Administration des périphériques de Cisco WLC à l'aide de TACACS+

Contenu

Introduction

Ce document décrit comment configurer TACACS+ pour l'administration des périphériques du contrôleur LAN sans fil Cisco (WLC) avec Identity Service Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de Identity Service Engine (ISE)
- Connaissances de base du contrôleur LAN sans fil Cisco (WLC)

Components Used

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

- Cisco Identity Service Engine 2.4
- Contrôleur LAN sans fil Cisco 8.5.135

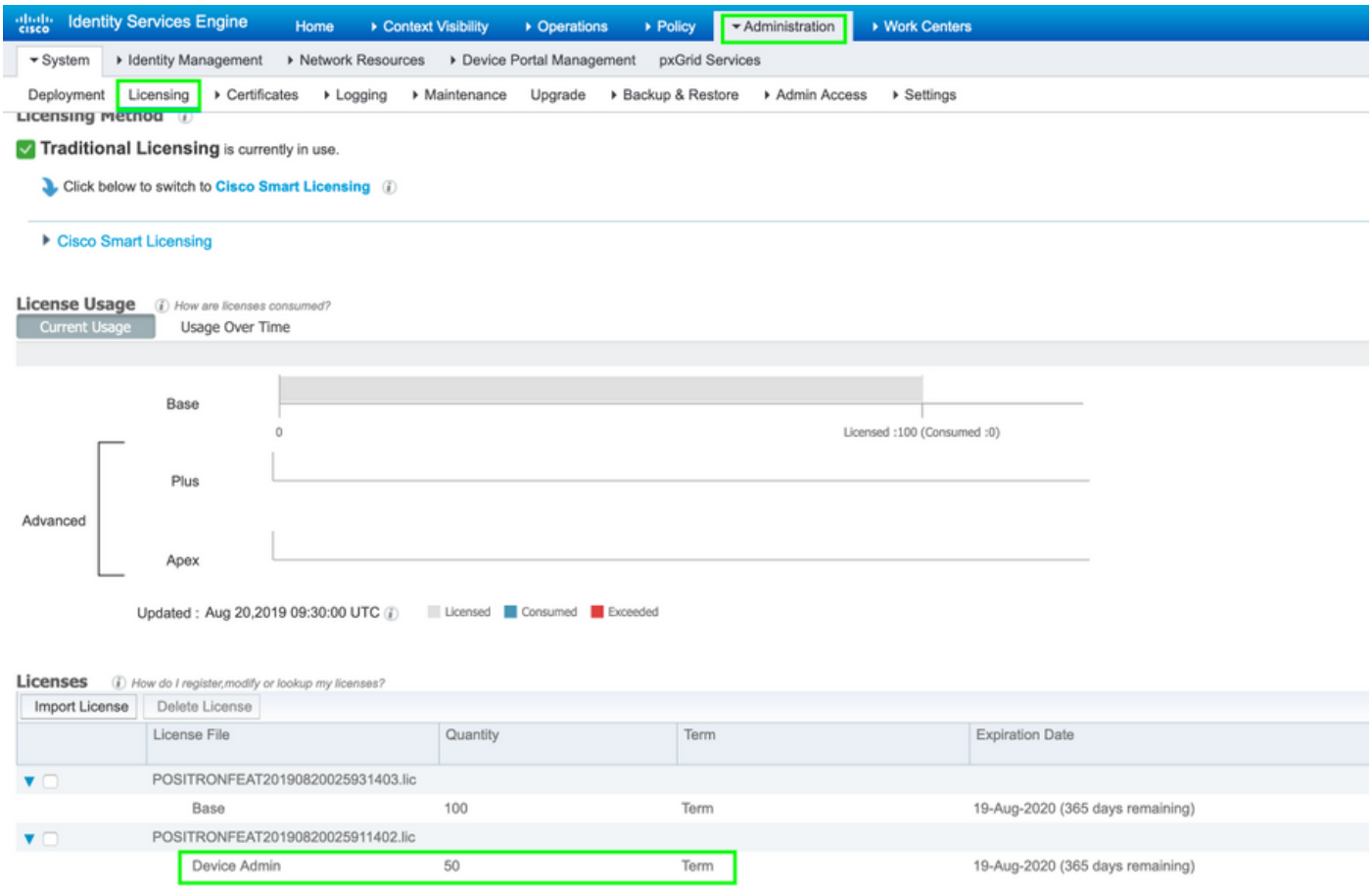
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Configuration

Étape 1. Vérifiez la licence d'administration de périphériques.

