

# CSM TACACS-integratie met ISE

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Verificatieprocedure](#)

[ISE-configuratie](#)

[CSM-configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft de procedure om Cisco Security Manager (CSM) te integreren met Identity Services Engine (ISE) voor beheergebruikers en verificatie met TACACS+ Protocol.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CSM Server versie 4.2.2
- ISE versie 3.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

Standaard gebruikt Cisco Security Manager (CSM) een verificatiemodus die Cisco heet, werken om gebruikers lokaal te authentifieren en te autoriseren, om een gecentraliseerde verificatiemethode te kunnen gebruiken die u Cisco Identity Services Engine via het TACACS-protocol kunt gebruiken.

## Configureren

### Netwerkdigram



### Verificatieprocedure

Stap 1. Meld u aan bij de CSM-toepassing met de referenties van de beheerder.

Stap 2. Het verificatieproces start en ISE bevestigt de referenties lokaal of via de actieve map.

Stap 3. Zodra de authenticatie een succesvol ISE is, verstuurt u een vergunningspakket om de toegang tot CSM te verlenen.

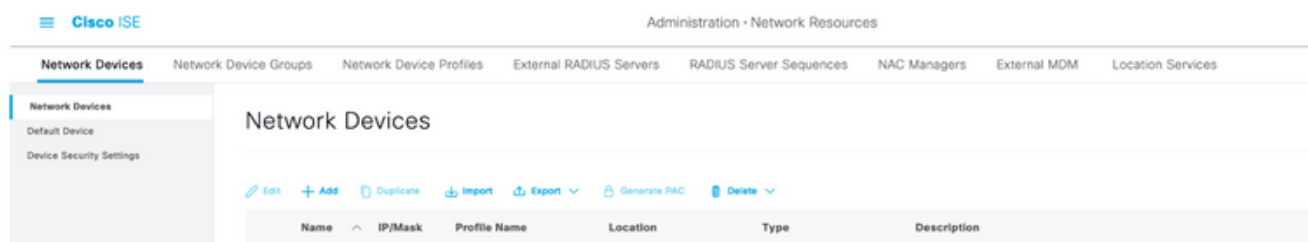
Stap 4. CSM brengt de gebruikersnaam in kaart met de lokale gebruikersrol-toewijzing.

Stap 5. ISE toont een succesvol authenticatielevend logbestand.

### ISE-configuratie



**Stap 1.** Selecteer het pictogram drie lijnen  bevindt zich in de linker bovenhoek en navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**.



**Stap 2.** Selecteer de knop **+Add** en voer de juiste waarden voor de naam en het IP-adres van het netwerktoegangsapparaat in. Controleer vervolgens het selectieteken van de **TACACS-verificatie** en definieer een gedeeld geheim. Selecteer de knop **Indienen**.

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

Description

IP Address  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings



**Stap 3.** Selecteer het pictogram drie regels bevindt zich in de linker bovenhoek en navigeer naar **Administratie > identiteitsbeheer > Groepen**.

**Cisco ISE** Administration • Identity Management

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

**Identity Groups**

EQ

<

> 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

**Stap 4.** Navigeer naar de map **Gebruikersgroepen** en selecteer de knop **+Add**. Definieert een naam en selecteer de knop **Indienen**.

The screenshot shows the 'User Identity Groups' management page. The left sidebar has 'Identity Groups' with 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. Below the toolbar is a table with columns 'Name' and 'Description'. The table lists three groups: 'ALL\_ACCOUNTS (default)' with description 'Default ALL\_ACCOUNTS (default) User Group', 'CSM Admin', and 'CSM Oper'. Each row has a checkbox for selection. The top right of the main area shows 'Selected 0 Total 10' and some utility icons.

**Opmerking:** Dit voorbeeld maakt CSM Admin en CSM Oper Identity Services groepen. U kunt Stap 4 voor elk type Admin-gebruikers op CSM herhalen



**Stap 5.** Selecteer het pictogram drie lijnen en navigeer naar **Administratie > Identity Management > Identificaties**. Selecteer de knop **+Add** en definieer de gebruikersnaam en het wachtwoord en selecteer vervolgens de groep waartoe de gebruiker behoort. In dit voorbeeld maakt u de **csmadmin-** en **csmoper-**gebruikers aan en toegewezen aan respectievelijk CSM Admin en CSM Oper groep.

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"/>	<span style="color: green;">■</span> Enabled <span>👤</span> csmadmin					CSM Admin	
<input type="checkbox"/>	<span style="color: green;">■</span> Enabled <span>👤</span> csmoper					CSM Oper	



**Stap 6.** Selecteer en navigeer naar **Administratie > Systeem > Plaatsing**. Selecteer het hostname-knooppunt en stel **de apparaatbeheerservice** in

Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/> Ise30	Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER, DE...	<input checked="" type="checkbox"/>

> Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

**Opmerking:** Selecteer in het geval van gedistribueerde implementatie het PSN-knooppunt dat TACACS-verzoeken behandelt

**Stap 7.** Selecteer het pictogram drie regels en navigeer naar **Administratie > Apparaatbeheer > Beleidselementen**. Navigeer naar **resultaten > TACACS Opdrachten**. Selecteer de knop **+Add**, definieer een naam voor de Opdrachtset en stel de **opdracht** in die **niet onder** het selectieteken staat. Selecteer **Indienen**.

