Intégration de CSM TACACS à ISE

Contenu

Introduction

Ce document décrit la procédure d'intégration de Cisco Security Manager (CSM) avec Identity Services Engine (ISE) pour l'authentification des utilisateurs administrateurs avec le protocole TACACS+.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Security Manager (CSM).
- Identity Services Engine (ISE).
- protocole TACACS.

Components Used

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

- Serveur CSM version 4.22
- ISE version 3.0

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

Par défaut, Cisco Security Manager (CSM) utilise un mode d'authentification appelé CiscoWorks pour authentifier et autoriser les utilisateurs localement, afin d'avoir une méthode d'authentification centralisée que vous pouvez utiliser Cisco Identity Service Engine via le protocole TACACS.

Configuration

Diagramme du réseau

Procédure d'authentification

Étape 1.Connectez-vous à l'application CSM avec les informations d'identification de l'utilisateur Admin.

Étape 2. Le processus d'authentification se déclenche et ISE valide les informations d'identification localement ou via Active Directory.

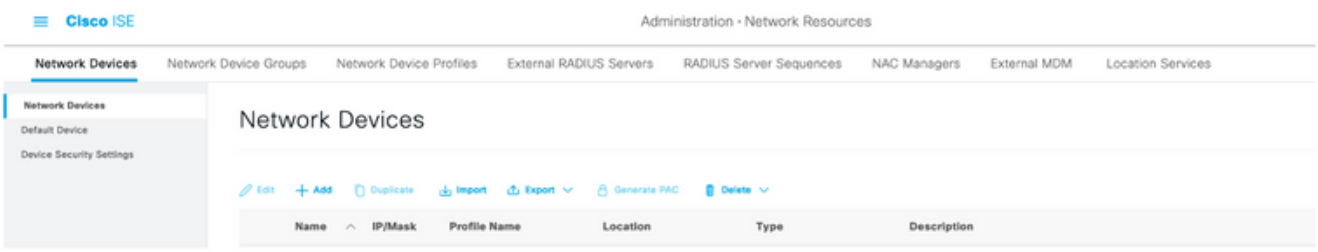
Étape 3. Une fois l'authentification réussie, ISE envoie un paquet d'autorisation pour autoriser l'accès au CSM.

Étape 4. CSM mappe le nom d'utilisateur avec l'affectation du rôle d'utilisateur local.

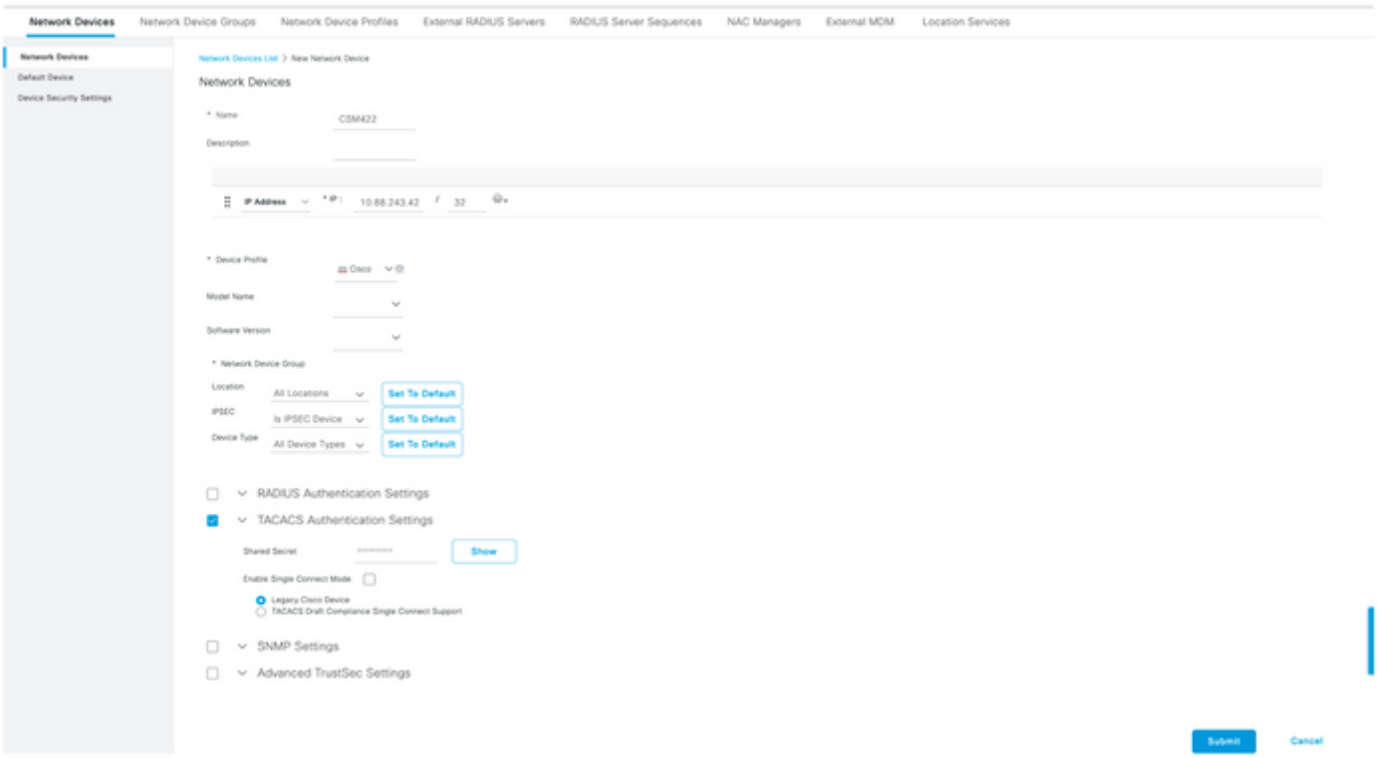
Étape 5. ISE affiche un journal en direct d'authentification réussi.

Configuration ISE

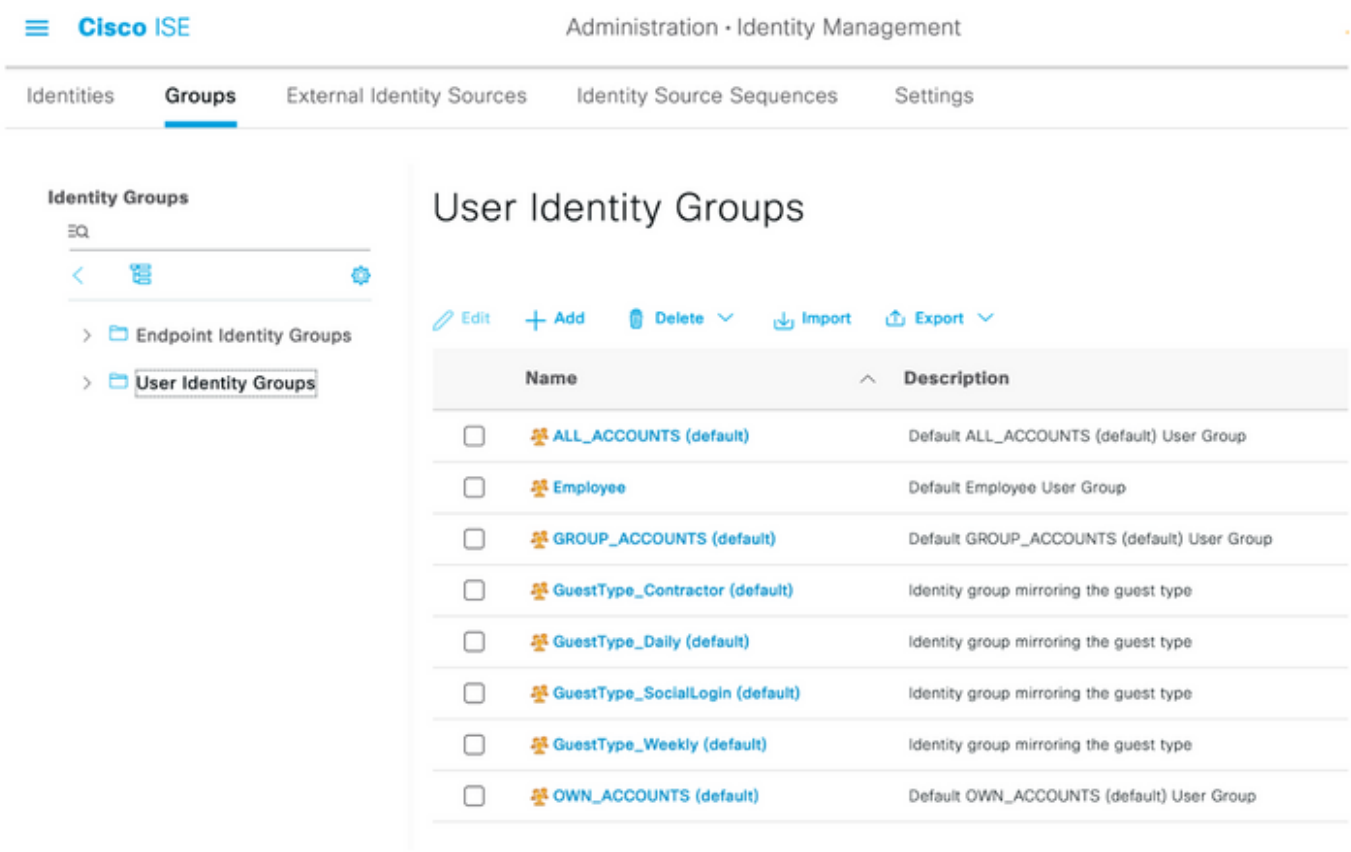
Étape 1. Sélectionner l'icône des trois lignes situé dans le coin supérieur gauche et accédez à **Administration > Network Resources > Network Devices.**



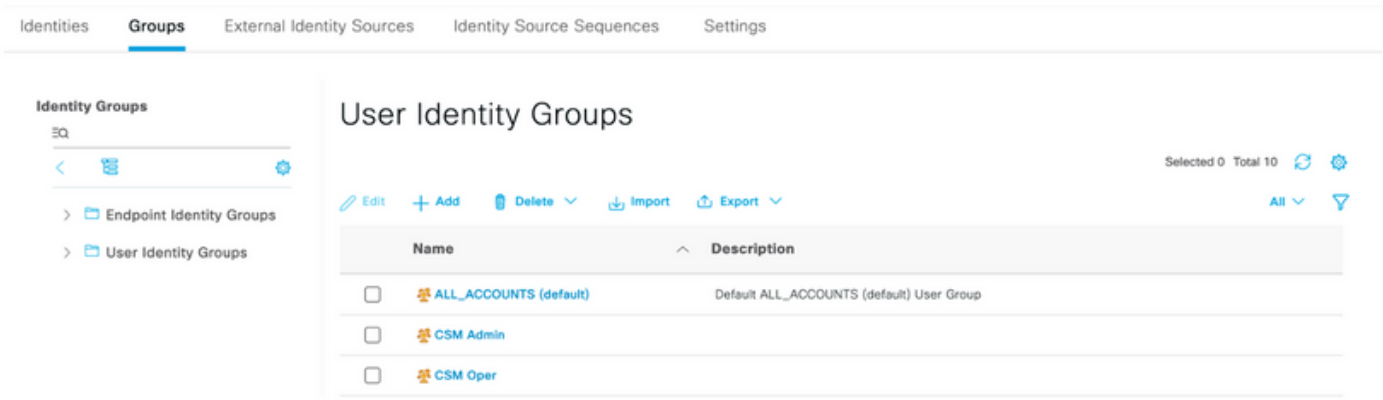
Étape 2. Cliquez sur le bouton **+Ajouter** et entrez les valeurs appropriées pour le nom du périphérique d'accès réseau et l'adresse IP, puis vérifiez la case **TACACS Authentication Settings** et définissez un secret partagé. Sélectionnez le bouton **Soumettre**.



