

Intégration de CSM TACACS à ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Procédure d'authentification](#)

[Configuration ISE](#)

[Configuration CSM](#)

[Vérification](#)

[Dépannage](#)

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.

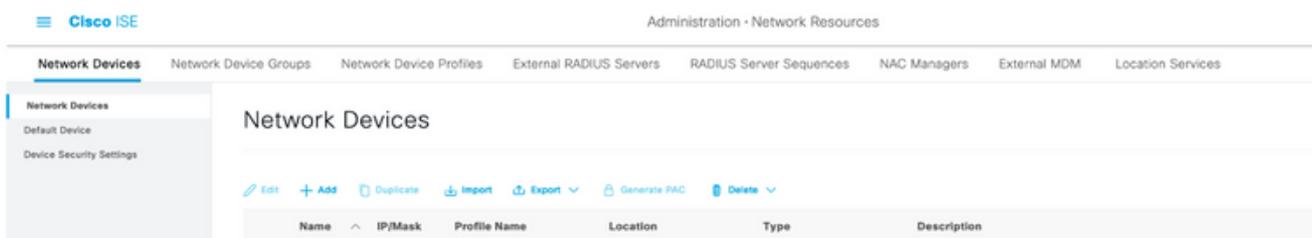
Étape 3. Une fois l'authentification réussie, ISE envoie un paquet d'autorisation pour autoriser l'accès au CSM.

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**.

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > New Network Device

Network Devices

Name CSM422

Description

IP Address * IP: 10.88.243.42 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations [Set To Default](#)

IPSEC Is IPSEC Device [Set To Default](#)

Device Type All Device Types [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret [Show](#)

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

[Submit](#) [Cancel](#)



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

☰ Cisco ISE Administration • Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

EQ

< [Icon] [Icon]

> Endpoint Identity Groups

> **User Identity Groups**

User Identity Groups

[Edit](#) [+ Add](#) [Delete](#) [Import](#) [Export](#)

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

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

The screenshot shows the 'User Identity Groups' management page. The navigation menu on the left includes 'Identities', 'Groups' (selected), 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. Under 'Identity Groups', there is a search bar and a list of folders: 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups' and features a toolbar with 'Edit', '+ Add', 'Delete', 'Import', and 'Export' buttons. A table lists the following groups:

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> CSM Admin	
<input type="checkbox"/> CSM Oper	

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.

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users List > csmadmin

Network Access User

Name: csmadmin

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: _____ Re-linear Password: _____

* Login Password: _____ * Generate Password

These Password: _____ * Generate Password

User Information

First Name: _____

Last Name: _____

Account Options

Description: _____

Change password on next login:

Account Disable Policy

Disable account if date exceeds: 2021-05-15 (every min=60)

User Groups

CSM Admin

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Edit + Add Change Status Import Export Delete Duplicate All

Status	Name	Description	First Name	Last Name	Email Address	User Identity Grou...	Ad...
<input type="checkbox"/>	Enabled csmadmin					CSM Admin	
<input type="checkbox"/>	Enabled csmoper					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

Hostname	Personas	Role(s)	Services	Node Status
Ise30	Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER, DE...	✔

> Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

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**.

Cisco ISE Work Centers - Device Administration Evaluation Mode 39 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets More

Conditions > TACACS Command Sets > New Command Set

Network Conditions >

Results > Permit all

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Description

Commands

Permit any command that is not listed below

+ Add Trash Edit Move Up Move Down

Grant	Command	Arguments
No data found.		

Cancel Submit

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

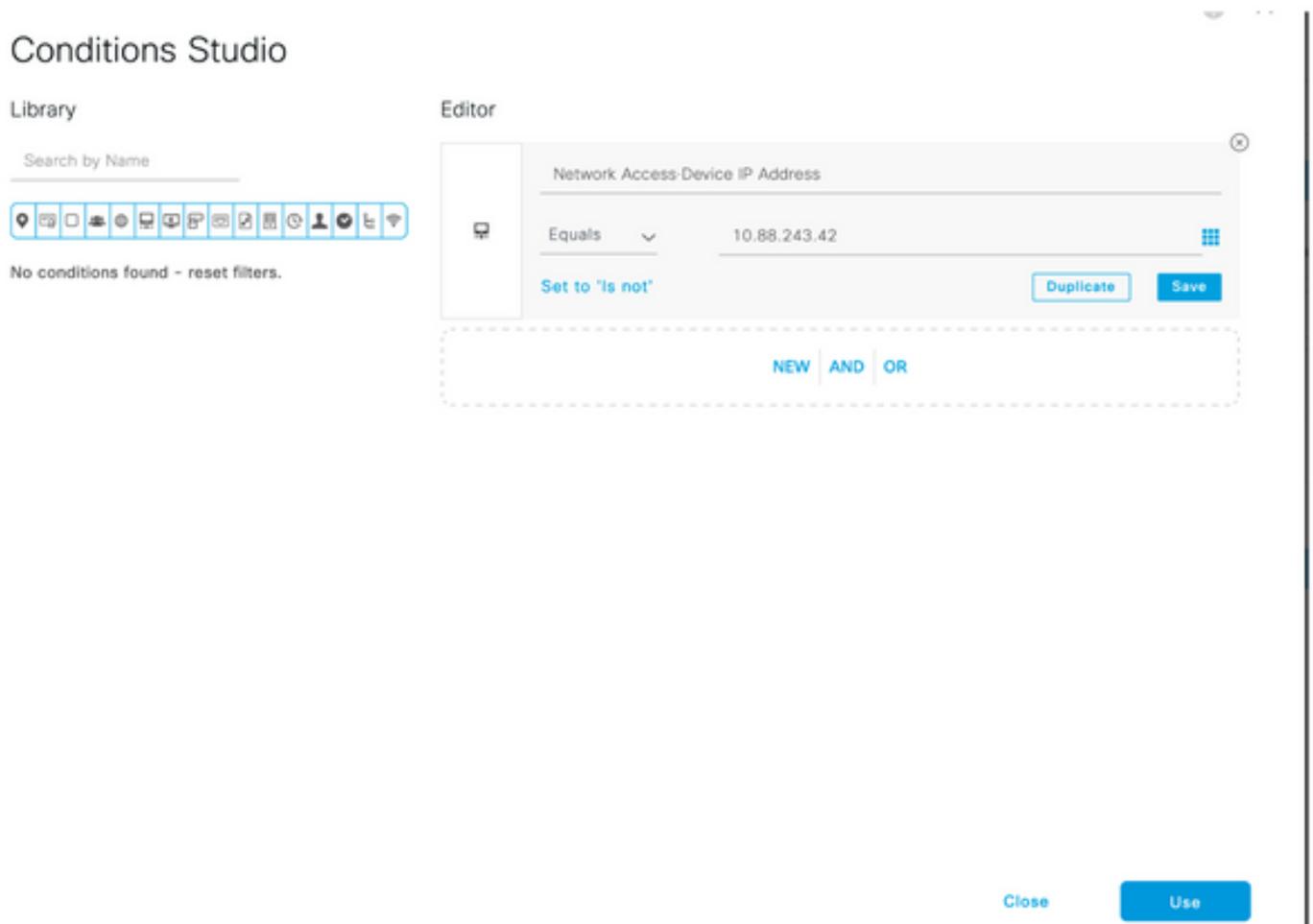
Administration->Administration des périphériques->Jeux de stratégies d'administration des