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

TACACS Command Sets > New Command Set

Name Permit all

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

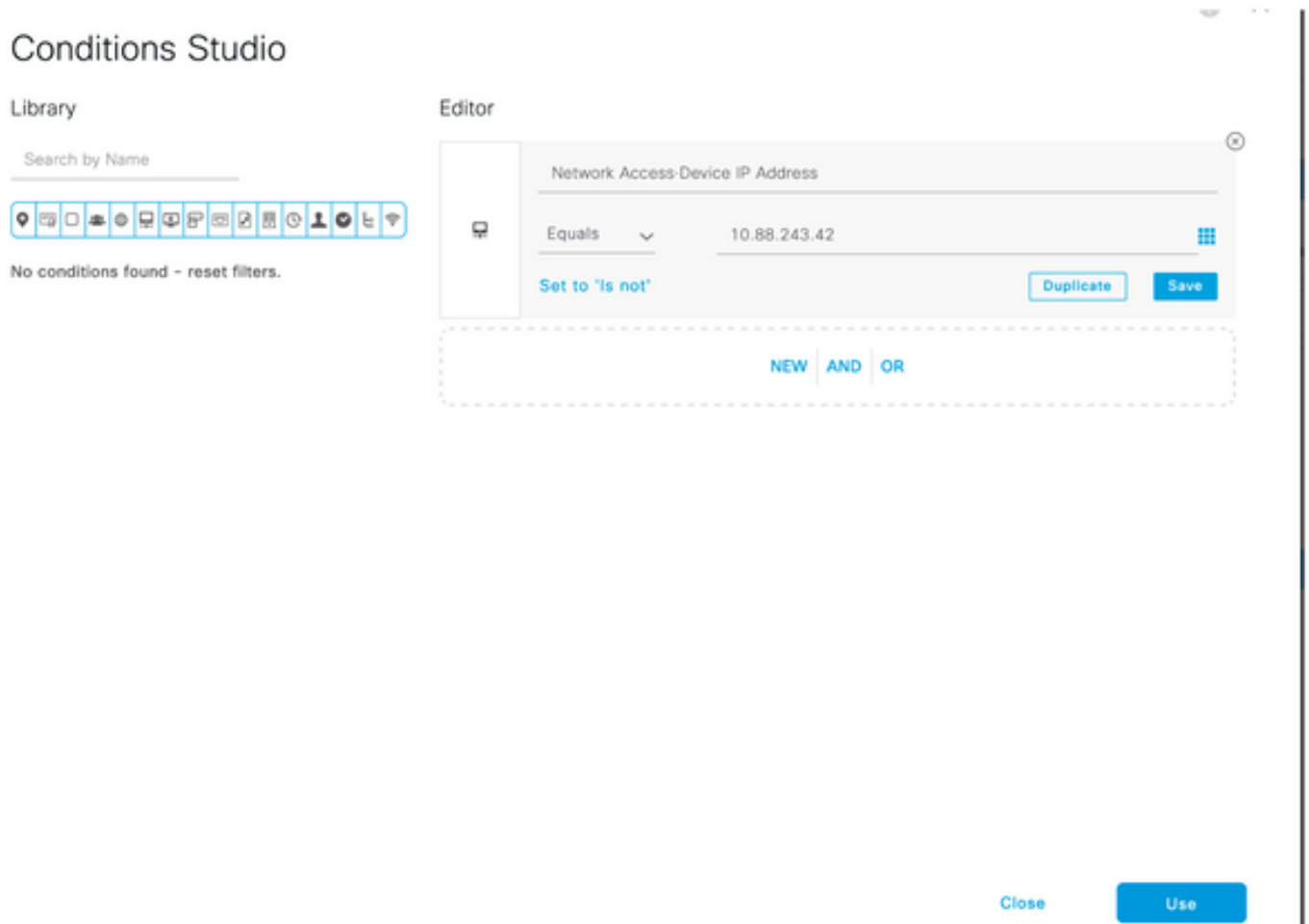
**Stap 8.** Selecteer het pictogram drie regels in de linker bovenhoek en navigeer naar **Administratie-**

>Apparaatbeheer->Beleidssets voor apparaatbeheer. Selecteren  Hieronder staat de titel Policy Sets, definieer een naam en selecteer de knop + in het midden om een nieuwe voorwaarde toe te voegen.



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	⚙️	➔

**Stap 9.** Selecteer onder het venster conditionering een eigenschap toevoegen en selecteer vervolgens **het** pictogram **Netwerkapparaat**, gevolgd door het IP-adres van het netwerktoegangsapparaat. Selecteer **Waarde van** eigenschappen en voeg het CSM IP-adres toe. Selecteer **Gebruik** als u klaar bent.



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

**Stap 10.** Selecteer onder het gedeelte Protocollen toestaan de optie **Apparaatstandaardinstellingen**. Selecteer **Opslaan**

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	CSM 4.22		Network Access-Device IP Address EQUALS 10.88.243.42	Default Device Admin	0		

**Stap 1.** Selecteer de juiste pijl  pictogram van het beleidskader dat is ingesteld om het echtheids- en autorisatiebeleid te definiëren


**Stap 12.** Selecteer  Hieronder vindt u een naam voor verificatiebeleid. Selecteer vervolgens een naam en selecteer de optie + in het midden om een nieuwe voorwaarde toe te voegen. Selecteer onder het venster Condition een eigenschap toevoegen en selecteer vervolgens het pictogram **Netwerkapparaat**, gevolgd door het IP-adres van het netwerktoegangsapparaat. Selecteer **Waarde van** eigenschappen en voeg het CSM IP-adres toe. Selecteer **Gebruik** als u klaar bent

