

# Integrazione CSM TACACS con ISE

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Procedura di autenticazione](#)

[Configurazione di ISE](#)

[Configurazione CSM](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

Questo documento descrive la procedura per integrare Cisco Security Manager (CSM) con Identity Services Engine (ISE) per autenticare gli utenti amministratori con il protocollo TACACS+.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CSM Server versione 4.2
- ISE versione 3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Per impostazione predefinita, Cisco Security Manager (CSM) utilizza una modalità di autenticazione chiamata Ciscoworks per autenticare e autorizzare gli utenti a livello locale, in modo da avere un metodo di autenticazione centralizzato che è possibile utilizzare Cisco Identity Service Engine tramite il protocollo TACACS.

## Configurazione

### Esempio di rete



### Procedura di autenticazione

Passaggio 1. Accedere all'applicazione CSM con le credenziali dell'utente amministratore.

Passaggio 2. Il processo di autenticazione attiva e ISE convalida le credenziali localmente o tramite Active Directory.

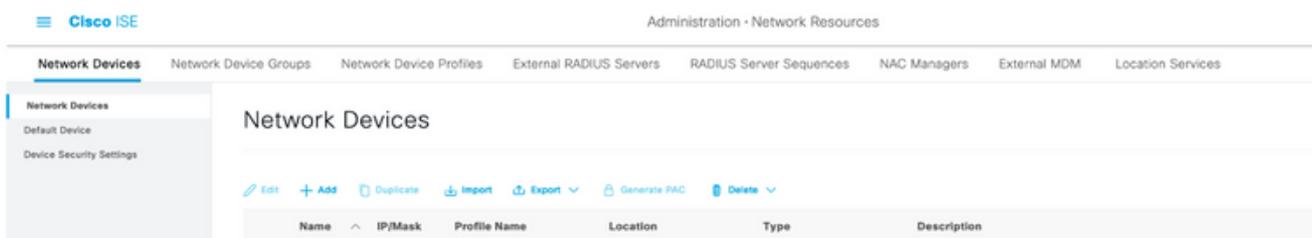
Passaggio 3. Una volta completata l'autenticazione, ISE invia un pacchetto di autorizzazione per autorizzare l'accesso al CSM.

Passaggio 4. CSM esegue il mapping del nome utente con l'assegnazione del ruolo utente locale.

Passaggio 5. ISE mostra un log live di autenticazione completato.

### Configurazione di ISE

Passaggio 1. Selezionare l'icona a tre righe  nell'angolo superiore sinistro e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**.



Passaggio 2. Selezionare il pulsante **+Add** e immettere i valori corretti per Network Access Device Name e IP Address, quindi verificare la casella di controllo **TACACS Authentication Settings** e definire un segreto condiviso. Selezionare il pulsante **Invia**.

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: CSM432

Description:

IP Address: 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](#)



**Passaggio 3.** Selezionare l'icona delle tre linee nell'angolo superiore sinistro e selezionare **Amministrazione > Gestione delle identità > Gruppi**.

**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

**Passaggio 4.** Passare alla cartella **Gruppi di identità utente** e selezionare il pulsante **+Aggiungi**. Definire un nome e selezionare il pulsante **Invia**.

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 icons for refresh and settings.

**Nota:** In questo esempio vengono creati i gruppi CSM Admin e CSM Oper Identity. È possibile ripetere il passaggio 4 per ogni tipo di utente Admin su CSM



**Passaggio 5.** Selezionare l'icona a tre righe e selezionare **Amministrazione > Gestione delle identità > Identità**. Selezionare il pulsante **+Aggiungi** e definire il nome utente e la password, quindi selezionare il gruppo a cui appartiene l'utente. In questo esempio vengono creati gli utenti **csmadmin** e **csmoper**, assegnati rispettivamente ai gruppi CSM Admin e 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

Other 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 (yyyy-mm-dd)

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 Refresh Settings

Edit + Add Change Status Import Export Delete Duplicate All Filter

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	



**Passaggio 6.** Selezionare  e selezionare **Amministrazione > Sistema > Distribuzione**.  
 Selezionare il nodo hostname e abilitare il **servizio Device Admin**

Hostname	Personas	Role(s)	Services	Node Status
Ise30	Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER, DE...	<span style="color: green;">✔</span>

> Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

**Nota:** In caso di distribuzione distribuita, selezionare il nodo PSN che gestisce le richieste TACACS

**Passaggio 7.** Selezionare l'icona a tre righe e passare ad **Amministrazione > Amministrazione dispositivi > Elementi della policy**. Passare a **Risultati > Set di comandi TACACS**. Selezionare **+Pulsante Aggiungi**, definire un nome per il set di comandi e attivare la **casella di controllo Consenti qualsiasi comando non elencato sotto** la casella di controllo. Selezionare **Sottometti**.