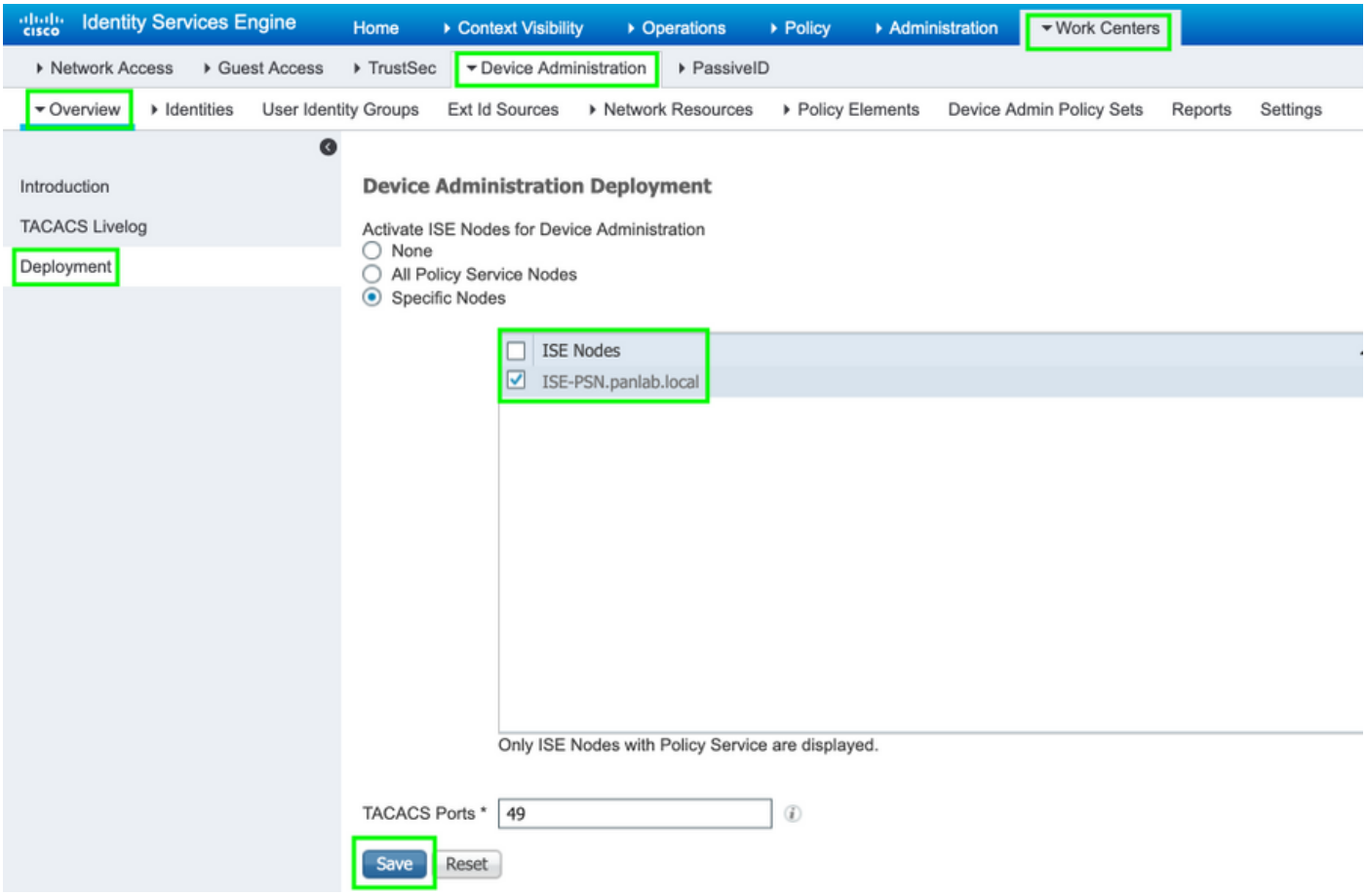
Accédez à **Administration > System > Licensing** et vérifiez que la licence **Device Admin** est installée, comme le montre l'image.



> **Note**: Une licence d'administration de périphérique est requise pour utiliser la fonctionnalité TACACS+ sur ISE.

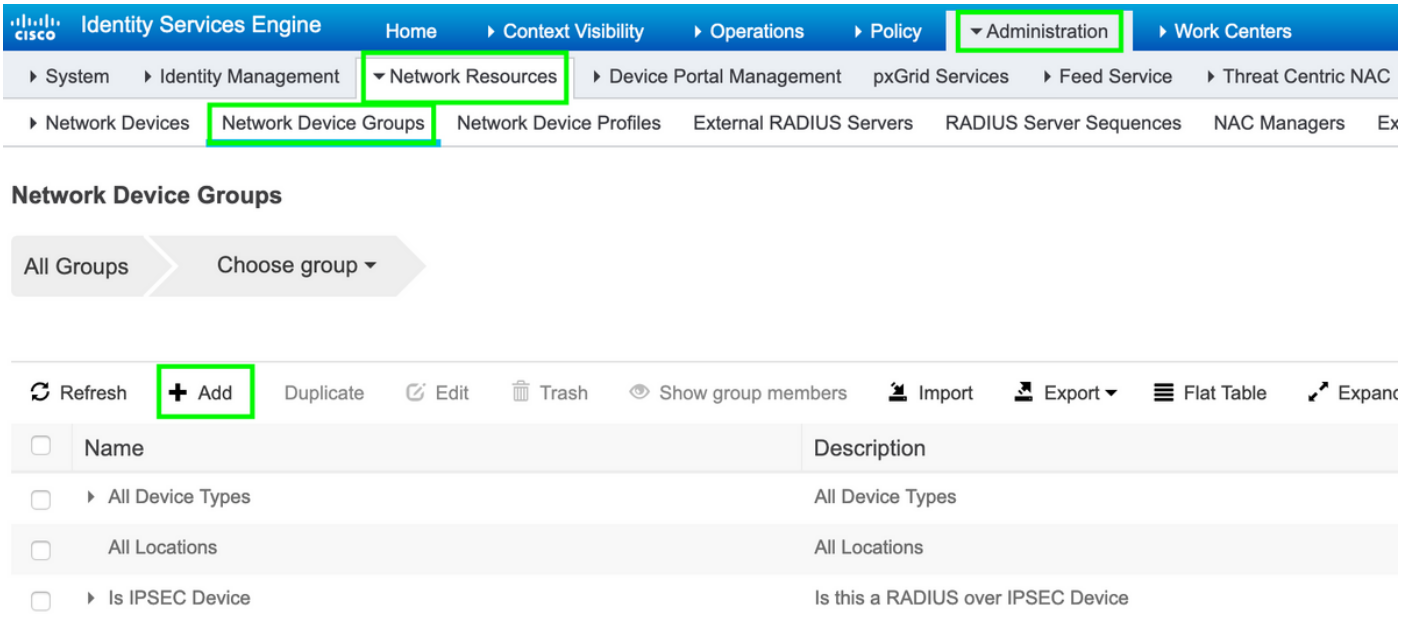
Étape 2. Activez l'administration des périphériques sur les noeuds PSN ISE.

