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

Table des matières

- Introduction
- Aperçu
  - Utilisation de ce guide
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Licences
- Partie 1 : configuration d'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
  - Création de périphériques réseau et de groupes de périphériques réseau
  - Configurer les magasins d'identités
  - Configurer les profils TACACS+
    - IOS XE_RW - Profil d'administrateur
    - IOS XE_RO - Profil d'opérateur
  - Configurer les jeux de commandes TACACS+
    - CISCO_IOS XE_RW - Ensemble de commandes de l'administrateur
    - CISCO_IOS XE_RO - Jeu de commandes opérateur
  - Configurer les ensembles de stratégies d'administration des périphériques
- Partie 2 : configuration de CiscoIOS XE pour TACACS+ sur TLS 1.3
- Méthode de configuration 1 - Paire de clés générée par le périphérique
  - Configuration du serveur TACACS+
  - Configuration du point de confiance
  - TACACS et AAA avec configuration TLS
- Méthode de configuration 2 - Paire de clés générée par CA
  - TACACS et AAA avec configuration TLS
- Vérification

Introduction

Ce document décrit un exemple pour TACACS+ sur TLS avec Cisco Identity Services Engine (ISE) comme serveur et un périphérique Cisco IOS® XE 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 XE.
· Partie 1 : configuration d'ISE pour l'administration des périphériques
· Partie 2 : configuration de Cisco IOS XE 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
- Logiciel Cisco IOS XE, version 17.18.1+

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.

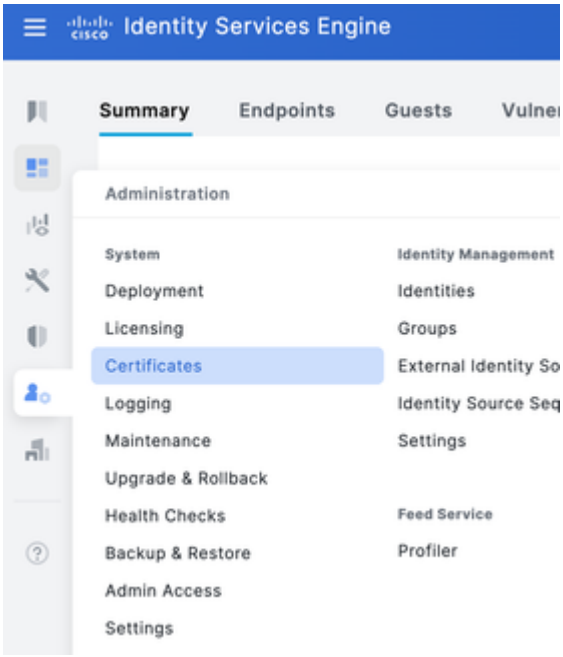
Partie 1 : configuration d'ISE pour l'administration des périphériques

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.



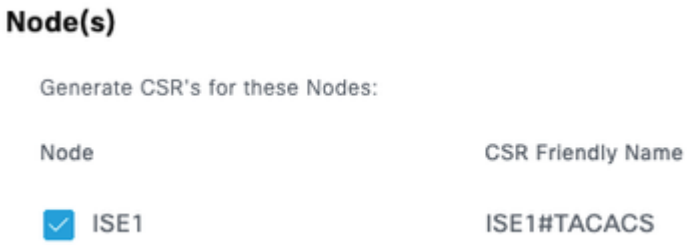
Étape 3. Sous Certificate Signing Requests, cliquez sur Generate Certificate Signing Request.



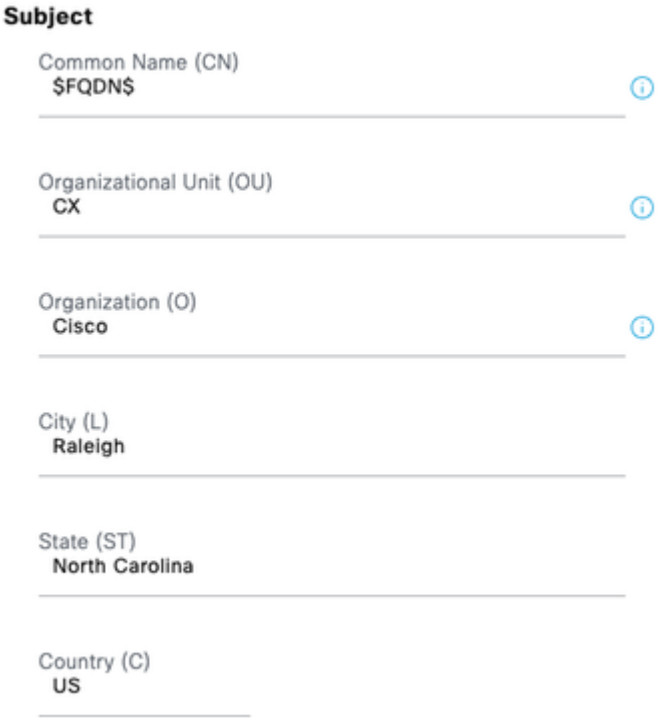
Étape 4. Sélectionnez TACACS dans Utilisation.



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



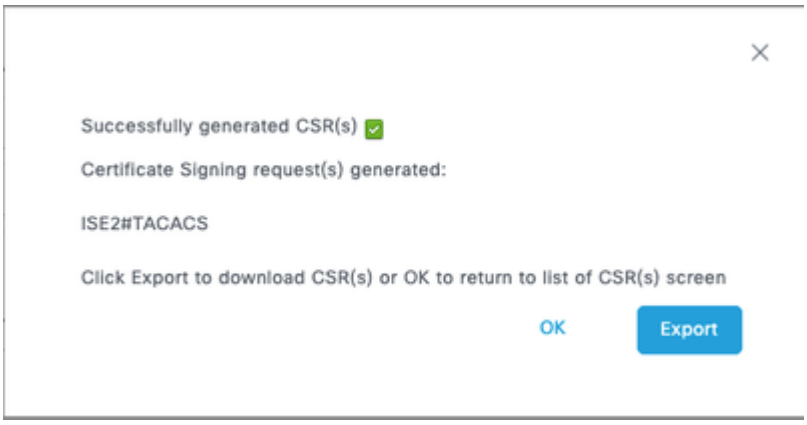
Étape 6. Remplissez les champs Subject avec les informations appropriées.



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



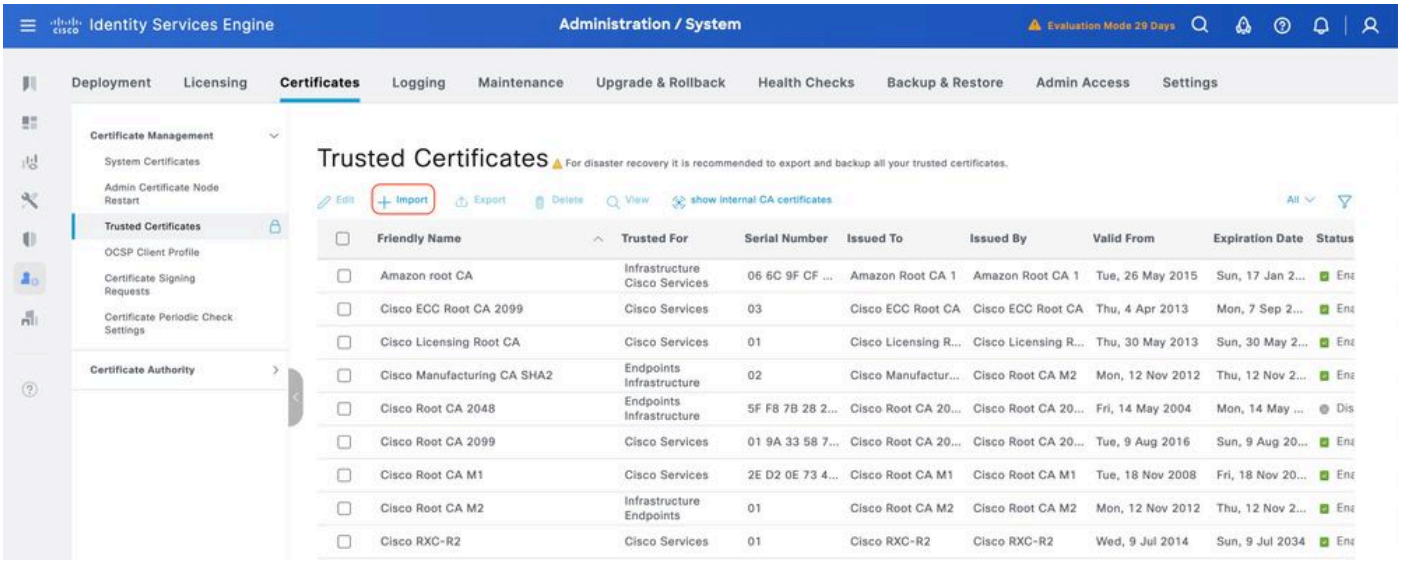
Étape 8. Cliquez sur Generate, puis sur Export.



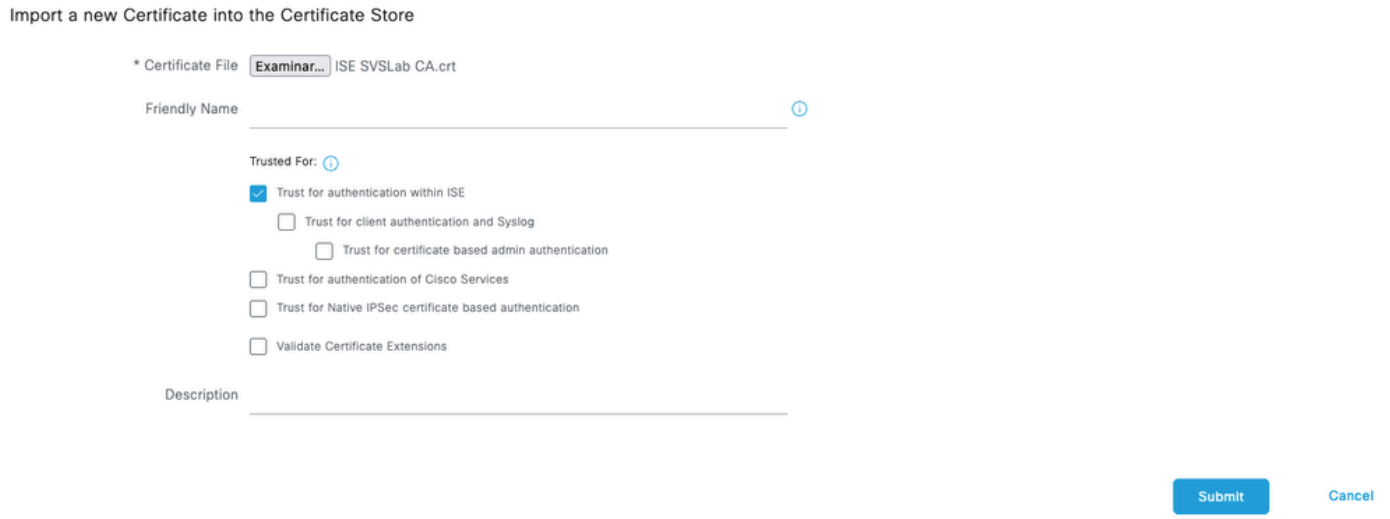
Vous pouvez maintenant faire signer le certificat (CRT) par votre autorité de certification (CA).

