Configuration de l'authentification externe TACACS avec ISE

Table des matières

Introduction

Ce document décrit les étapes requises pour intégrer Cisco Identity Services Engine avec Catalyst Center afin d'activer l'authentification TACACS+.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès administrateur à Cisco ISE et à Cisco Catalyst Center.
- Compréhension de base des concepts AAA (Authentication, Authorization, and Accounting).
- Connaissance pratique du protocole TACACS+.
- Connectivité réseau entre Catalyst Center et le serveur ISE.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions matérielles et logicielles suivantes :

- Cisco Catalyst Center version 2.3.7.x
- Cisco Identity Services Engine (ISE) version 3.x (ou ultérieure)
- Protocole TACACS+ pour l'authentification des utilisateurs externes

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.

Informations générales

Cette intégration permet aux utilisateurs externes de se connecter à Catalyst Center pour l'accès administratif et la gestion.

Configurer

Cisco Identity Services Engine (ISE)

Licence et activation des services TACACS+

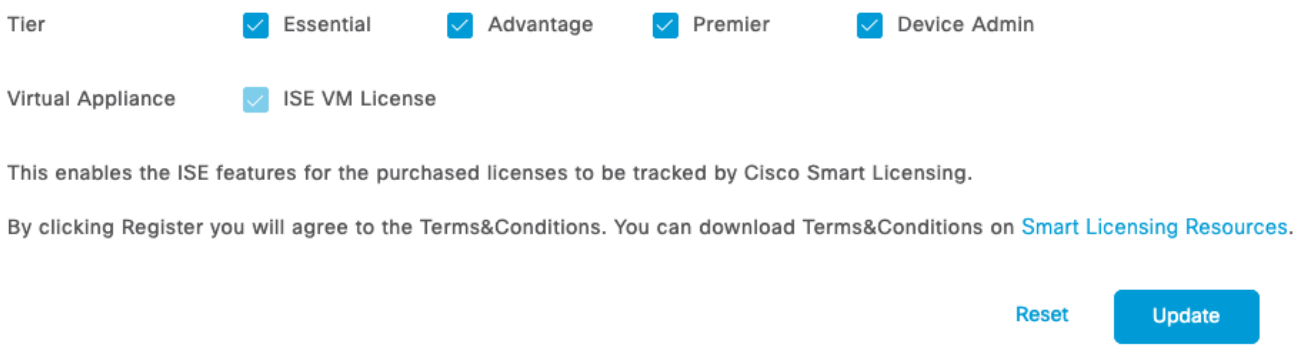
Avant de commencer à configurer TACACS+ dans ISE, vous devez vérifier que la licence appropriée est installée et que la fonctionnalité est activée.

1. Vérifiez que vous disposez de la licence PID L-ISE-TACACS-ND= dans le portail Cisco Smart Software Manager ou Cisco License Central.

Activez Device Administration dans le portail de gestion des licences ISE.

- La licence Device Admin (PID : L-ISE-TACACS-ND=) active les services TACACS+ sur un noeud de service de stratégie (PSN).
- Naviguez jusqu’à l’adresse :

  Administration > Système > Licences
- Cochez la case Device Admin sous les options de niveau.



Administrateur de périphériques

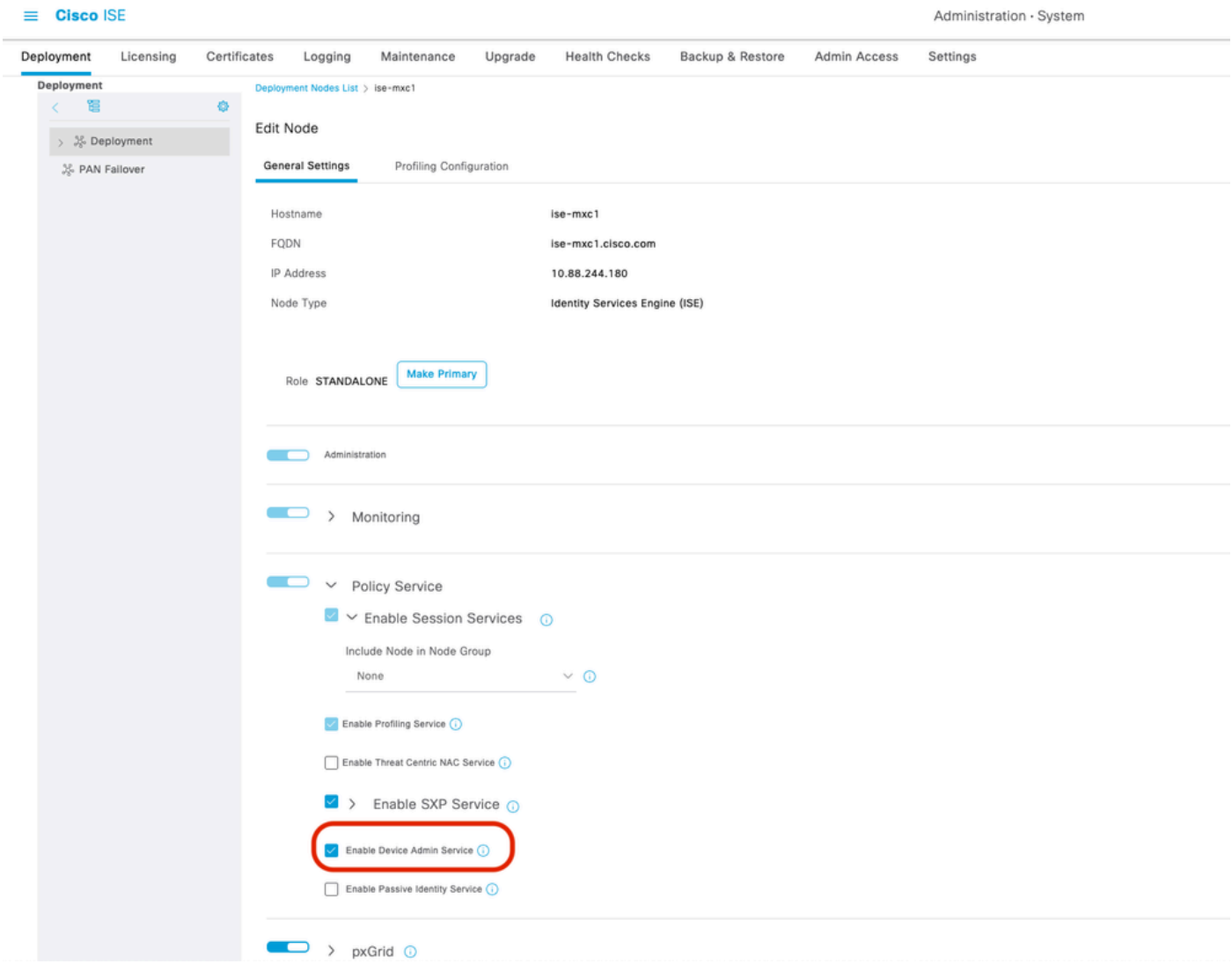
Administrateur de périphérique de licence

3. Activez le service d'administration de périphériques sur le noeud ISE qui exécute le service TACACS+.

- Naviguez jusqu’à l’adresse :

  Administration > System > Deployment > Sélectionnez le noeud

- Cochez l'option Enable Device Admin Service.