Accédez à **Work Centers > Device Administration > Overview**, cliquez sur l'onglet **Deployment, sélectionnez** la case d'option Specific PSN Node**. Activez** l'administration des périphériques sur le noeud ISE en cochant la **case** et en cliquant sur **enregistrer**, comme illustré dans l'image :



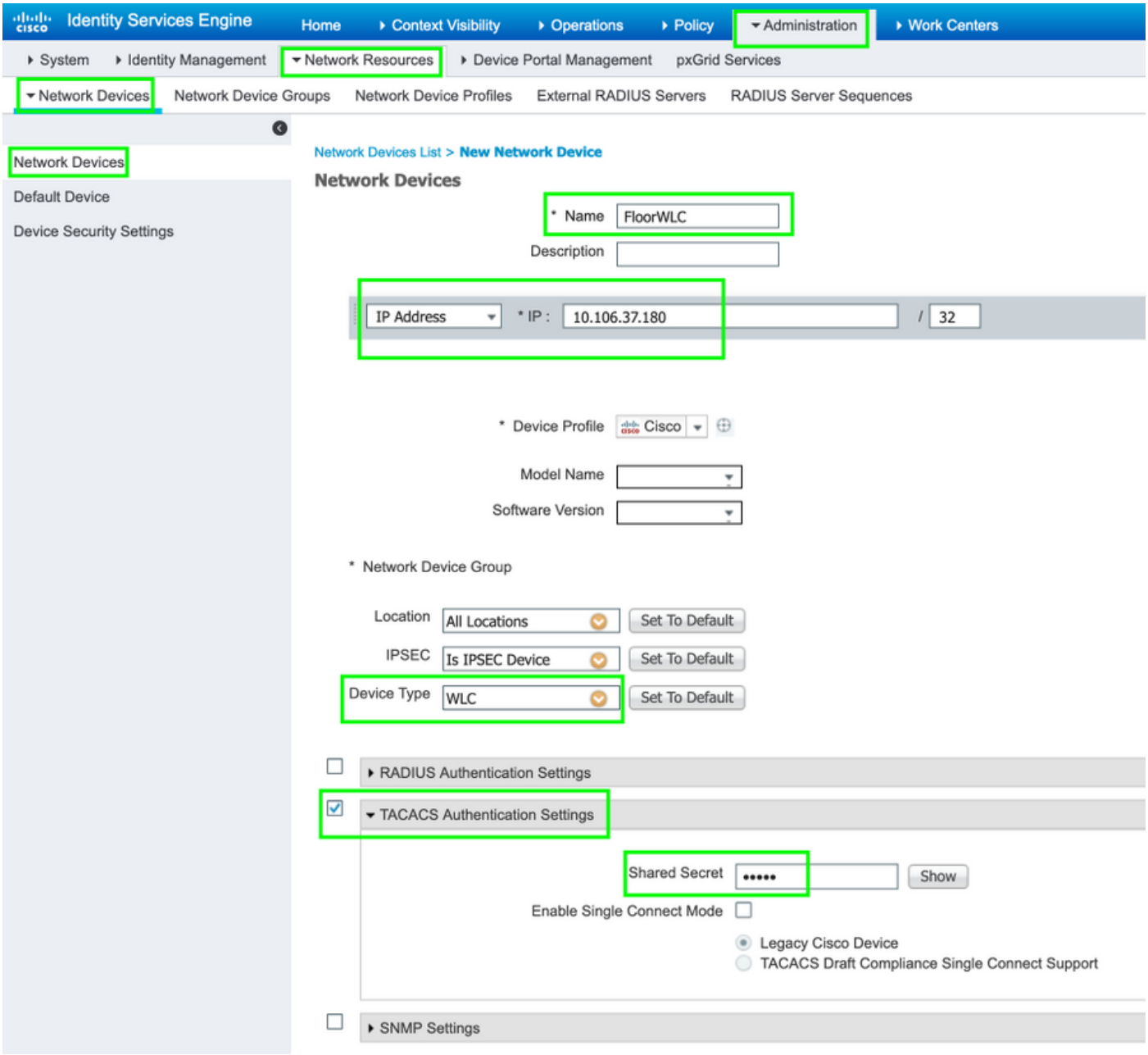
Étape 3. Créez un groupe de périphériques réseau.