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

**Passaggio 8.** Selezionare l'icona a tre righe nell'angolo superiore sinistro e selezionare

## Amministrazione->Amministrazione dispositivi->Set di criteri di amministrazione dispositivi.

Seleziona  situato sotto il titolo Set di criteri, definire un nome e selezionare il pulsante + al centro per aggiungere una nuova condizione.

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 Administrators		+	Select from list	+	 	
<span style="color: green;">✔</span>	Default	Tacacs Default policy set		Default Device Admin	0	 	

**Passaggio 9.** Nella finestra Condizione, selezionare Aggiungi attributo, quindi selezionare Icona **periferica di rete** seguito da Indirizzo IP periferica di accesso alla rete. Selezionare **Attribute Value** (Valore attributo) e aggiungere l'indirizzo IP del CSM. Selezionare **Use** once done (Usa al termine).

### Conditions Studio

#### Library

Search by Name



No conditions found - reset filters.

#### Editor

Network Access-Device IP Address

 Equals

[Set to 'is not'](#) Duplicate Save

NEW | AND | OR

Close

Use

**Passaggio 10.** In Consenti protocolli, sezione, selezionare **Device Default Admin**. Selezionare **Salva**

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		

**Passaggio 11.** Selezionare la freccia destra



icona del set di criteri per la definizione dei criteri di autenticazione e autorizzazione

**Passaggio 12.** Selezionare  situato sotto il titolo del criterio di autenticazione, definire un nome e selezionare il segno + al centro per aggiungere una nuova condizione. Nella finestra Condizione selezionare Aggiungi attributo, quindi **Icona periferica di rete** seguito da Indirizzo IP periferica di accesso alla rete. Selezionare **Attribute Value** (Valore attributo) e aggiungere l'indirizzo IP del CSM. Selezionare **Use** once done (Usa al termine)

**Passaggio 13.** Selezionare gli utenti **interni** nell'archivio identità e selezionare **Salva**

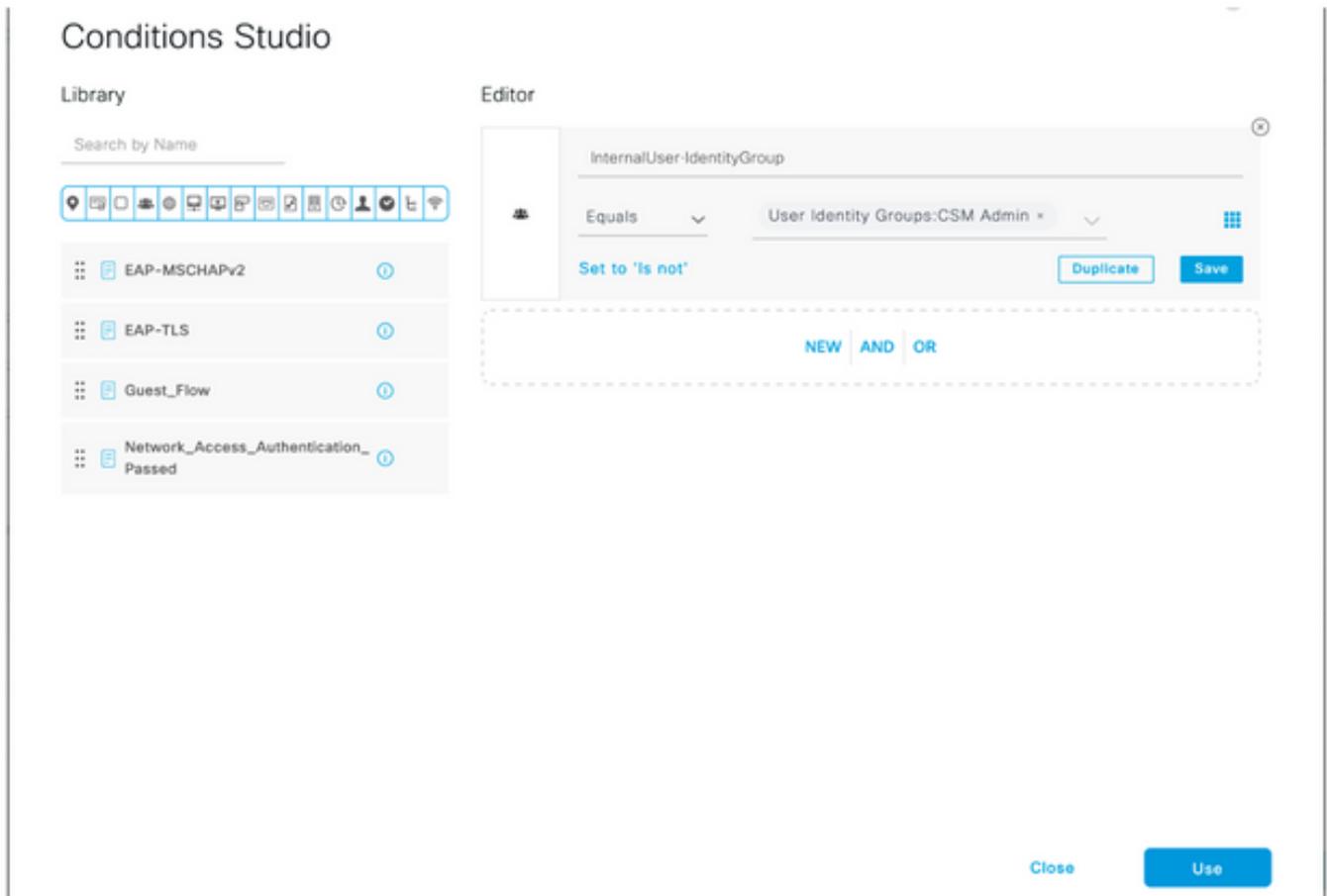
Authentication Policy (1)