**Stap 13.** Selecteer **Interne** gebruikers als Identity Store en selecteer **Opslaan**

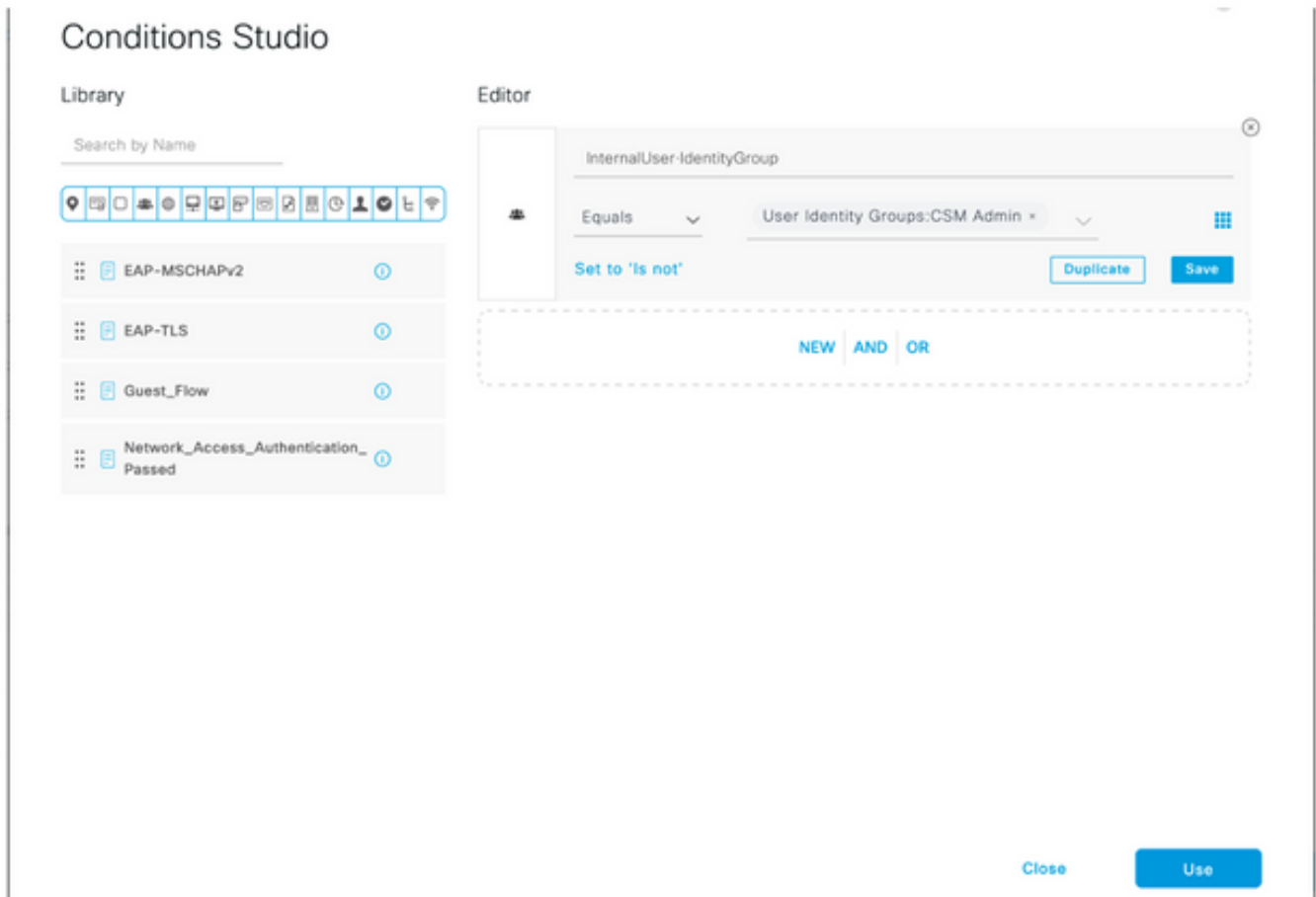
Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
<span style="color: green;">●</span>	CSM Authentication	Network Access-Device IP Address EQUALS 10.88.243.42	Internal Users		Options

**Opmerking:** Identity Store kan worden gewijzigd in AD-winkel als ISE is aangesloten op een actieve map.

**Stap 14.** Selecteer  Voer onder de titel Automation Policy een naam in en selecteer de knop + in het midden om een nieuwe voorwaarde toe te voegen. Selecteer onder het venster conditioner een eigenschap toevoegen en selecteer vervolgens **het** pictogram **Identity Group**, gevolgd door **Interne gebruiker: Identiteitsgroep**. Selecteer de CSM Admin Group en selecteer **Gebruik**.





**Stap 15.** Selecteer onder Opdrachtset alle opdracht toestaan die in Stap 7 is gemaakt en selecteer Opslaan

Stap 14 en 15 herhalen voor de CSM-groep

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	⚙️	

**Stap 16 (optioneel).** Selecteer het pictogram drie regels in de linker bovenhoek en selecteer **Beheer>Onderhoud>Bedieningsgebied**, selecteer **+Add** om een opslagplaats toe te voegen die wordt gebruikt om TCP-pompbestand op te slaan voor probleemoplossing.

**Stap 17 (optioneel).** Definieert een opslagnaam, protocol, servernaam, pad en Credentials. Selecteer **Indienen** als dit eenmaal is gedaan.

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

## CSM-configuratie

**Stap 1.** Meld u aan bij de Cisco Security Manager-clienttoepassing met de lokale beheeraccount. In het menu navigeren naar **Gereedschappen > Beveiligingsbeheer**