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

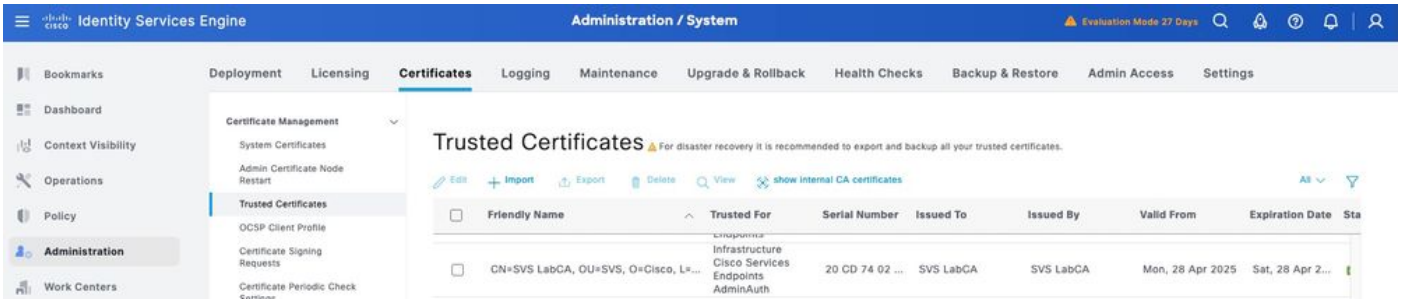
Étape 1. Accédez à Administration > System > Certificates. Sous Certificats approuvés, cliquez sur Importer.



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 leConfiance pour l'authentification dans ISE est activée.



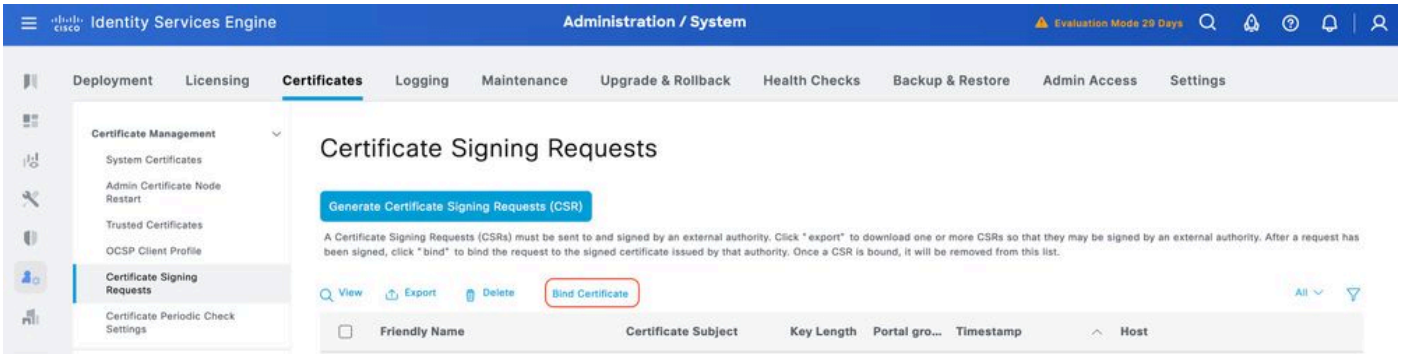
Étape 3. Cliquez sur Submit. Le certificat doit maintenant apparaître sous Trusted Certificates.



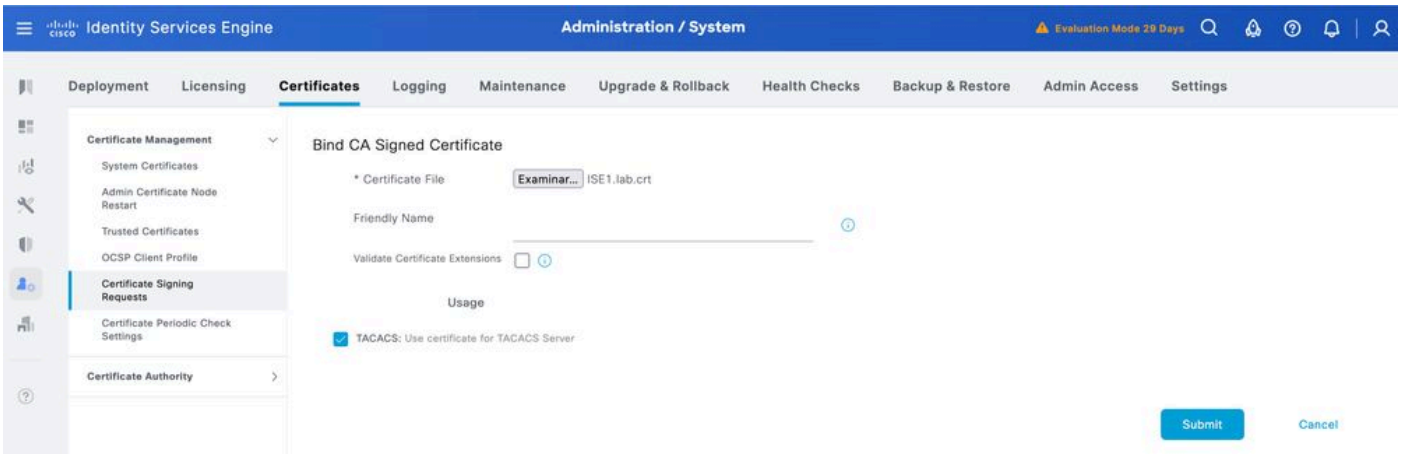
Lier la demande de signature de certificat signé (CSR) à ISE

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.



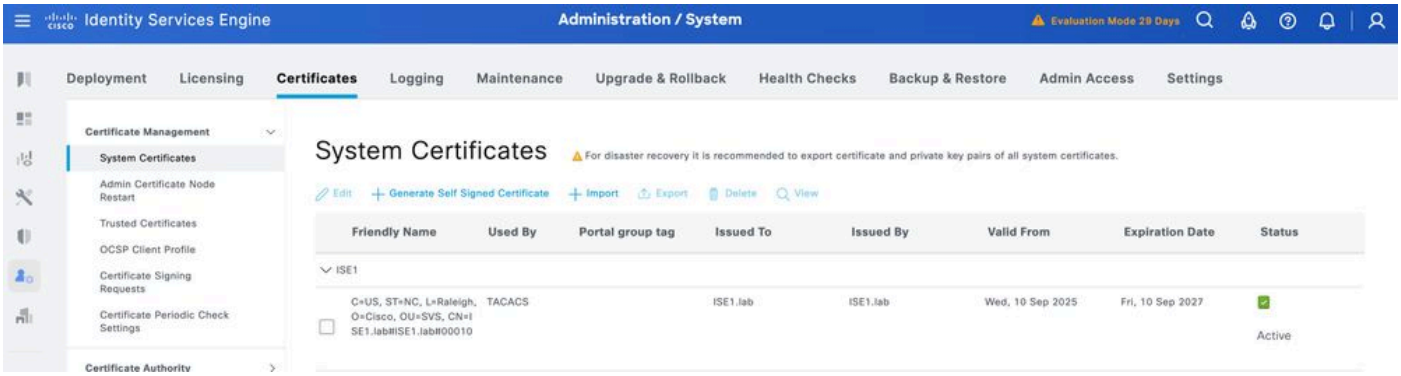
Étape 2. Sélectionnez le certificat signé et assurez-vous que la case à cocher TACACS sous Usage reste sélectionnée.



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



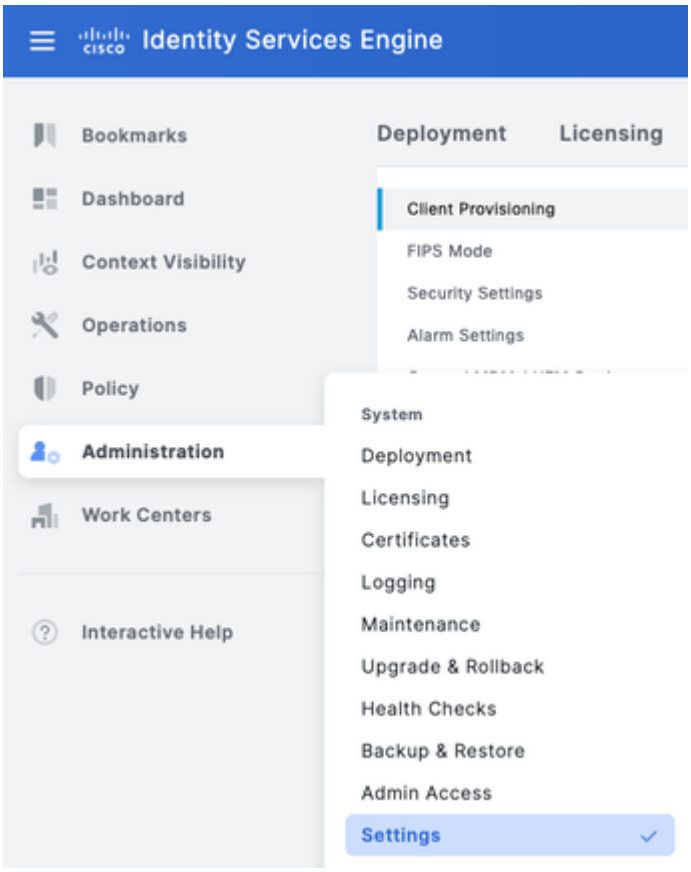
Le certificat doit maintenant être correctement installé. Vous pouvez le vérifier sous Certificats système.



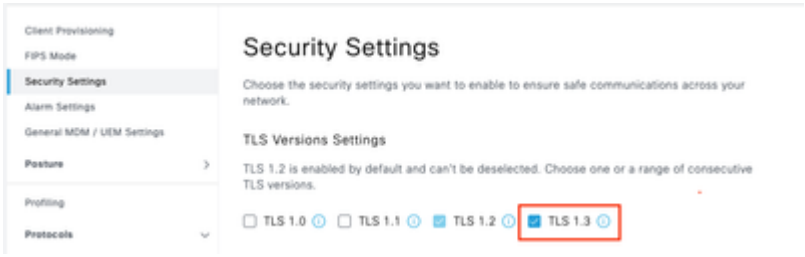
Activer TLS 1.3

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.