périphériques. Sélectionner  situé sous le titre Jeux de stratégies, définissez un nom et sélectionnez le bouton + au milieu pour ajouter une nouvelle condition.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	CSM Administrators		+	Select from list	+	⚙️	➔
+	Default	Tacacs Default policy set		Default Device Admin	0	⚙️	➔

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.



Conditions Studio

Library

Search by Name

No conditions found - reset filters.

Editor

Network Access-Device IP Address

Equals 10.88.243.42

Set to 'is not' Duplicate Save

NEW AND OR

Close Use

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

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	CSM 4.22		Network Access-Device IP Address EQUALS 10.88.243.42	Default Device Admin	0		

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**

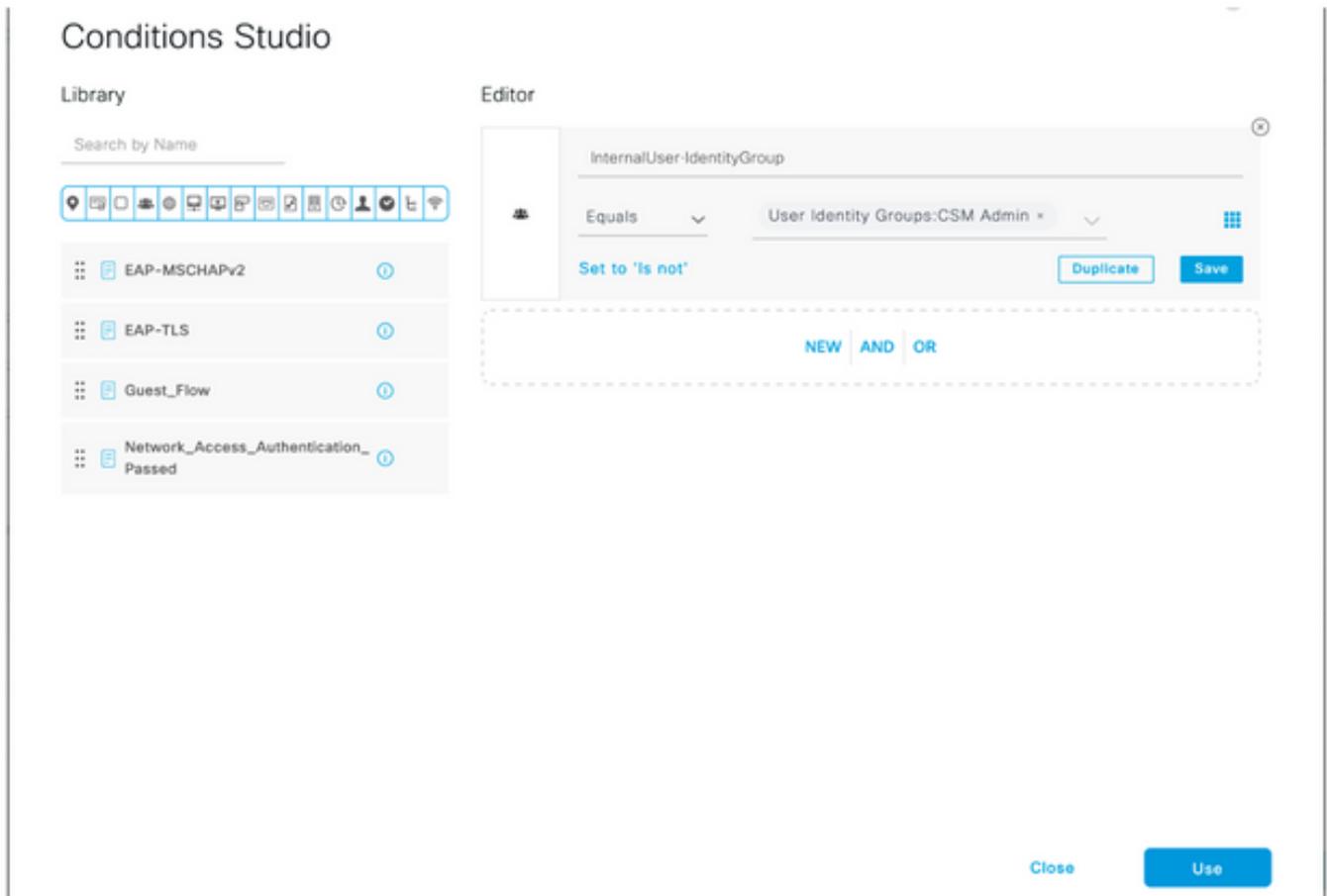
Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
●	CSM Authentication	Network Access-Device IP Address EQUALS 10.88.243.42	Internal Users		

> Options 

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

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	CSM Oper	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	Permit all ×	Select from list	0	⚙️	
✓	CSM Admin	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	Permit all ×	Select from list	0	⚙️	
✓	Default		DenyAllCommands ×	Deny All Shell Profile	0	⚙️	

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.