Cisco Security Manager  
Version 4.22.0 Service Pack 1

Server Name

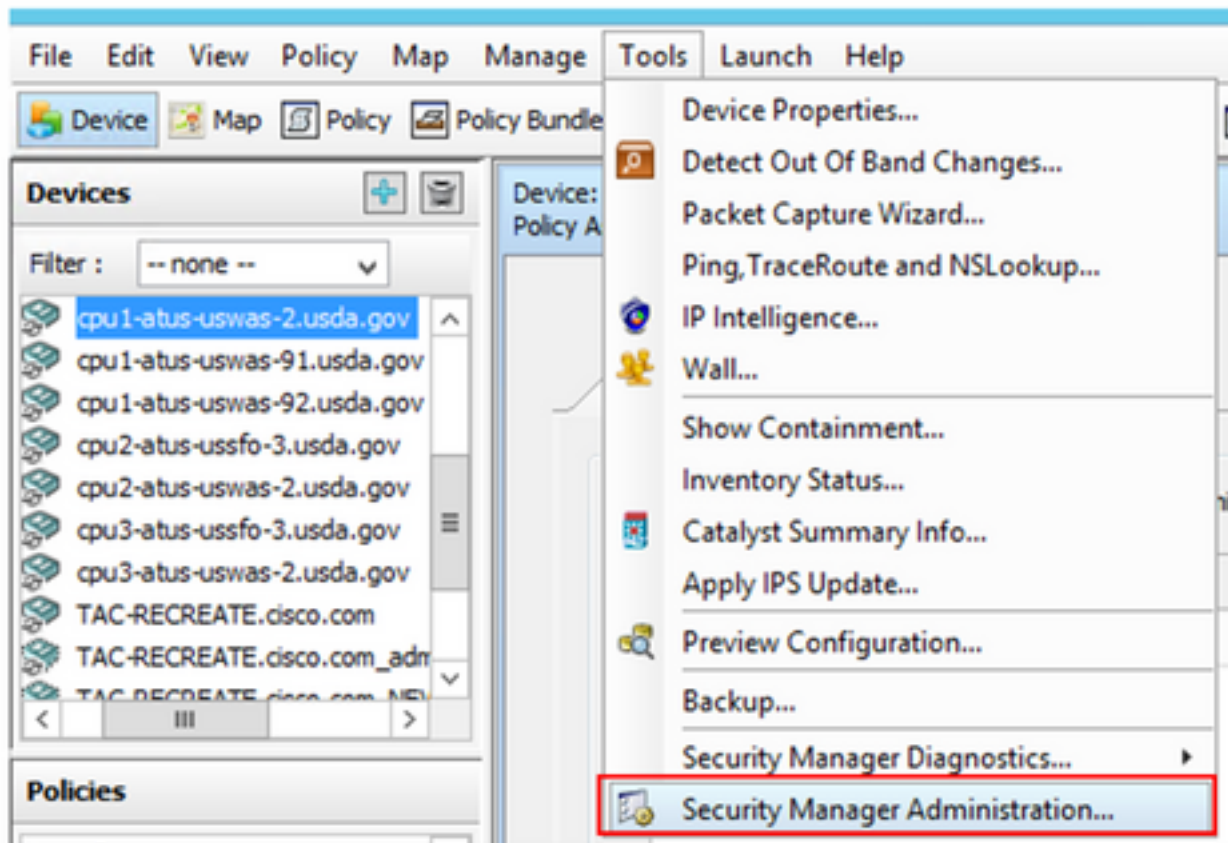
Username

Password

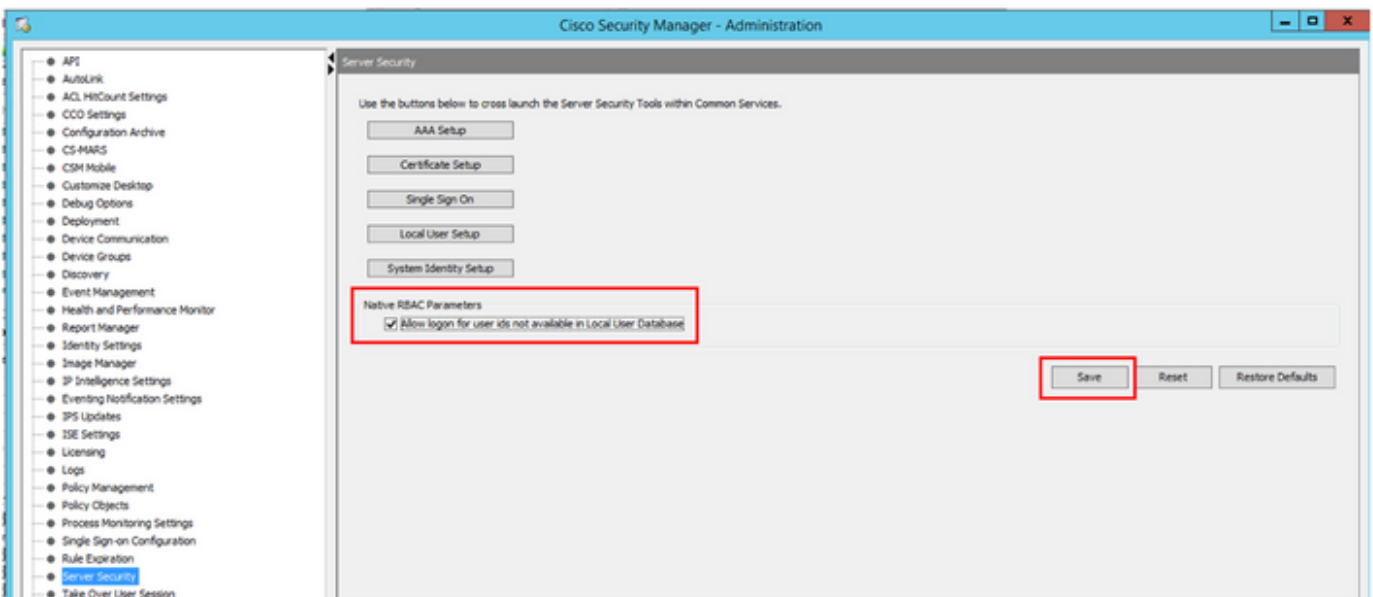
Default View

[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.



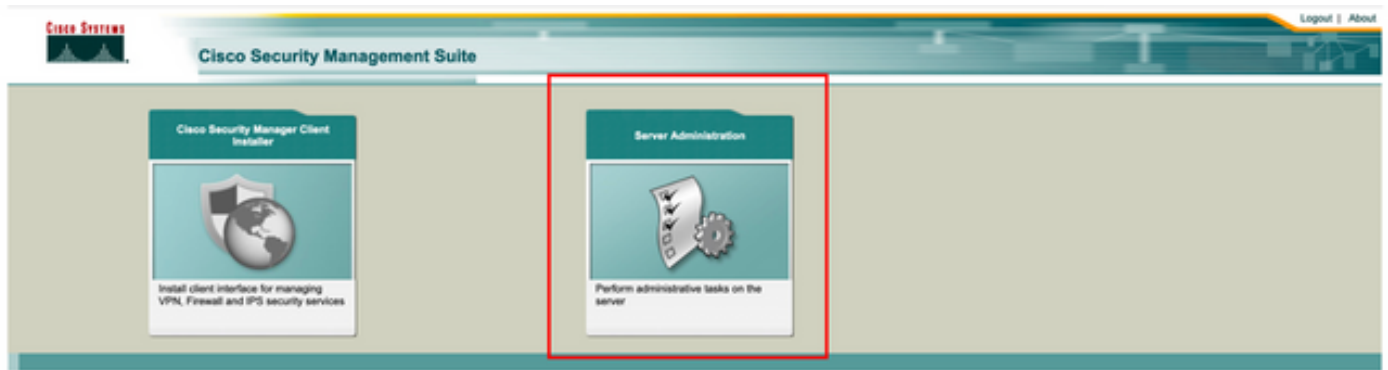
Stap 2. Controleer het vakje onder **Native RBAC-parameters**. Selecteer **Opslaan en Sluiten**



Stap 3. Selecteer in het menu **Bestand > Verzenden**. Bestand > Indienen.