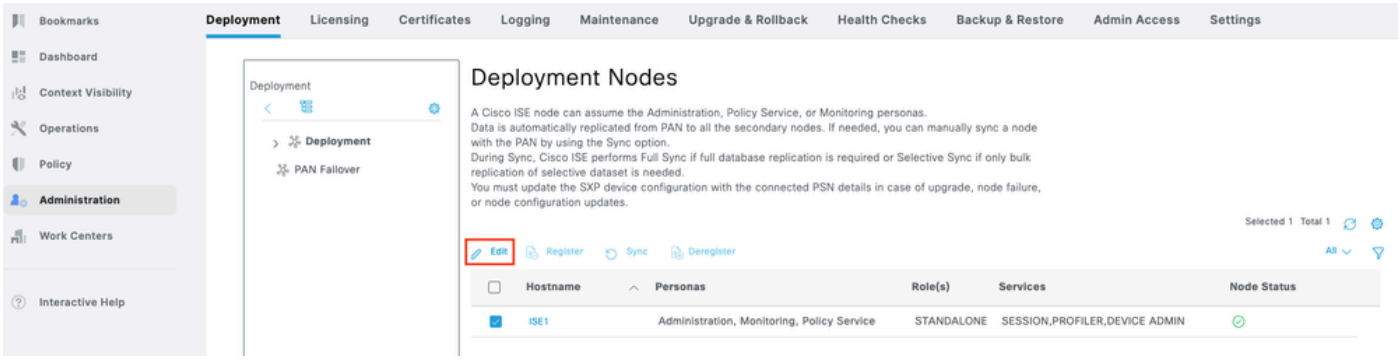


Avertissement : Lorsque vous modifiez la version TLS, le serveur d'applications Cisco ISE redémarre sur toutes les machines de déploiement Cisco ISE.

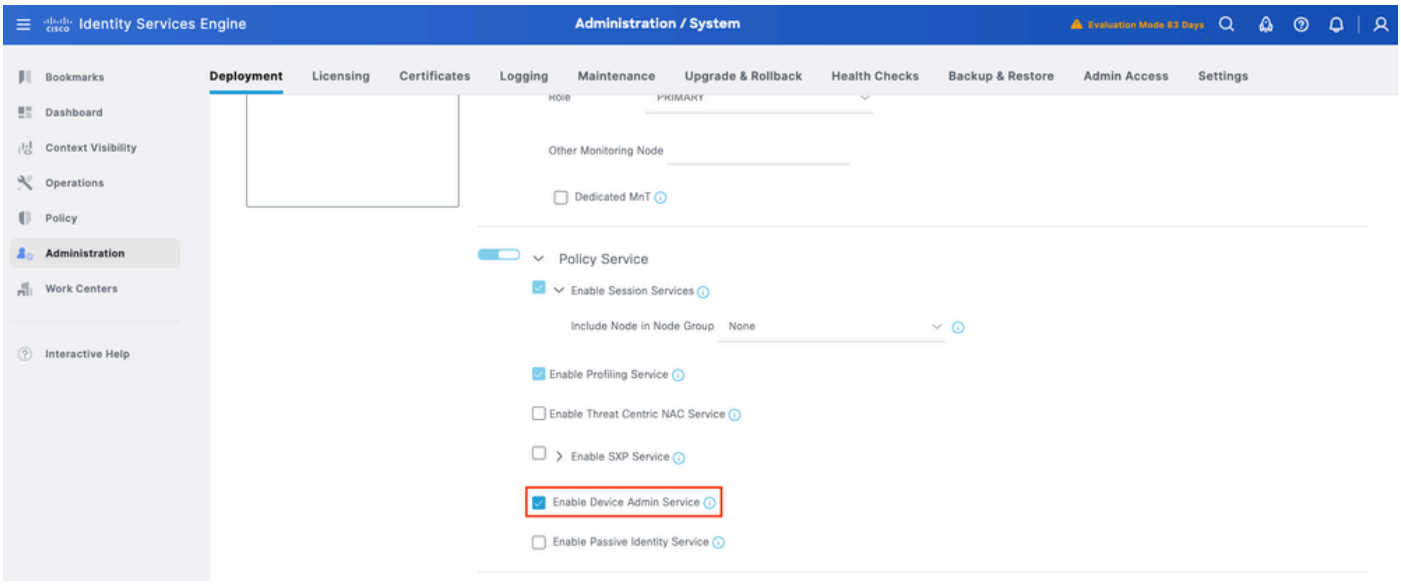
Activer l'administration des périphériques sur ISE

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. Cochez la case en regard du noeud ISE et cliquez sur Modifier.



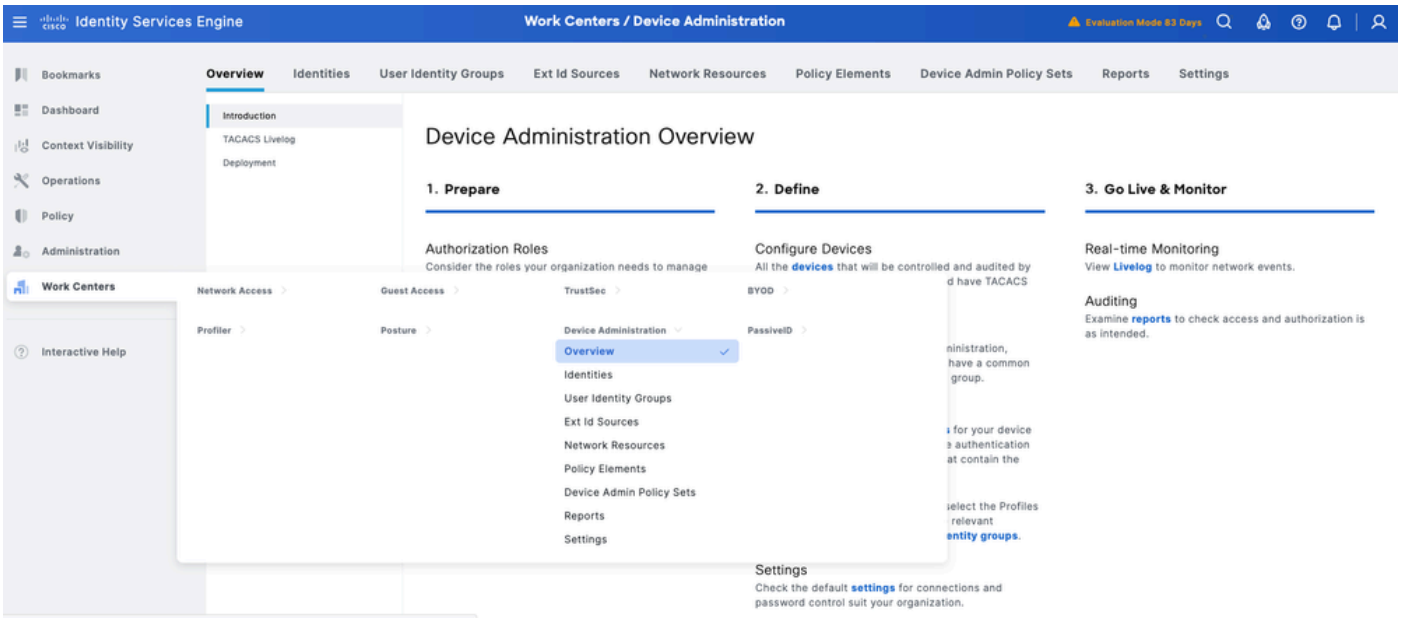
Étape 2.Sous GeneralSettings, faites défiler la page vers le bas et activez la case à cocher en regard de Enable Device Admin Service.



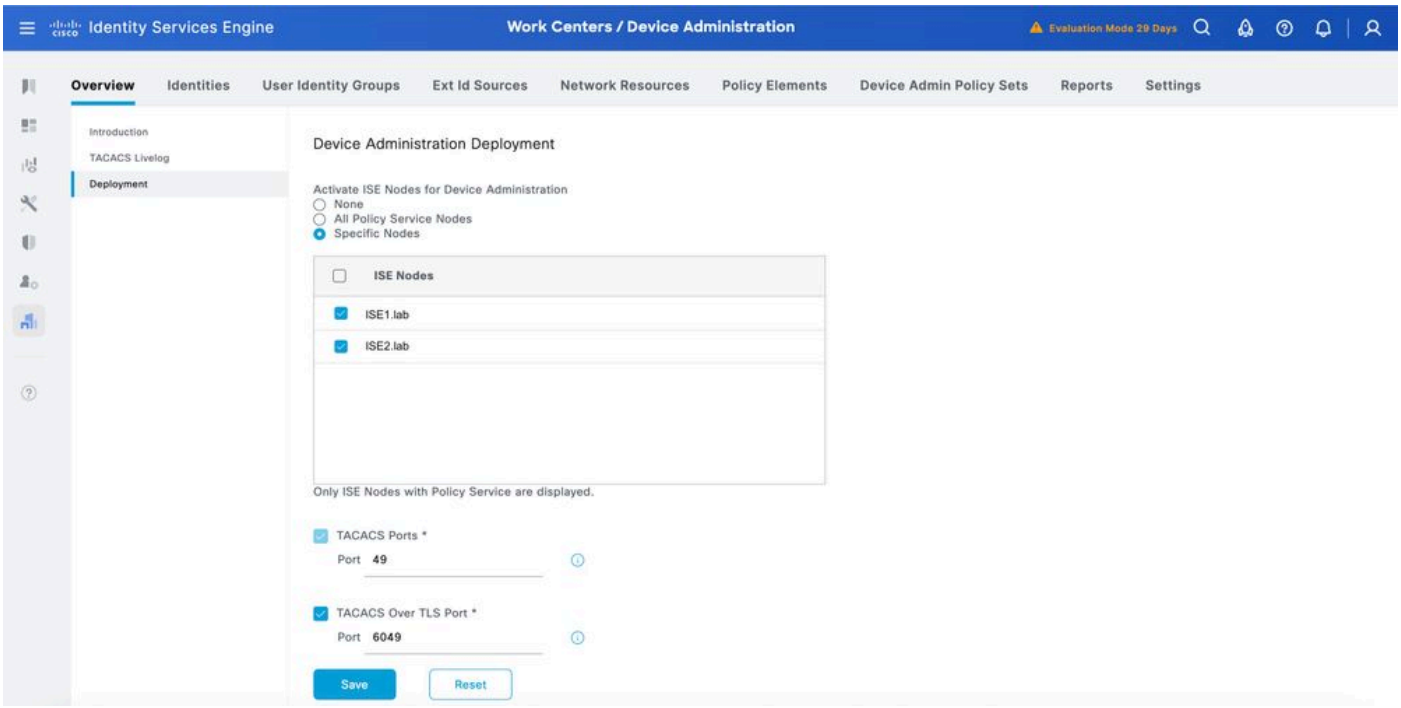
Étape 3 : enregistrement de la configuration Le service d'administration des périphériques est désormais activé sur ISE.

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.