Activer le service d'administration des périphériques

Créer un utilisateur admin et ajouter un périphérique réseau

1. Créez l'utilisateur Admin.

   - Ce compte d'utilisateur est utilisé pour se connecter à l'interface utilisateur de Catalyst Center via l'authentification ISE.
   - Naviguez jusqu'à l'adresse :

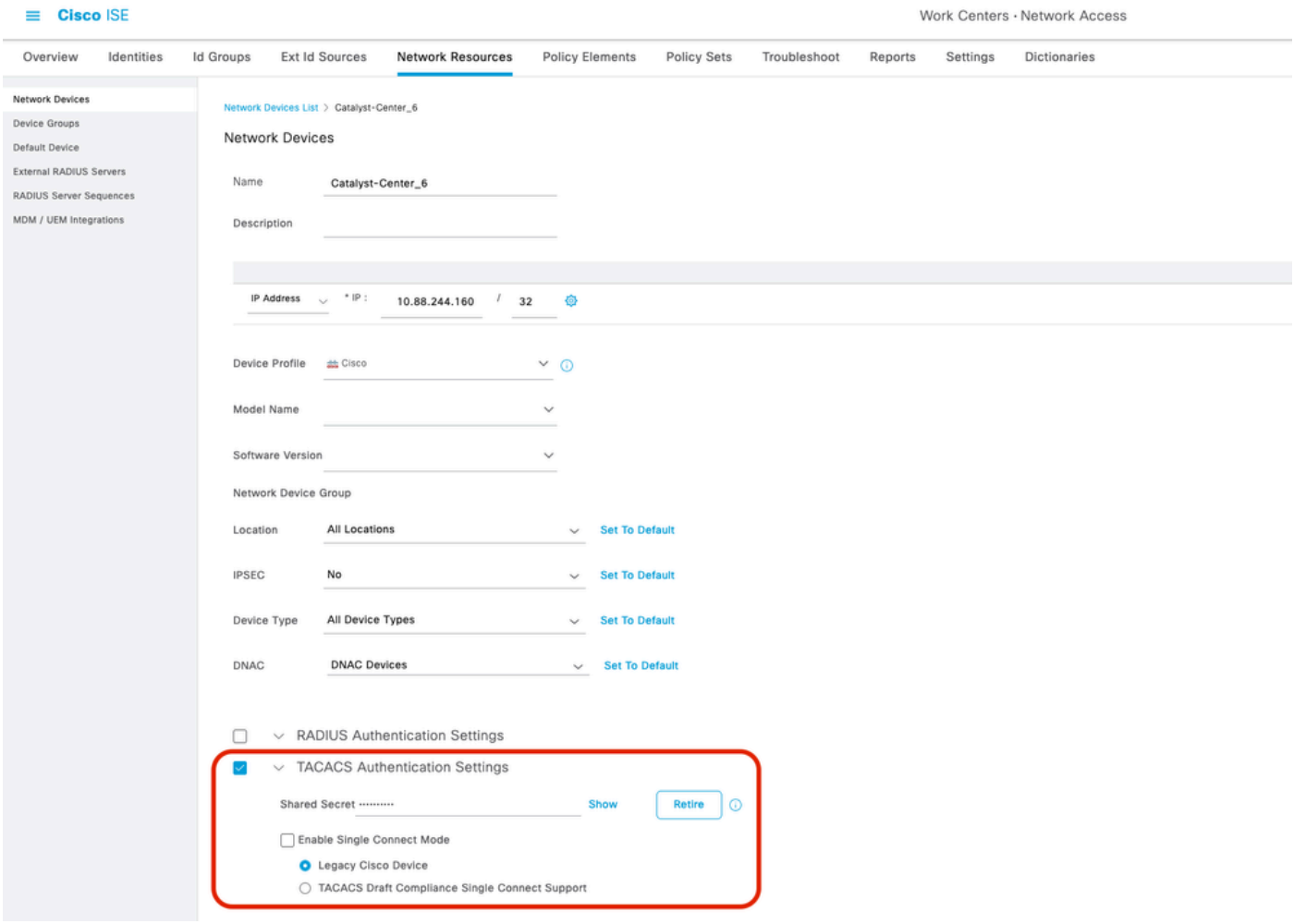
     Centres de travail > Accès réseau > Identités > Utilisateur d'accès réseau
   - Ajoutez un nouvel utilisateur (par exemple, catc-user).
   - Si l'utilisateur existe déjà, passez à l'étape suivante.

2. Créez le périphérique réseau.

   - Naviguez jusqu'à l'adresse :

     Centres de travail > Accès réseau > Identités > Ressource réseau

- Ajoutez l'adresse IP de Catalyst Center, ou définissez le sous-réseau où l'adresse IP de Catalyst Center est située.
- Si le périphérique existe déjà, vérifiez qu'il contient les paramètres suivants :
    - Les paramètres d'authentification TACACS sont activés.
    - Le secret partagé est configuré et connu (enregistrez cette valeur, car elle est requise ultérieurement dans Catalyst Center).



Paramètres d'authentification TACACS

Configurer le profil TACACS+

1. Créez un nouveau profil TACACS+.

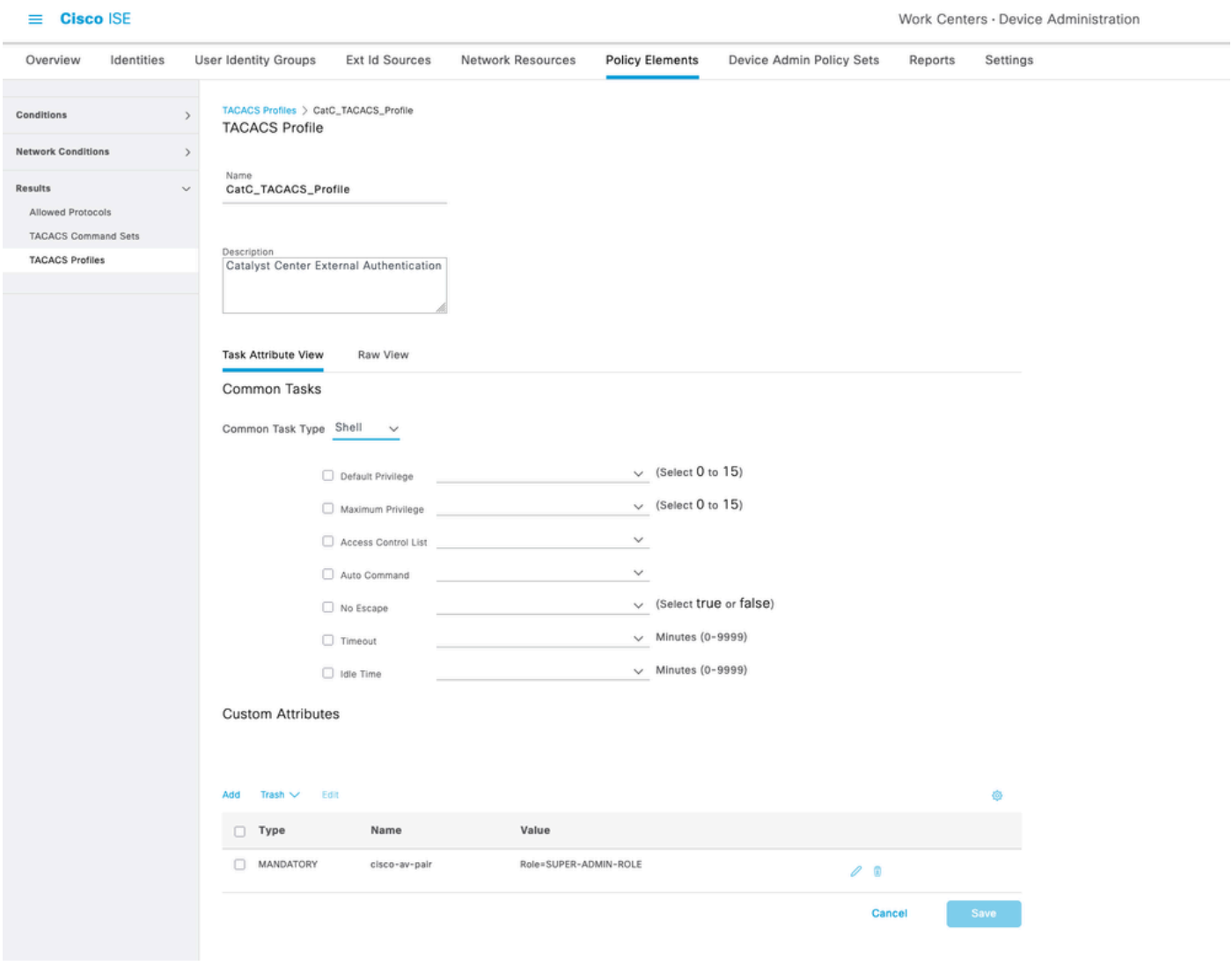
- Naviguez jusqu'à l'adresse :