Deployment Licensing Certificates Logging **Maintenance** Upgrade Health Checks Backup [Click here to do visibility setup Do not show this again.](#)

Patch Management

Repository

Operational Data Purging

[Repository List](#) > [Add Repository](#)

Repository Configuration

* Repository Name

* Protocol

Location

* Server Name

* Path

Credentials

* User Name

* Password

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**

Cisco Security Manager
Version 4.22.0 Service Pack 1

Server Name

Username

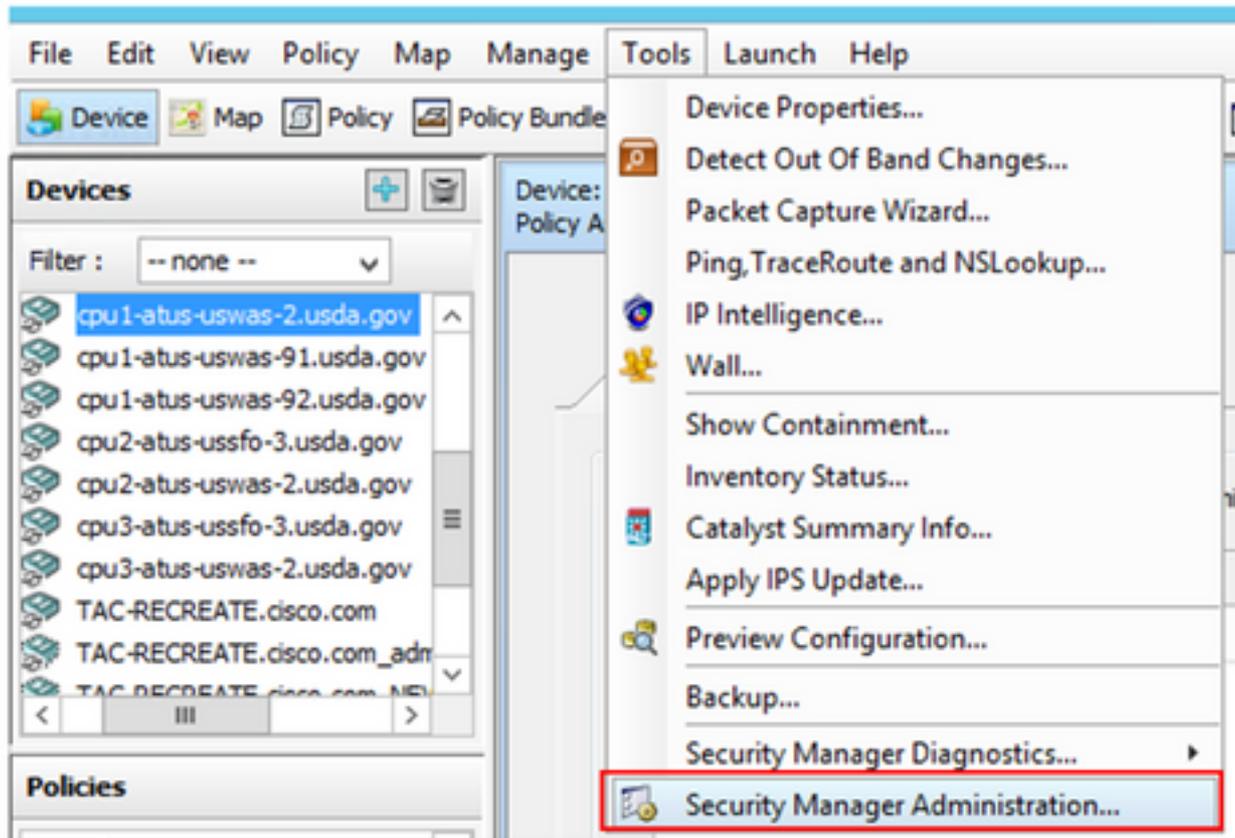
Password

Default View

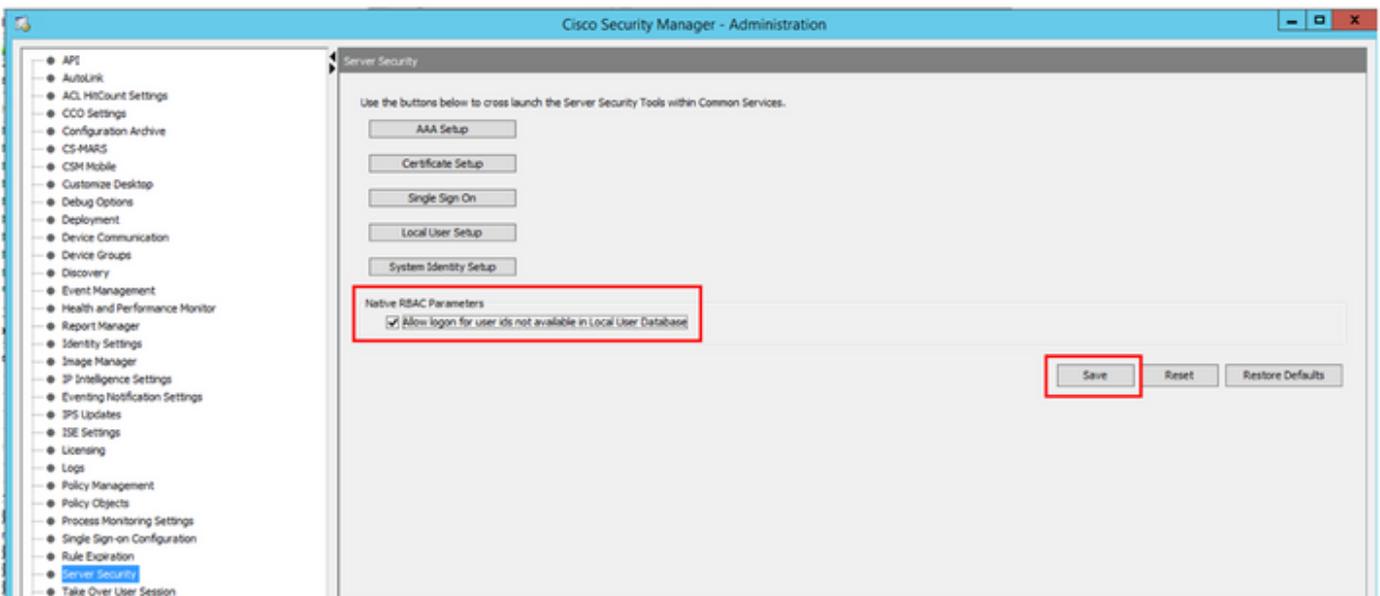
[Login](#) [Help](#)

© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

CISCO



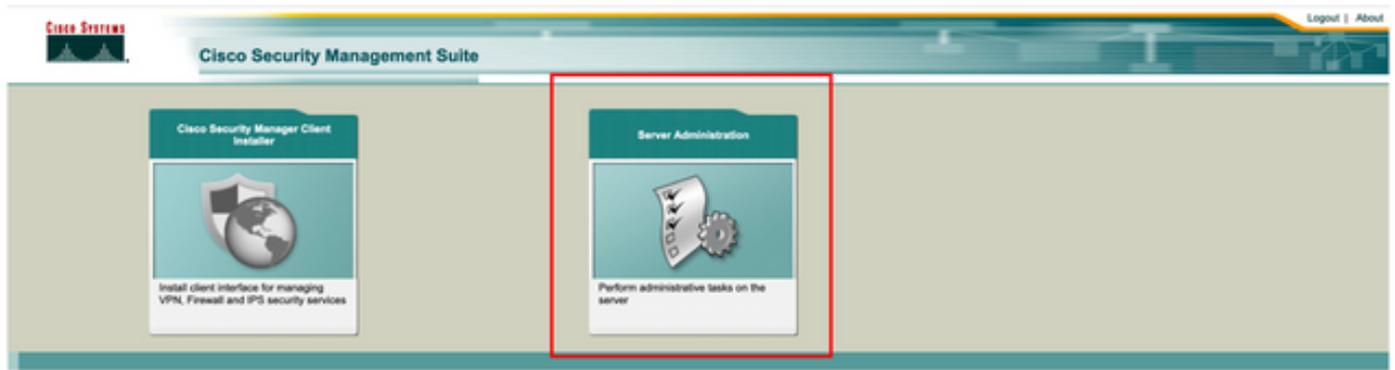
Étape 2. Cochez la case sous **Paramètres RBAC natifs**. Sélectionnez **Enregistrer** et **Fermer**



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.