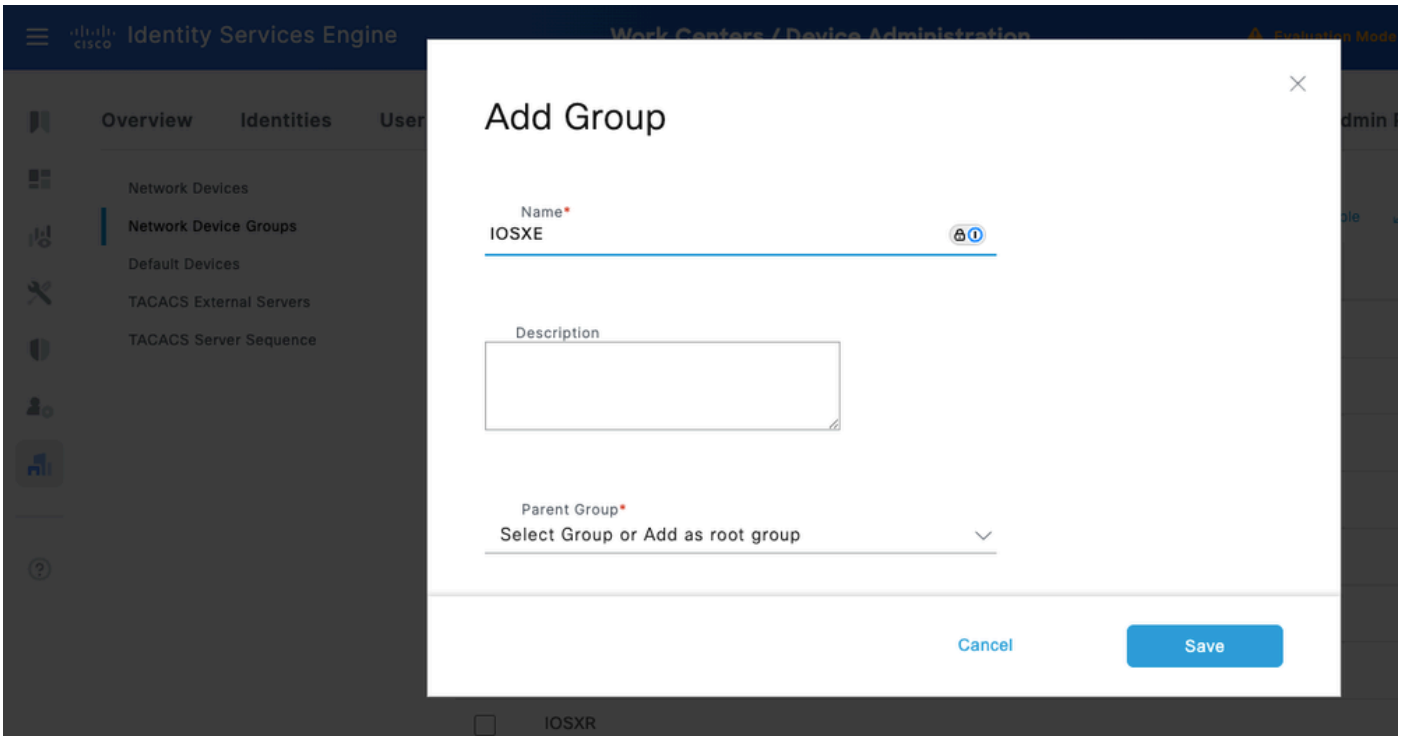


Étape 3.Conservez le port par défaut 6049 ou spécifiez un autre port TCP pour TACACS sur TLS, puis cliquez sur Save.

Création de périphériques réseau et de groupes de périphériques réseau

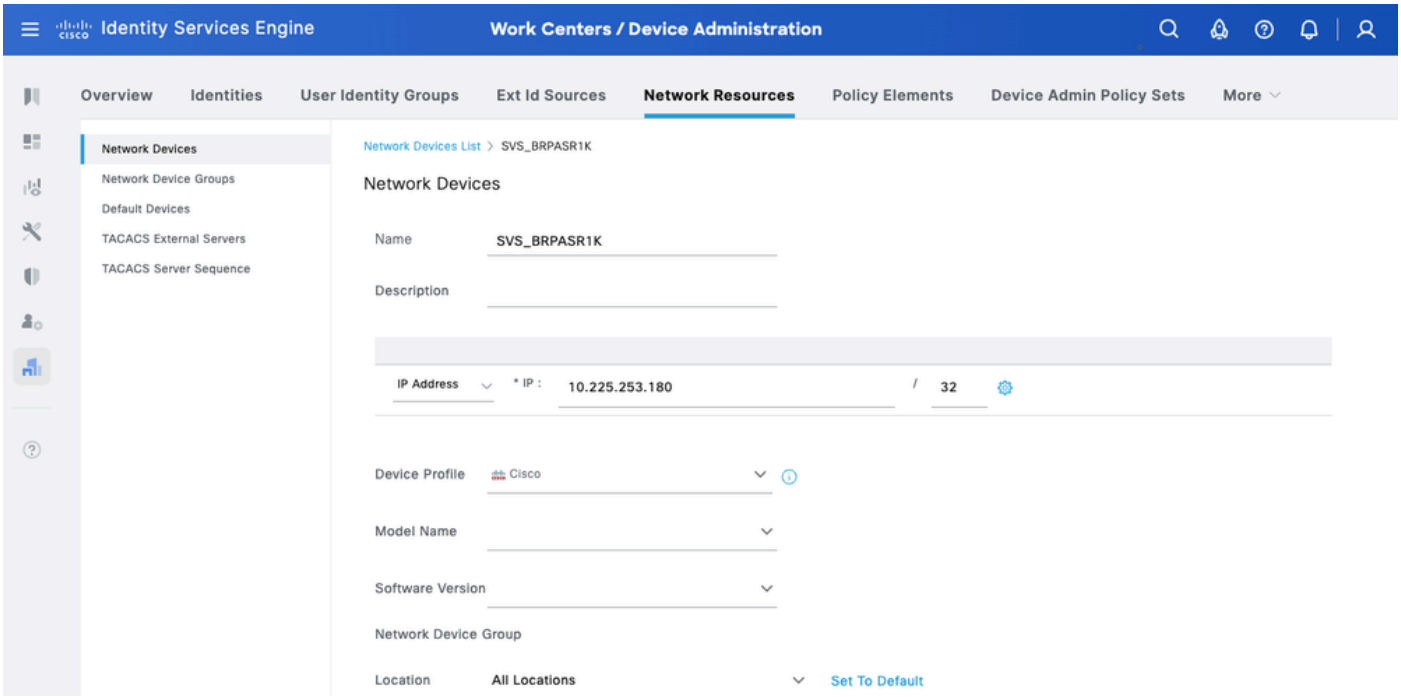
ISE fournit un regroupement de périphériques puissant avec plusieurs hiérarchies de groupes de périphériques. Chaque hiérarchie représente une classification distincte et indépendante des périphériques réseau.

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

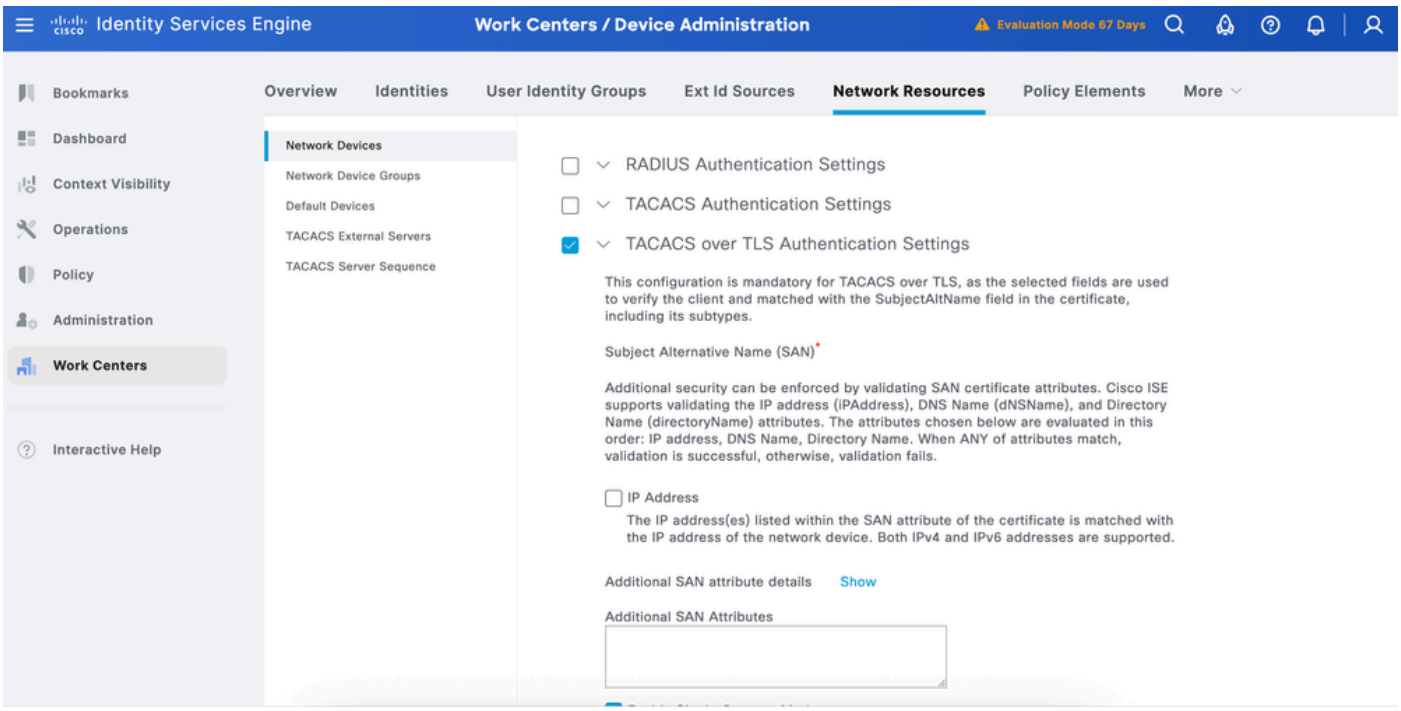


Conseil : Tous les types de périphériques et tous les emplacements sont des hiérarchies par défaut fournies par ISE. Vous pouvez ajouter vos propres hiérarchies et définir les différents composants pour identifier un périphérique réseau qui pourra être utilisé ultérieurement dans la condition de stratégie

Étape 2. Ajoutez à présent un périphérique Cisco IOS XE en tant que périphérique réseau. Accédez à Work Centers > Device Administration > Network Resources > Network Devices. Cliquez sur Add pour ajouter un nouveau périphérique réseau. Pour ce test, il s'agit de SVS_BRPASR1K.



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

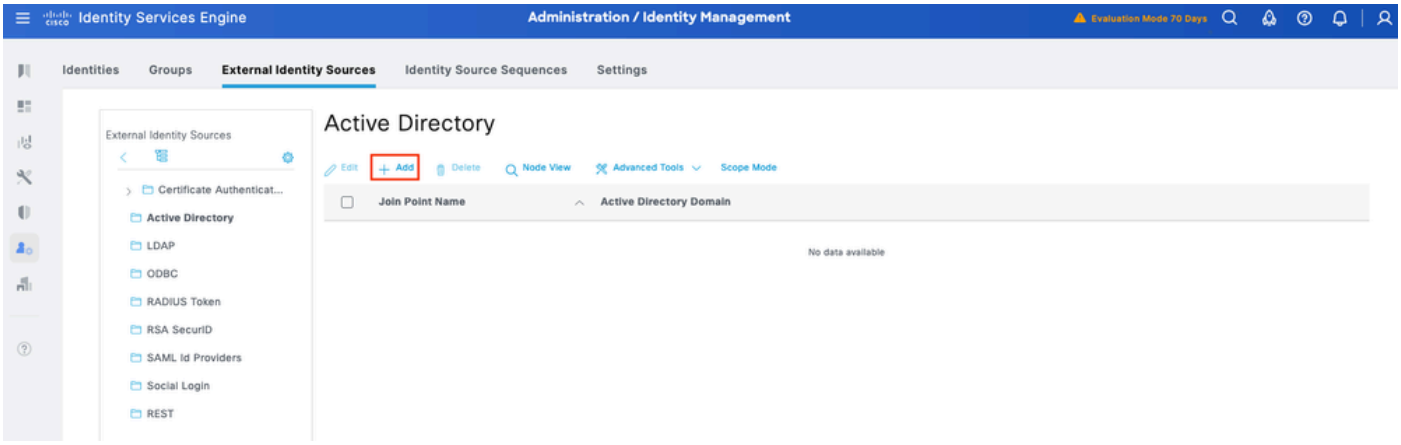


Conseil : Il est recommandé d'activer le mode de connexion unique pour éviter de redémarrer la session TCP chaque fois qu'une commande est envoyée au périphérique.