Centres de travail > Administration des périphériques > Éléments de stratégie > Résultats > Profils TACACS

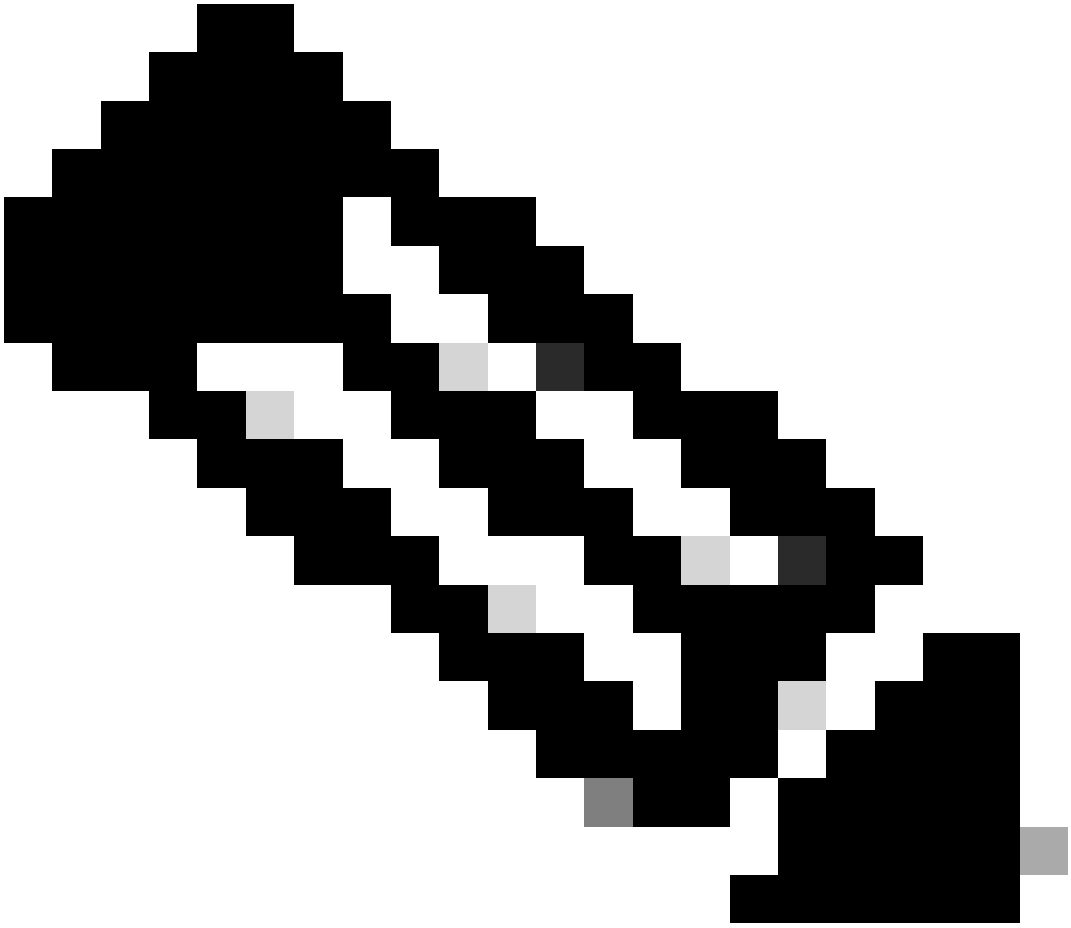
- Ajoutez un nom de profil.
- Ajoutez un attribut personnalisé comme suit :

- type : Obligatoire
- Name : paire cisco-av
- Valeur: Role=SUPER-ADMIN-ROLE

- Enregistrez le profil.



Profil TACACS+



Remarque : Cisco Catalyst Center prend en charge les serveurs AAA (Authentication, Authorization and Accounting) externes pour le contrôle d'accès. Si vous utilisez un serveur externe pour l'authentification et l'autorisation d'utilisateurs externes, vous pouvez activer l'authentification externe dans Cisco Catalyst Center. Le paramètre d'attribut AAA par défaut correspond à l'attribut de profil utilisateur par défaut.

La valeur d'attribut AAA par défaut du protocole TACACS est cisco-av-pair.

La valeur d'attribut AAA par défaut du protocole RADIUS est Cisco-AVPair.

La modification n'est requise que si votre serveur AAA a un attribut personnalisé dans le profil utilisateur. Sur le serveur AAA, le format de la valeur de l'attribut AAA est Role=role1. Sur le serveur Cisco Identity Services Engine (Cisco ISE), lors de la configuration du profil RADIUS ou TACACS, l'utilisateur peut sélectionner ou entrer cisco av-pair comme attribut AAA.