**Opmerking:** Alle veranderingen moeten worden opgeslagen, in het geval van configuratieveranderingen die moeten worden voorgelegd en ingezet.

Stap 4. Navigeer naar CSM Management UI en type [https://<enter\\_CSM\\_IP\\_Address>](https://<enter_CSM_IP_Address>) en selecteer **Server Administration**.



**Opmerking:** De stappen 4 tot 7 tonen de procedure om de standaardrol voor alle beheerders te definiëren die niet op ISE worden bepaald. Deze stappen zijn optioneel.

**Stap 5.** Verifieer de verificatiemodus op **CiscoWorks Local** en **Online** userID is de lokale admin-account die op CSM is gemaakt.

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

**Stap 6.** Navigeer naar **server** en selecteer **Beheer met één server**



Common

Auto R

Authentica

Authorizat

Single Sig

Local Use

Multi-Serv

Configure

AAA Mode Setup

Security

**Single-Server Management**

Multi-Server Trust Management

Cisco.com Connection Management

AAA Mode Setup

Admin

Processes

Backup

Log Rotation

Collect Server information

Selftest

Notify Users

Job Browser

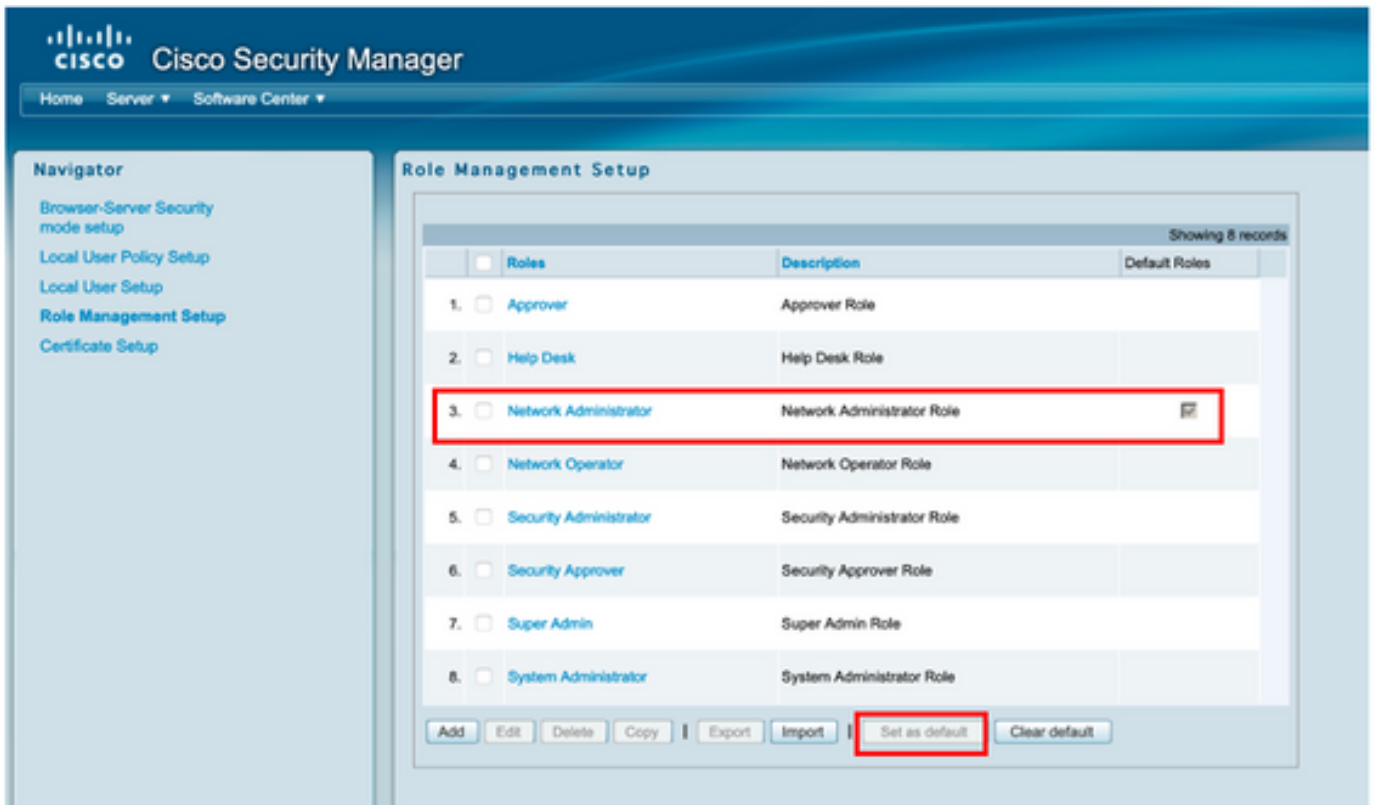
Resource Browser

System Preferences

CS Log Configurations

DiskWatcher Configuration

**Stap 7.** Selecteer de optie Rollend beheer instellen en selecteer het standaardrecht dat alle beheergebruikers bij verificatie ontvangen. U kunt bijvoorbeeld de netwerkbeheerder gebruiken. Nadat u deze optie hebt geselecteerd, selecteert u **deze standaard**.



Stap 8. Selecteer **Server>Setup-rol AAA-modus** en selecteer vervolgens **TACACS+** optie **wijzigen** en ISE-informatie toevoegen.





**Stap 9.** Definieer ISE IP-adres en -toets, kunt u naar keuze de optie selecteren om alle lokale authenticatiegebruikers of slechts één gebruiker toe te staan als het inloggen mislukt. Bij dit voorbeeld is de enige beheerder toegestaan als back-upmethode. Selecteer **OK** om de wijzigingen op te slaan.