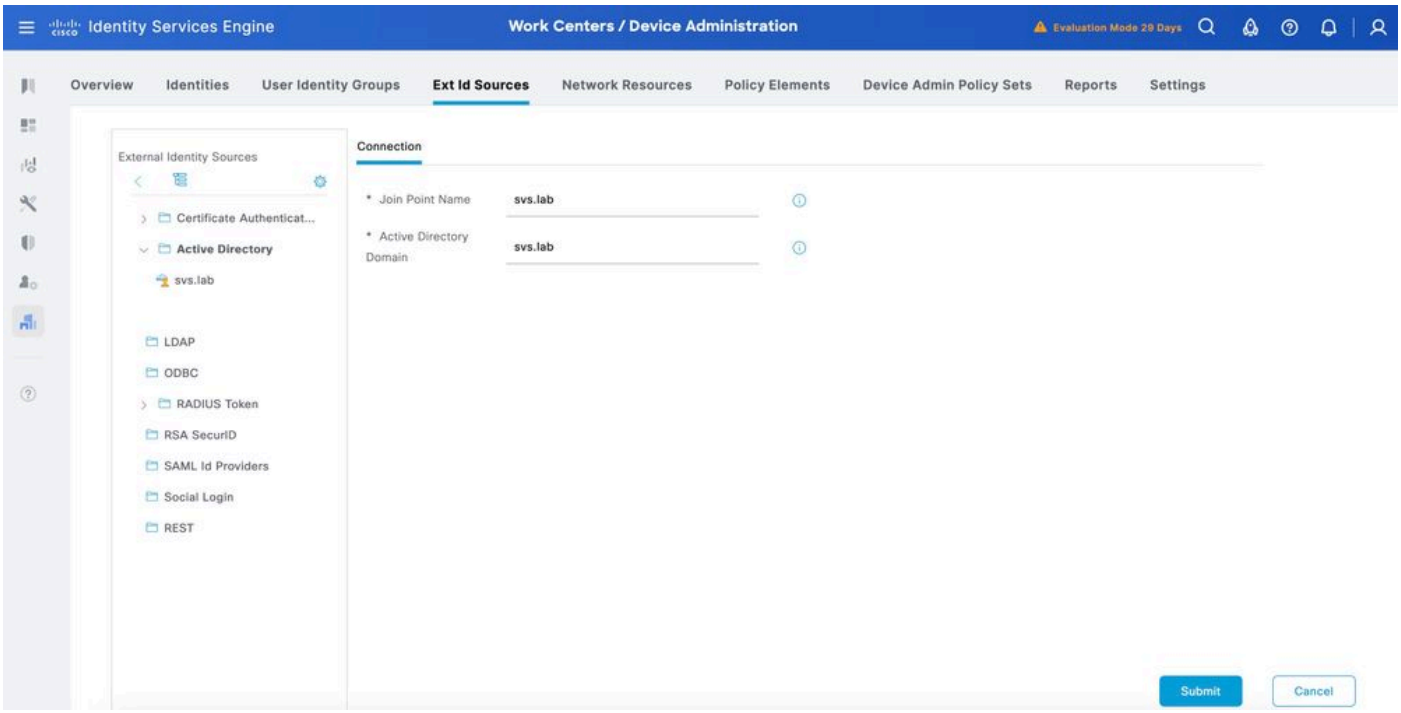
Configurer les magasins d'identités

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.

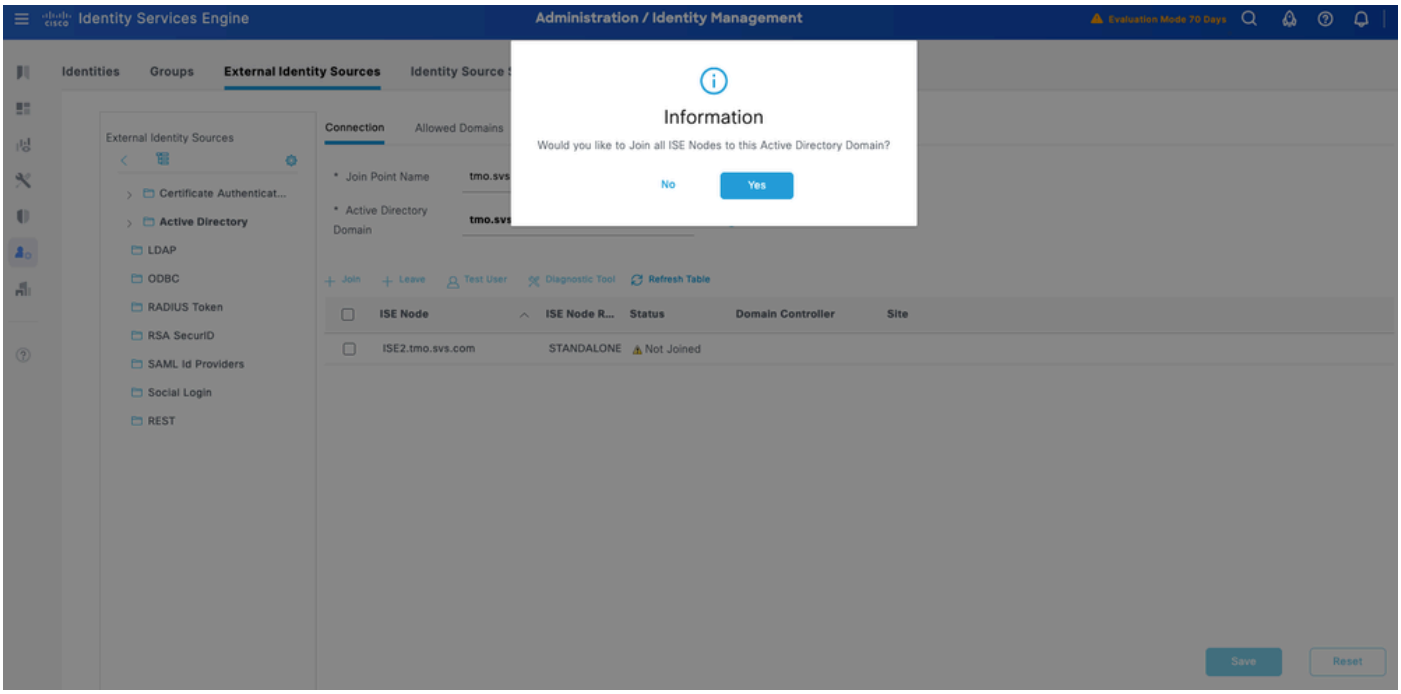
Étape 1. Accédez à Administration > Identity Management > External Identity Stores > Active Directory. Cliquez sur Add pour définir un nouveau point de jonction AD.



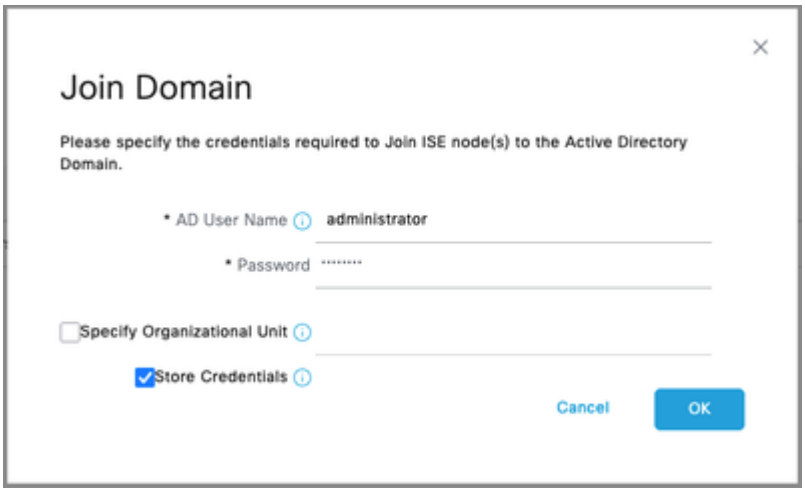
Étape 2. Spécifiez le nom du point de jonction et le nom de domaine AD, puis cliquez sur Submit.

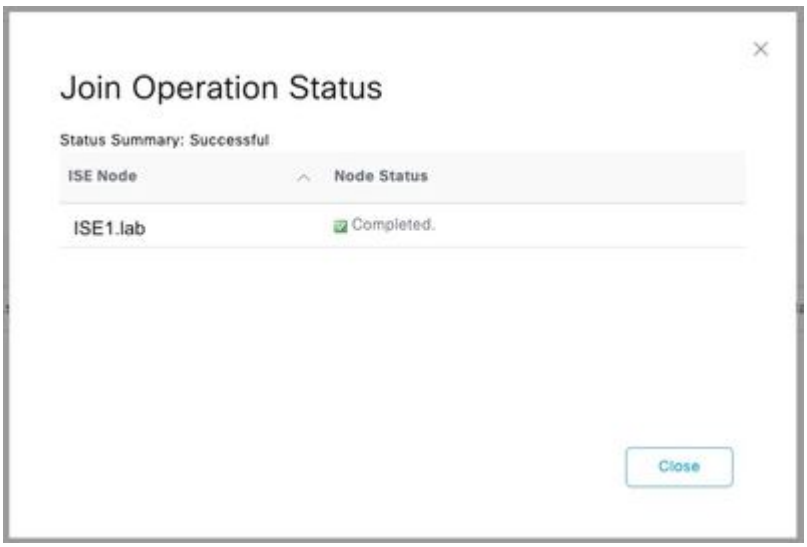


Étape 3. Cliquez sur Yes lorsque vous y êtes invité. Voulez-vous joindre tous les noeuds ISE à ce domaine Active Directory ?