Afin d'ajouter le WLC en tant que périphérique réseau sur l'ISE, accédez à **Administration > Network Resources > Network Device Groups > All Device Types**, créez un **nouveau groupe** pour le WLC, comme illustré dans l'image :



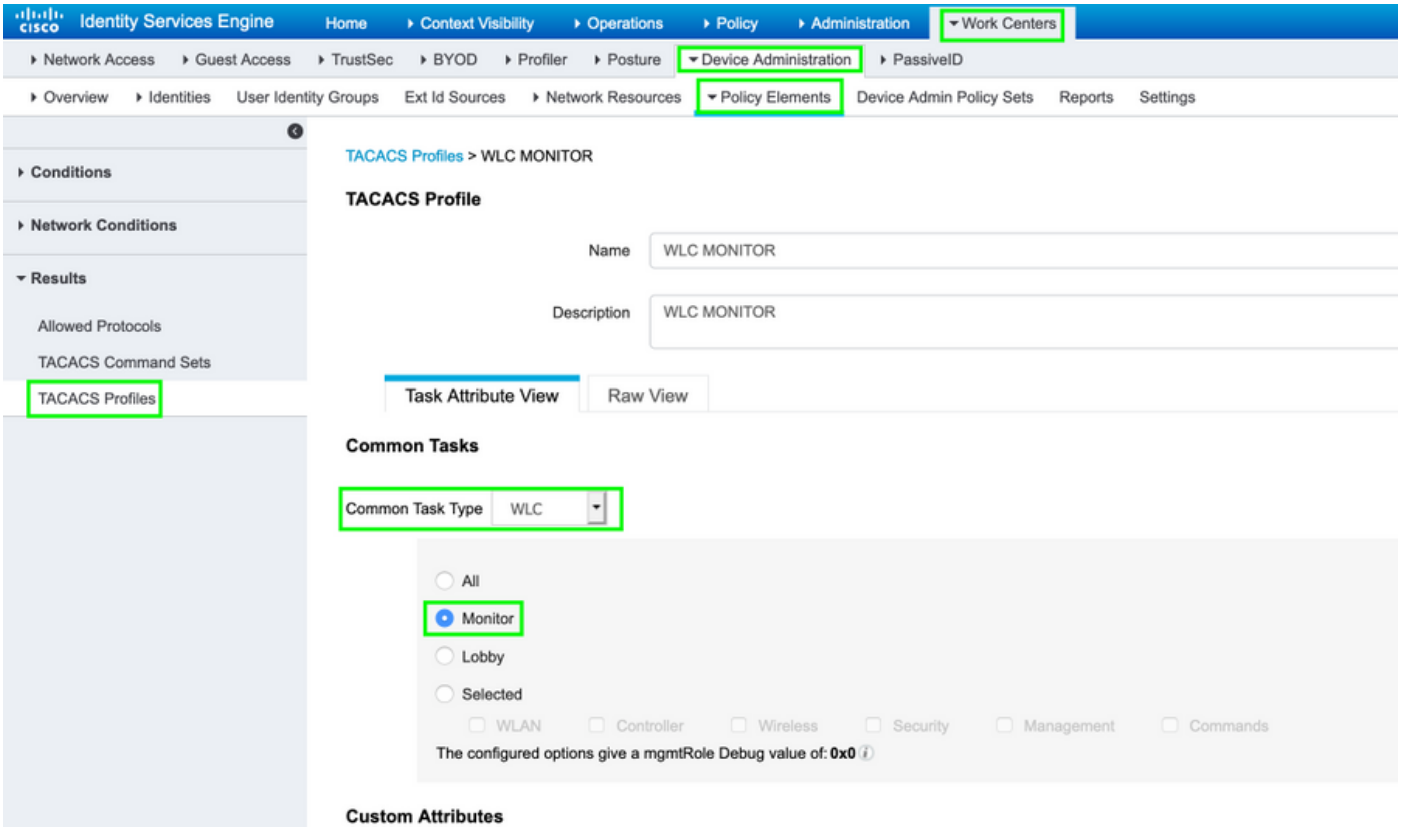
Étape 4. Ajoutez le WLC en tant que périphérique réseau.