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

**Nota:** È possibile modificare l'archivio identità in archivio AD se ISE è aggiunto a un Active Directory.

**Passaggio 14.** Selezionare  sotto il titolo del criterio di autorizzazione, definire un nome e selezionare il pulsante + al centro per aggiungere una nuova condizione. Nella finestra Condizione selezionare Aggiungi attributo, quindi selezionare l'icona **Gruppo di identità** seguita da **Utente interno: Gruppo di identità**. Selezionare il gruppo CSM Admin e **Usa**.



**Passaggio 15.** In Set di comandi selezionare Consenti tutti i set di comandi creati nel passaggio 7, quindi selezionare **Salva**

Ripetere i passaggi 14 e 15 per il gruppo Oper CSM

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	⚙️	

**Passaggio 16 (facoltativo).** Selezionare l'icona a tre righe nell'angolo superiore sinistro e Selezionare **Amministrazione>Sistema>Manutenzione>Repository**, selezionare **+Aggiungi** per aggiungere un repository utilizzato per memorizzare il file di dump TCP per la risoluzione dei problemi.

**Passaggio 17 (facoltativo).** Definire un nome repository, un protocollo, un nome server, un percorso e le credenziali. Al termine, selezionare **Invia**.

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

## Configurazione CSM

**Passaggio 1.** Accedere all'applicazione client Cisco Security Manager con l'account admin locale. Dal menu passare a **Strumenti > Amministrazione di Security Manager**