Étape 3. Sélectionner l'icône des trois lignes situé dans le coin supérieur gauche et accédez à **Administration > Identity Management > Groups.**

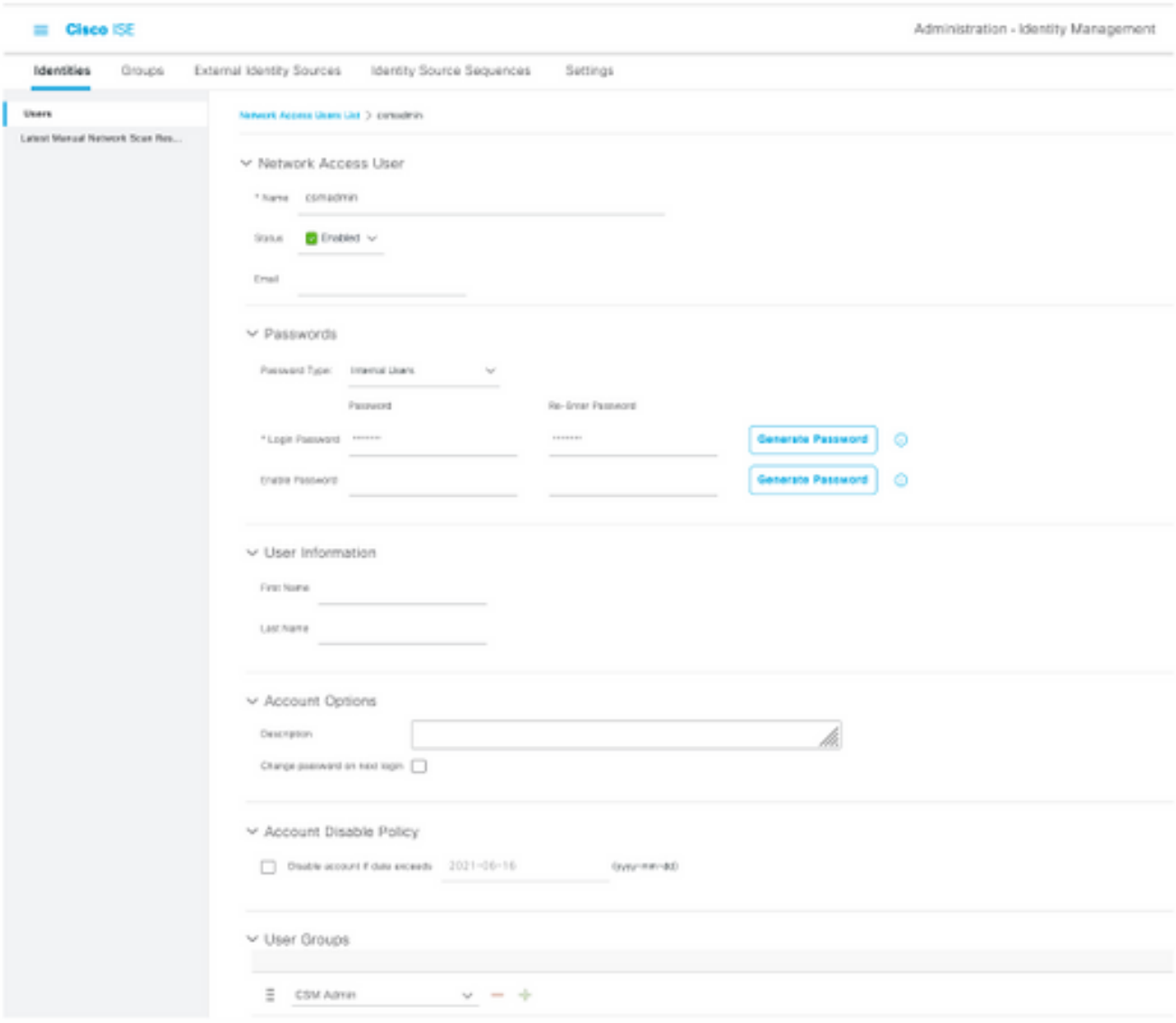


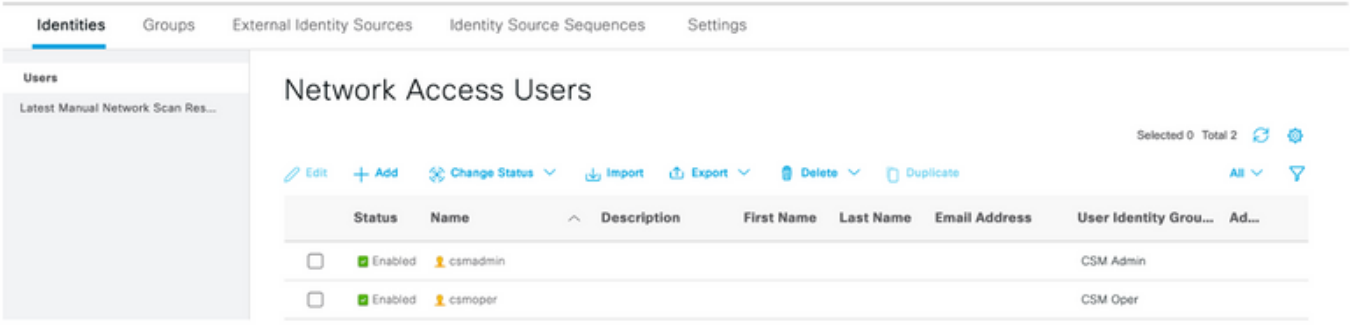
Étape 4. Accédez au dossier **Groupes d'identités utilisateur** et sélectionnez le bouton **+Ajouter**. Définissez un nom et sélectionnez le bouton **Soumettre**.



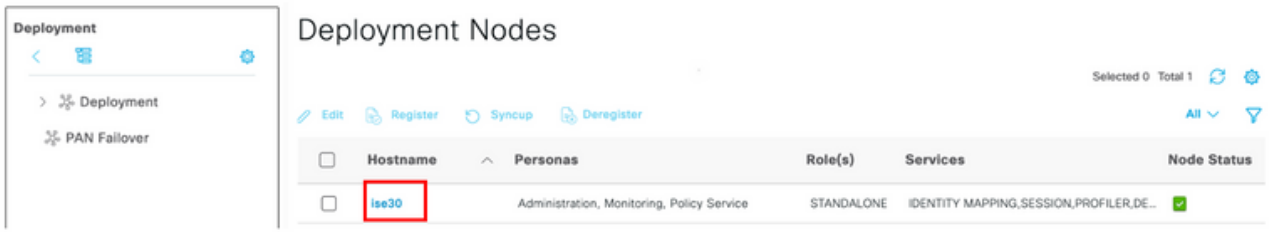
Note: Cet exemple montre comment créer des groupes CSM Admin et CSM Oper Identity. Vous pouvez répéter l'étape 4 pour chaque type d'utilisateurs Admin sur CSM

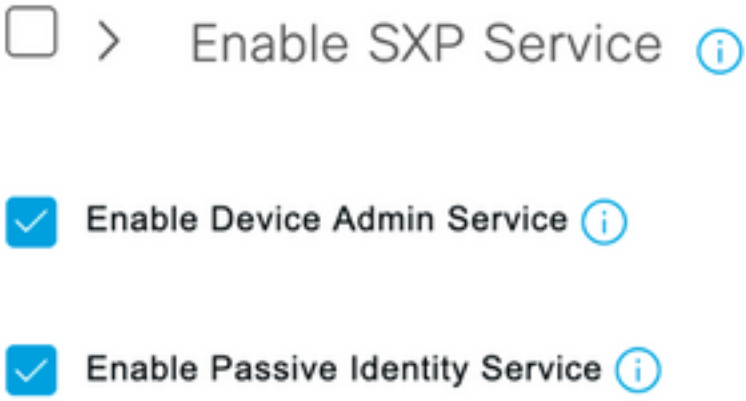
Étape 5. Sélectionner l'icône des trois lignes et accédez à **Administration > Identity Management > Identities.** Cliquez sur le bouton **+Ajouter** et définissez le nom d'utilisateur et le mot de passe, puis sélectionnez le groupe auquel appartient l'utilisateur. Dans cet exemple, crée les utilisateurs **csmadmin** et **csmoper** et affectés respectivement aux groupes CSM Admin et CSM Oper.





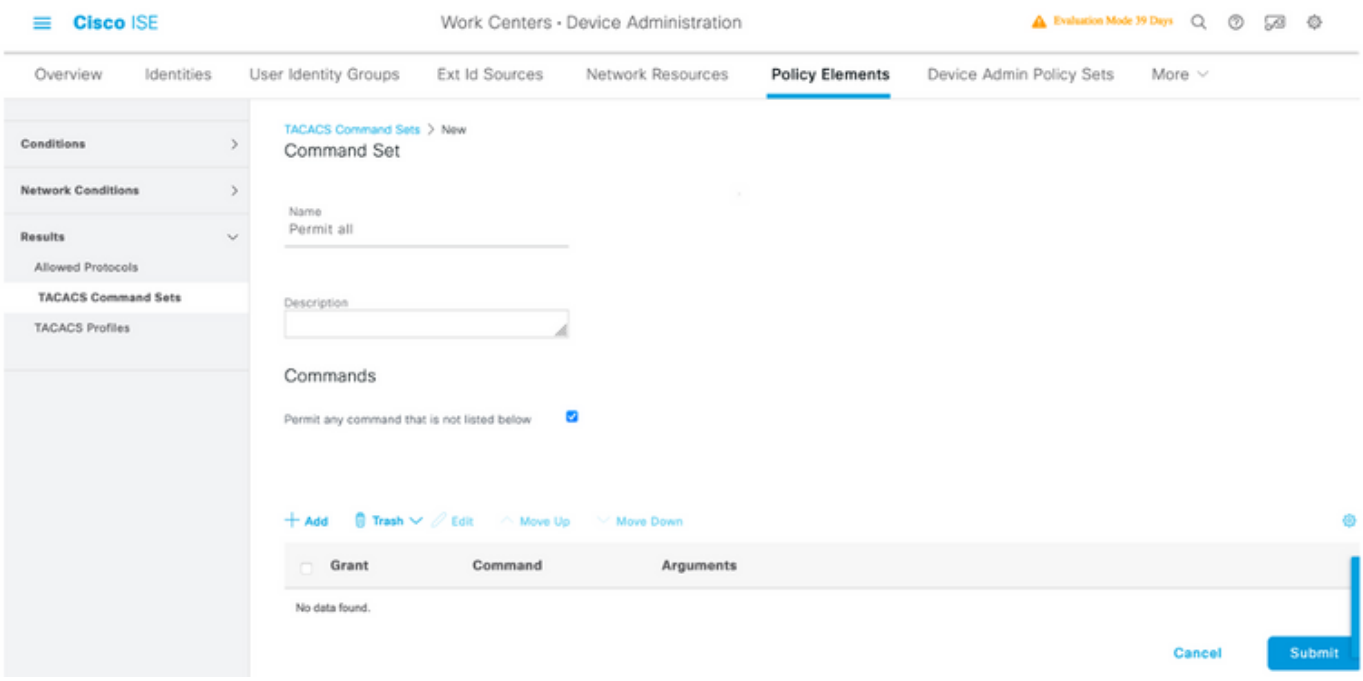
Étape 6. Sélectionner et accédez à **Administration > System > Deployment.** Sélectionnez le noeud de nom d'hôte et activez le **service d'administration de périphérique**