Accédez à **Centres de travail > Administration des périphériques > Ressources réseau > Périphériques réseau**. Cliquez sur Add, indiquez Name, IP Address et sélectionnez le type de périphérique en tant que **WLC**, activez la case à cocher **TACACS+ Authentication Settings** et fournissez la **clé Shared Secret**, comme illustré dans l'image :

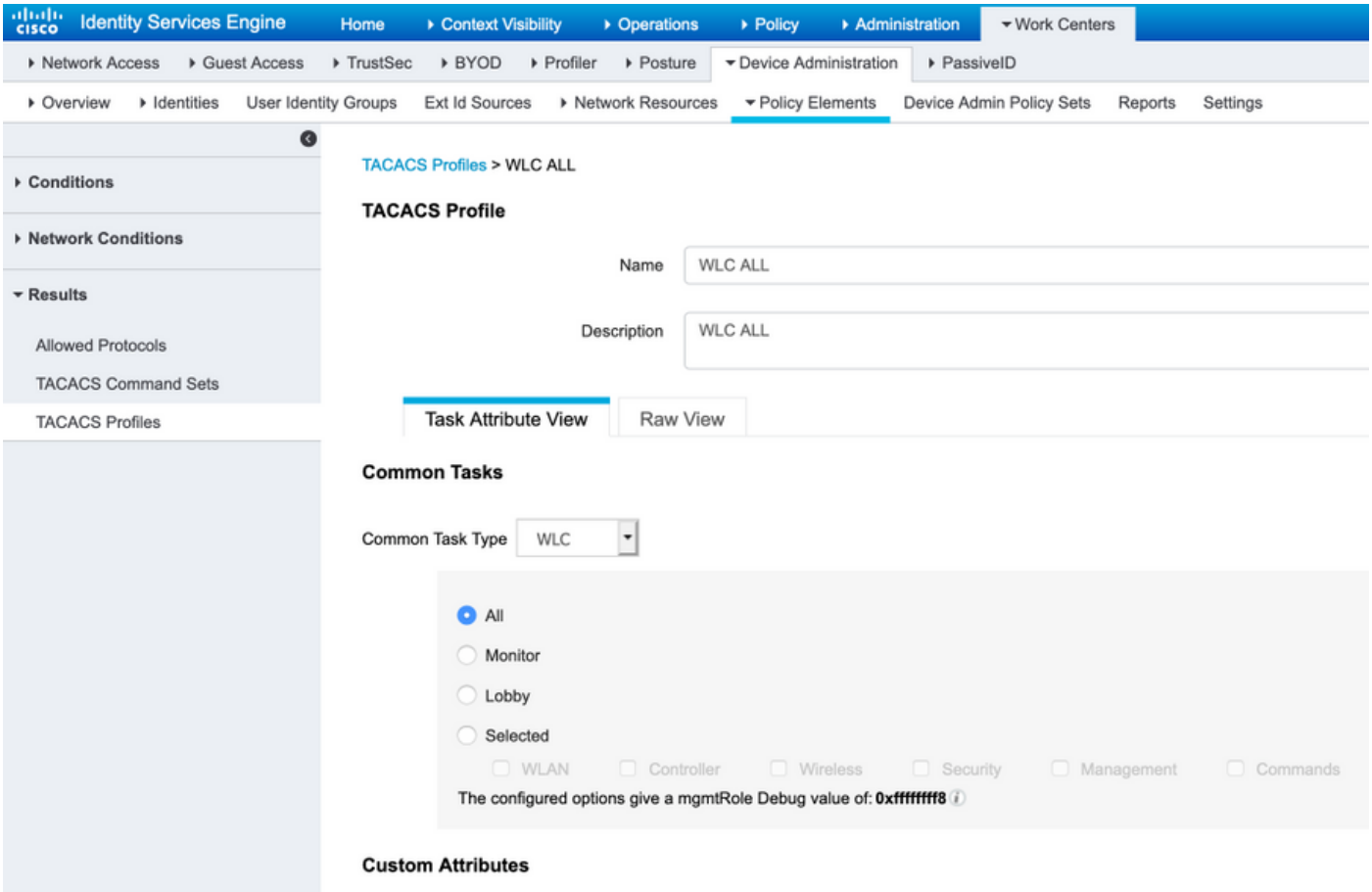


Étape 5. Créez un profil TACACS pour WLC.

Accédez à **Centres de travail > Administration des périphériques > Éléments de stratégie > Résultats > Profils TACACS.** Cliquez sur **Ajouter et** indiquez un **nom.** Dans l'onglet **Affichage des attributs de tâche**, sélectionnez **WLC** pour **Common Task Type.** Il existe des profils par défaut à partir desquels sélectionner **Monitor** pour autoriser un accès limité aux utilisateurs, comme l'illustre l'image.

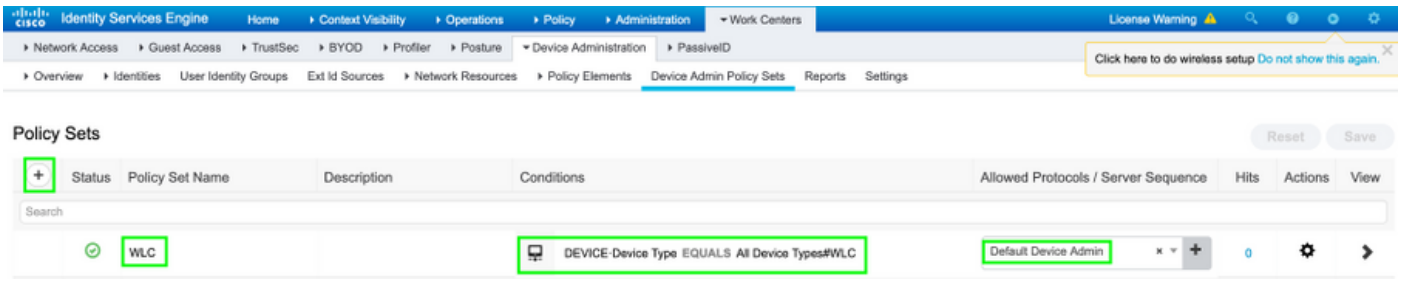


Il existe un autre profil par défaut **All** qui permet un accès complet à l'utilisateur comme illustré dans l'image.