Cisco Security Manager  
 Version 4.22.0 Service Pack 1

Server Name

Username

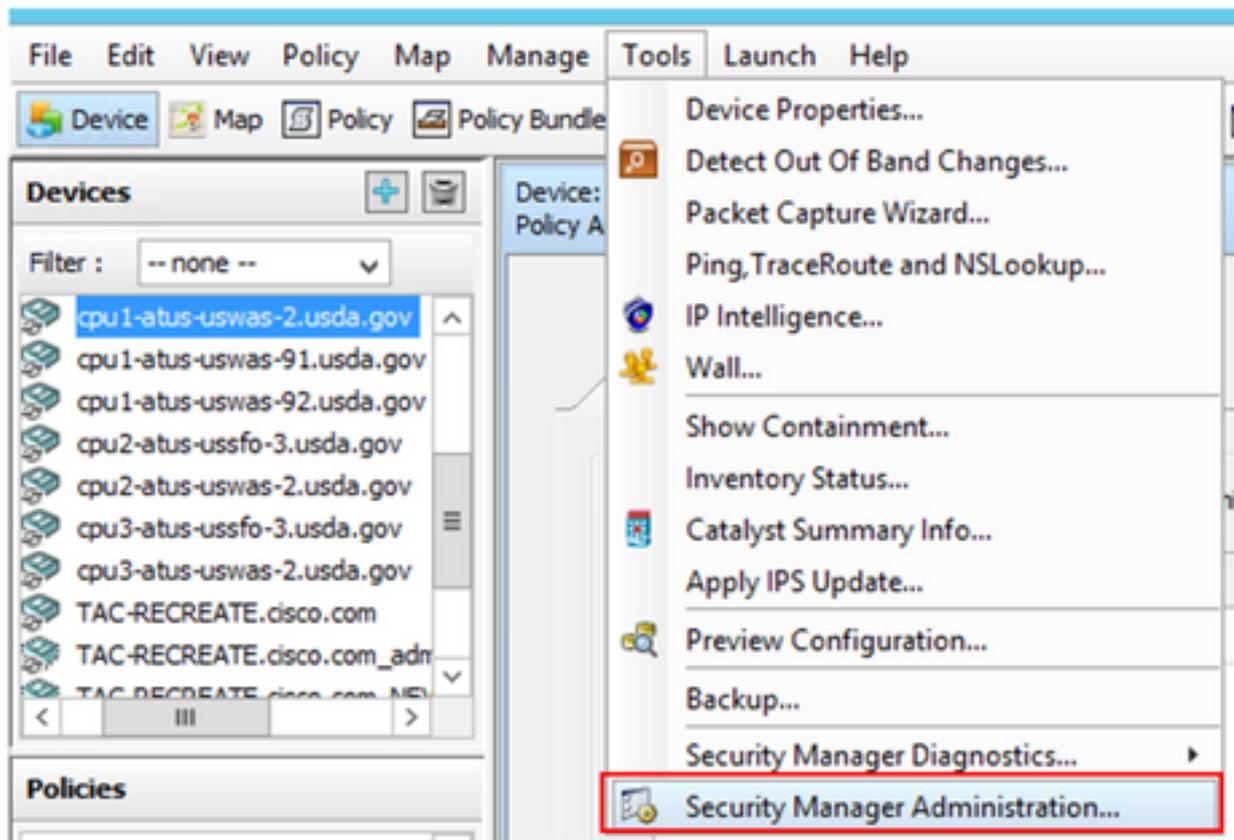
Password

Default View

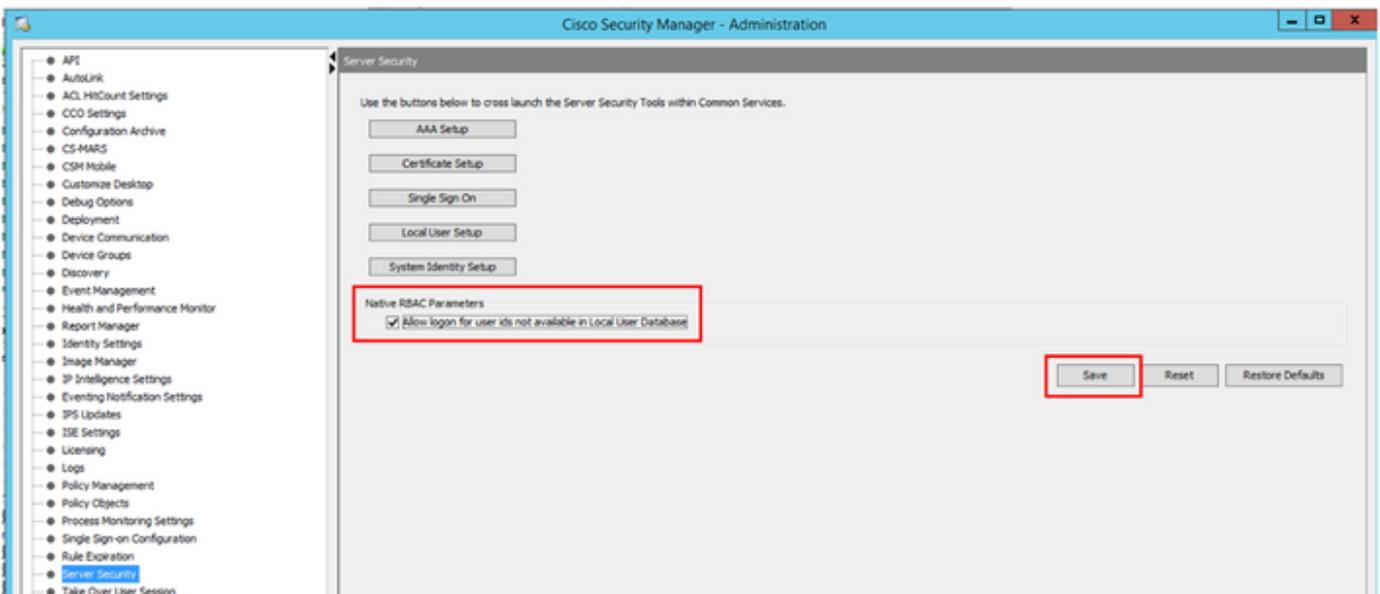
[Login](#) [Help](#)