The screenshot shows the 'Login Module Options' dialog box. It is configured for the 'TACACS+' login module. The fields are as follows: Selected Login Module: TACACS+; Description: Cisco Prime TACACS+ login module; Server: 10.122.112.4; Port: 49; SecondaryServer: (empty); SecondaryPort: 49; TertiaryServer: (empty); TertiaryPort: 49; Key: (masked with dots); Debug: False (selected); Login fallback options: 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. (unselected). The dialog has 'OK' and 'Cancel' buttons at the bottom right.

### Login Module Change Summary

Login Module changes updated.

OK

Stap 10. Selecteer **Server**> **Single Server Management** en selecteer vervolgens **Local User Setup** en selecteer **Add**.





The screenshot shows the Cisco Security Manager interface. On the left is a 'Navigator' pane with the following items: 'Browser-Server Security mode setup', 'Local User Policy Setup', 'Local User Setup' (highlighted with a red box), 'Role Management Setup', and 'Certificate Setup'. The main area is titled 'Local User Setup' and displays a table of users. The table has a header 'Users' and a 'Showing 206 records' indicator. The table contains 18 rows of user information, each with a checkbox and a name. At the bottom of the table, there are several buttons: 'Import Users', 'Export Users', 'Edit', 'Delete', 'Add' (highlighted with a red box), and 'Modify My Profile'. A tooltip is visible over the 'Add' button, stating 'Select items then take an action'.

	Users
1.	<input type="checkbox"/> Aaron Logan
2.	<input type="checkbox"/> Adrian Lotrean
3.	<input type="checkbox"/> Adrian Richards
4.	<input type="checkbox"/> ahohenstein
5.	<input type="checkbox"/> Aida Agular
6.	<input type="checkbox"/> Alaric Castain
7.	<input type="checkbox"/> alem.weldehimanot
8.	<input type="checkbox"/> allen.spiegel
9.	<input type="checkbox"/> Andrew OConnor
10.	<input type="checkbox"/> Anwar Khan
11.	<input type="checkbox"/> amand.smith
12.	<input type="checkbox"/> Bernard Alston
13.	<input type="checkbox"/> bthess
14.	<input type="checkbox"/> Bill Mason
15.	<input type="checkbox"/> bill.nash
16.	<input type="checkbox"/> Billy Vaughan
17.	<input type="checkbox"/> bpiotnik
18.	<input type="checkbox"/> Bruffler, Loran

**Stap 1.** Definieer de zelfde gebruikersnaam en het wachtwoord die op ISE op stap 5 zijn gemaakt onder de ISE configuratie sectie, de rol van de **taakautorisatie van de Help-Desktop** worden gebruikt in dit voorbeeld. Selecteer **OK** om de beheerder op te slaan.

**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

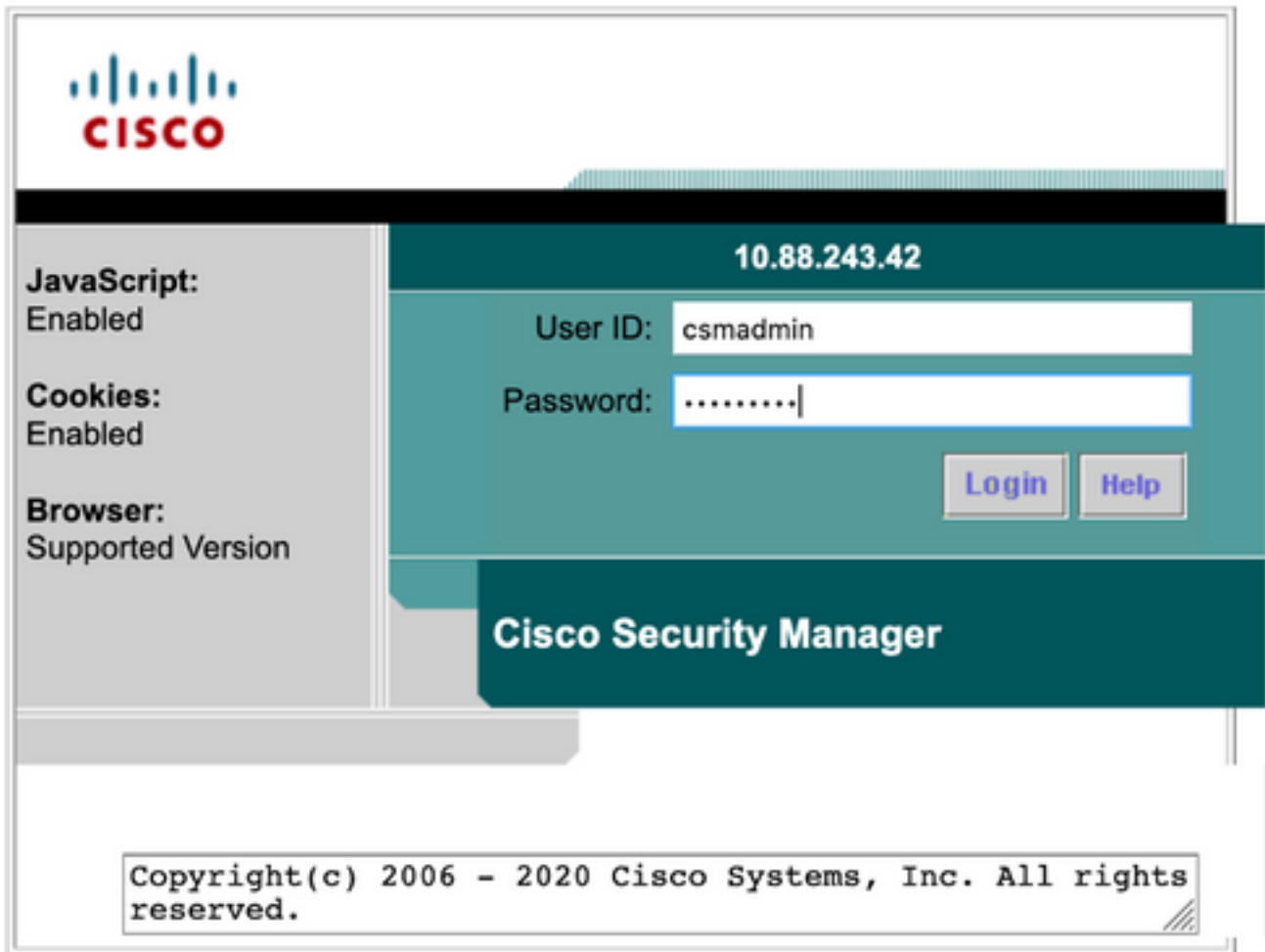
**Device level Authorization**

Not Applicable

## Verifiëren

### Cisco Security Manager-client voor UI

**Stap 1.** Open een nieuwe browser van het venster en type [https://<enter\\_CSM\\_IP\\_Address>](https://<enter_CSM_IP_Address>), gebruik csmadmin gebruikersnaam en wachtwoord die zijn gemaakt op stap 5 onder het configuratiescherm van ISE.