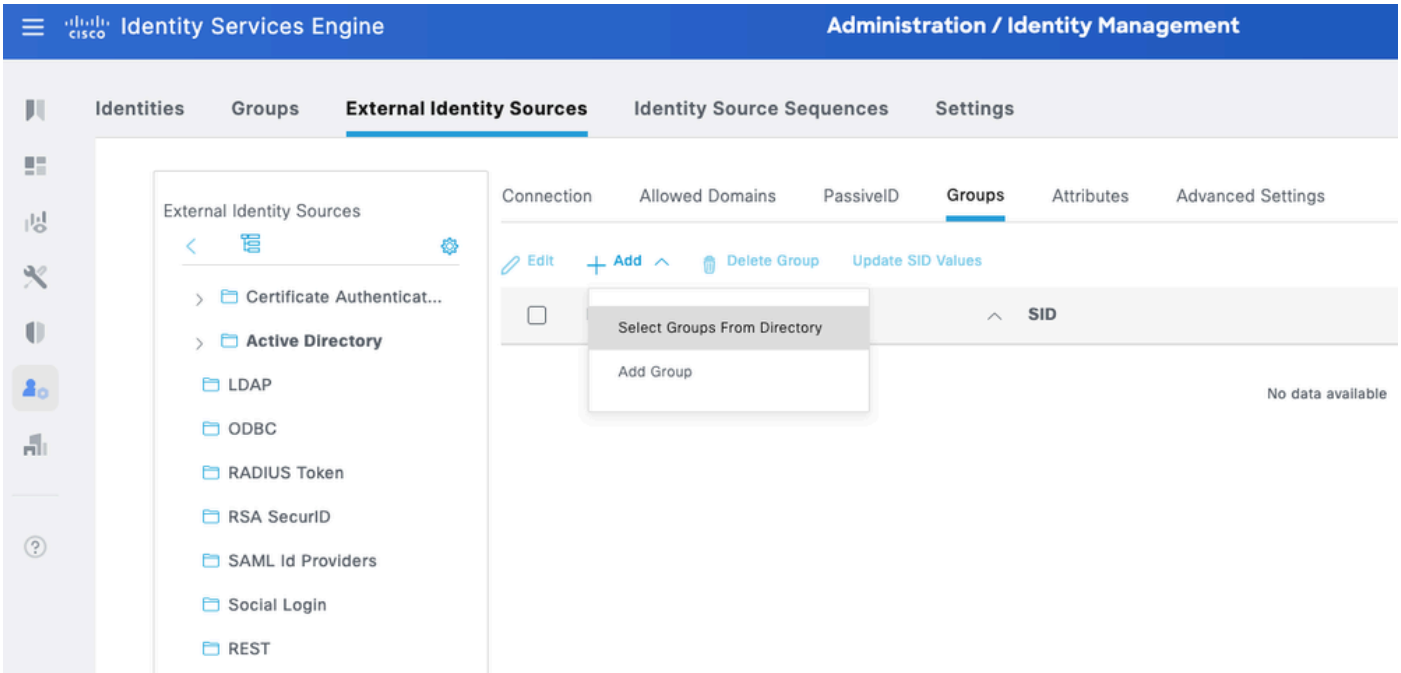


Étape 4. Entrez les informations d'identification avec les privilèges de jointure AD et Joignez ISE à AD. Vérifiez l'état pour vous assurer qu'il est opérationnel.

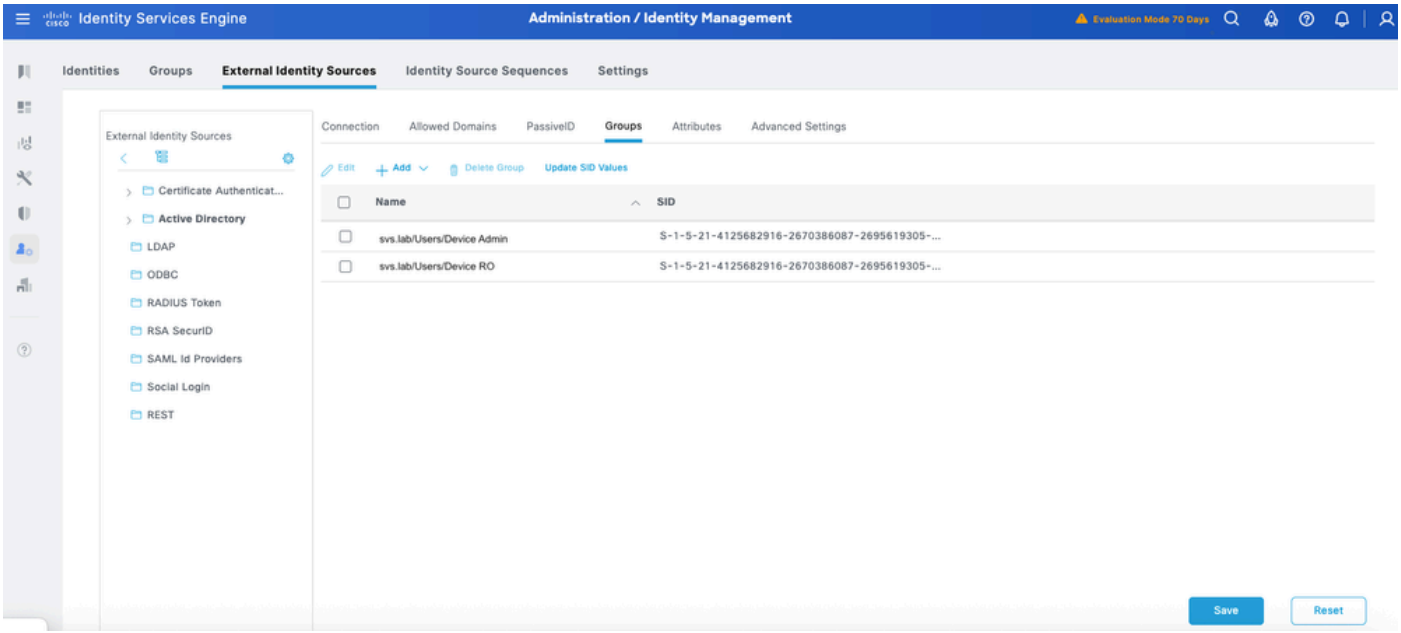




Étape 5. Accédez à l'onglet Groups, et cliquez sur Add pour obtenir tous les groupes nécessaires en fonction des utilisateurs autorisés à accéder au périphérique. Cet exemple montre les groupes utilisés dans la stratégie d'autorisation de ce guide







Configurer les profils TACACS+

Vous allez mapper les profils TACACS+ aux deux rôles d'utilisateur principaux sur les périphériques Cisco IOS XE :

- 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.

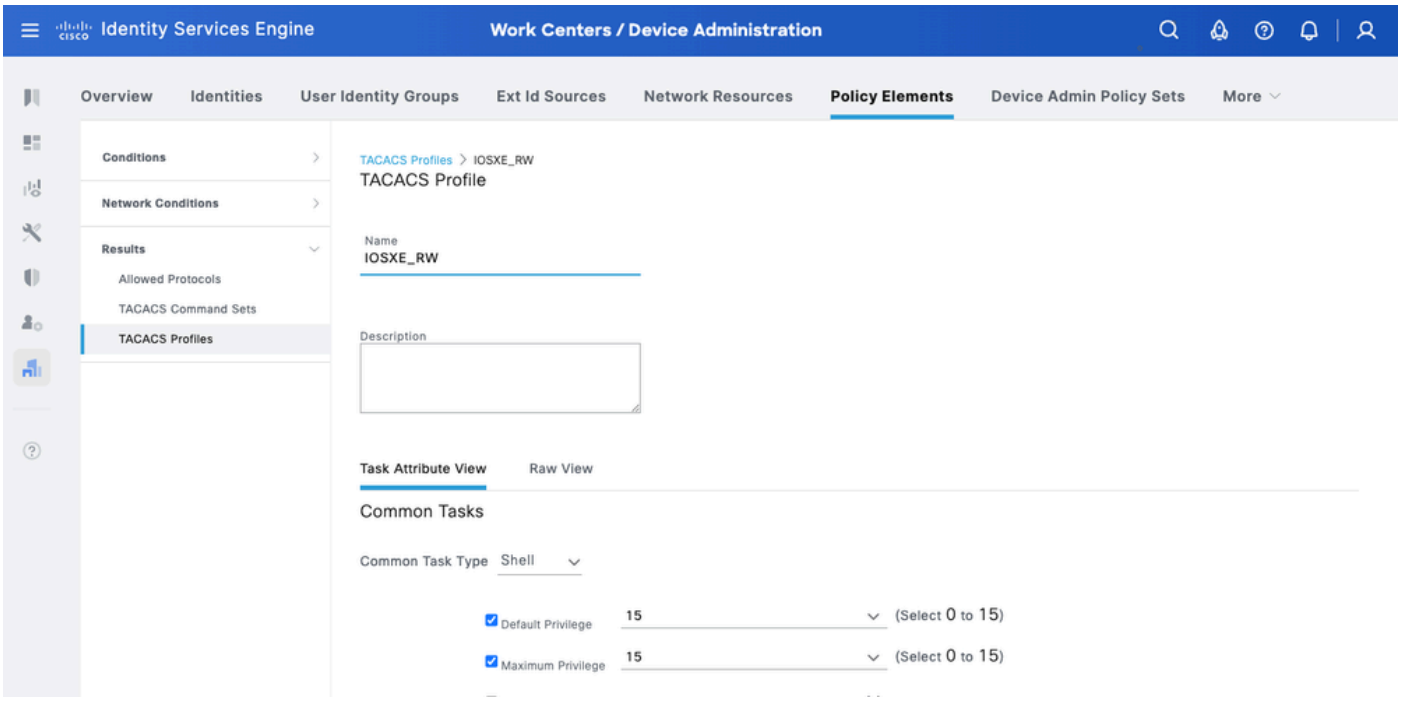
Il s'agit de deux profils TACACS+ : IOS XE_RW et IOSXR_RO.

IOS XE_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 IOS XE_RW.

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

Étape 3 : confirmation de la configuration et enregistrement.

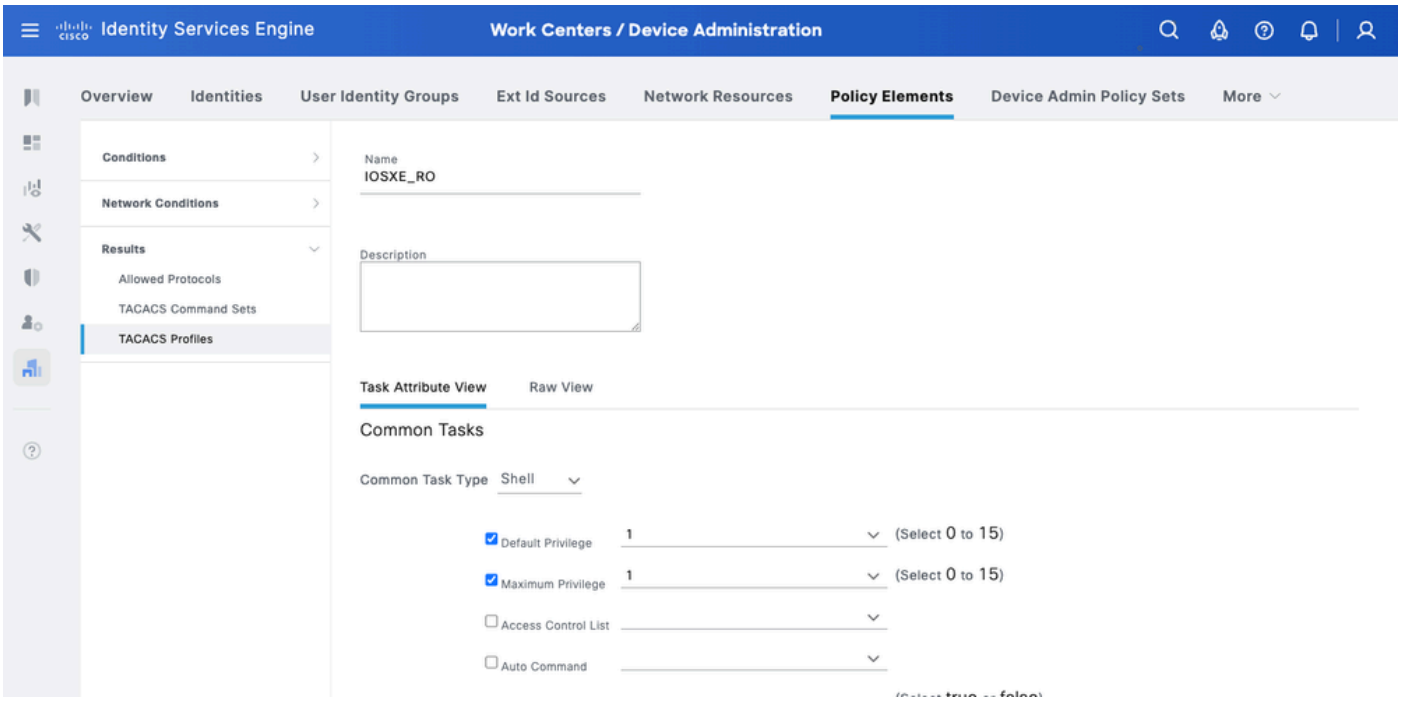


IOS XE_RO - Profil d'opérateur

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

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

Étape 3 : confirmation de la configuration et enregistrement.