Étape 6. Créer un jeu de stratégies.

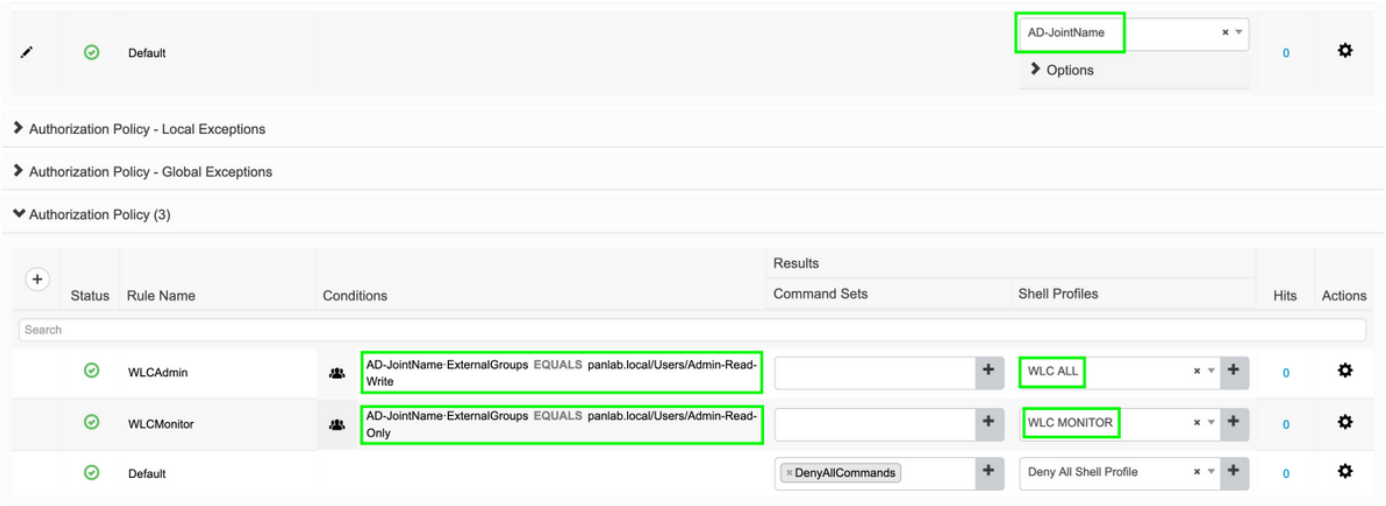
Accédez à **Centres de travail > Administration de périphériques > Jeux de stratégies d'administration de périphériques.** Cliquez sur **(+)** et donnez un nom au jeu de stratégies. Dans la condition de stratégie, sélectionnez **Type de périphérique** en tant que WLC, les protocoles autorisés peuvent être **Default Device Admin**, comme l'illustre l'image.



Étape 7. Créez des stratégies d'authentification et d'autorisation.

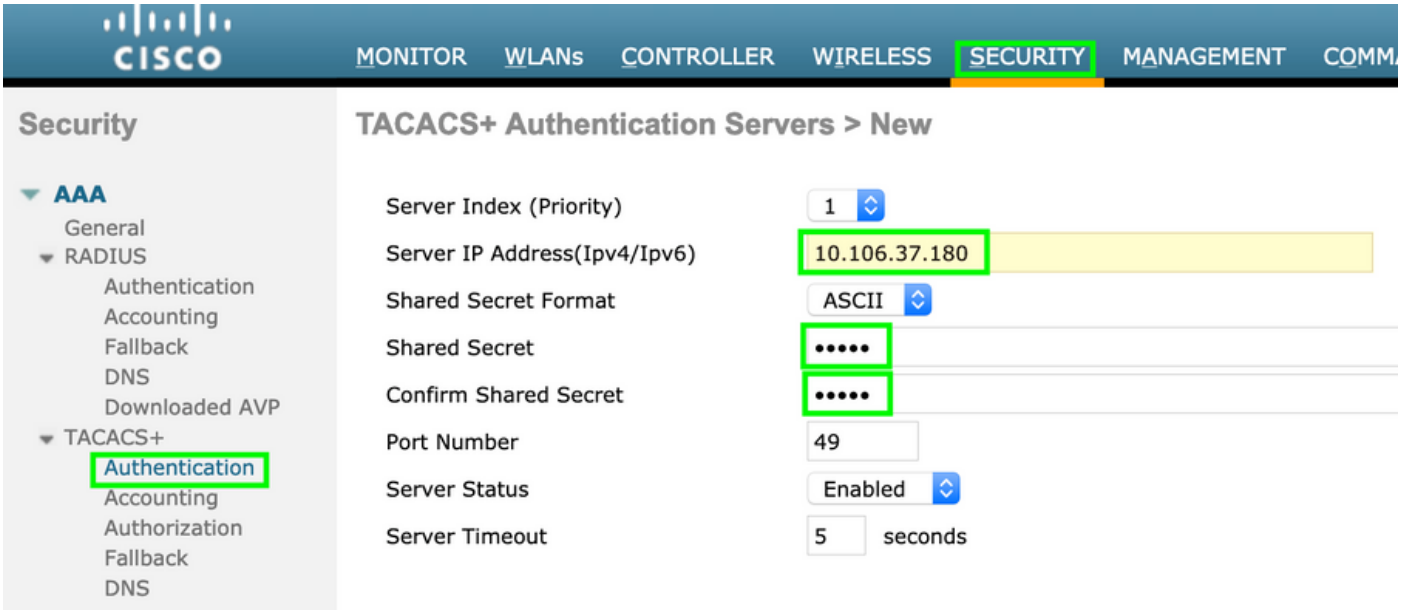
Dans ce document, deux groupes d'exemples **Admin-Read-Write** et **Admin-Read-Only** sont configurés sur le répertoire Active et un utilisateur dans chaque groupe **admin1**, **admin2** respectivement. Active Directory est intégré à l'ISE via un point d'accès appelé **AD-JointName.**