Common Services Home

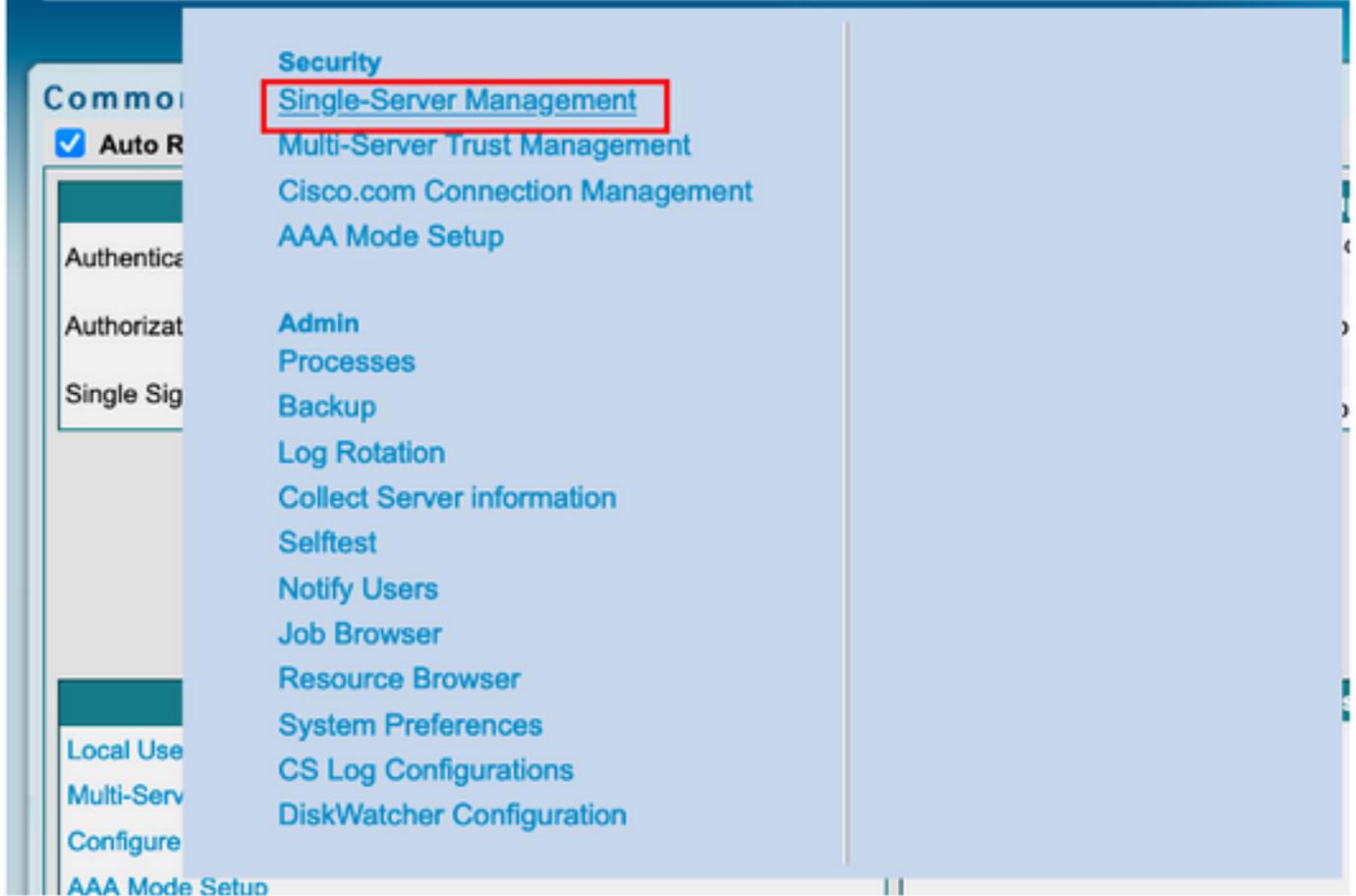
Version: 4.2.2

Last Updated: Sat Apr 17 14:11:20 PDT 2021

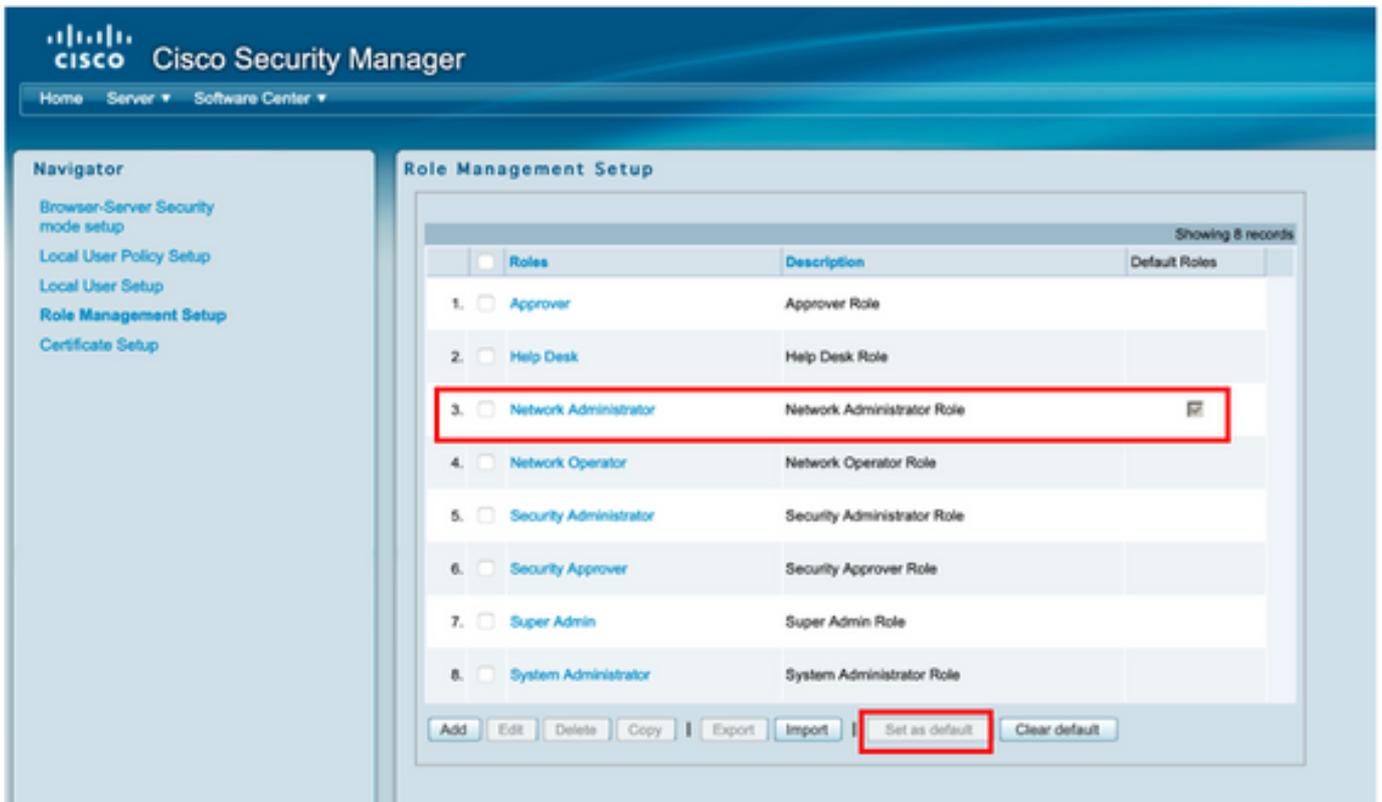
Security		Backup		Recently Completed Jobs				
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job ID	Job Type	Status	Description	Completed At
Authorization Mode	CiscoWorks Local	Last Backup Completed at	Not found or unable to detect	1001.1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 17 05:01:56 PDT 2021
Single Sign-on Mode	Standalone	Recent Backup Status	Not found or unable to detect	1001.1369	SystemCheckUtility	Succeeded	SysCheckTest	Fri Apr 16 05:00:58 PDT 2021
				1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
				1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021
				1001.1366	SystemCheckUtility	Succeeded	SysCheckTest	Tue Apr 13 05:00:54 PDT 2021
				1001.1365	SystemCheckUtility	Succeeded	SysCheckTest	Mon Apr 12 05:00:56 PDT 2021
				1001.1364	SystemCheckUtility	Succeeded	SysCheckTest	Sun Apr 11 05:00:55 PDT 2021
				1001.1363	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 10 05:00:56 PDT 2021

System Tasks	Online Users	Management Tasks	Reports
Local User Setup Multi-Server Trust Management Configure Single Sign-On AAA Mode Setup	Number of Online users: 1 Online User ID(s): admin Send Message	Schedule Backup Check for Software Updates Check for Device Updates Collect Server Information	Permission Report Log File Status Process Status System Audit Log

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.

Login Module Options

Selected Login Module: TACACS+
Description: Cisco Prime TACACS+ login module

Server: 10.122.112.4
Port: 49
SecondaryServer:
SecondaryPort: 49
TertiaryServer:
TertiaryPort: 49
Key:

Debug: True False

Login fallback options:

- Allow all Local Authentication users to fallback to the Local Authentication login.
- Only allow the following user(s) to fallback to the Local Authentication login if preceding login fails:
admin (comma separated)
- Allow no fallbacks to the Local Authentication login.