Par exemple, vous pouvez sélectionner et configurer manuellement l'attribut AAA en tant que cisco-av-pair=Role=SUPER-ADMIN-ROLE ou Cisco-AVPair=Role=SUPER-ADMIN-

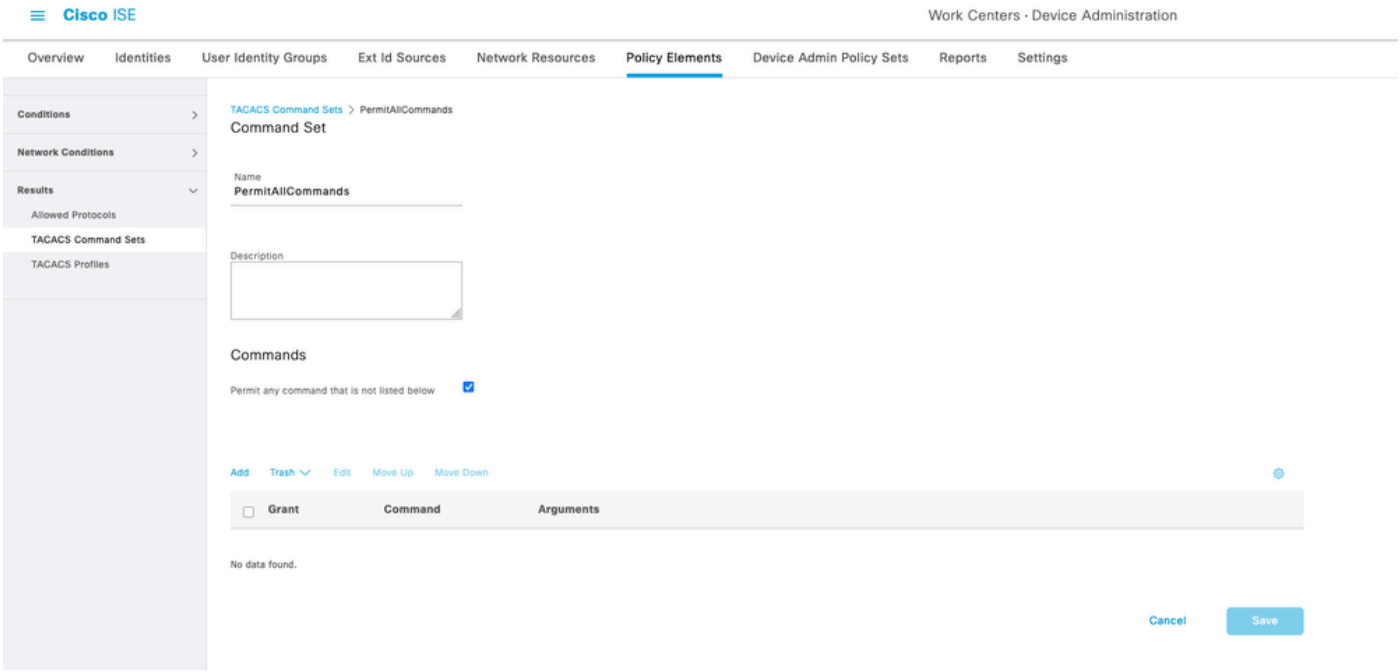
ROLE.

2. Créez un jeu de commandes TACACS+.

- Naviguez jusqu'à l'adresse :

Centres de travail > Administration des périphériques > Éléments de stratégie > Résultats > Jeux de commandes TACACS

- Ajoutez un nom.
- Cochez l'option Autoriser toute commande qui n'est pas répertoriée ci-dessous.
- Enregistrez le jeu de commandes.



Jeux de commandes TACACS

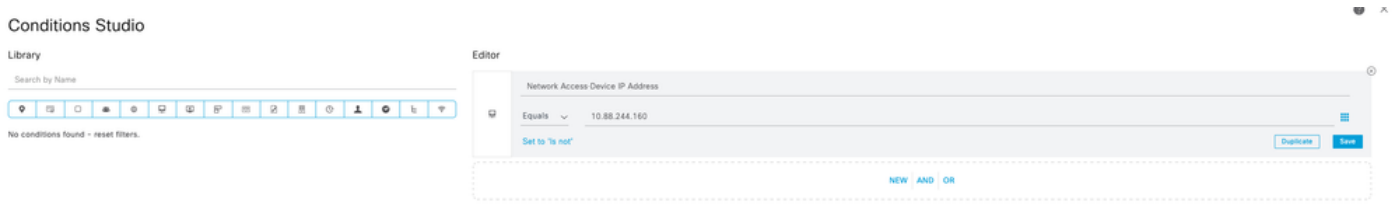
Configurer les stratégies TACACS+

1. Créez un nouvel ensemble de stratégies TACACS+.

- Naviguez jusqu'à l'adresse :

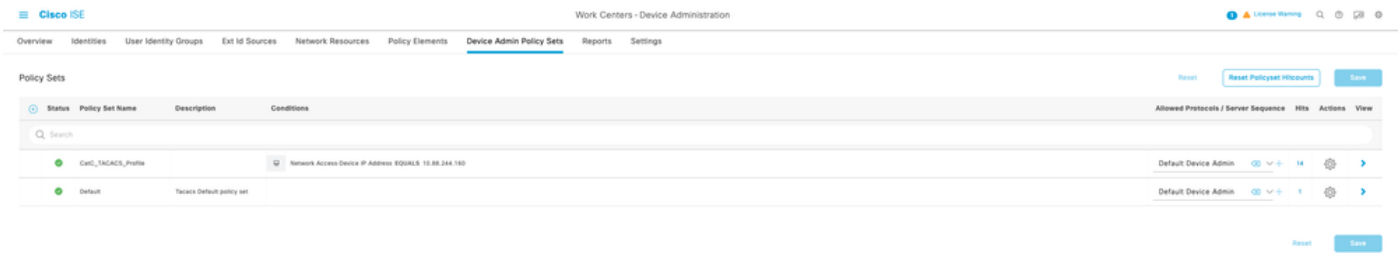
Centres de travail > Administration des périphériques > Ensemble de politiques d'administration des périphériques

- Ajoutez un nom pour l'ensemble de stratégies.
- Configurez la condition.
  - Dans cet exemple, la condition correspond à l'adresse IP de Catalyst Center.



Adresse IP de Catalyst Center

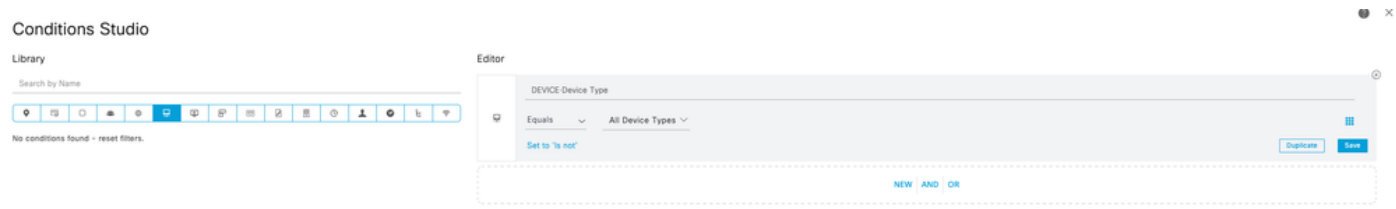
1.3 Dans le champ Protocoles autorisés / Séquence de serveur, sélectionnez Administration de périphérique par défaut.