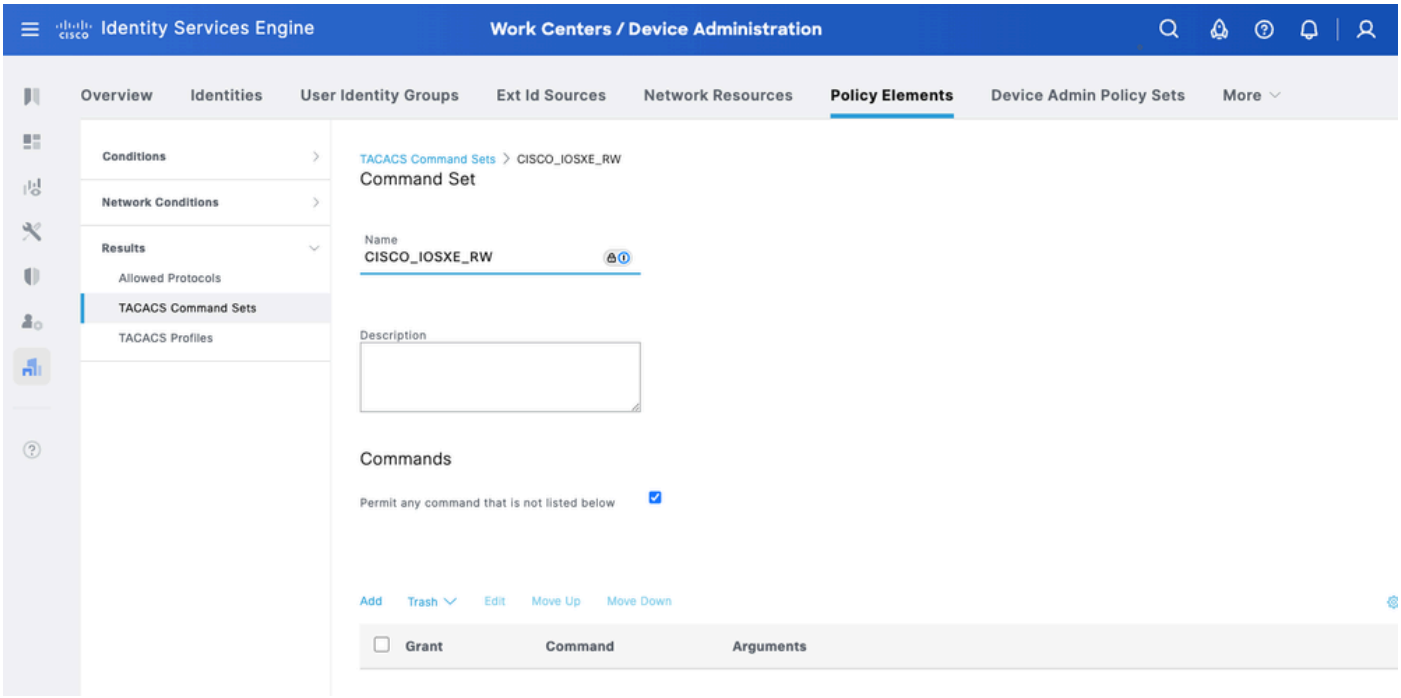
Configurer les jeux de commandes TACACS+

il s'agit de deux ensembles de commandes TACACS+ : CISCO_IOS XE_RW et CISCO_IOS XE_RO.

CISCO_IOS XE_RW - Ensemble de commandes de l'administrateur

Étape 1. Accédez à Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. Ajoutez un nouveau jeu de commandes TACACS et nommez-le CISCO_IOS XE_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.



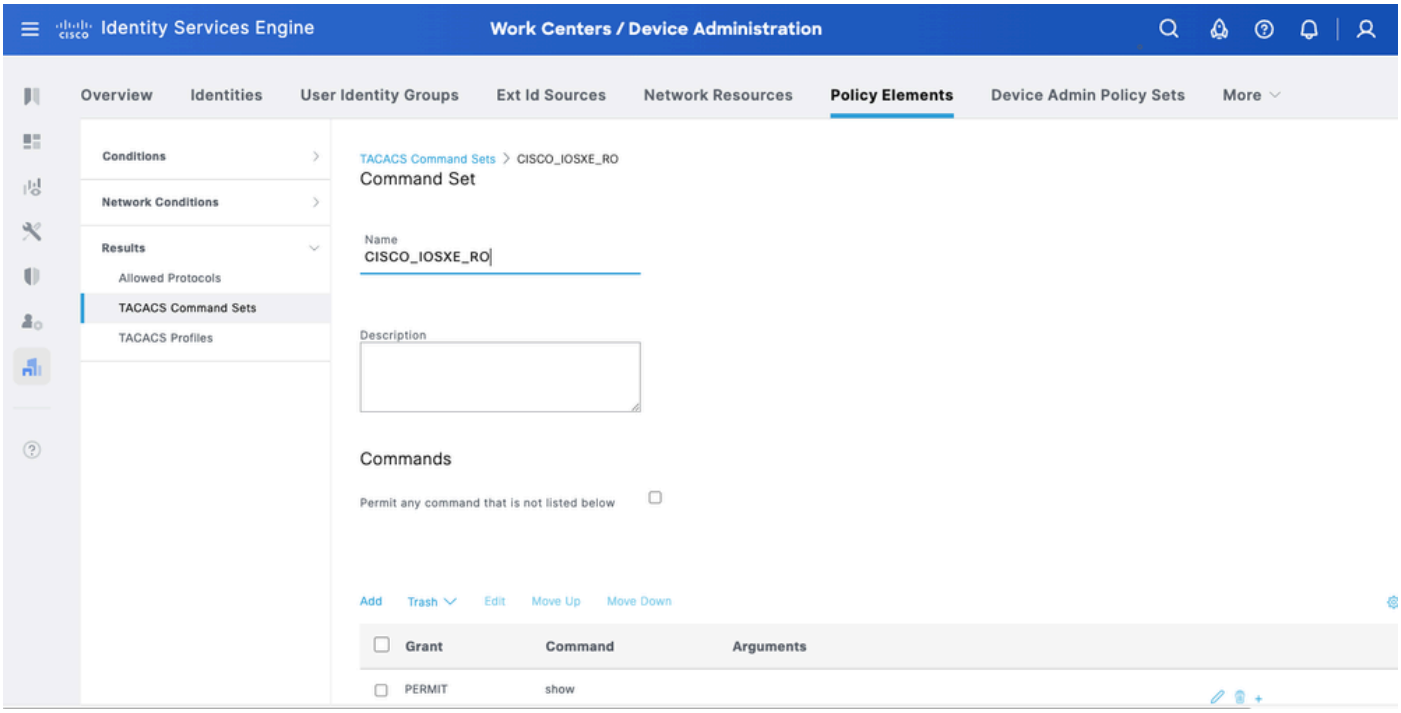
CISCO_IOS XE_RO - Jeu de commandes opérateur

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_IOS XE_RO.

Étape 2. Dans la section Commandes, 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.

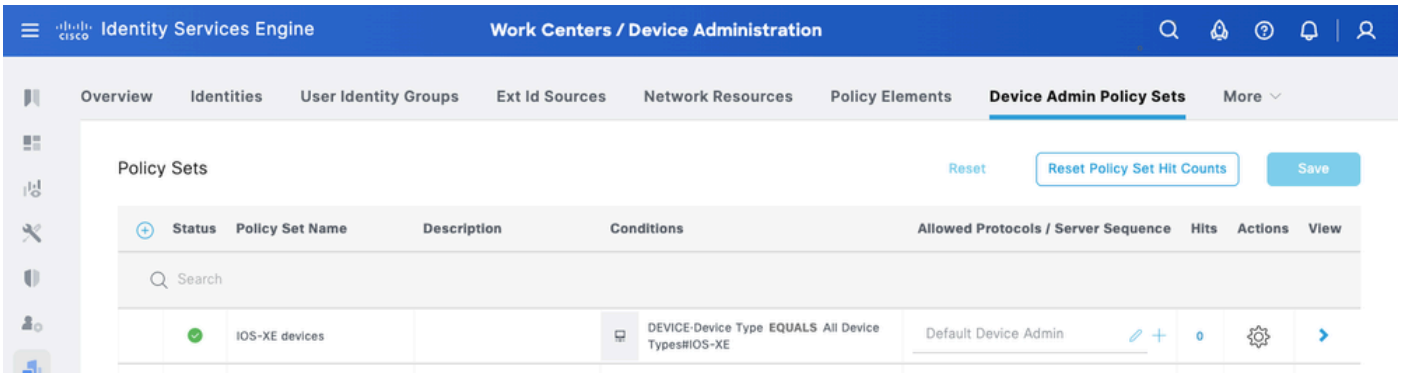
Étape 4. Confirmez les données et cliquez sur Save.