OK Cancel

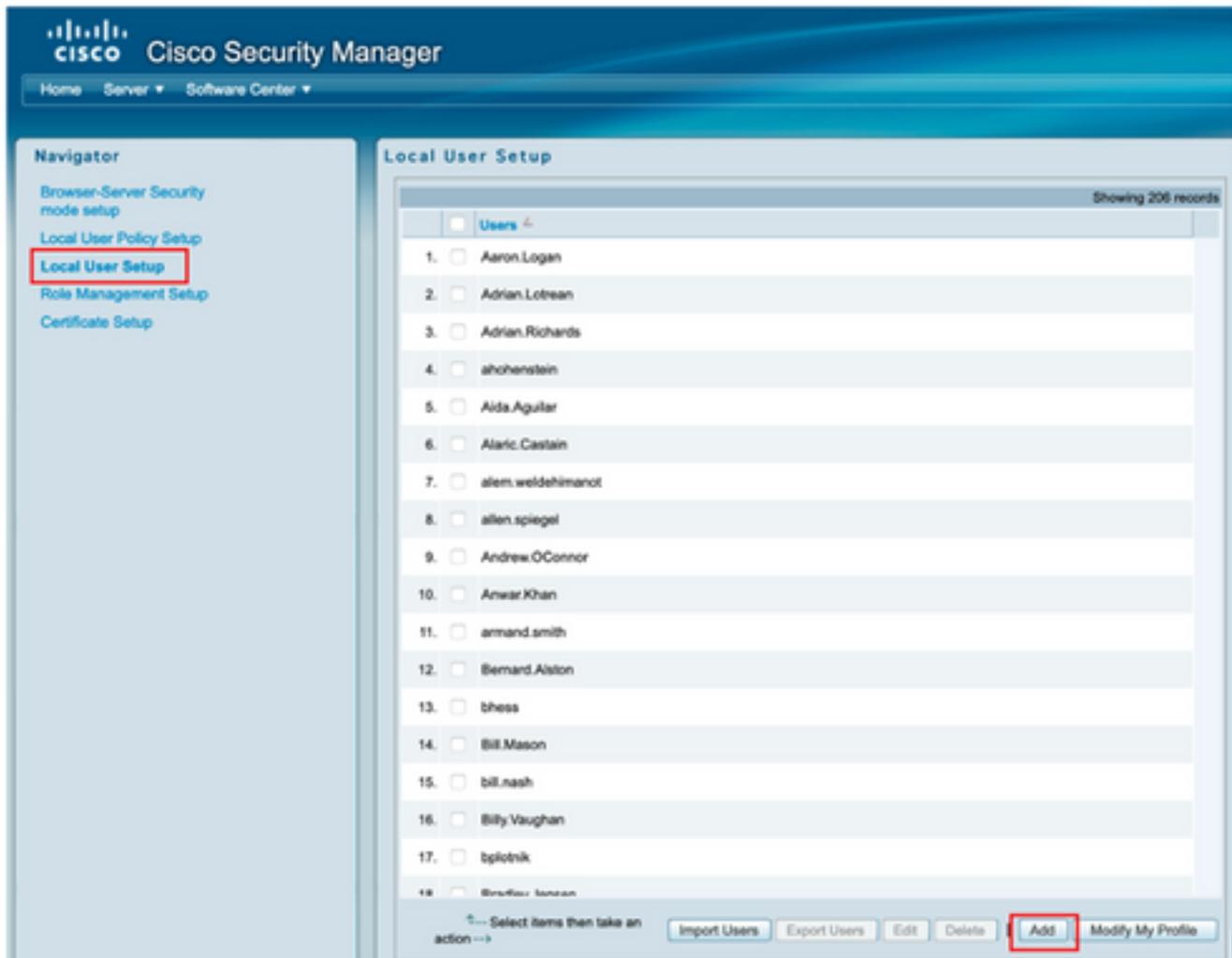
Login Module Change Summary

Login Module changes updated.

OK

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 **csmpoper** et d'**autorisation des tâches du centre d'assistance** sont utilisés dans cet exemple. Sélectionnez **OK** afin d'enregistrer l'utilisateur admin.

User Information

User Login Details

Username:

Password: Verify Password:

Email:

Authorization Type

Select an option: Full Authorization Enable Task Authorization Enable Device Authorization

Roles

- Help Desk
- Approver
- Network Operator
- Network Administrator
- System Administrator
- Super Admin
- Security Administrator
- Security Approver

