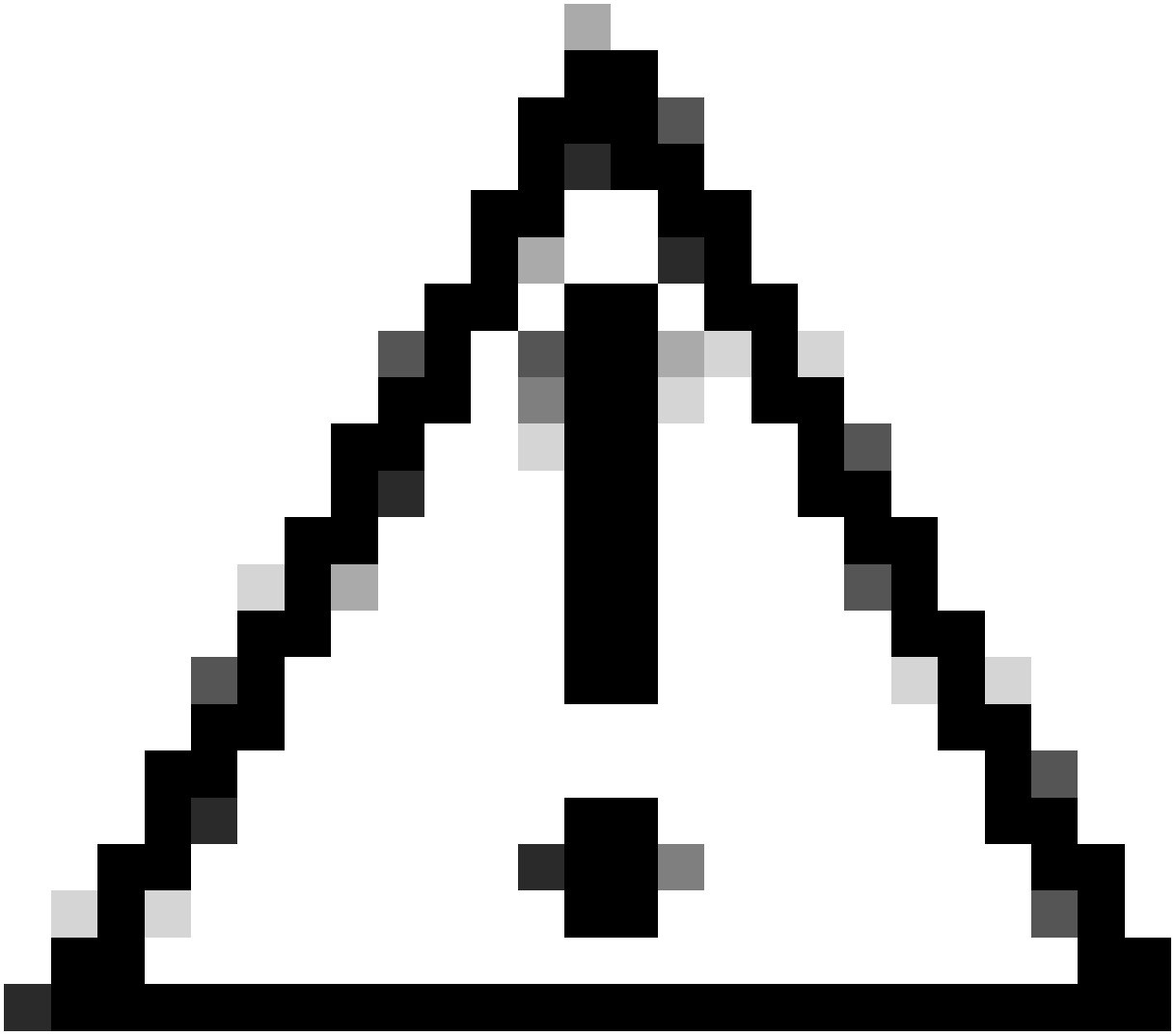
show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FDO26490P4T
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=0BACD2EFA5D80E6F
notBefore=May  7 19:10:00 2025 GMT
notAfter=May  7 19:10:00 2026 GMT
SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13
purposes: sslserver sslclient

CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient

POD2IPN2(config)#
```

Configuration de TACACS+ TLS



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

Étape 1 : configuration de tls tacacs globaux.

<#root>

```
POD2IPN2(config)#
```

tacacs-server secure tls

Étape 2. Remplacez le port ISE par le port TLS configuré avec le serveur ISE.

<#root>

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

Étape 3. Associez le serveur ISE configuré sur le commutateur au point d'approbation pour la connexion TLS.

<#root>

```
POD2IPN2(config)#
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

Étape 4 : création du groupe de serveurs tacacs.