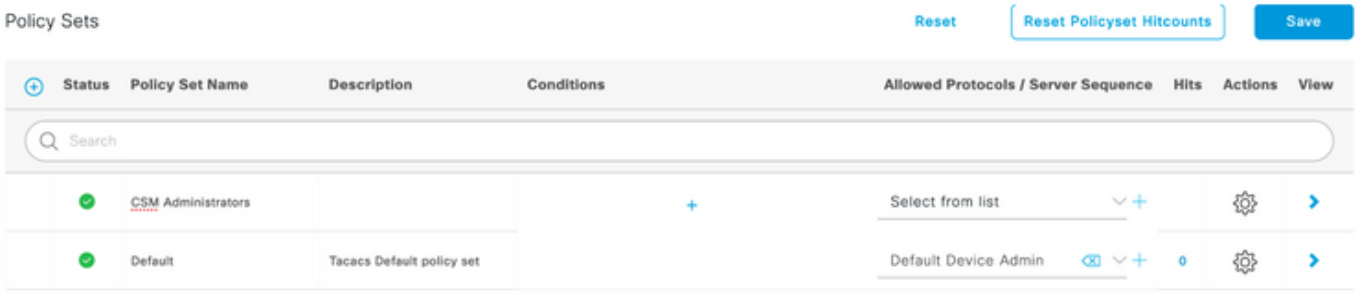
Note: En cas de déploiement distribué, sélectionnez le noeud PSN qui gère les requêtes TACACS.

Étape 7. Sélectionnez l'icône des trois lignes et accédez à **Administration > Device Administration > Policy Elements.** Accédez à **Résultats > Jeux de commandes TACACS.** Cliquez sur le bouton **+Ajouter,** définissez un nom pour le jeu de commandes et activez la **commande Permit any qui n'est pas répertoriée sous** la case à cocher. Sélectionnez **Submit.**

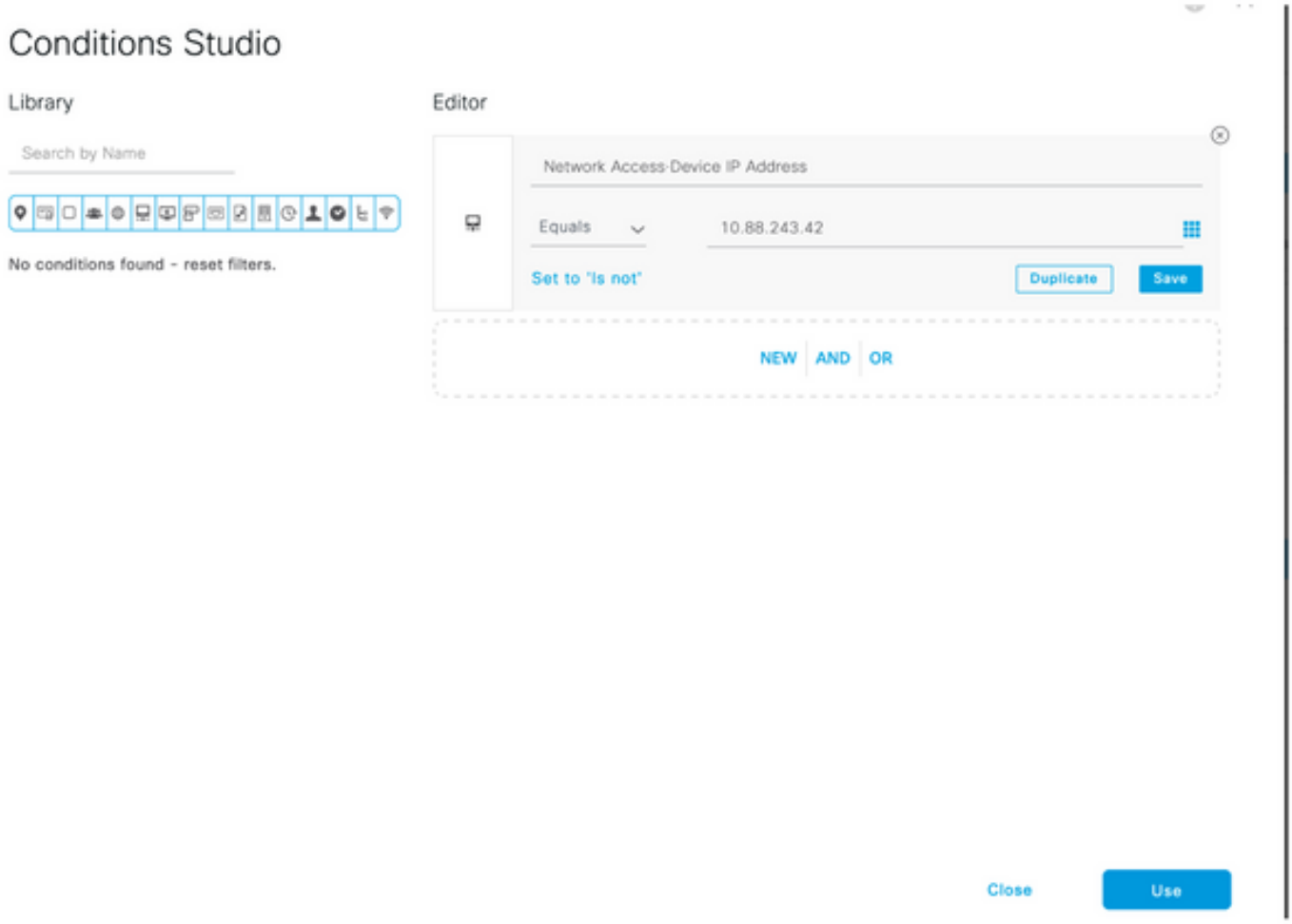


Étape 8. Sélectionnez l'icône de trois lignes située dans le coin supérieur gauche et accédez à

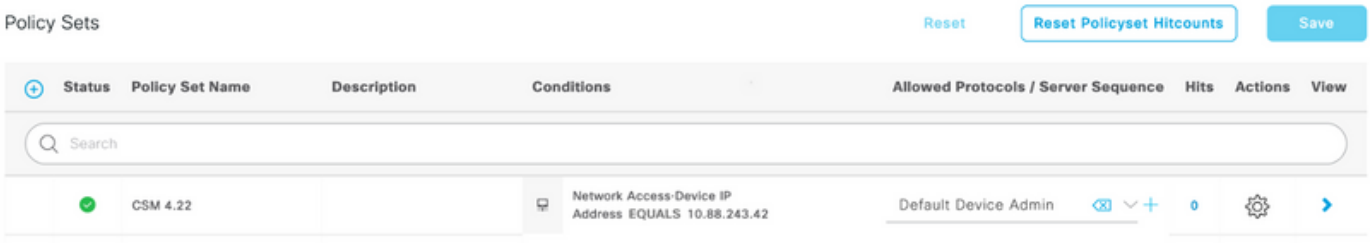
Administration->Administration des périphériques->Jeux de stratégies d'administration des périphériques. Sélectionner  situé sous le titre Jeux de stratégies, définissez un nom et sélectionnez le bouton **+** au milieu pour ajouter une nouvelle condition.



Étape 9. Sous Condition, sélectionnez Ajouter un attribut, puis sélectionnez **Network Device** Icon, suivi de Network Access device IP address. Sélectionnez **Attribute Value** et ajoutez l'adresse IP CSM. Sélectionnez **Utiliser** une fois terminé.



Étape 10. Dans la section Allow protocols, sélectionnez **Device Default Admin**. Sélectionnez Save (enregistrer)



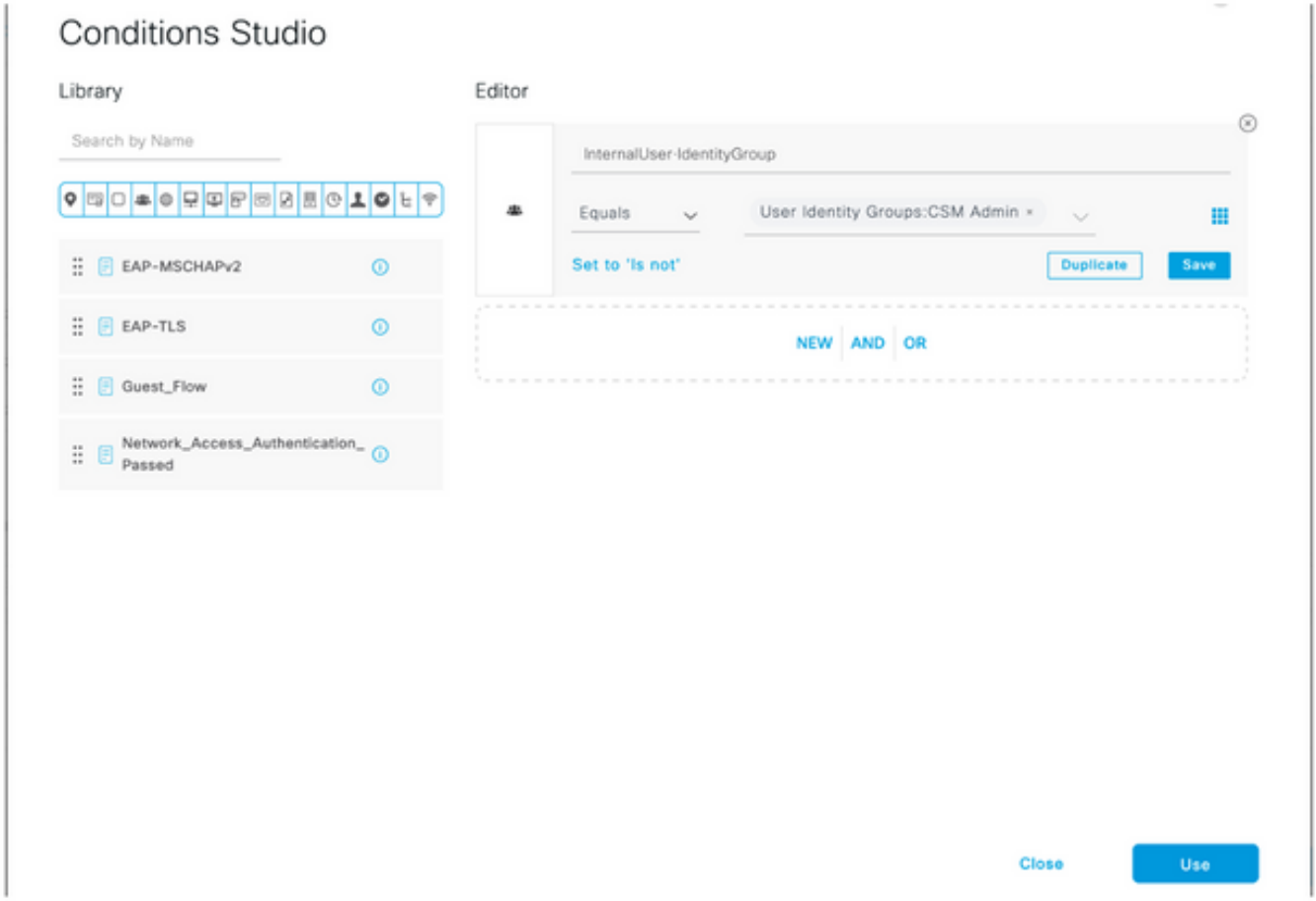
Étape 11. Sélectionner la flèche droite icône du jeu de stratégies pour définir les stratégies d'authentification et d'autorisation