© 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**



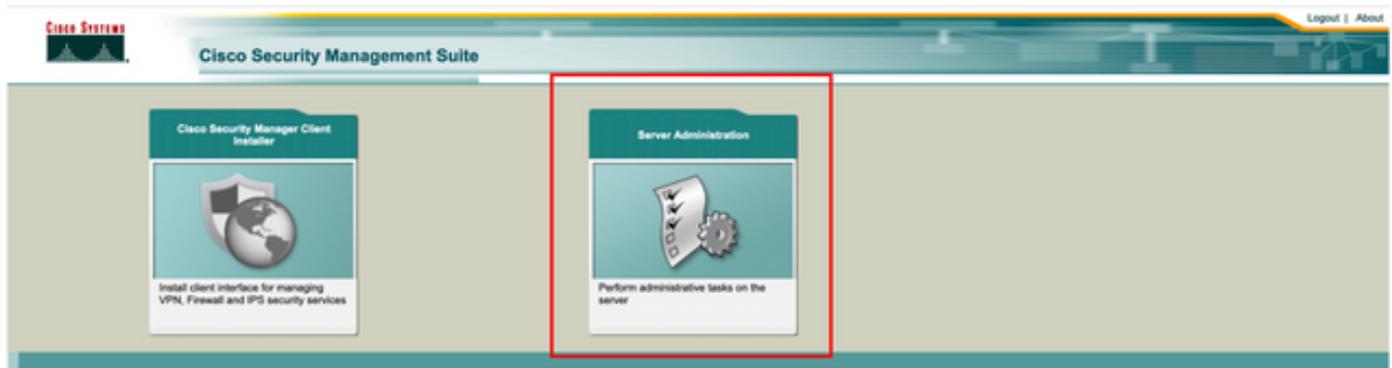
**Passaggio 2.** Selezionare la casella in **Parametri RBAC nativo**. Selezionare **Salva** e chiudi



**Passaggio 3.** Dal menu selezionare **File > Sottometti**. **File > Invia (Submit)**.

**Nota:** Tutte le modifiche devono essere salvate e, in caso di modifiche alla configurazione, devono essere inviate e distribuite.

**Passaggio 4.** Passare all'interfaccia utente di gestione CSM, digitare [https://<enter\\_CSM\\_IP\\_Address>](https://<enter_CSM_IP_Address>) e selezionare **Amministrazione server**.



**Nota:** I passaggi da 4 a 7 mostrano la procedura per definire il ruolo predefinito per tutti gli amministratori che non sono definiti su ISE. Questi passaggi sono facoltativi.

**Passaggio 5.** Verificare che la modalità di autenticazione sia impostata su **CiscoWorks Local e Online** userID è l'account amministratore locale creato su CSM.