<#root>

```
POD2IPN2(config)#
aaa group server tacacs+ tacacs2

POD2IPN2(config-tacacs+)#
server 10.225.253.209

POD2IPN2(config-tacacs+)#
use-vrf management
```

Étape 5 : vérification de la configuration

<#root>

```
POD2IPN2#
sho run tacacs

feature tacacs+

tacacs-server secure tls
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
aaa group server tacacs+ tacacs2
    server 10.225.253.209
    use-vrf management
```

Étape 6 : test de l'utilisateur distant avant de configurer l'authentification AAA

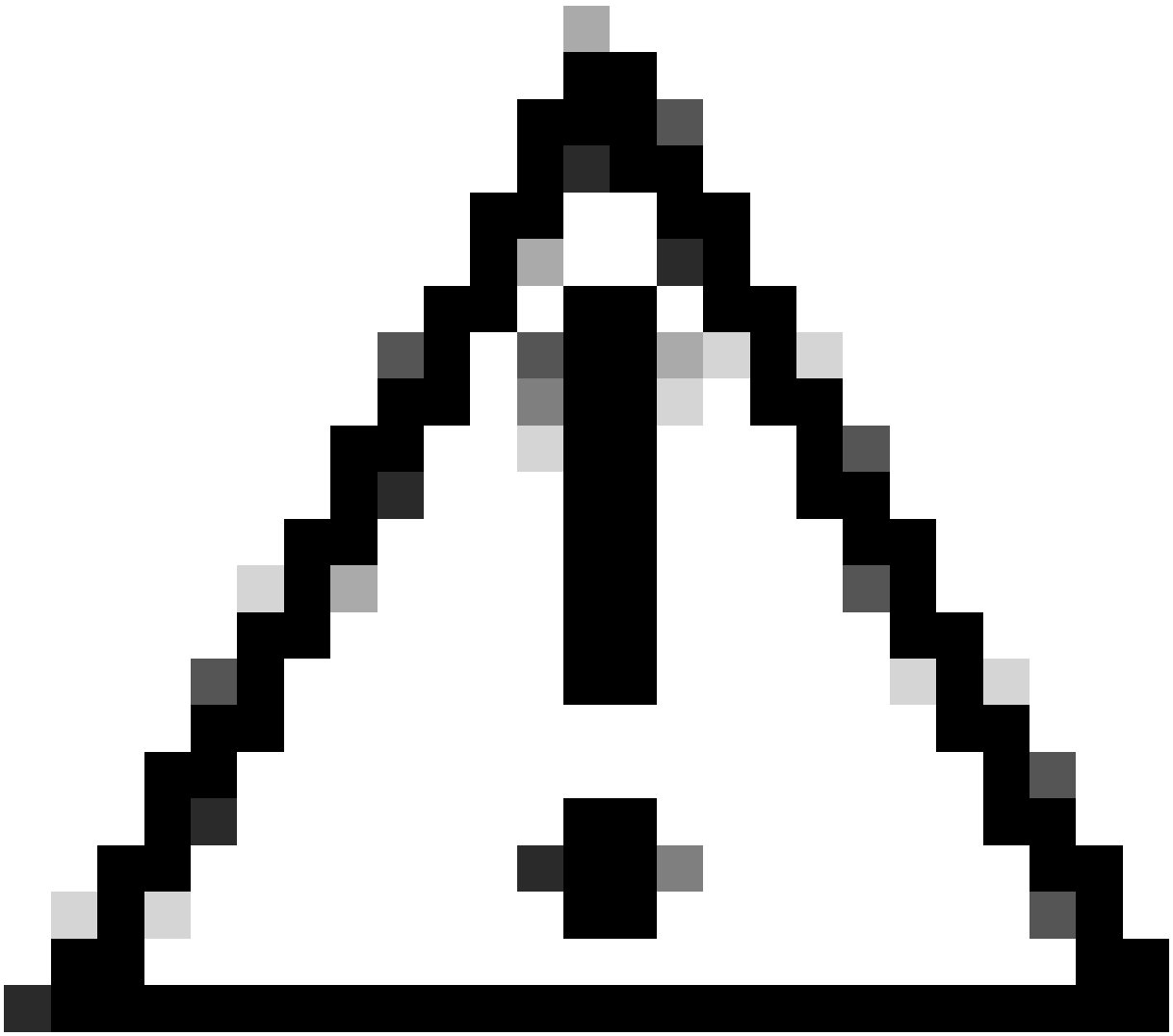
<#root>

POD2IPN2#

test aaa group tacacs2

user has been authenticated
POD2IPN2#

Configuration AAA



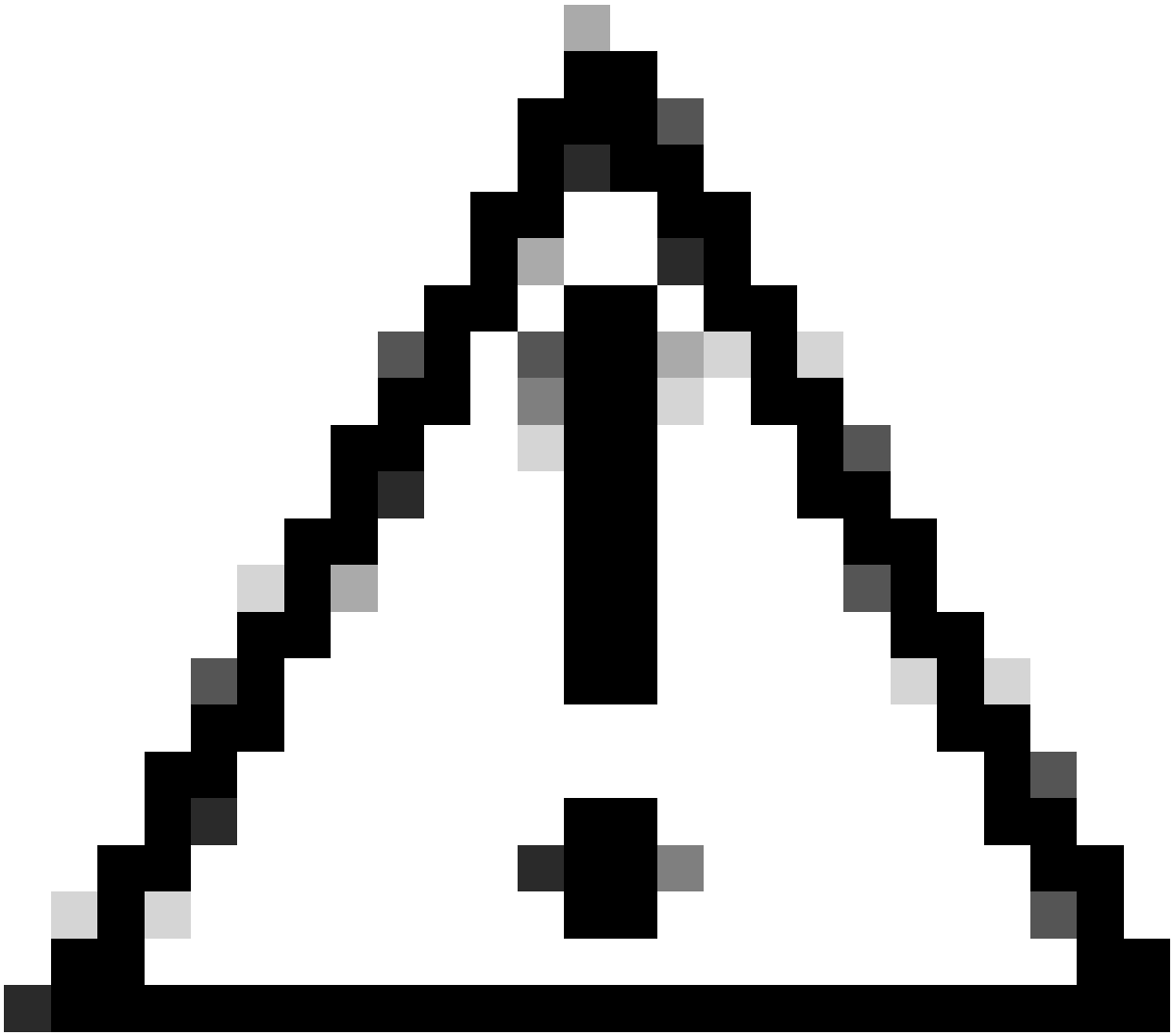
Mise en garde : Assurez-vous que l'authentification de l'utilisateur distant est réussie avant de poursuivre les configurations AAA.

Étape 1 : configuration de l’authentification à distance AAA.