Étape 12. Sélectionner situé sous le titre de la stratégie d'authentification, définissez un nom et sélectionnez le + au milieu pour ajouter une nouvelle condition. Sous Condition, sélectionnez Ajouter un attribut, puis sélectionnez **Network Device** Icon, suivi de Network Access device IP address. Sélectionnez **Attribute Value** et ajoutez l'adresse IP CSM. Sélectionner **Utiliser** une fois terminé

Étape 13. Sélectionnez **Utilisateurs internes** comme magasin d'identité et sélectionnez **Enregistrer**

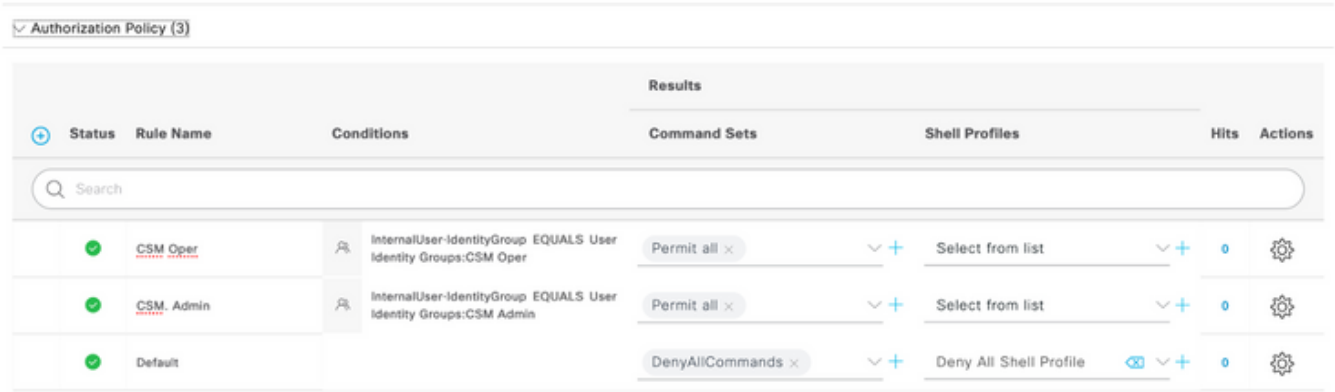
Note: Le magasin d'identités peut être modifié en magasin AD si ISE est joint à Active Directory.

Étape 14. Sélectionner situé sous le titre de la stratégie d'autorisation, définissez un nom et sélectionnez le bouton **+** au milieu pour ajouter une nouvelle condition. Sous la fenêtre Condition, sélectionnez Ajouter un attribut, puis sélectionnez **l'**icône **Groupe d'identités** suivie de **Utilisateur interne : Groupe d'identités.** Sélectionnez le groupe d'administration CSM et sélectionnez **Utiliser**.



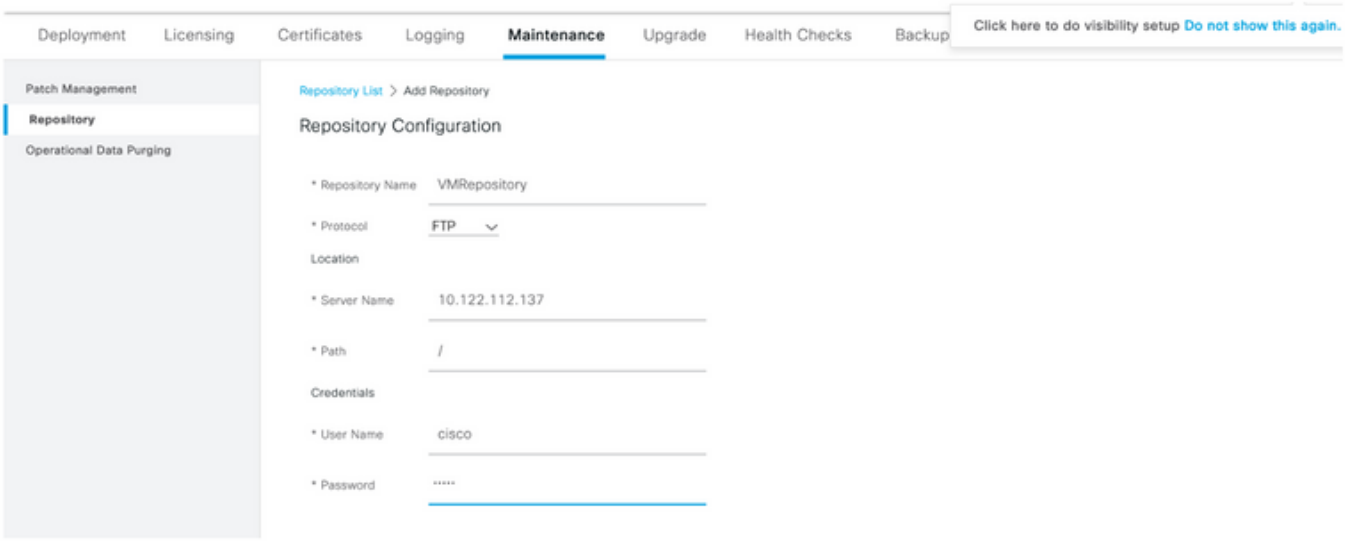
Étape 15. Sous Jeu de commandes, sélectionnez Autoriser tout jeu de commandes créé à l'étape 7, puis sélectionnez **Enregistrer**

Répétez les étapes 14 et 15 pour le groupe CSM Oper



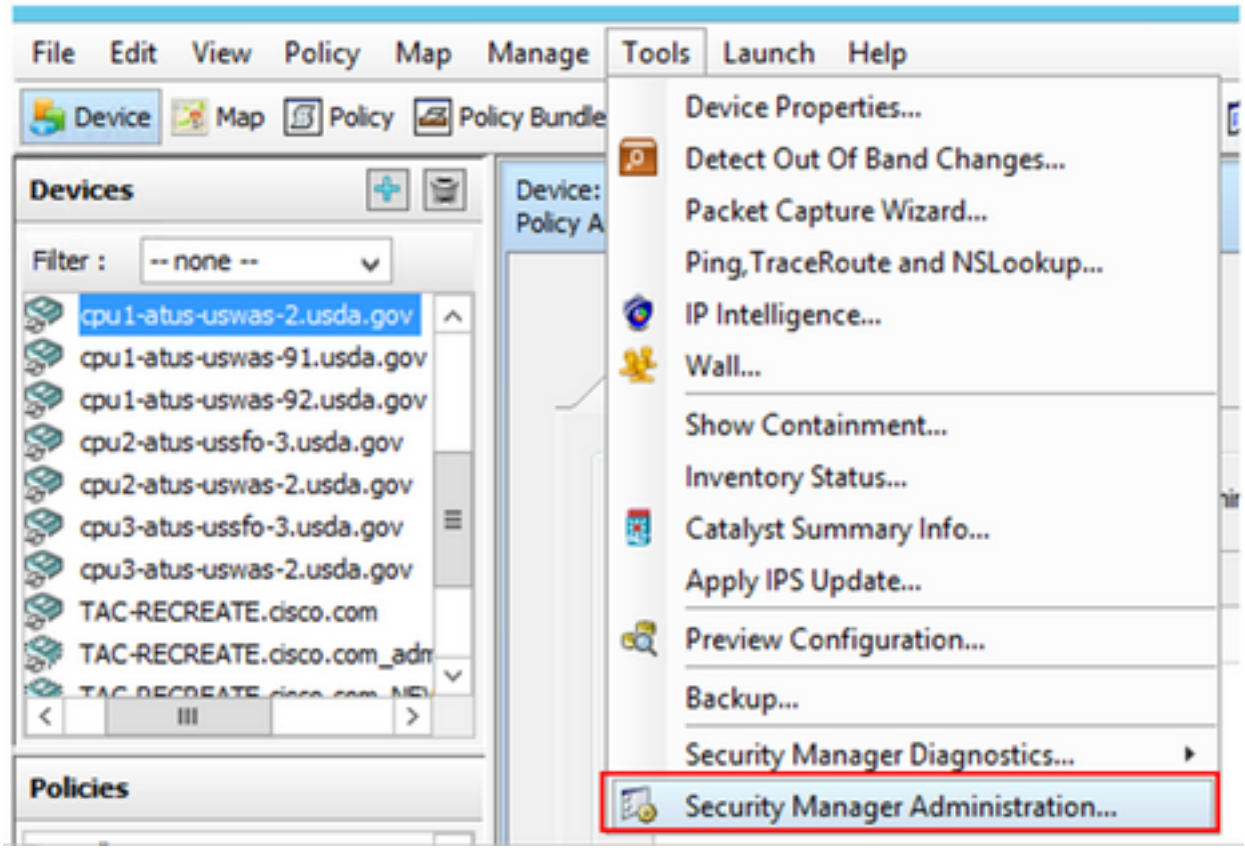
Étape 16 (Facultatif). Sélectionnez l'icône de trois lignes située dans le coin supérieur gauche et sélectionnez **Administration>Système>Maintenance>Référentiel**, sélectionnez **+Ajouter** pour ajouter un référentiel utilisé pour stocker le fichier de vidage TCP à des fins de dépannage.

Étape 17 (Facultatif). Définissez un nom de référentiel, un protocole, un nom de serveur, un chemin d'accès et des informations d'identification. Sélectionnez **Soumettre** une fois terminé.