Succesvolle loggen in de poging kunnen worden geverifieerd op ISE TACACS-levende stammen

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		ise30	CSM422

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

## Cisco Security Manager-clienttoepassing

**Stap 1.** Meld u aan bij de Cisco Security Manager-clienttoepassing met de helpdesk Admin-account.



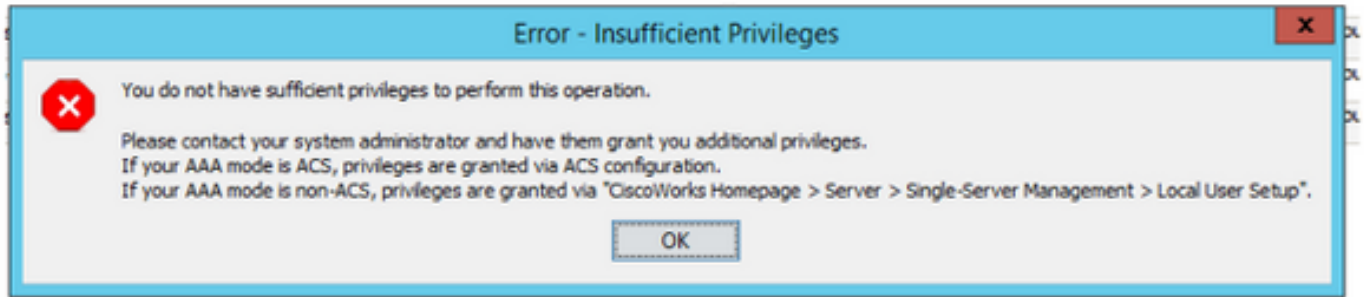
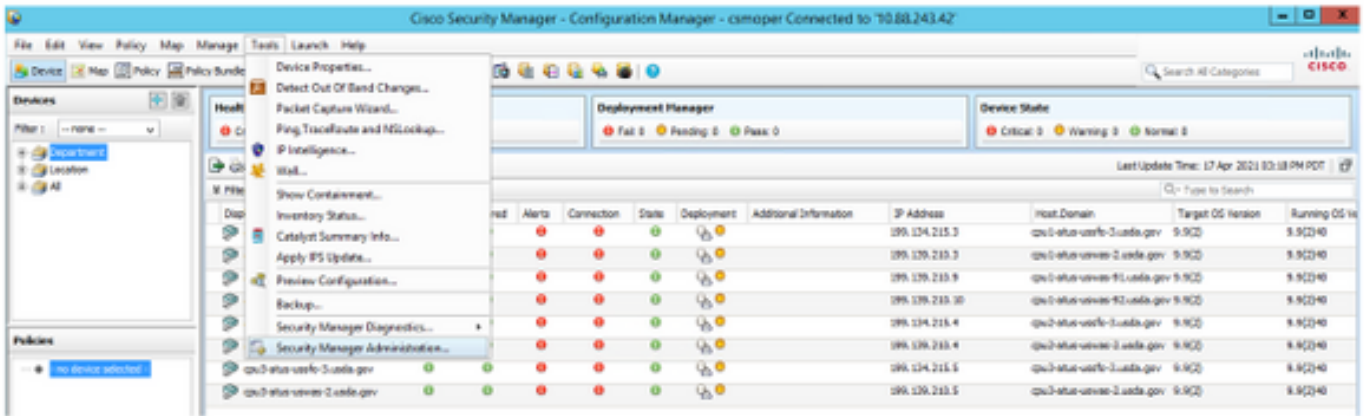
Succesvolle loggen in de poging kunnen worden geverifieerd op ISE TACACS-levende stammen

#### 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

**Stap 2.** Selecteer **Gereedschappen > Security Manager-beheerprogramma** van de CSM-client en er verschijnt een foutbericht dat er geen rechten zijn.



**Stap 3.** Herhaal stappen 1 tot en met 3 met **csadmin**-account om de juiste rechten te valideren, is aan deze gebruiker geleverd.

## Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

### Communicatievalidatie met TCP-pomp op ISE

**Stap 1.** Meld u aan bij ISE en navigeer naar het pictogram drie regels in de linker bovenhoek en selecteer **Operations>Troubleshooter>Diagnostische tools**.

**Stap 2.** Selecteer onder **Algemene gereedschappen** de optie **TCP-pompen** en selecteer vervolgens **Add+**. Selecteer Hostname, de naam van het Netwerkinterfacebestand, de bestandsnaam en naar keuze een filter om alleen CSM IP-adrescommunicatiestroom te verzamelen. Selecteer **Opslaan en uitvoeren**