Common Services Home

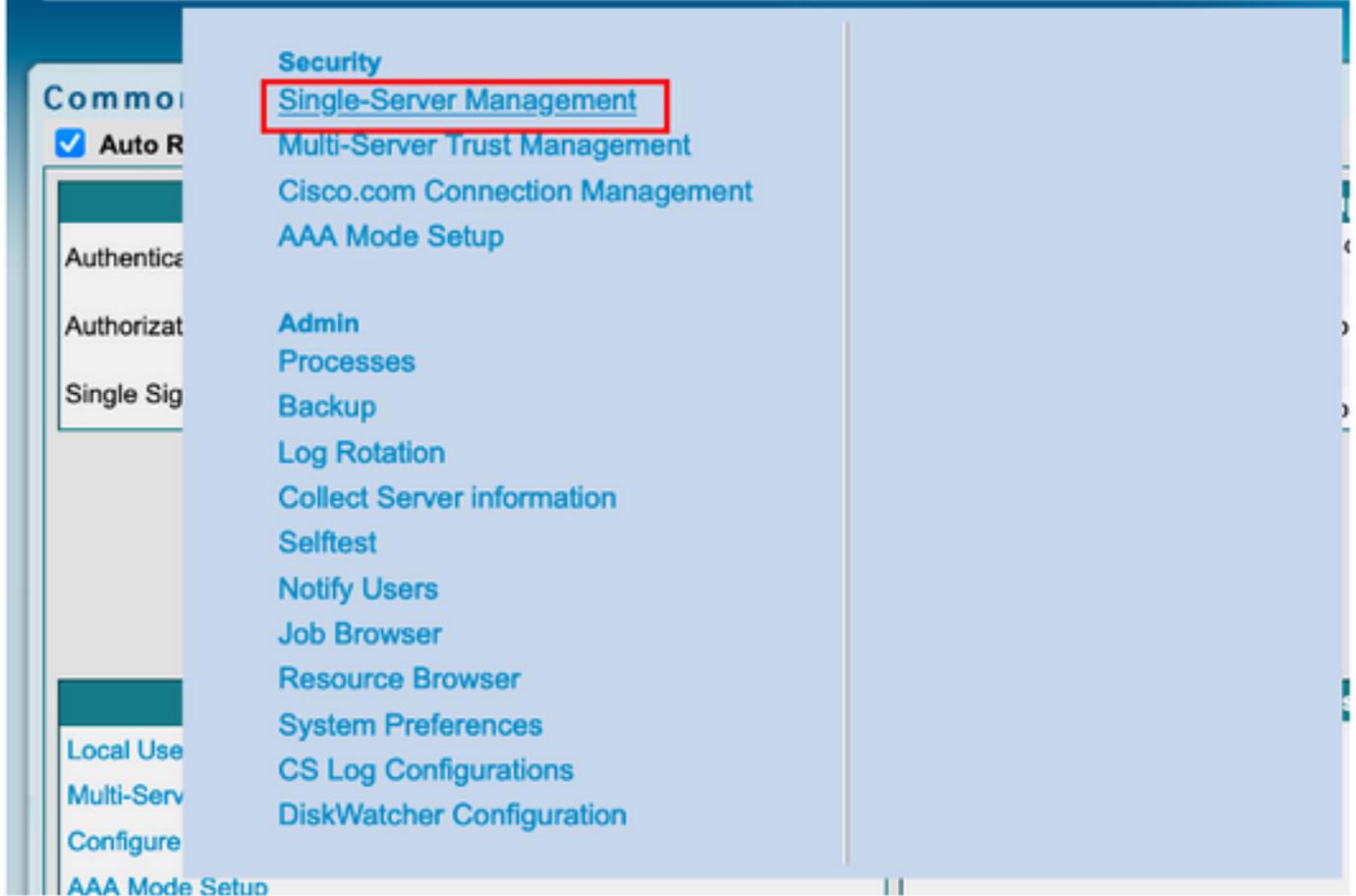
Version: 4.2.2

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

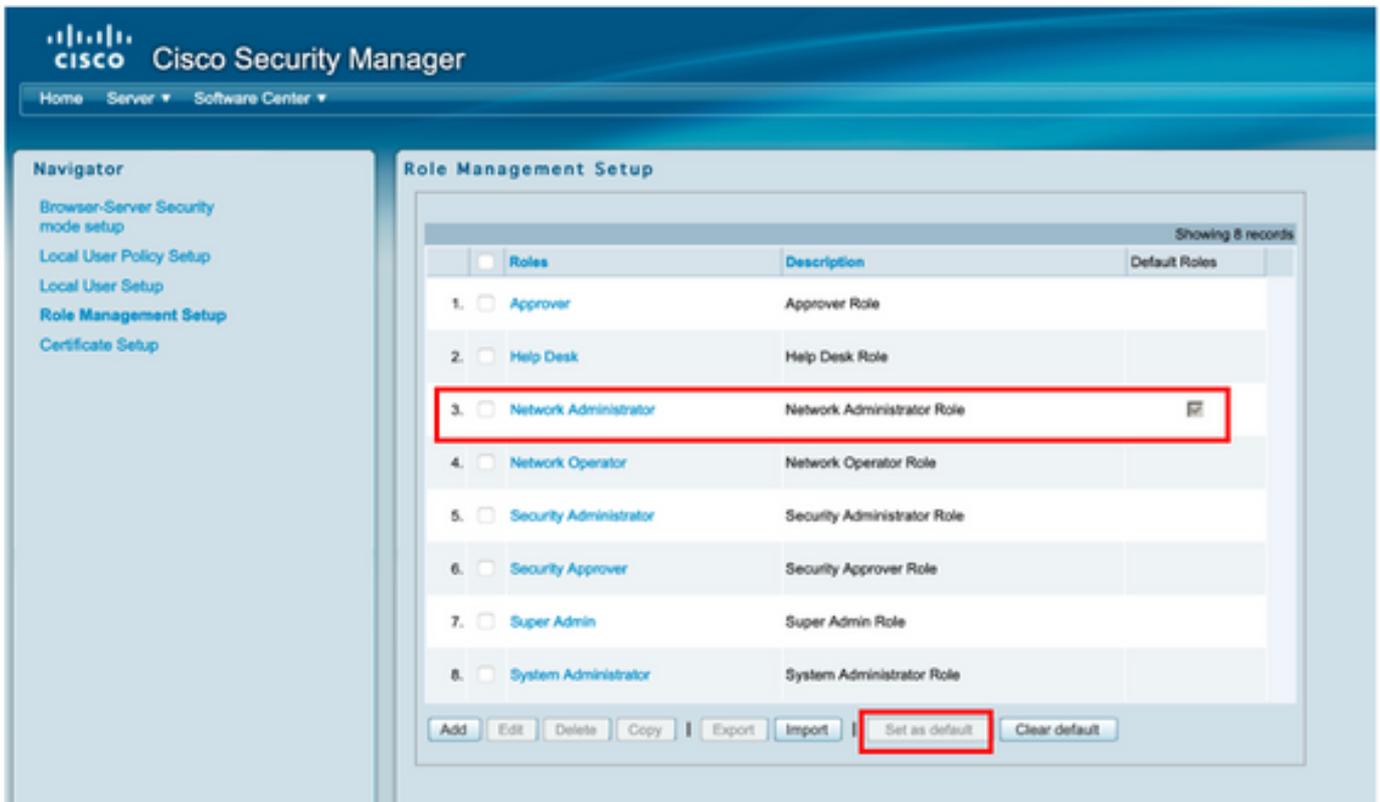
Security		Backup		Recently Completed Jobs				
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job ID	Job Type	Status	Description	Completed At
Authorization Mode	CiscoWorks Local	Last Backup Completed at	Not found or unable to detect	1001.1370	SystemCheckUtility	Succeeded	SysCheckTest	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