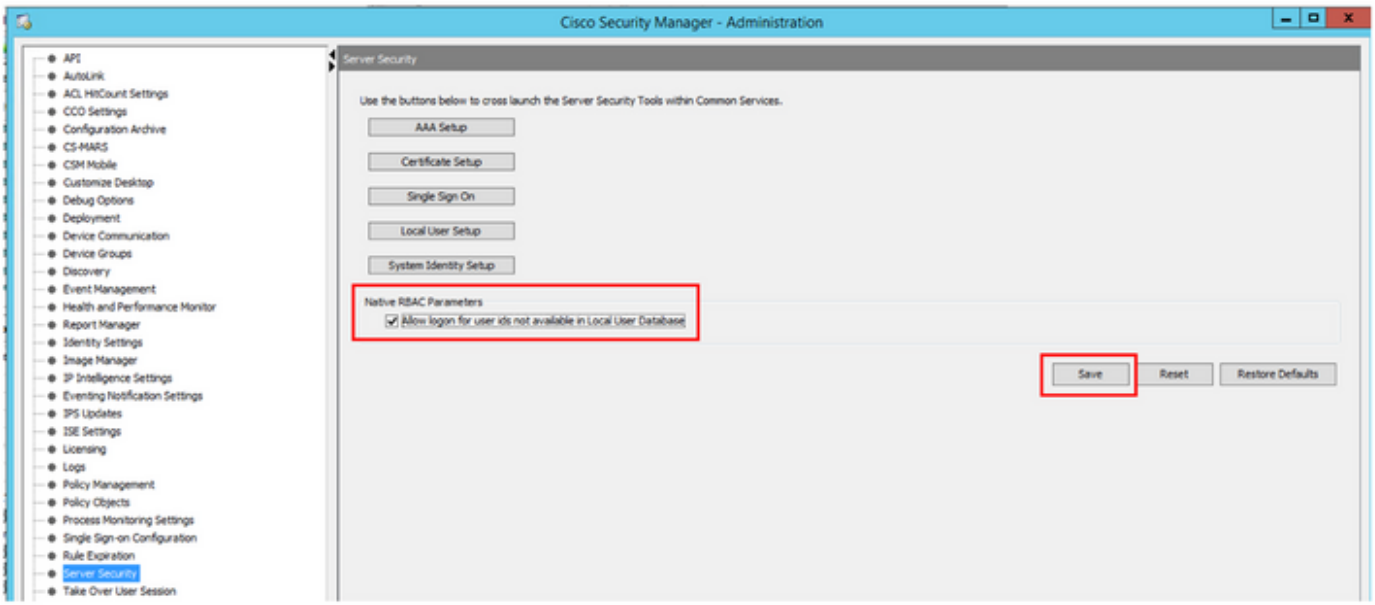


Configuration CSM

Étape 1. Connectez-vous à l'application Client Cisco Security Manager avec le compte d'administrateur local. Dans le menu, accédez à **Outils > Administration de Security Manager**



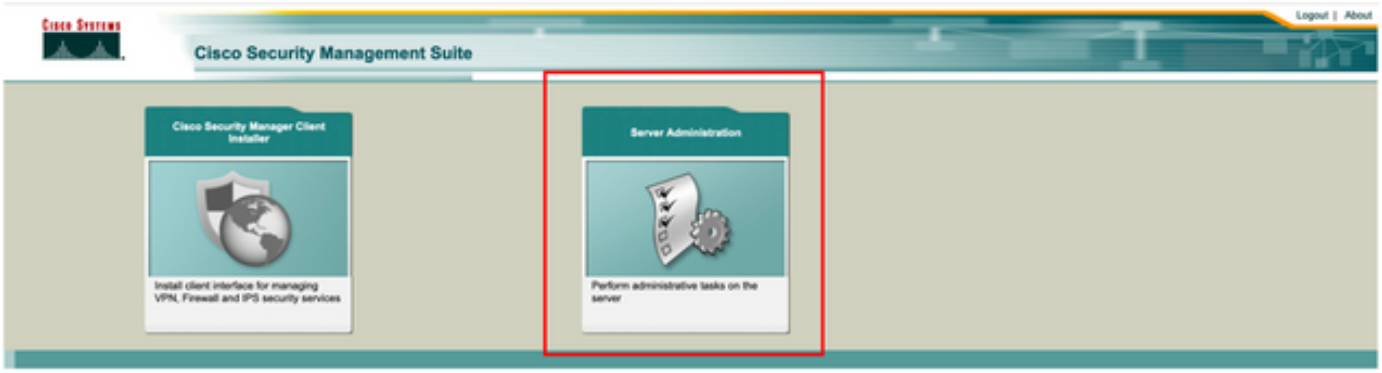
Étape 2. Cochez la case sous **Paramètres RBAC natifs.** Sélectionnez **Enregistrer** et **Fermer**



Étape 3. Dans le menu, sélectionnez **Fichier > Soumettre. Fichier > Soumettre.**

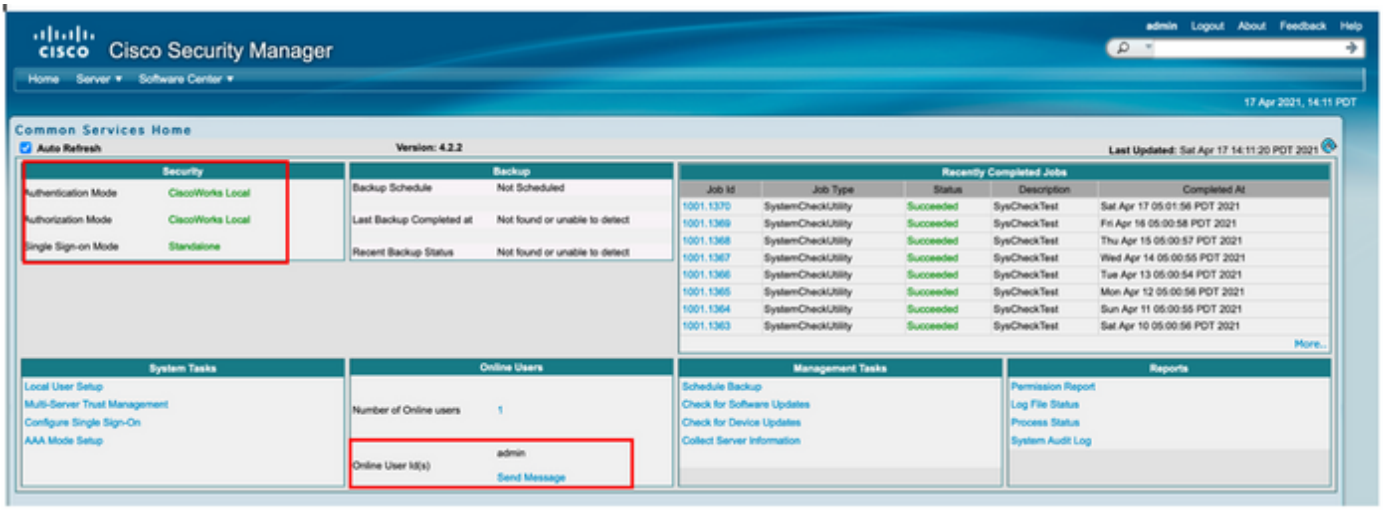
> **Note**: Toutes les modifications doivent être enregistrées, en cas de modifications de configuration, elles doivent être soumises et déployées.

Étape 4. Accédez à CSM Management UI et tapez https://<enter_CSM_IP_Address et sélectionnez **Administration du serveur.**



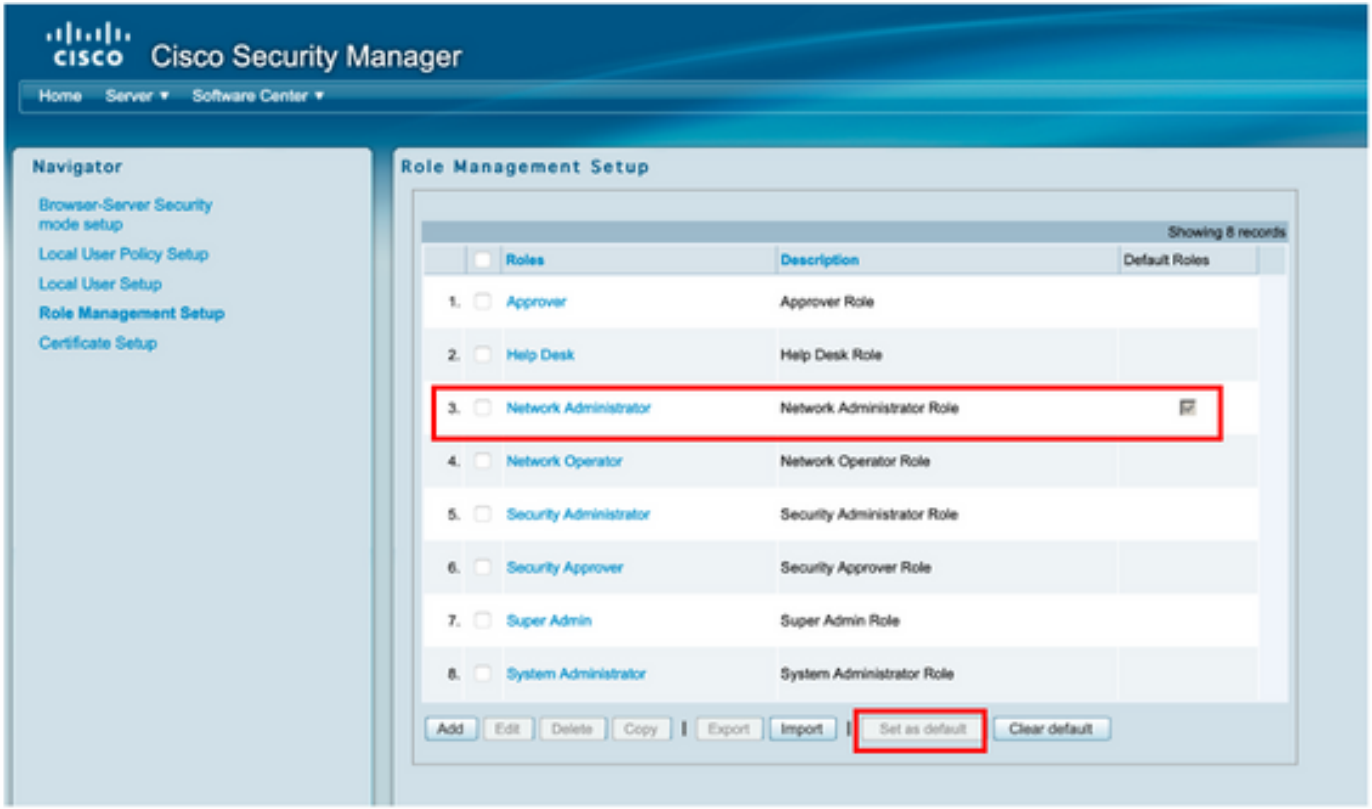
Note: Les étapes 4 à 7 montrent la procédure permettant de définir le rôle par défaut de tous les administrateurs qui ne sont pas définis sur ISE. Ces étapes sont facultatives.

Étape 5. Valider le mode d'authentification est défini sur **CiscoWorks Local** et **Online** userID est le compte d'administrateur local créé sur CSM.