<#root>

```
POD2IPN2(config)#
aaa authentication login default group tacacs2
```

Étape 2 : configuration de l’autorisation à distance AAA après le test de la commande



Mise en garde : Assurez-vous que vous voyez « authorization-status » sous la forme « AAA_AUTHOR_STATUS_PASS_ADD.

<#root>

POD2IPN2#

test aaa authorization command-type config-commands default user

command "feature bgp"

sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD)

Étape 3 : configuration de la commande AAA et de l'autorisation config-command

<#root>

POD2IPN2(config)#

aaa authorization config-commands default group tacacs2 local

POD2IPN2(config)#

aaa authorization commands default group tacacs2 local

Test et dépannage de l'accès utilisateur pour NX-OS

Vérification

La configuration de l'administration des périphériques pour Cisco NX-OS est terminée. Vous devez valider la configuration.

Étape 1 : connexion SSH et connexion aux périphériques NX-OS sous différents rôles

Étape 2. Une fois sur l'interface de ligne de commande (CLI) du périphérique, vérifiez que l'utilisateur a accès aux bonnes commandes. Par exemple, un utilisateur du centre d'assistance doit pouvoir envoyer une requête ping à une adresse IP normale (par exemple, 10.225.253.129), mais ne peut pas afficher la configuration en cours.

```
POD2IPN1# ping 10.225.253.129 vrf management
PING 10.225.253.129 (10.225.253.129): 56 data bytes
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms
```

```
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms

--- 10.225.253.129 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.638/0.692/0.817 ms
POD2IPN1#
POD2IPN1# show running-config
% Permission denied for the role
```

Dépannage

Validation de la configuration NX-OS.

```
POD2IPN2# show crypto ca certificates
POD2IPN2# show crypto ca trustpoints
POD2IPN2# show tacacs-server statistics <server ip>
```

Pour afficher les connexions et les rôles des utilisateurs, utilisez ces commandes.

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
NAME LINE TIME IDLE PID COMMENT
Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh *
POD2IPN1# show user-account Admin-ro
user:Admin-ro
roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

Voici des débogages utiles pour le dépannage de TACACS+ :

```
debug TACACS+ aaa-request
2016 Jan 11 03:03:08.652514 TACACS[6288]:  process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]:  process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]:  process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]:  process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]:  state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]:  is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]:  is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]:  debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]:  35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]:  36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]:  36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 TACACS[6288]:  debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]:  tplus_encrypt(659):key is configured for this aaa sessin.
```

```
2016 Jan 11 03:03:08.655054 TACACS[6288]:  num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]:  non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 TACACS[6288]:  non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]:  non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 TACACS[6288]:  non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]:  tplus_decode_authen_response: copying hostname into context
```

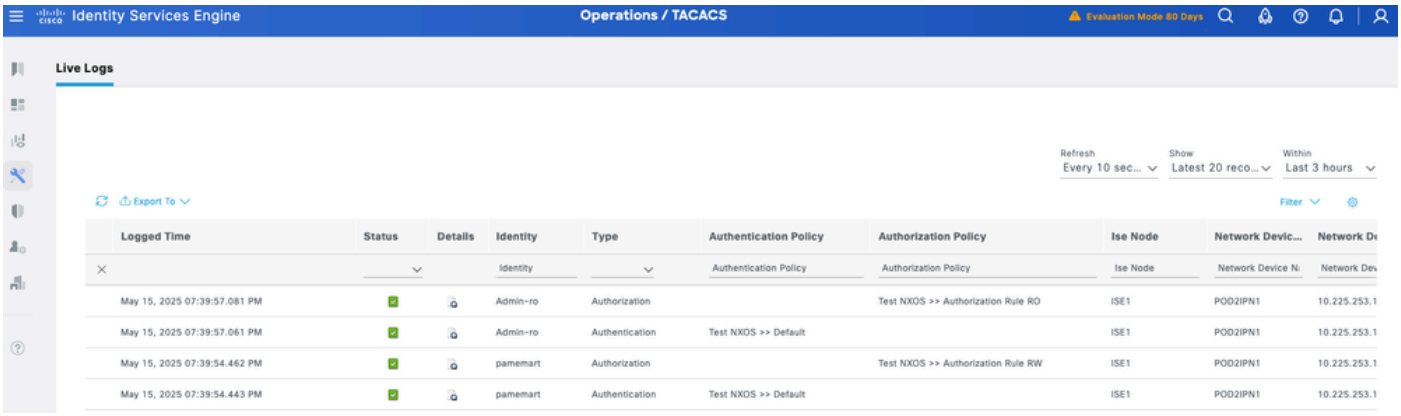
Activez le débogage SSL.

```
touch '/bootflash/.enable_ssl_debugs'
```