**Passaggio 6.** Passare a **Server** e selezionare **Gestione server singolo**



**Passaggio 7.** Selezionare Impostazione gestione ruoli e selezionare il privilegio predefinito che tutti gli utenti amministratori ricevono al momento dell'autenticazione. Nell'esempio viene utilizzato Amministratore di rete. Una volta selezionato, selezionare **Imposta come predefinito**.



Passaggio 8. Selezionare **Server>Ruolo di installazione della modalità AAA**, quindi selezionare l'opzione **TACACS+** e infine selezionare **change** per aggiungere informazioni ISE.





**Passaggio 9.** Definire l'indirizzo IP e la chiave ISE. Facoltativamente, è possibile selezionare l'opzione che consente a tutti gli utenti con autenticazione locale o a un solo utente se l'accesso non riesce. Per questo esempio, come metodo di fallback è consentito l'utilizzo dell'opzione Solo utente amministratore. Selezionare **OK** per salvare le modifiche.

The 'Login Module Options' dialog box is shown. It contains the following fields and options:

- 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:** Radio buttons for 'True' and 'False', with 'False' selected.
- Login fallback options:** Radio buttons for three 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: (selected)
  - Allow no fallbacks to the Local Authentication login.

The text field for the selected fallback option contains 'admin' followed by '(comma separated)'. 'OK' and 'Cancel' buttons are at the bottom right.

### Login Module Change Summary

Login Module changes updated.

OK

Passaggio 10. Selezionare **Server**> **Gestione server singolo**, quindi selezionare **Configurazione utente locale** e selezionare **Aggiungi**.



The screenshot shows the Cisco Security Manager interface. The top navigation bar includes the Cisco logo and the text 'Cisco Security Manager'. Below the navigation bar, there are links for 'Home', 'Server', and 'Software Center'. On the left side, there is a 'Navigator' pane with several menu 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 content area is titled 'Local User Setup' and displays a table of users. The table has a header row with a checkbox and the text 'Users'. Below the header, there are 17 rows of user entries, each with a checkbox and a name. The names are: 1. Aaron Logan, 2. Adrian Lotrean, 3. Adrian Richards, 4. ahohenstein, 5. Aida Agular, 6. Alaric Castain, 7. alem.weldehimanot, 8. allen.spiegel, 9. Andrew OConnor, 10. Anwar Khan, 11. amand.amith, 12. Bernard Alston, 13. bthess, 14. Bill Mason, 15. bill.nash, 16. Billy Vaughan, 17. bpiotnik. At the bottom of the table, there is a text prompt: 'Select items then take an action'. Below this prompt are several buttons: 'Import Users', 'Export Users', 'Edit', 'Delete', 'Add' (highlighted with a red box), and 'Modify My Profile'.

**Passaggio 11.** Definire lo stesso nome utente e la stessa password creati per ISE nel passaggio 5 nella sezione Configurazione ISE. In questo esempio vengono utilizzati i ruoli di autorizzazione delle attività **csmoper** e **Help Desk**. Per salvare l'utente amministratore, selezionare **OK**.