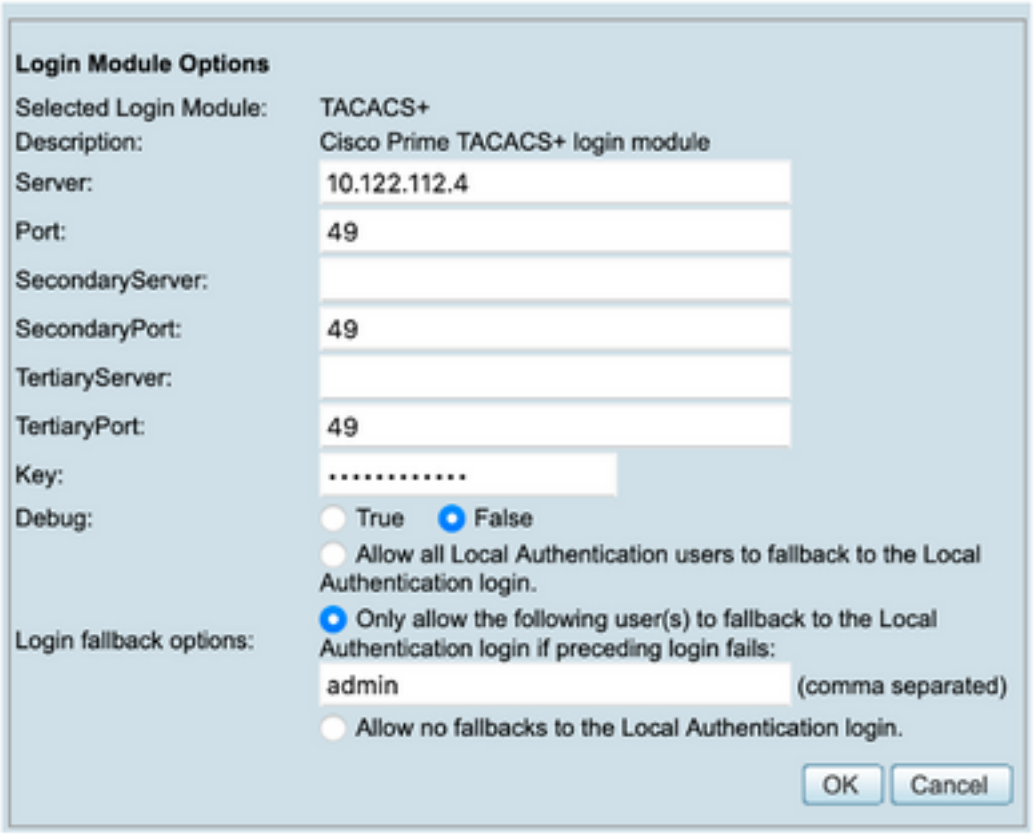
Étape 6. Accédez à **Serveur** et sélectionnez **Gestion à serveur unique**

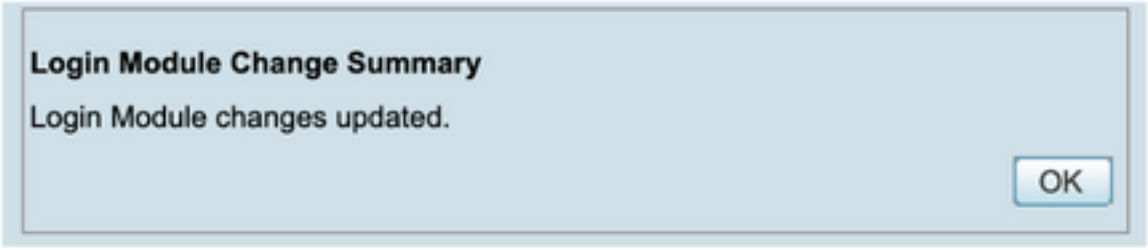
Étape 7. Sélectionnez Configuration de la gestion des rôles et sélectionnez le privilège par défaut que tous les utilisateurs admin reçoivent lors de l'authentification. Dans cet exemple, Network Administrator est utilisé. Une fois sélectionné, sélectionnez **défini par défaut.**



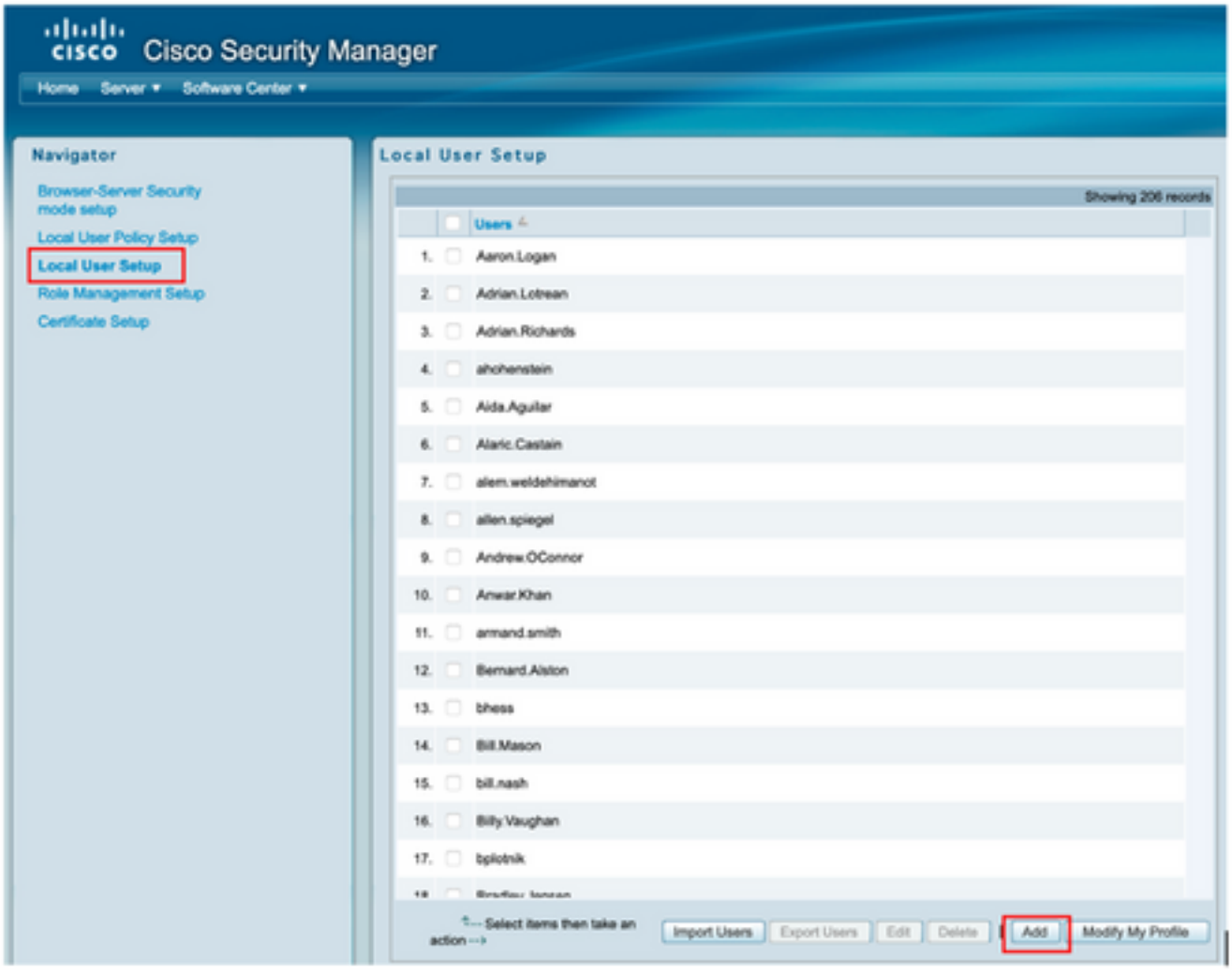
Étape 8. Sélectionnez **Serveur>Rôle de configuration du mode AAA**, puis sélectionnez **TACACS+**, enfin sélectionnez **modifier** pour ajouter des informations ISE.

Étape 9. Définissez l'adresse IP ISE et la clé, si vous le souhaitez, vous pouvez sélectionner l'option permettant d'autoriser tous les utilisateurs d'authentification locale ou un seul utilisateur si la connexion échoue**.** Dans cet exemple, l'utilisateur Only admin est autorisé comme méthode de secours. Sélectionnez **OK** pour enregistrer les modifications.

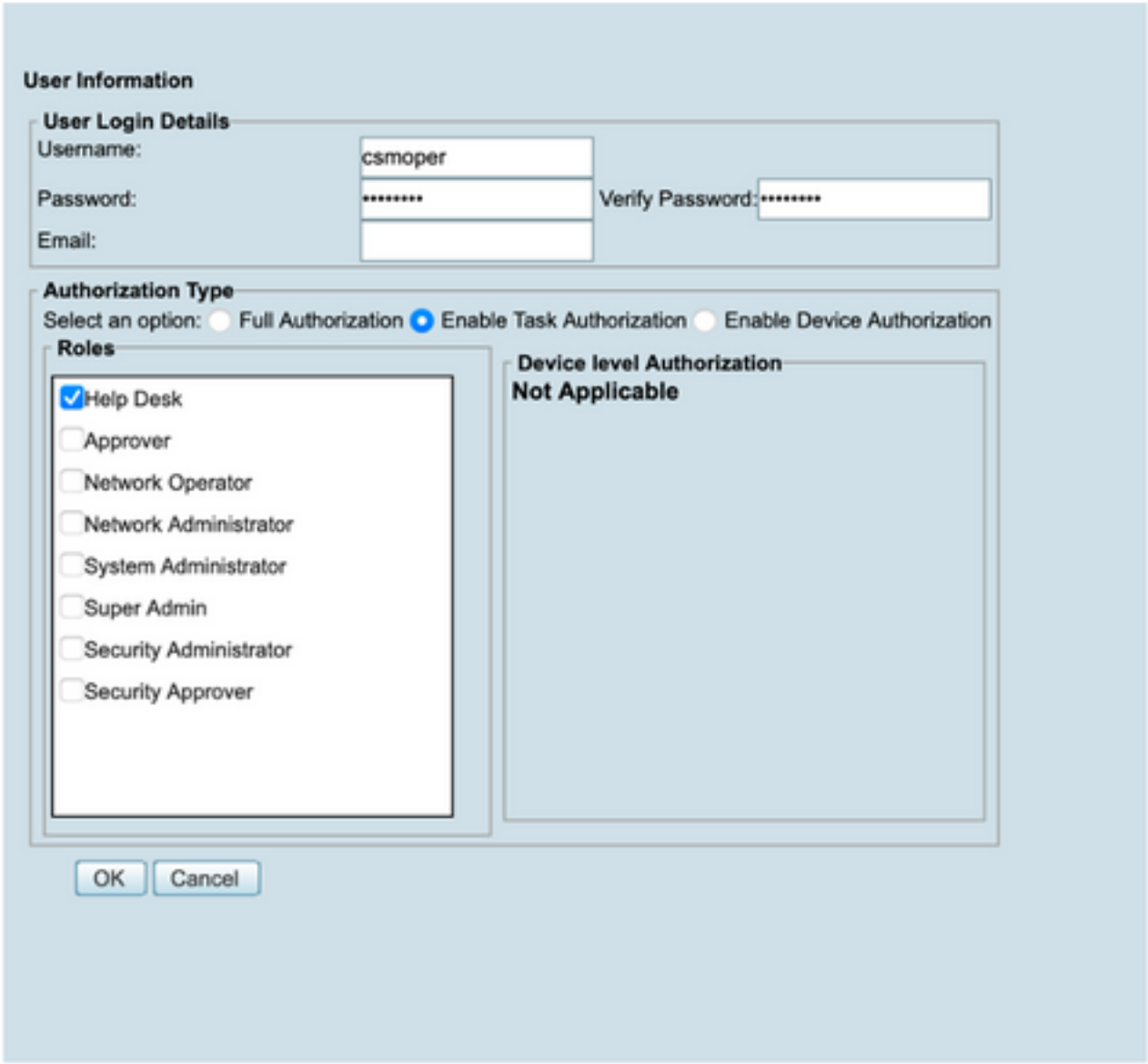




Étape 10. Sélectionnez **Server> Single Server Management**, puis sélectionnez **Local User Setup** et sélectionnez **Add.**