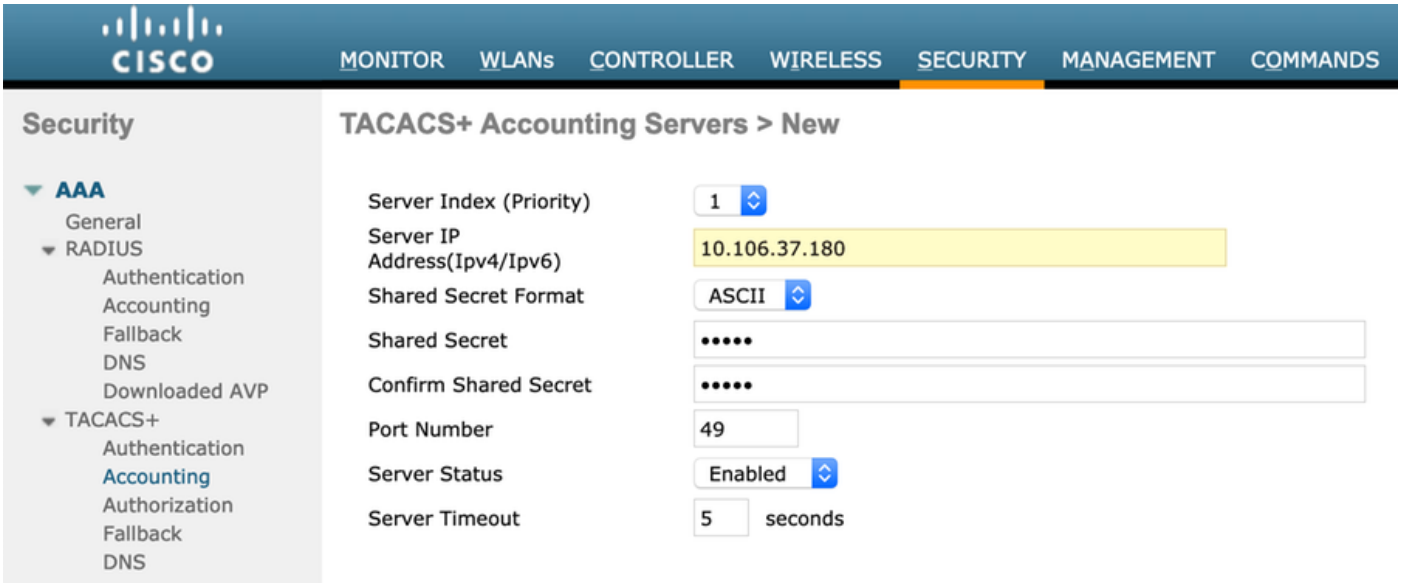
Créez deux stratégies d'autorisation, comme l'illustre l'image :