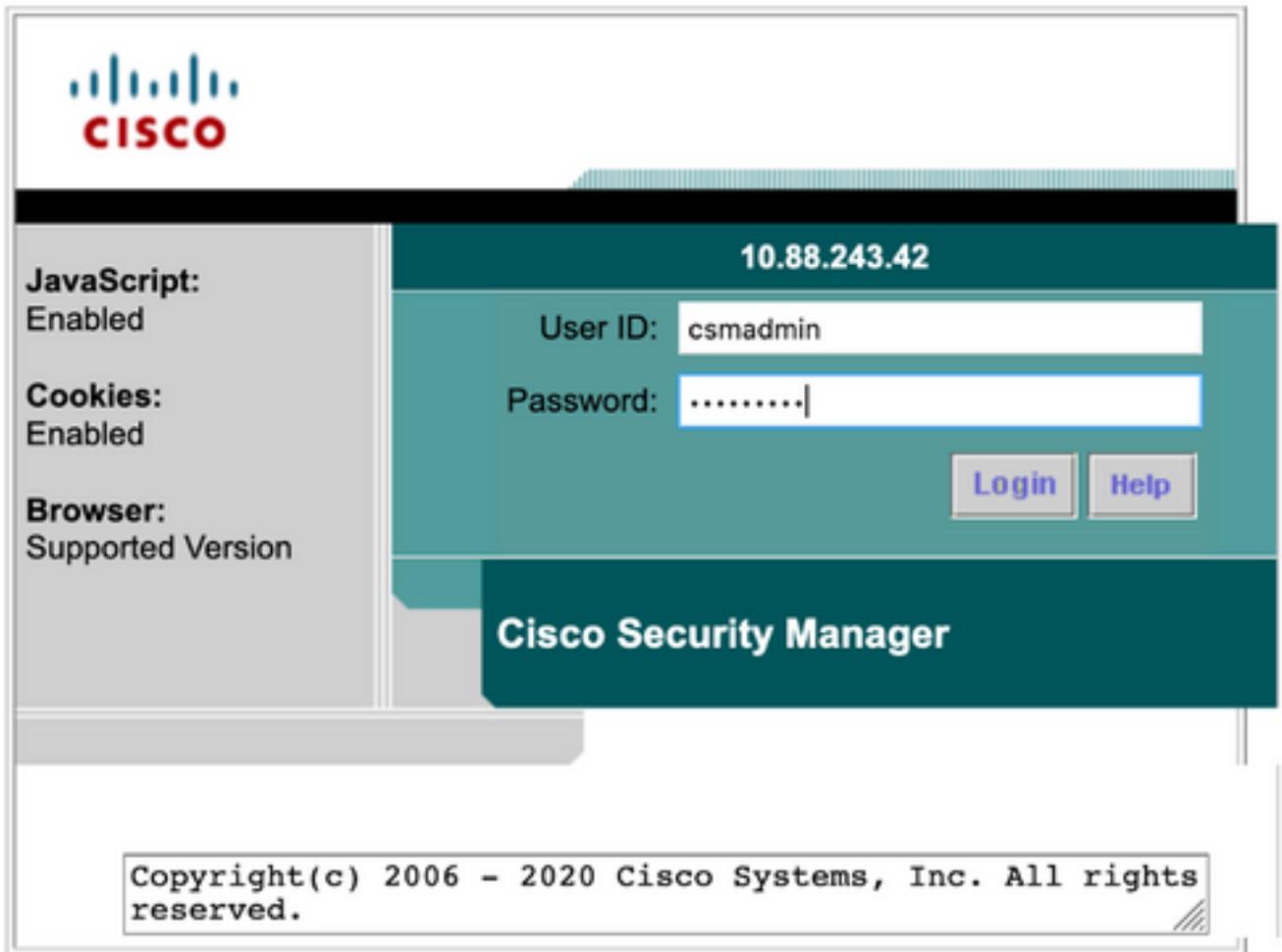
Device level Authorization

Not Applicable

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

Cisco ISE Operations - TACACS Evaluation Made 39 Days

Live Logs

Refresh Every 3 seconds Show Latest 20 records Within Last 3 hours

Refresh Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
Apr 17, 2021 02:34:54.1...	✓		csmadmin	Authentic...	CSM 4.22 >> Default	Authorization Policy	ise30	CSM422

Last Updated: Sat Apr 17 2021 09:37:58 GMT-0500 (Central Daylight Time) Records Shown: 1

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.



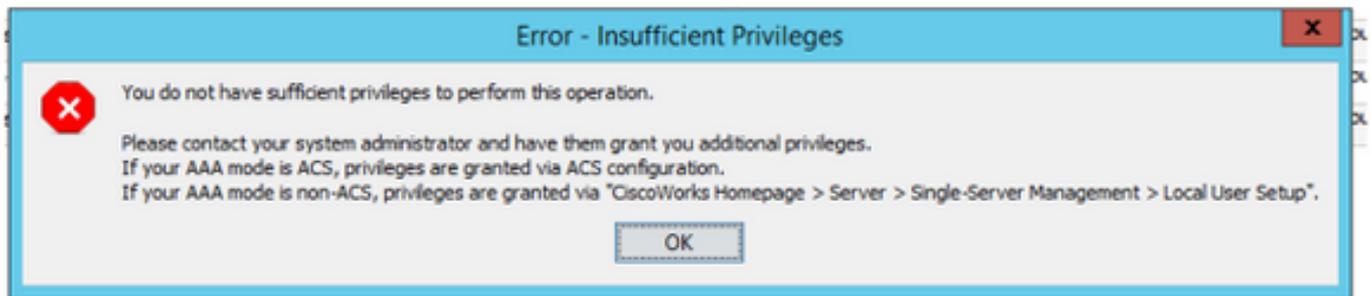
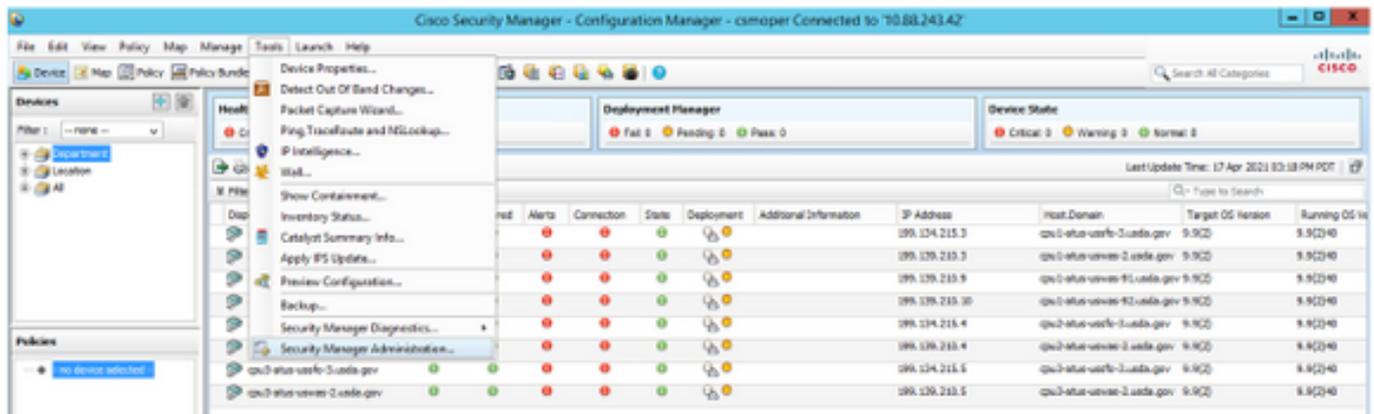
La tentative de connexion réussie peut être vérifiée sur les journaux en direct ISE TACACS

Live Logs

Refresh Every 3 seconds Show Latest 20 records Within Last 3 hours Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
Apr 17, 2021 03:05:58.5...	✓		csmoper	Authentic...	CSM 4.22 >> Default		ise30	CSM422

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**

Diagnostic Tools Download Logs Debug Wizard

General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug
- TCP Dump**
- Session Trace Tests

TrustSec Tools

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name *
ise30

Network Interface *
GigabitEthernet 0

Filter
ip host 10.88.243.42

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name
CSM_Tshoot

Repository
VMRepository

File Size
100 Mb

Limit to
1 File(s)

Time Limit
5 Minute(s)