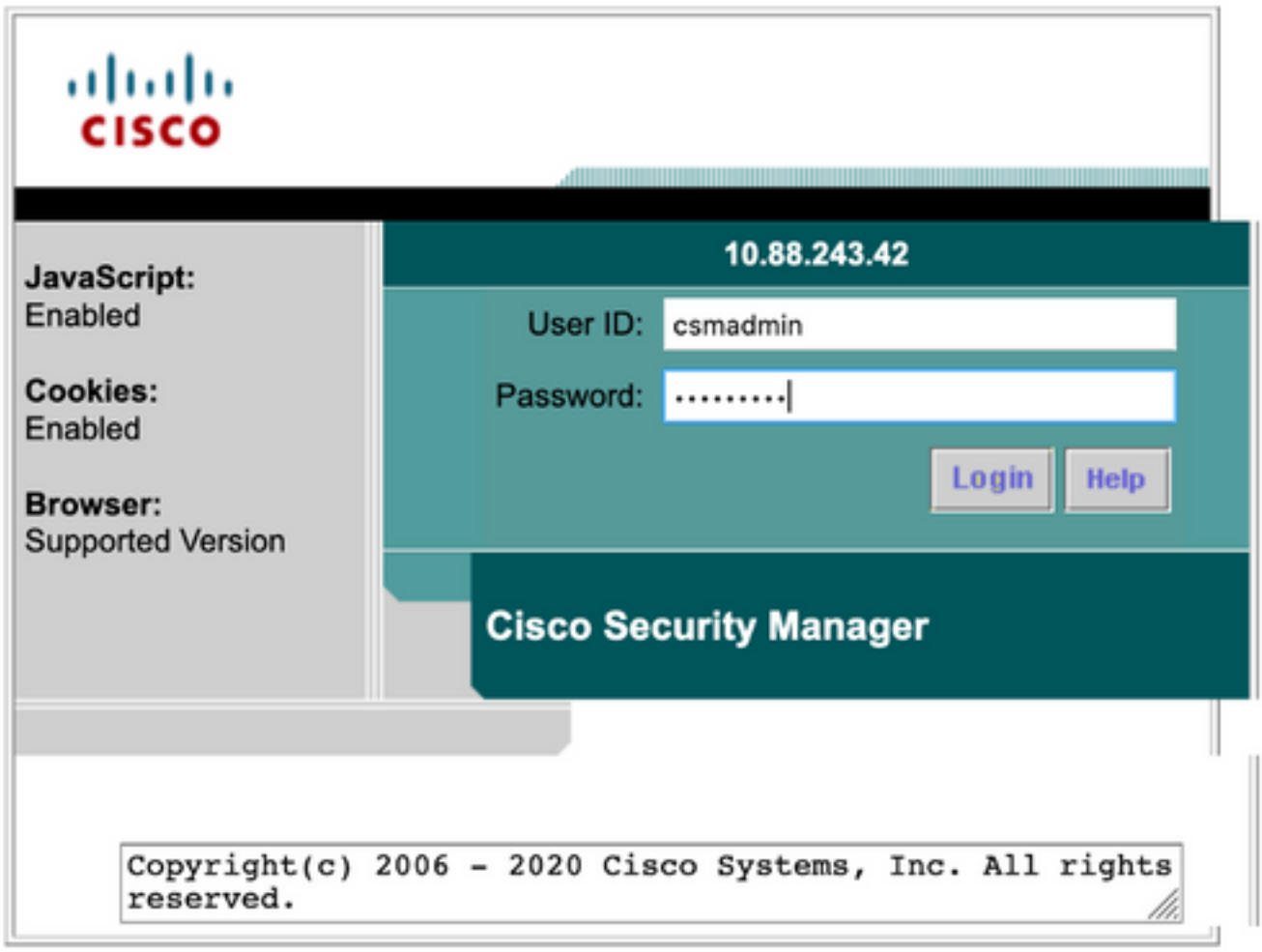
Étape 11. Définissez le même nom d'utilisateur et le même mot de passe créés sur ISE à l'étape 5 sous la section Configuration ISE, les **rôles csmoper** et d'**autorisation des tâches du centre d'assistance** sont utilisés dans cet exemple. Sélectionnez **OK** afin d'enregistrer l'utilisateur admin.



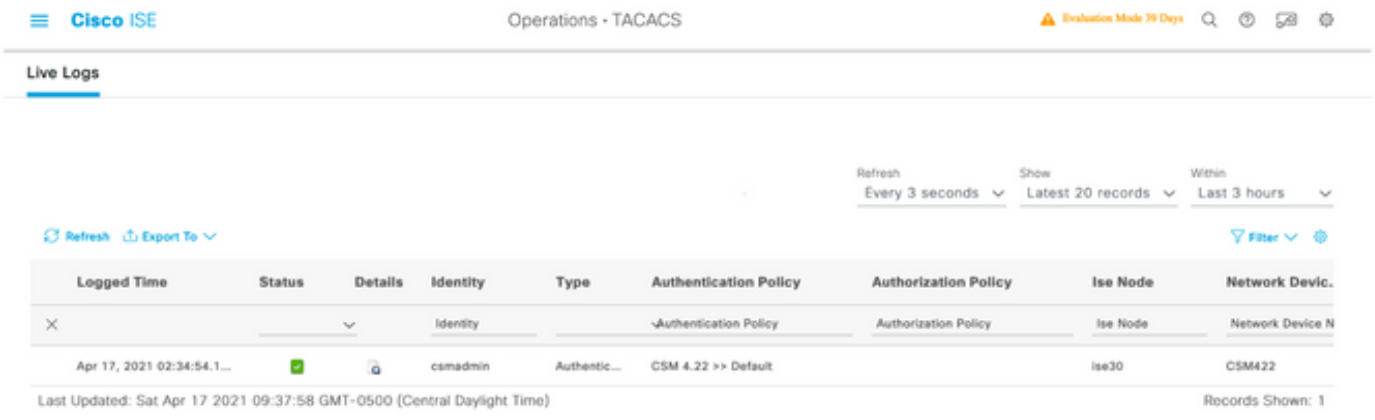
Vérification

Interface utilisateur du client Cisco Security Manager

Étape 1. Ouvrez un nouveau navigateur de fenêtre et tapez https://<enter_CSM_IP_Address, utilisez **csmadmin** nom d'utilisateur et mot de passe créés à l'étape 5 dans la section de configuration ISE.



La tentative de connexion réussie peut être vérifiée sur les journaux en direct ISE TACACS

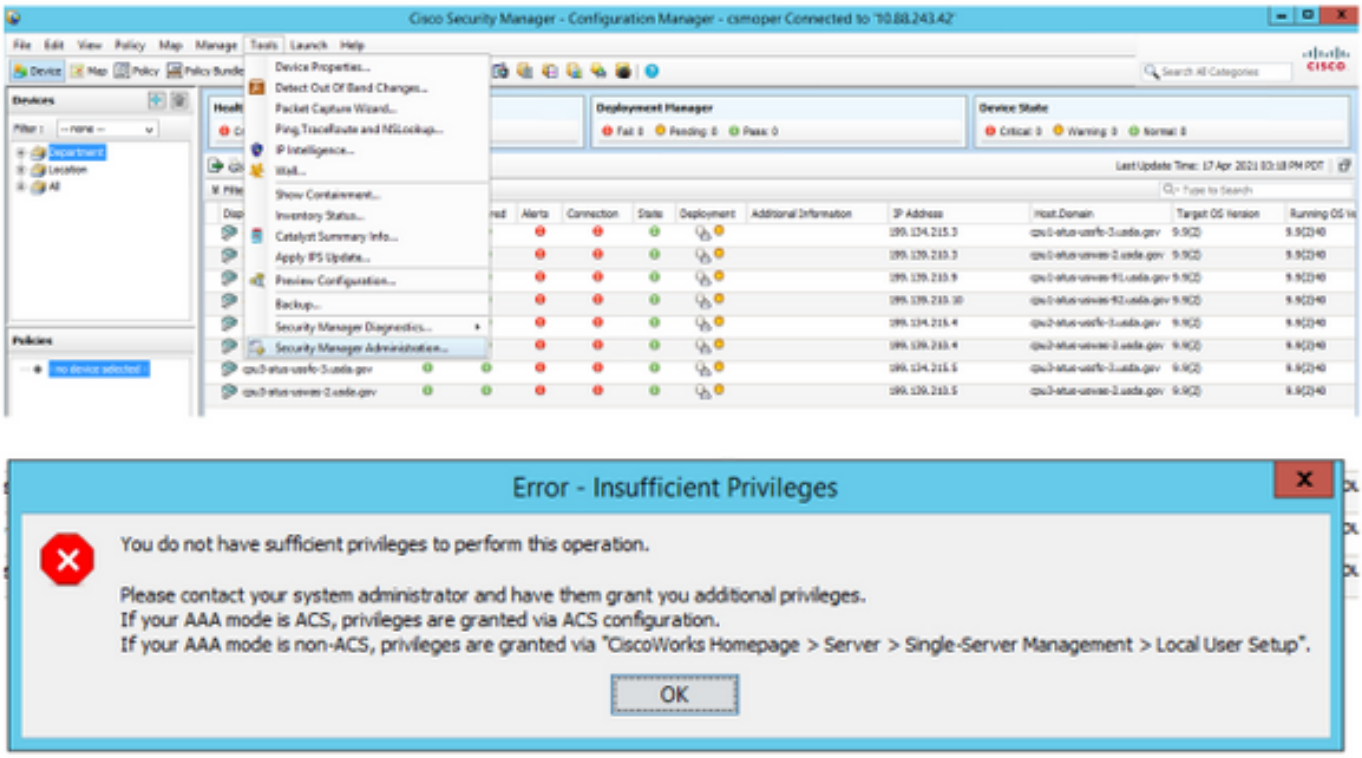


Application client Cisco Security Manager

Étape 1. Connectez-vous à l'application Client Cisco Security Manager avec le compte d'administration du centre d'assistance.

La tentative de connexion réussie peut être vérifiée sur les journaux en direct ISE TACACS

Étape 2. Dans le menu de l'application cliente CSM, sélectionnez **Outils > Administration du gestionnaire de sécurité**, un message d'erreur indique un manque de privilège.



Étape 3. Répétez les étapes 1 à 3 avec le compte **csmadmin** pour valider les autorisations appropriées ont été fournies à cet utilisateur.