Sélectionnez Default Device Admin

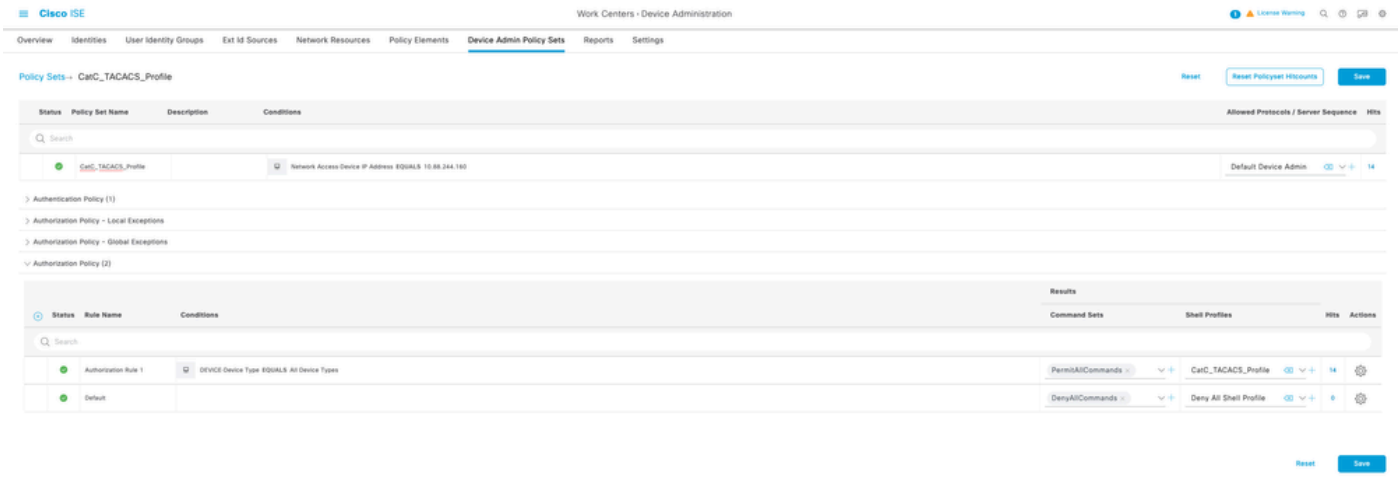
2. Configurez l'ensemble de stratégies.

- Cliquez sur la flèche (>) à droite pour développer et configurer l'ensemble de stratégies.
- Ajoutez une nouvelle règle sous Stratégie d'autorisation.
- Configurez la nouvelle règle comme suit :
  - Name : Entrez un nom de règle descriptif.
  - Condition : Dans cet exemple, la condition correspondait à Tous les types de périphériques.



Tous les types de périphériques

- Jeu de commandes : Sélectionnez l'ensemble de commandes TACACS+ créé précédemment.
- Profil du shell : Sélectionnez le profil TACACS+ créé précédemment.



Jeu de commandes TACACS+

Cisco Catalyst Center

Configuration du serveur ISE/AAA

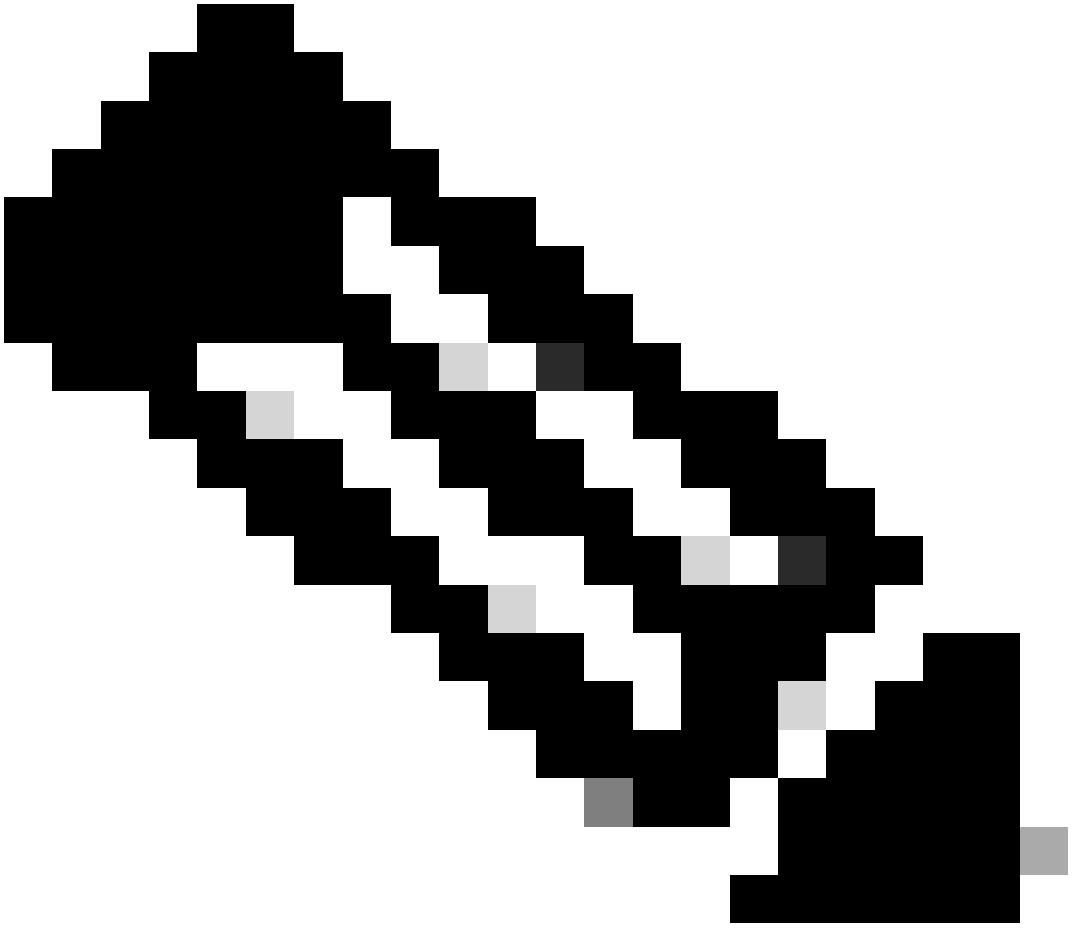
1. Connectez-vous à l'interface Web de Catalyst Center.

- Naviguez jusqu’à l’adresse :

Menu principal > Système > Paramètres > Services externes > Serveurs d'authentification et de stratégie