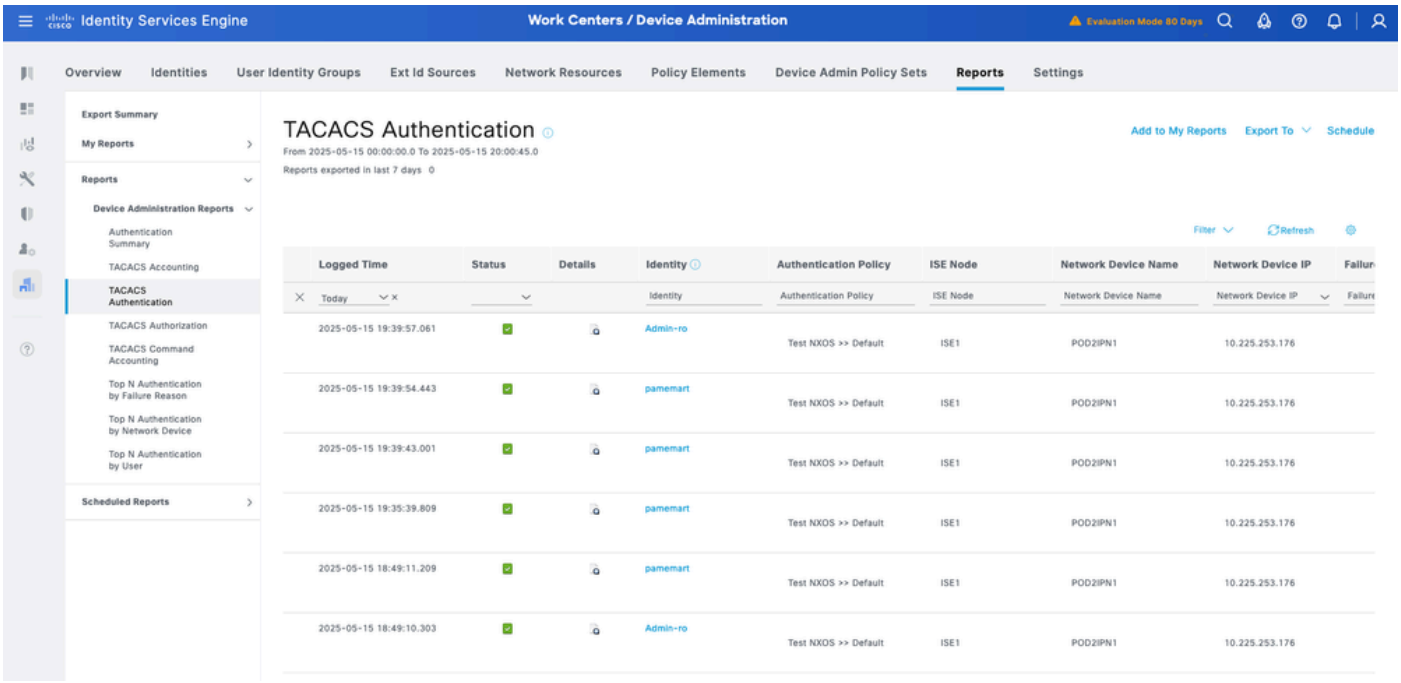
Afficher le contenu du fichier de débogage.

```
cat /tmp/ssl_wrapper.log.*
```

Dans l'interface utilisateur graphique d'ISE, accédez à Operations > TACACS Livellog. Toutes les demandes d'authentification et d'autorisation TACACS sont capturées ici, et le bouton Détails fournit des informations détaillées sur la raison pour laquelle une transaction particulière a réussi/échoué.



Pour les rapports historiques : Accédez à Work Centers > Device Administration > Reports > Device Administration pour obtenir les rapports d'authentification, d'autorisation et de comptabilité.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 80 Days
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Export Summary
My Reports
Reports
Device Administration Reports
Authentication Summary
TACACS Accounting
TACACS Authentication
TACACS Authorization
TACACS Command Accounting
Top N Authentication by Failure Reason
Top N Authentication by Network Device
Top N Authentication by User
Scheduled Reports
TACACS Authentication
From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0
Reports exported in last 7 days 0
Add to My Reports
Export To
Schedule
Filter
Refresh
Logged Time
Status
Details
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
Today
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
2025-05-15 19:39:57.061
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:54.443
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:43.001
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:35:39.809
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:11.209
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:10.303
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176

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.