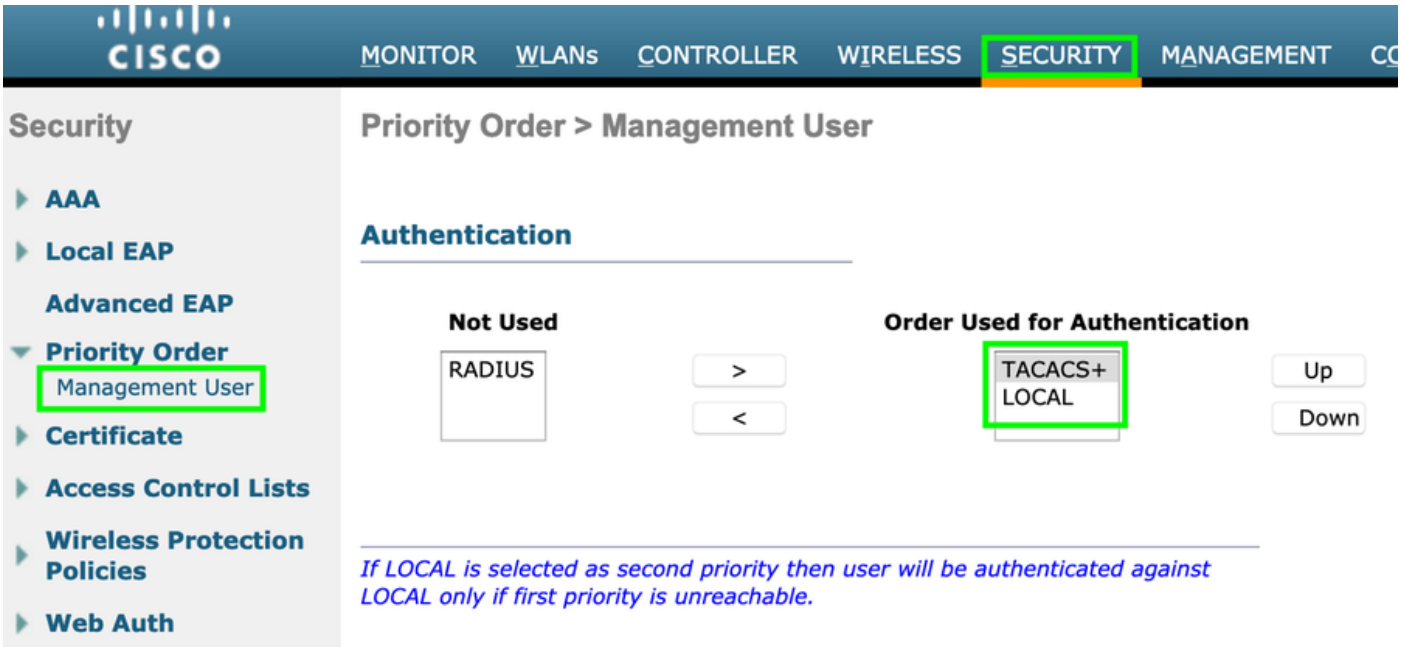
Étape 8. Configurez le WLC pour l'administration des périphériques.

Naviguez jusqu'à **Security > AAA > TACACS+** cliquez sur **New** et ajoutez Authentication, Accounting server, comme illustré dans l'image.





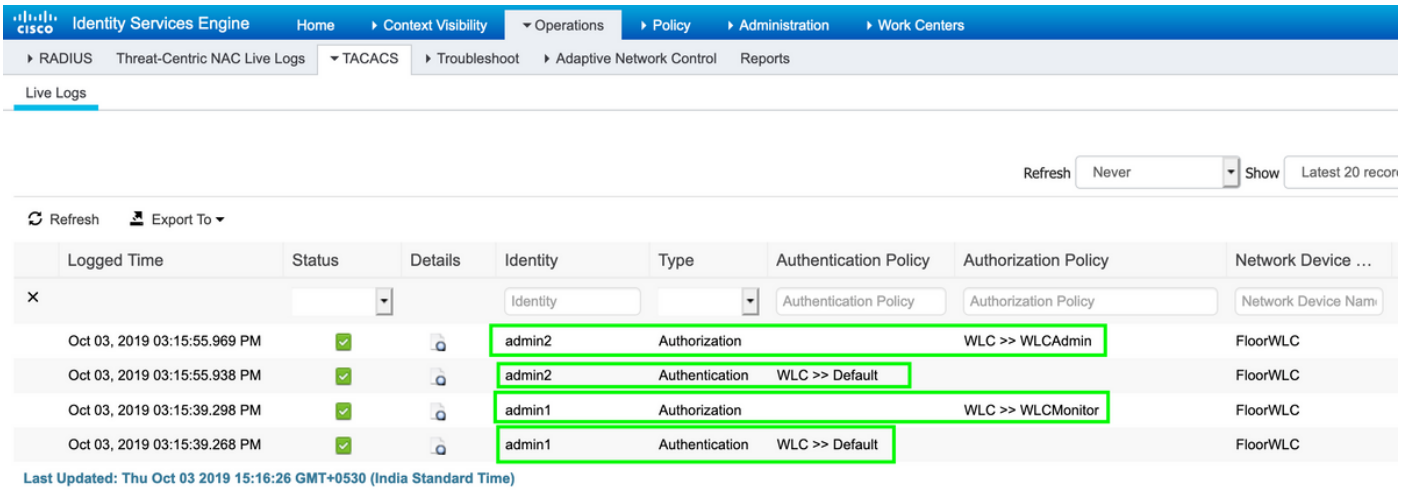
Modifiez l'ordre de priorité et placez TACACS+ en haut et Local en bas, comme illustré dans l'image :



Attention : Ne fermez pas la session GUI actuelle du WLC. Il est recommandé d'ouvrir l'interface graphique du WLC dans un navigateur Web différent et de vérifier si la connexion avec les informations d'identification TACACS+ fonctionne ou non. Dans le cas contraire, vérifiez la configuration et la connectivité au noeud ISE sur le port TCP 49.

Vérification

Accédez à **Opérations > TACACS > Journaux en direct** et surveillez les **Journaux en direct**. Ouvrez l'interface utilisateur graphique du WLC et connectez-vous avec les informations d'identification de l'utilisateur Active Directory, comme illustré dans l'image



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.