2. Ajoutez un nouveau serveur. Vous pouvez sélectionner ISE ou AAA.

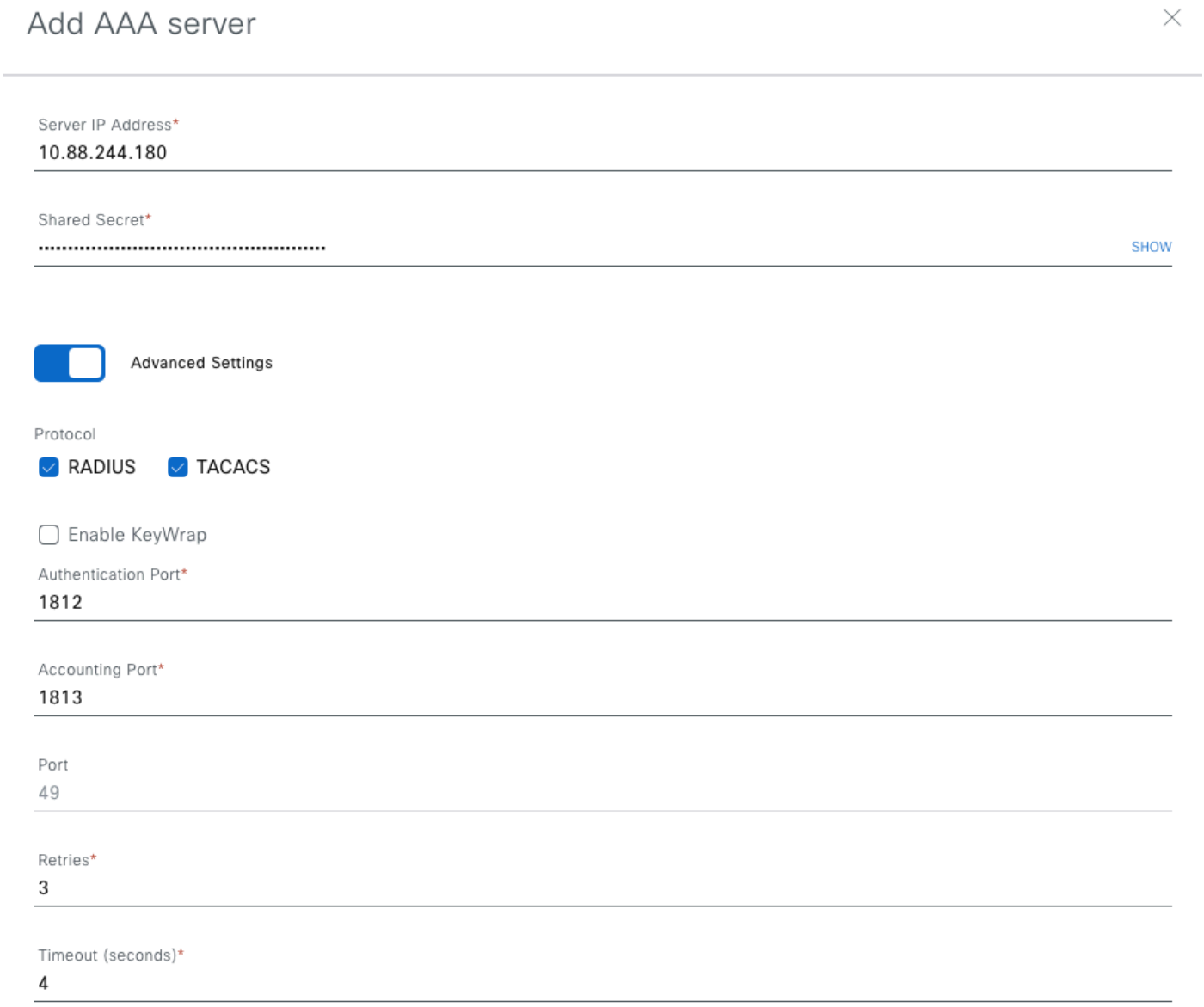
- Pour cette démonstration, l'option de serveur AAA est utilisée.



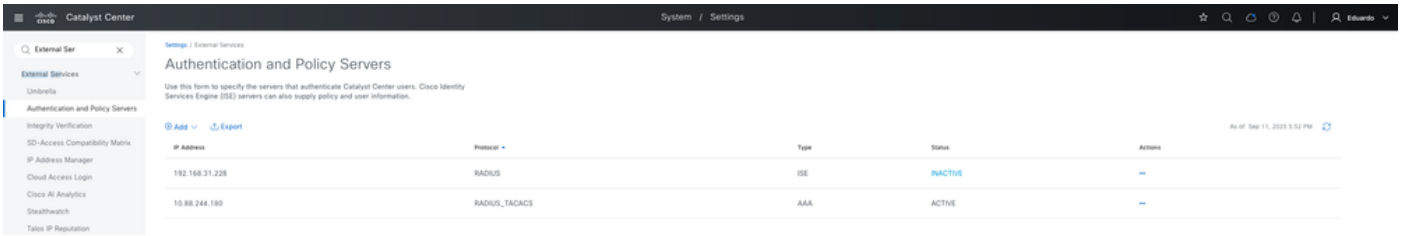
Remarque : Un cluster Catalyst Center ne peut avoir qu'un seul cluster ISE configuré.

3. Configurez ces options, puis enregistrez :

- Entrez l'adresse IP du serveur AAA.
- Ajoutez le secret partagé (le même secret configuré dans la ressource réseau Cisco ISE).
- Activez Advanced Settings (Paramètres avancés).
- Cochez l'option TACACS.



Serveurs d'authentification et de stratégie



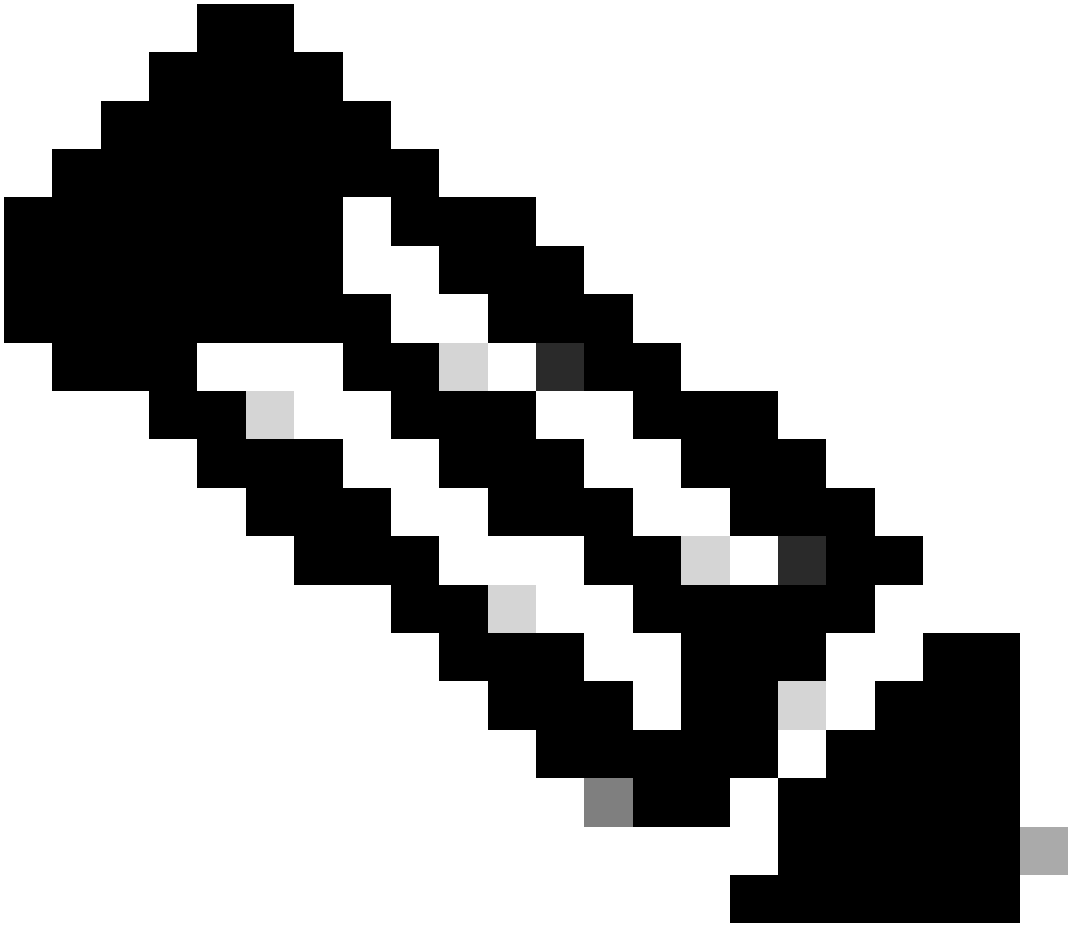
Paramètres avancés

Activez et configurez l'authentification externe.