Configurer les ensembles de stratégies d'administration des périphériques

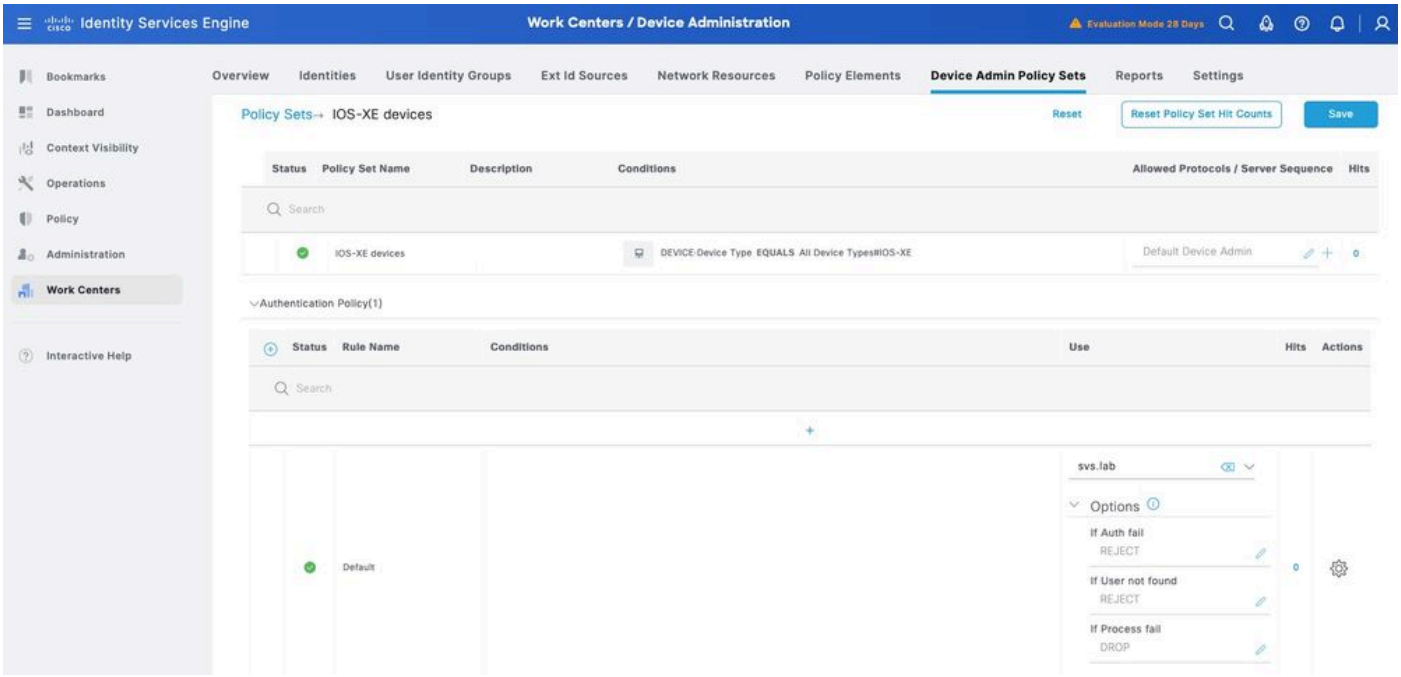
Les jeux de stratégies sont activés par défaut pour l'administration des périphériques. Les ensembles de politiques peuvent diviser les politiques en fonction des types de périphériques afin de faciliter l'application des profils TACACS.

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



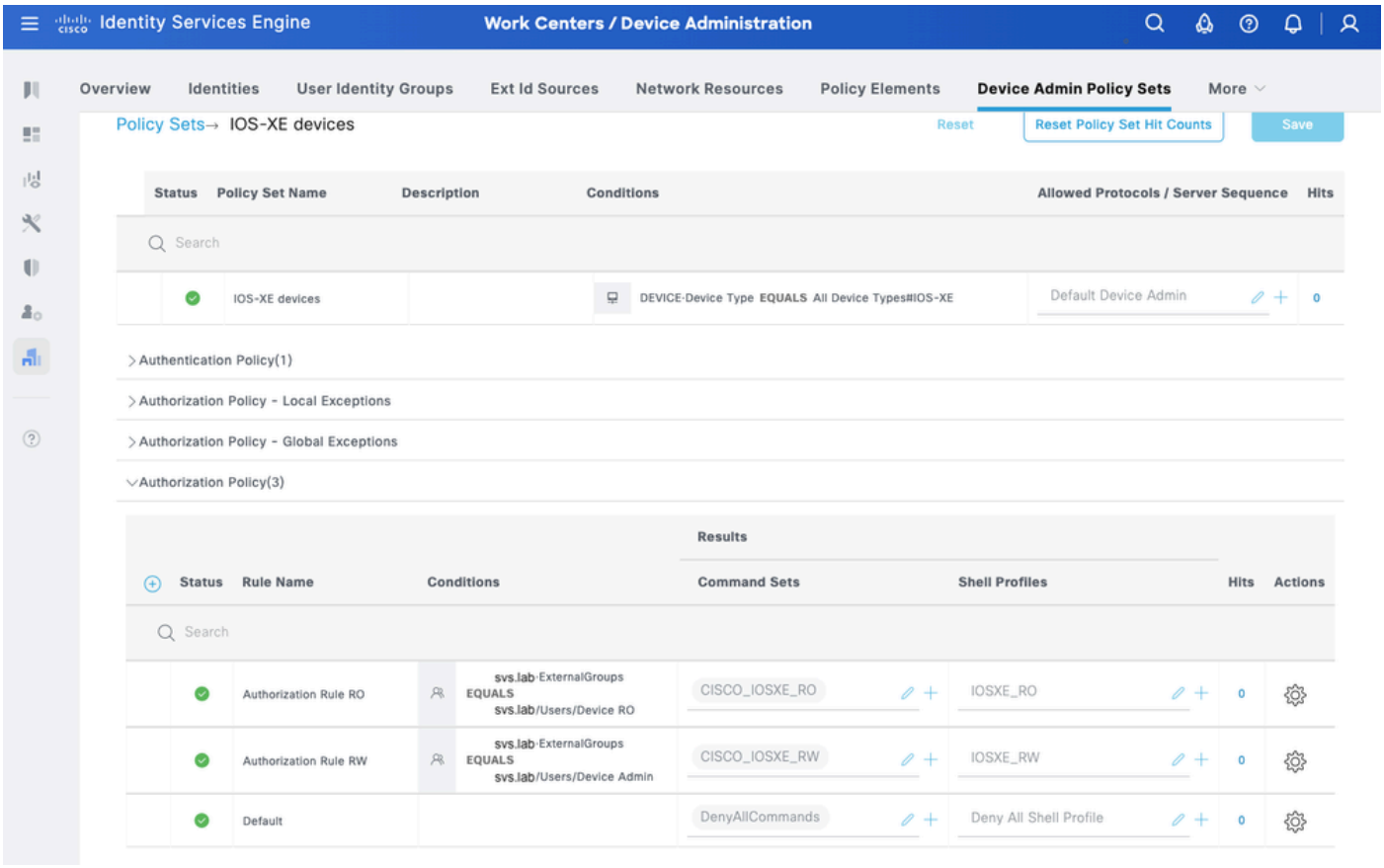
Étape 4 : définition de la politique d’autorisation

Créez la stratégie d'autorisation basée sur les groupes d'utilisateurs dans Active Directory (AD).

Exemple :

· Les utilisateurs du groupe AD Device RO 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 se voient attribuer le jeu de commandes CISCO_IOSXR_RW et le profil d'environnement de ligne de commande IOSXR_RW.



Partie 2 : configuration de Cisco IOS XE 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.

Méthode de configuration 1 - Paire de clés générée par le périphérique

Configuration du serveur TACACS+

Étape 1 : configuration du nom de domaine et génération d'une paire de clés utilisée pour le point de confiance du routeur

```
ip domain name svs.lab

crypto key generate ec keysize 256 label svs-256ec-key
```

Configuration du point de confiance

Étape 1 : création du point de confiance du routeur et association de la paire de clés

```
crypto pki trustpoint svs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svs-256ec-key
```

Étape 2 : authentification du point de confiance en installant le certificat CA.

<#root>

```
cat9k(config)#

crypto pki authenticate svs_cat9k


Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----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+t3c1sNbN2AtFi4cJovTA01xh6OI4QnK+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
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

-----END CERTIFICATE-----

Certificate has the following attributes:
   Fingerprint MD5: D9C4O4B2 EC08A26O EC3539E7 F54ED17D
   Fingerprint SHA1: OEB181E9 5A3ED78O 3BC5A8O5 9A854A95 C83AC737

% Do you accept this certificate? [yes/no]:
```

yes

```
Trustpoint CA certificate accepted.
% Certificate successfully imported

cat9k(config)#
```

Étape 3 : génération d'une demande de signature de certificat (CSR).

<#root>

```
cat9k(config)#
```

crypto pki enroll svs_cat9k

```
% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
```

```
% The subject name in the certificate will include: cat9k.svs.lab
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIBfDCCASMCAQAwgYQxGjAYBgNVBAMTEWNhdDlrLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMS0wKzAcBgNVHREEFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

no

```
cat9k(config)#
```

Étape 4. Importez le certificat signé par l'autorité de certification.

<#root>

```
cat9k(config)#
```

crypto pki import svs_cat9k certificate

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIID8zCCAdugAwIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTEOMTUxMjAwWhcNMjYwNTEOMTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ2lzY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTAlVTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABOlgTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFyOrLiyjxXmLpFcO3uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2Vy
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
Oc0NU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecrOWx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
```

```
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

TACACS et AAA avec configuration TLS

Étape 1 : création du serveur TACACSS et des groupes AAA, association du point de confiance du client (routeur)

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Étape 2 : configuration des méthodes AAA

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

Méthode de configuration 2 - Paire de clés générée par CA

Si vous importez les clés ainsi que les certificats de périphérique et d'autorité de certification

directement dans un format PKCS#12 au lieu de la méthode CSR, vous pouvez utiliser cette méthode.

Étape 1 : création du point de confiance client.

```
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

Étape 2. Copiez le fichier PKCS#12 dans bootflash.



Remarque : Assurez-vous que le fichier PKCS#12 contient la chaîne de certificats complète et la clé privée comme fichier chiffré.



Mise en garde : Les clés de la clé PKCS#12 importée doivent être RSA (par exemple : Type RSA 2048), pas ECC.

<#root>

```
cat9k#
```

copy sftp bootflash: vrf Mgmt-vrf

```
Address or name of remote host [10.225.253.247]?
Source username [svs-user]?
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
Destination filename [cat9k-25jun17.pfx]?
Password:
!
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

Étape 3. Importez le fichier PKCS#12 en utilisant la commande import.

<#root>

```
cat9k#
```

crypto pki import svs_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

```
 password C1sco.123
% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx
CRYPTO_PKI: Imported PKCS12 file successfully.
cat9k#

cat9k#
```

```
show crypto pki certificates svs_cat9k_25jun17


Certificate
  Status: Available
  Certificate Serial Number (hex): 586OBF33A2033365
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    Name: cat9k.svs.lab
    e=pkalkur@cisco.com
    cn=cat9k.svs.lab
    ou=svs
    o=cisco
    l=rtp
    st=nc
    c=us
  Validity Date:
    start date: 17:56:00 UTC Jun 17 2025
    end   date: 17:56:00 UTC Jun 17 2026
  Associated Trustpoints: svs_cat9k_25jun17

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 20CD7402C4DA37F5
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Validity Date:
    start date: 17:05:00 UTC Apr 28 2025
    end   date: 17:05:00 UTC Apr 28 2035
  Associated Trustpoints: svs_cat9k_25jun17 svs_cat9k
  Storage: nvram:SVSLabCA#37F5CA.cer
```

TACACS et AAA avec configuration TLS

Étape 1 : création du serveur TACACS et des groupes AAA, association du point de confiance du client (routeur)

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Étape 2 : configuration des méthodes AAA

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

Vérification

Vérifiez la configuration.

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

Débogage pour AAA et TACACS+.

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
```

```
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure

! Below debugs will be needed only if there is any issue with SSL Handshake
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

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.