Promiscuous Mode

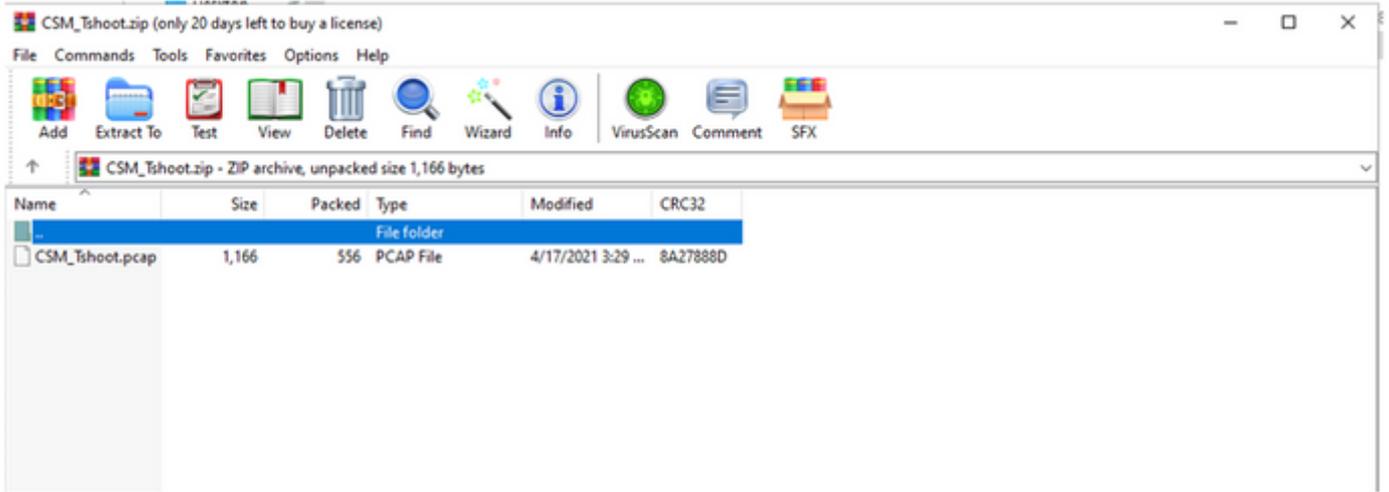
Cancel Save Save and Run

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

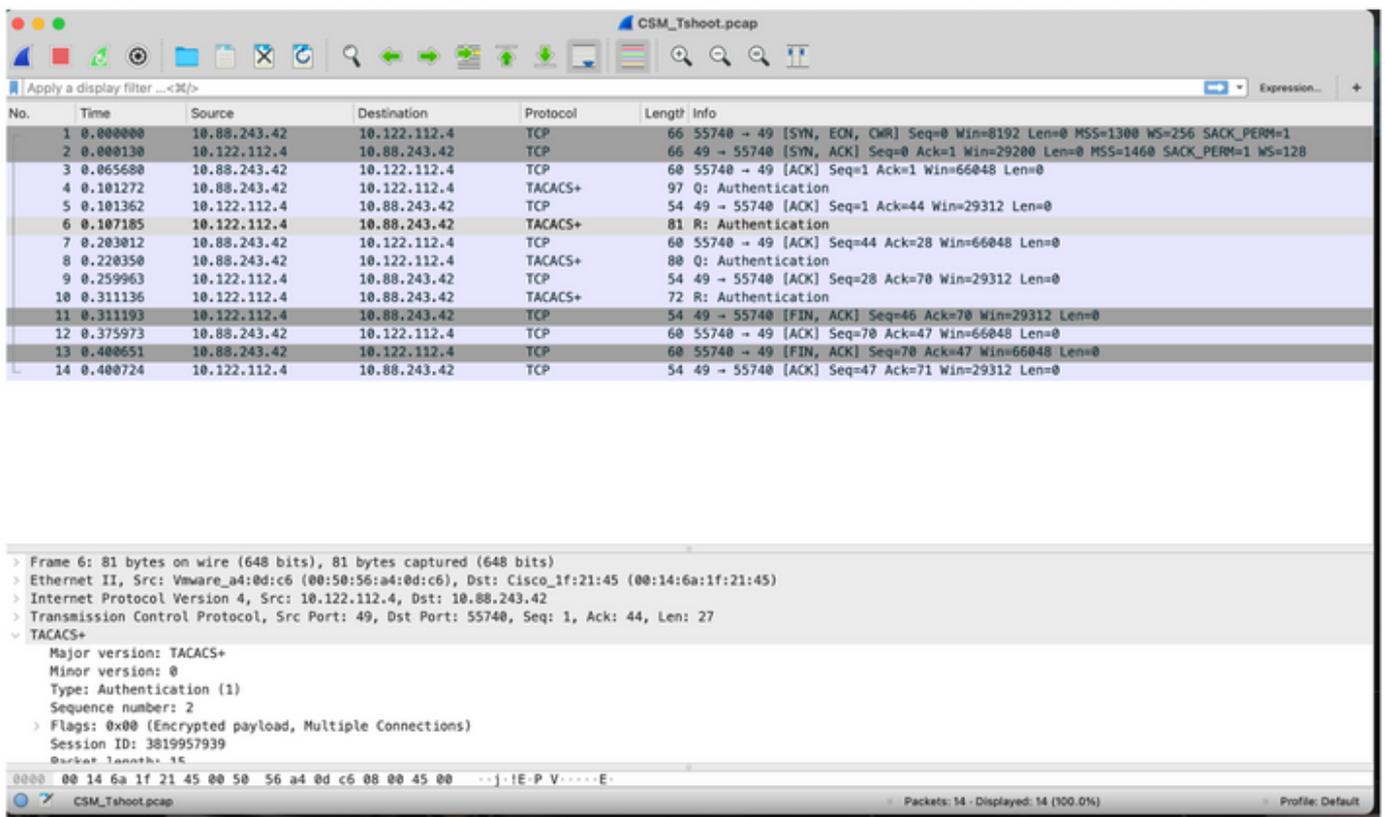
Étape 4. Sur ISE, sélectionnez le bouton **Arrêter** et vérifiez que le fichier pcap a été envoyé au référentiel défini.

Refresh + Add Edit Trash Start Stop Download Filter

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
<input type="checkbox"/> ise30.ciscoise.lab	GigabitEthernet 0	ip host 10.88.243.42	CSM_Tshoot	VMReposit...	100	1



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.