1. Accédez à la page Authentification externe :

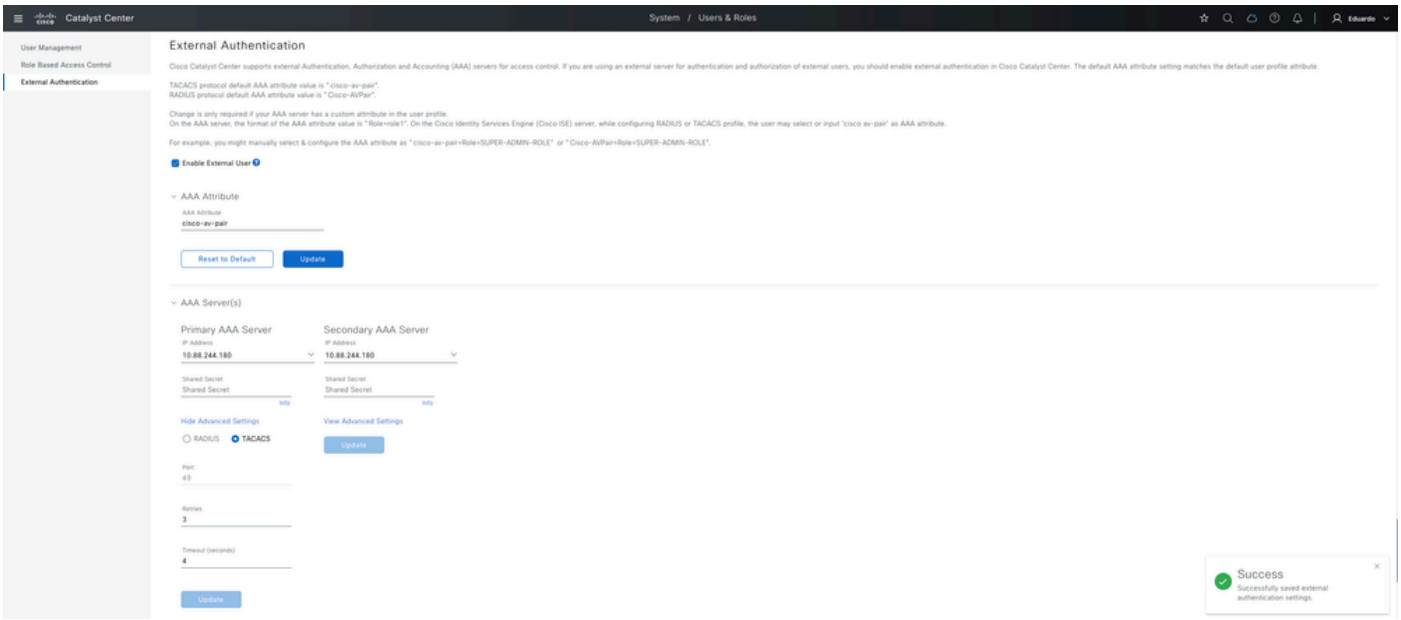
   Menu principal > Système > Utilisateur et rôle > Authentification externe

2. Ajoutez l'attribut AAA cisco-av-pair et cliquez sur Update pour enregistrer les modifications.



Remarque : Cette étape n'est pas obligatoire car l'attribut par défaut de TACACS+ est déjà cisco-av-pair, mais il est recommandé de le configurer explicitement.

3. Sous Serveur AAA principal, sélectionnez le serveur AAA configuré précédemment.
   - Cliquez sur View Advanced Settings pour afficher des options supplémentaires.
   - Sélectionnez l'option TACACS+.
   - Saisissez le secret partagé configuré dans la ressource réseau de Cisco ISE.
   - Cliquez sur Update pour enregistrer les modifications.
4. Cochez la case Utilisateur externe.
   - Cette action enregistre automatiquement la configuration.



Authentification externe

Vérifier

1. Ouvrez une nouvelle session de navigateur ou utilisez le mode Incognito et connectez-vous à la page Web Catalyst Center avec le compte d'utilisateur configuré dans Cisco ISE.

2. Dans Catalyst Center, vérifiez que la connexion a réussi.

Connexion Configurer l'authentification externe de Catalyst Center TACACS avec ISE

3. À partir de Cisco ISE, validez les journaux :

   Opérations > TACACS > Journaux actifs

- État d'authentification : Passe
- État d'autorisation : Passe

Journaux en direct

4. Dans les Détails d'autorisation, comparez avec le résultat suivant :

    - Texte du message : Device-Administration : Autorisation de session réussie
    - Tous les attributs de réponse : cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