**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

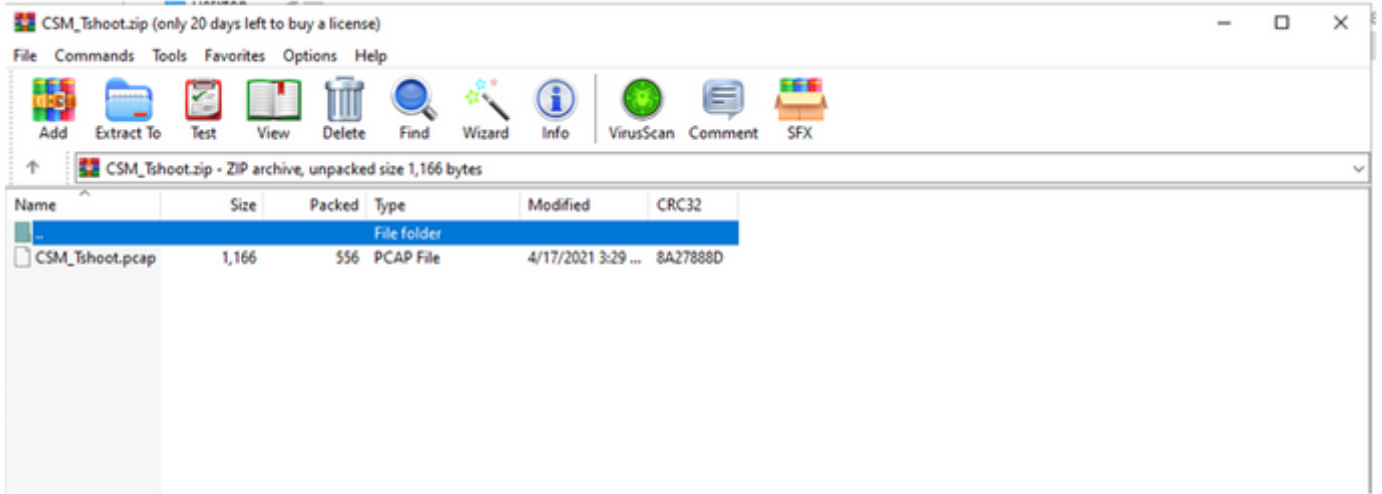
Cancel Save Save and Run

**Stap 3.** Meld u aan bij CSM-clienttoepassing of client-UI en typt u de admin-referenties.

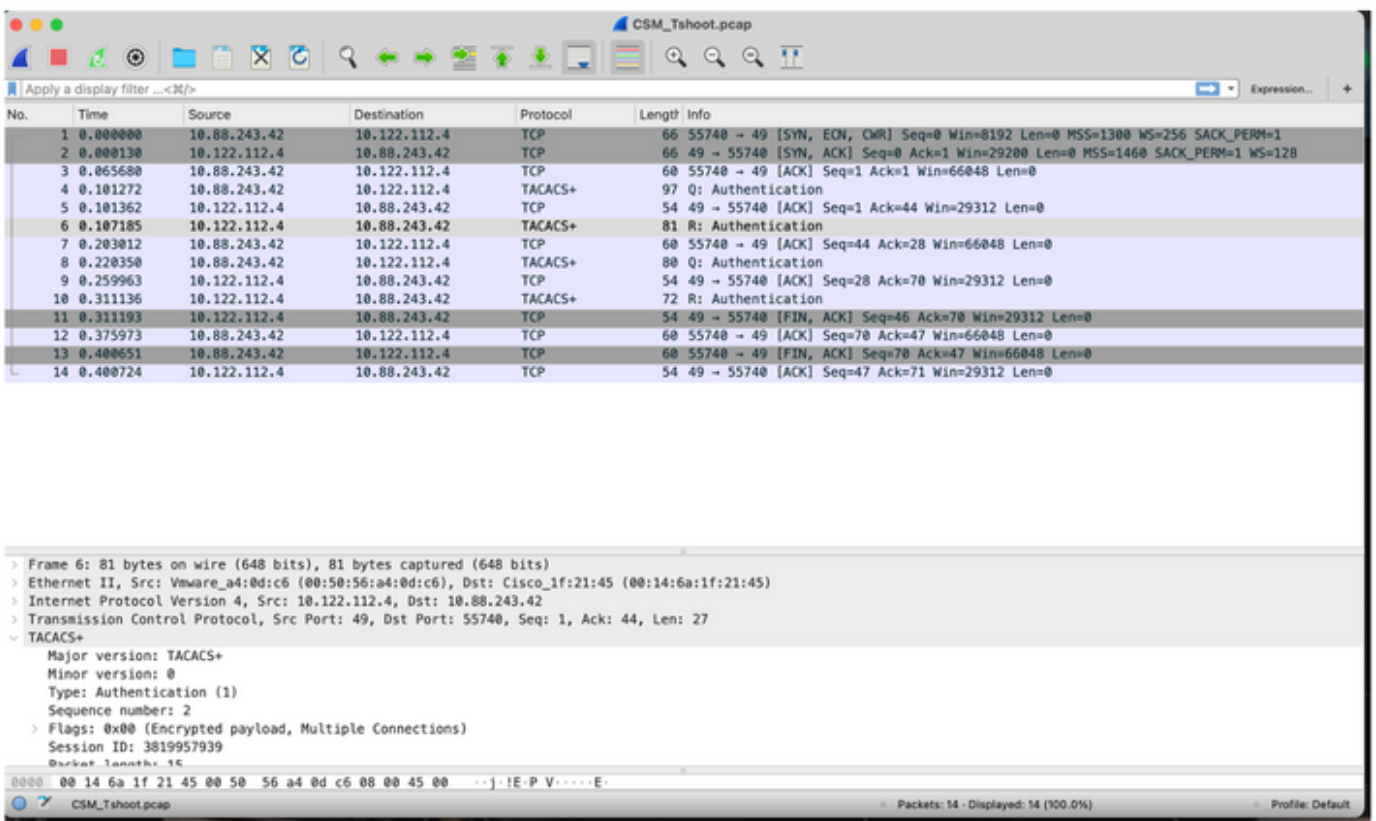
**Stap 4.** Selecteer op ISE de knop **Stop** en controleer of het PDF-bestand naar de gedefinieerde opslaglocatie is verzonden.

Refresh Add Edit Trash Start Stop Download Filter

<input type="checkbox"/>	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



Stap 5. Open het PDF-bestand om de succesvolle communicatie tussen CSM en ISE te valideren.



Als er geen items worden weergegeven in een cap-bestand, valideer dan het volgende:

1. Apparaatbeheerservice is ingeschakeld voor ISE-knooppunt
2. Rechts ISE IP-adres is toegevoegd aan de CSM-configuratie
3. Als er een firewall in het midden is, is poort 49 (TACACS) toegestaan.