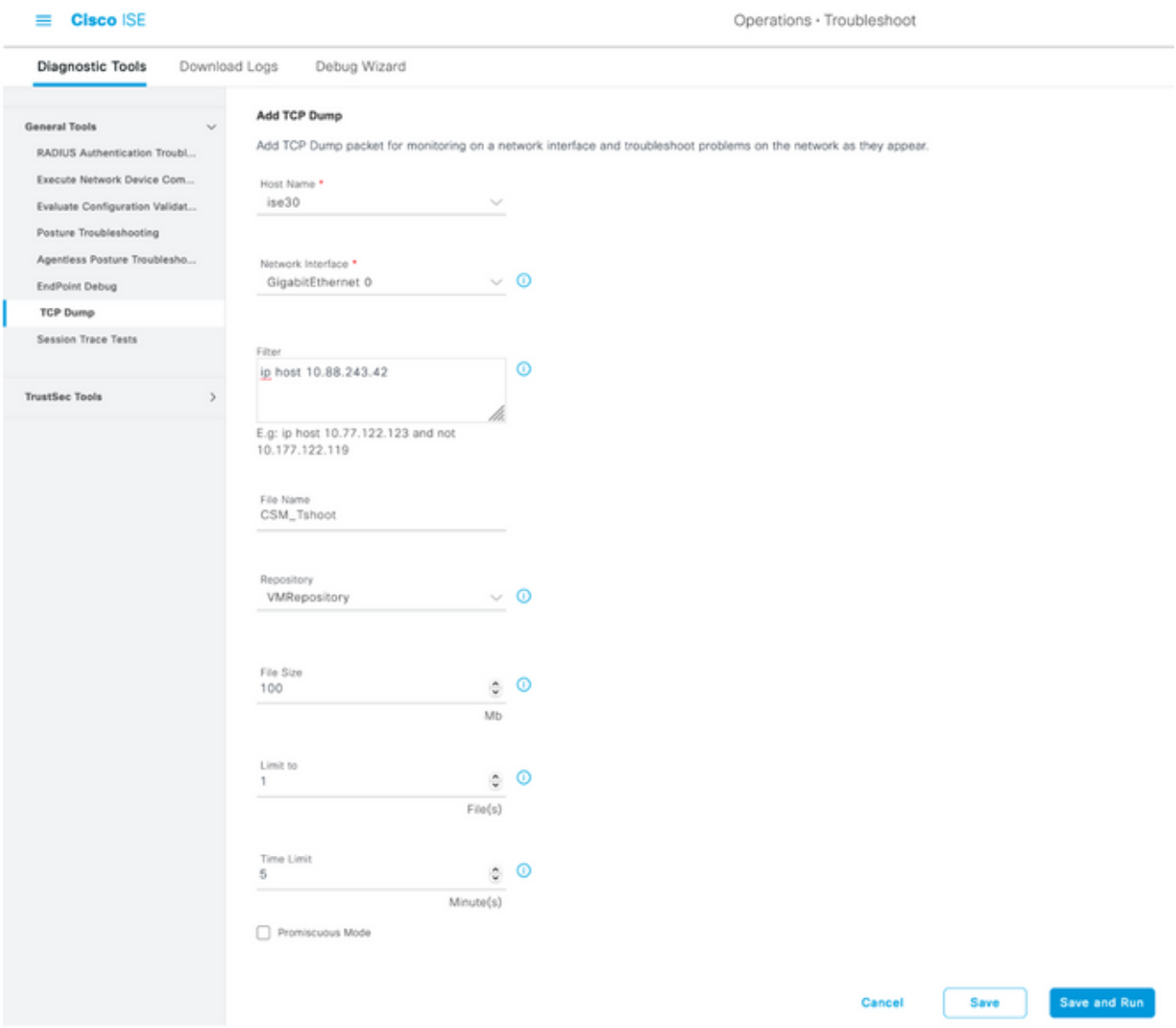
Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Validation de la communication avec l'outil TCP Dump sur ISE

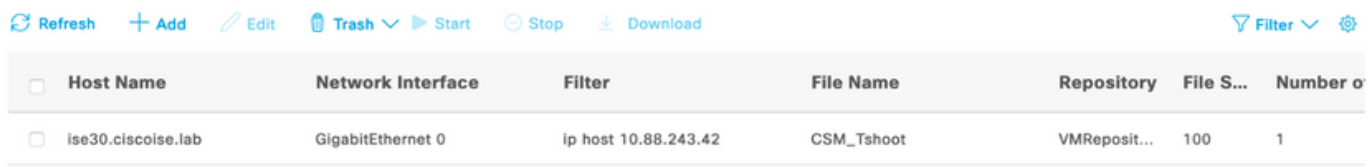
Étape 1. Connectez-vous à ISE et accédez à l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez **Operations>Troubleshoot>Diagnostic Tools.**

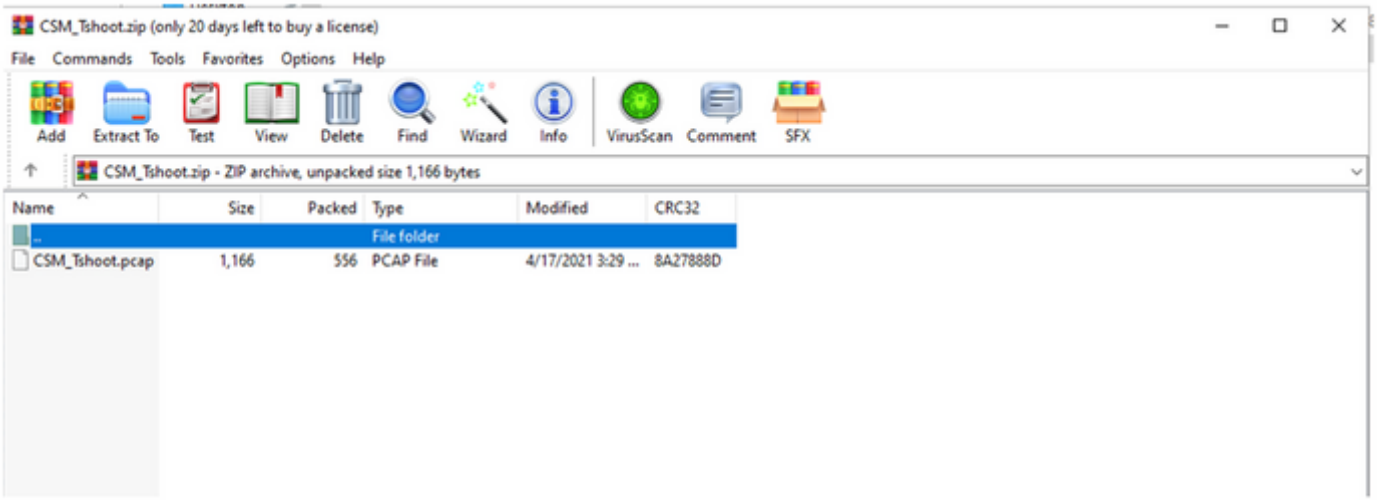
Étape 2. Sous **Outils généraux,** sélectionnez **Dumps TCP** puis sélectionnez **Ajouter+.** Sélectionnez Hostname, Network Interface File Name, Repository et éventuellement un filtre pour collecter uniquement le flux de communication d'adresse IP CSM**.** Sélectionnez **Enregistrer et exécuter**



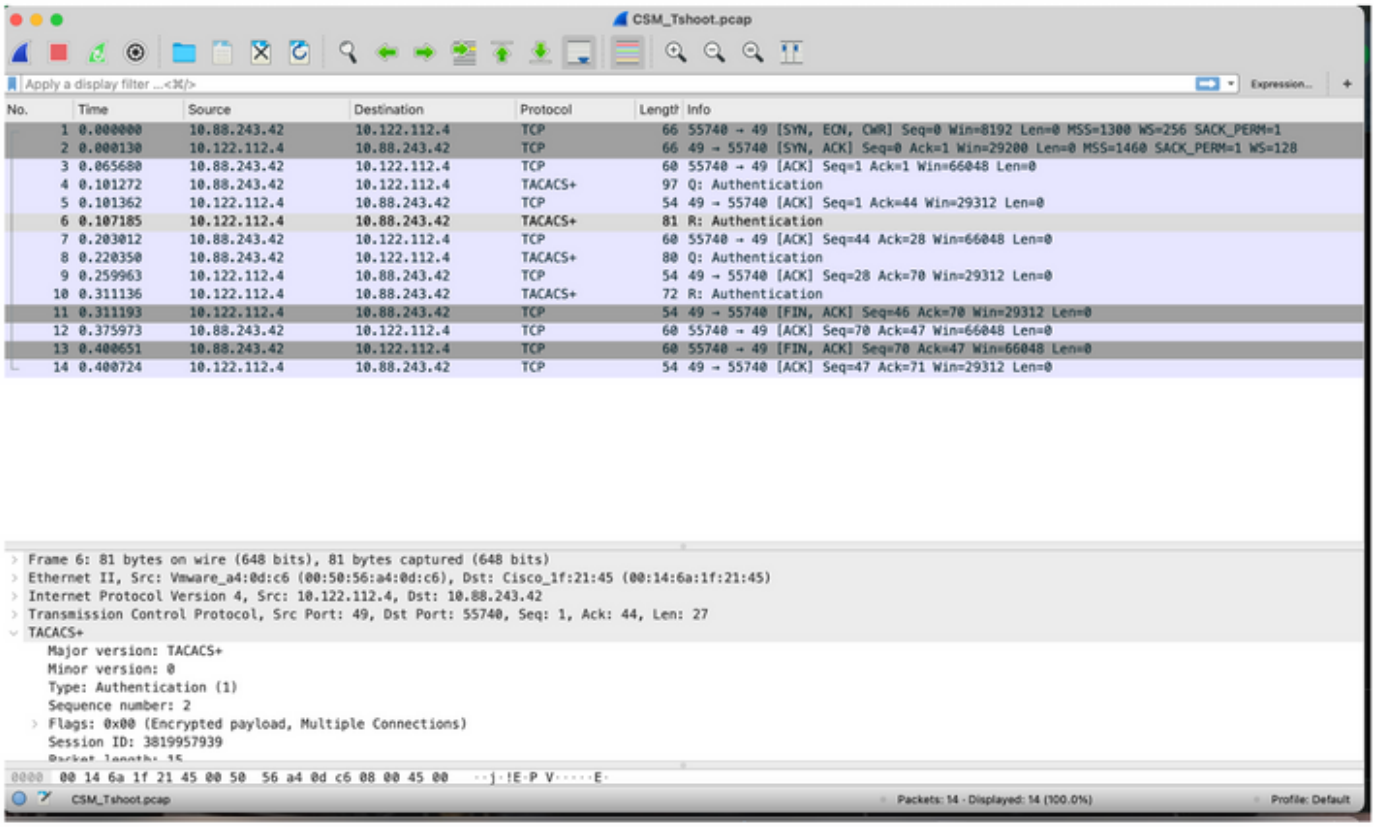
Étape 3. Connectez-vous à l'application cliente CSM ou à l'interface utilisateur du client et saisissez les informations d'identification d'administrateur.

Étape 4. Sur ISE, sélectionnez **le** bouton **Arrêter** et vérifiez que le fichier pcap a été envoyé au référentiel défini.





Étape 5. Ouvrez le fichier pcap pour valider la communication réussie entre CSM et ISE.



Si aucune entrée n'est affichée sur le fichier pcap, validez les éléments suivants :

1. Le service Administration des périphériques est activé sur le noeud ISE
2. L'adresse IP ISE correcte a été ajoutée à la configuration CSM
3. Si un pare-feu est au milieu, vérifiez que le port 49 (TACACS) est autorisé.