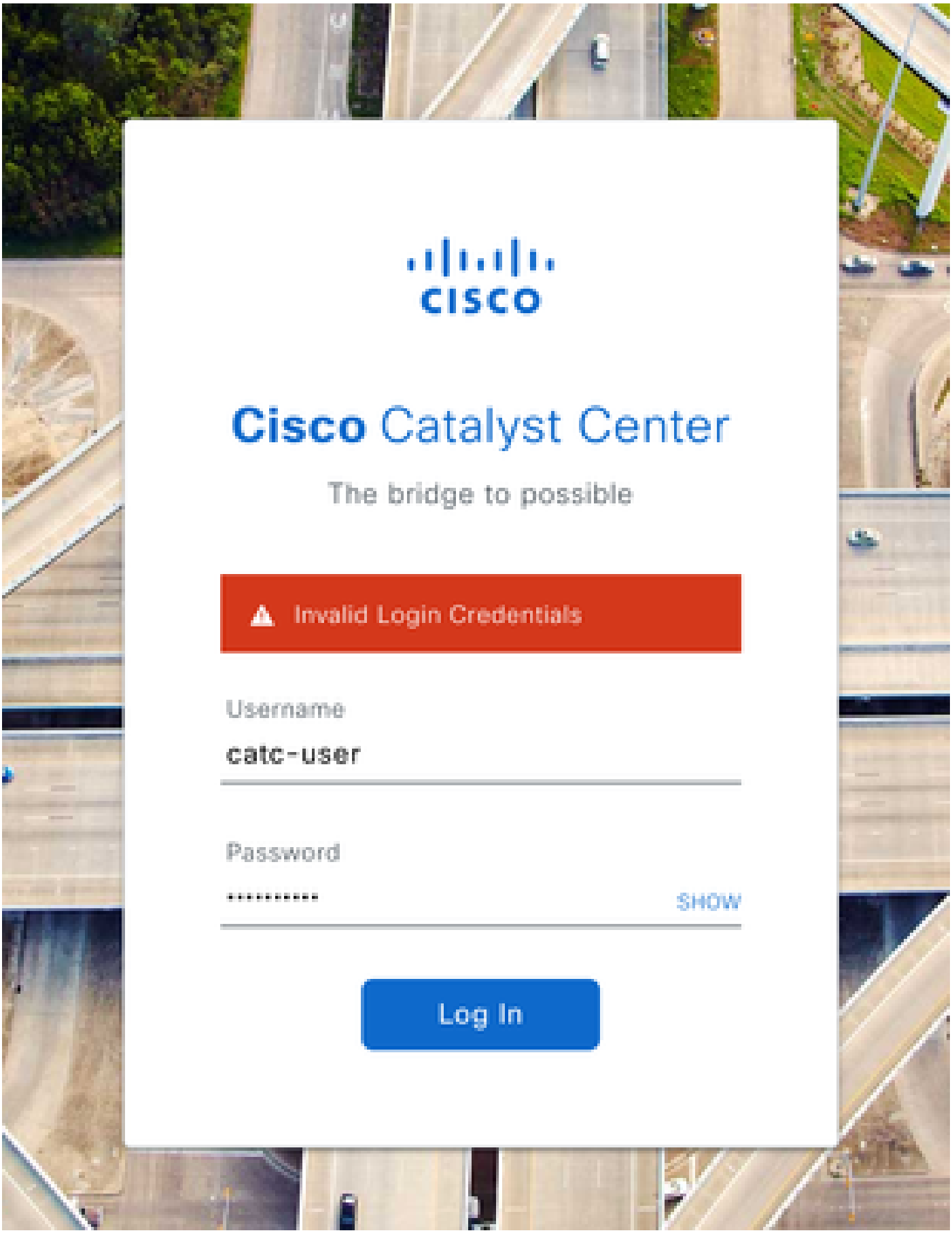
cisco-av-pair=Role=SUPER-ADMIN-ROLE

Dépannage

Voici quelques problèmes courants que vous pouvez rencontrer lors de l'intégration et comment les identifier :

1. Mauvaise configuration des attributs

Symptôme dans Catalyst Center : identifiants de connexion non valides



Mauvaise configuration des attributs

- Symptôme dans Cisco ISE (journaux TACACS) :

- Authentification: Passe
- Autorisation: Passe

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.801...	✓		catc-user	Authorization		CatC_TACACS_Profile >> Authoriz...	ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		CatC_TACACS_Pr...
Sep 12, 2025 12:12:20.788...	✓		catc-user	Authentication	CatC_TACACS_Profile >> Default		ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		

Mauvaise configuration des attributs

- Causes possibles:
  - Un espace existe dans la valeur d'attribut.

Exemple :

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Mauvaise configuration des attributs

- L'attribut n'est pas correctement configuré, le mot clé Role= est omis.

  Exemple :

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Mauvaise configuration des attributs

2. Non-concordance des secrets partagés

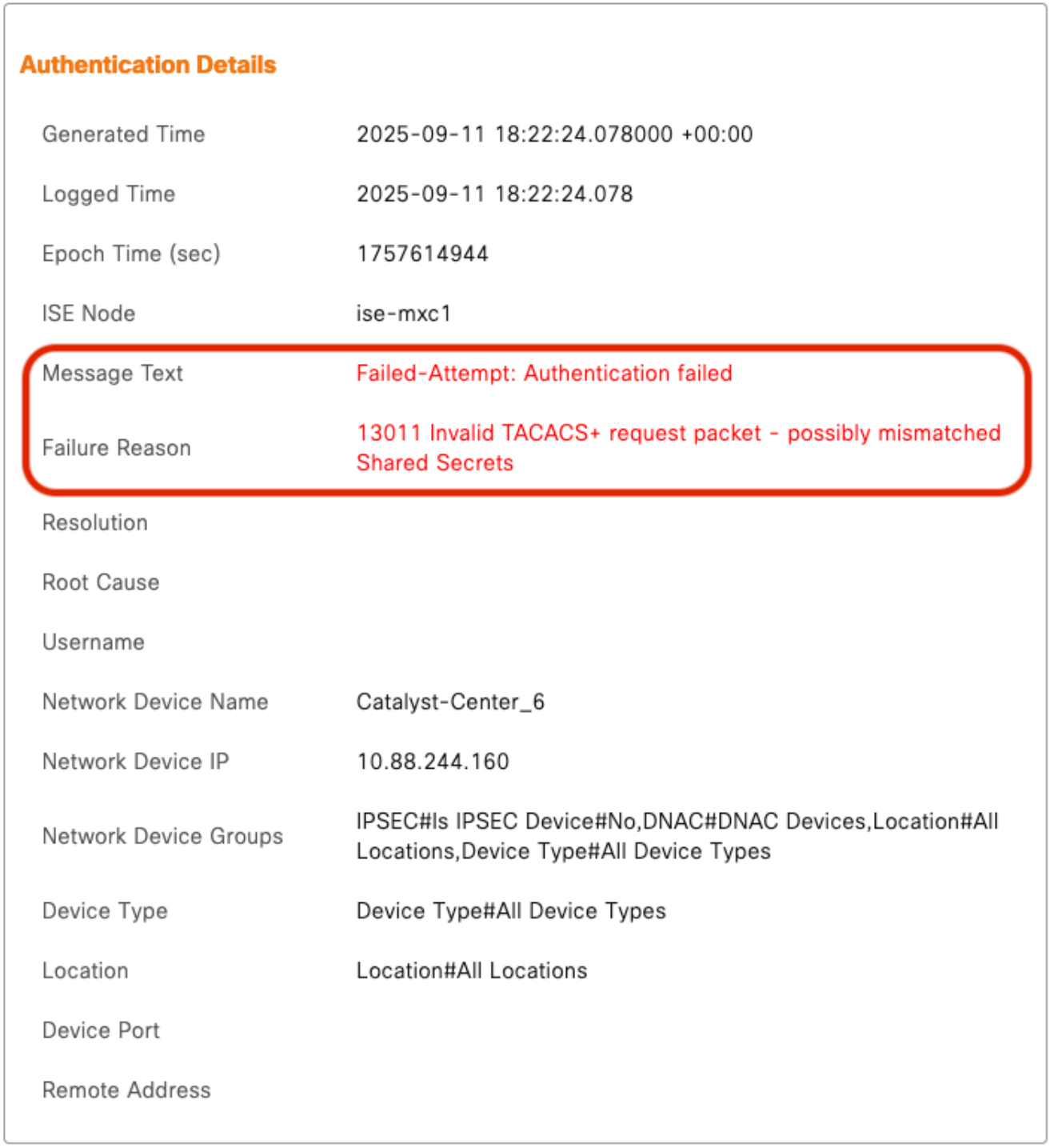
- Symptôme : Les paquets d'authentification échouent entre Catalyst Center et Cisco ISE.

- Cause possible: Le secret partagé configuré dans la ressource réseau d'ISE ne correspond pas à celui configuré dans la page Catalyst Center > Authentification externe.

Comment vérifier :

- Vérifiez la configuration des ressources réseau dans ISE.
- Comparez le secret partagé avec la configuration sous Catalyst Center > Authentification externe.

Exemple :



Authentication Details

Generated Time	2025-09-11 18:22:24.078000 +00:00
Logged Time	2025-09-11 18:22:24.078
Epoch Time (sec)	1757614944
ISE Node	ise-mxc1
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Resolution	
Root Cause	
Username	
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	
Remote Address	

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.