**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

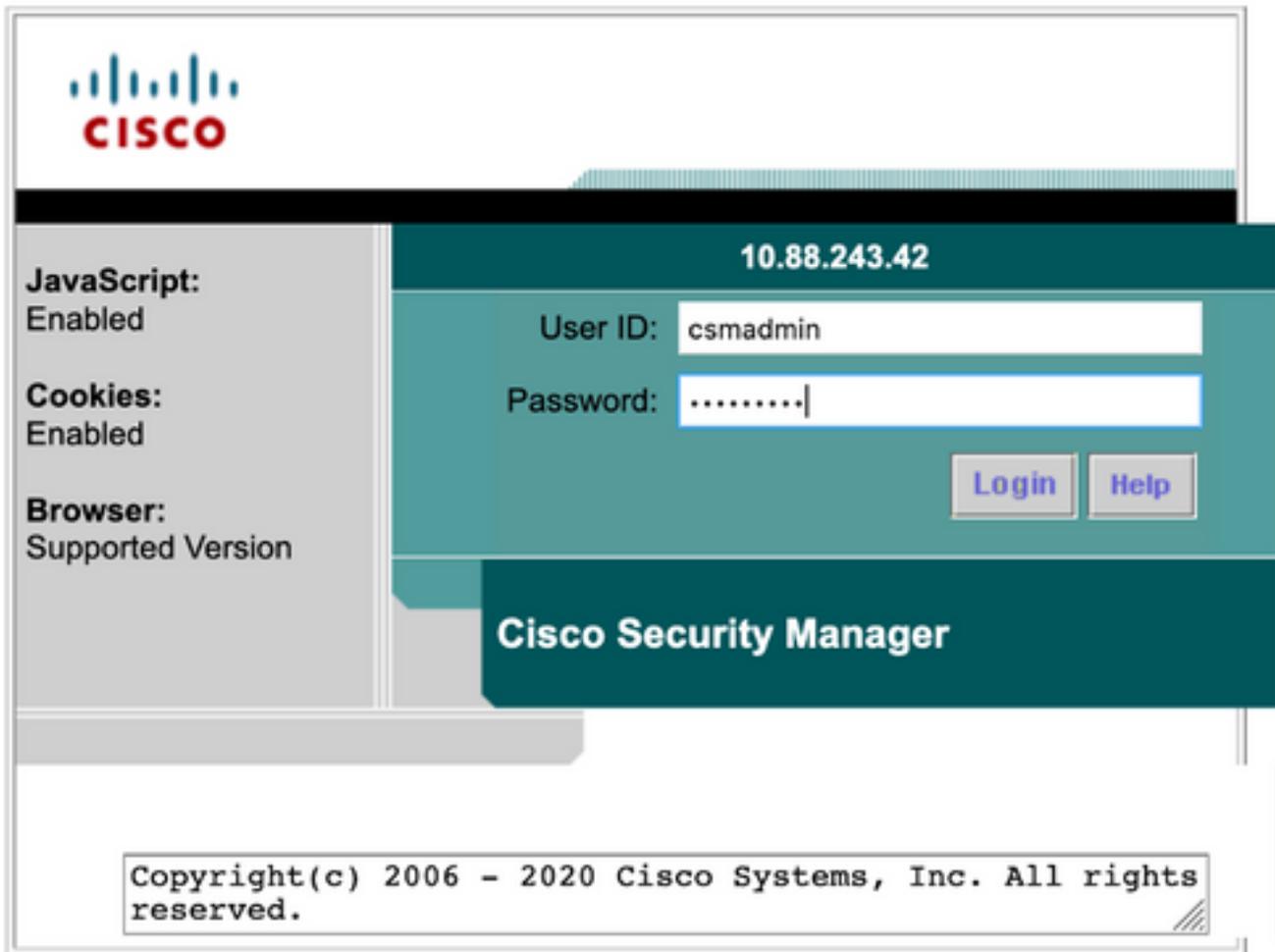
**Device level Authorization**

Not Applicable

## Verifica

### Interfaccia utente client di Cisco Security Manager

**Passaggio 1.** Aprire una nuova finestra del browser e digitare [https://<enter\\_CSM\\_IP\\_Address>](https://<enter_CSM_IP_Address>), utilizzare il nome utente e la password `csmadmin` creati nel passaggio 5 della sezione di configurazione ISE.



Sui log live ISE TACACS è possibile verificare l'esito del log nel tentativo

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

## Applicazione client Cisco Security Manager

**Passaggio 1.** Accedere all'applicazione client Cisco Security Manager con l'account di amministratore dell'helpdesk.



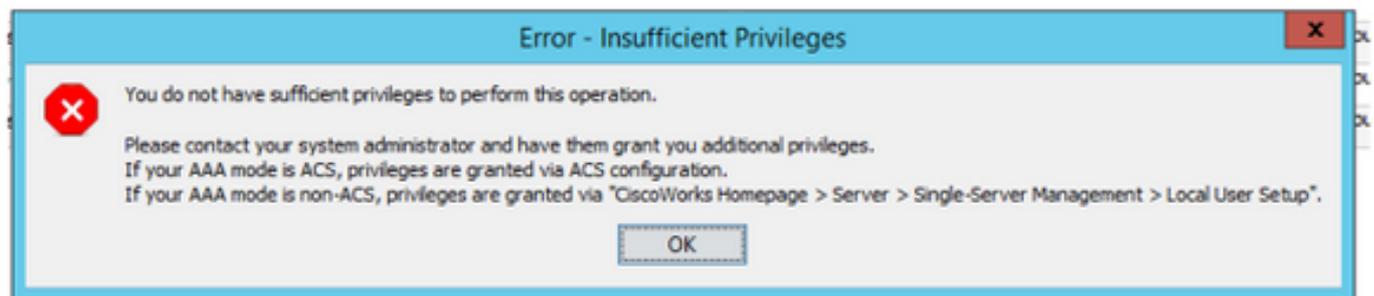
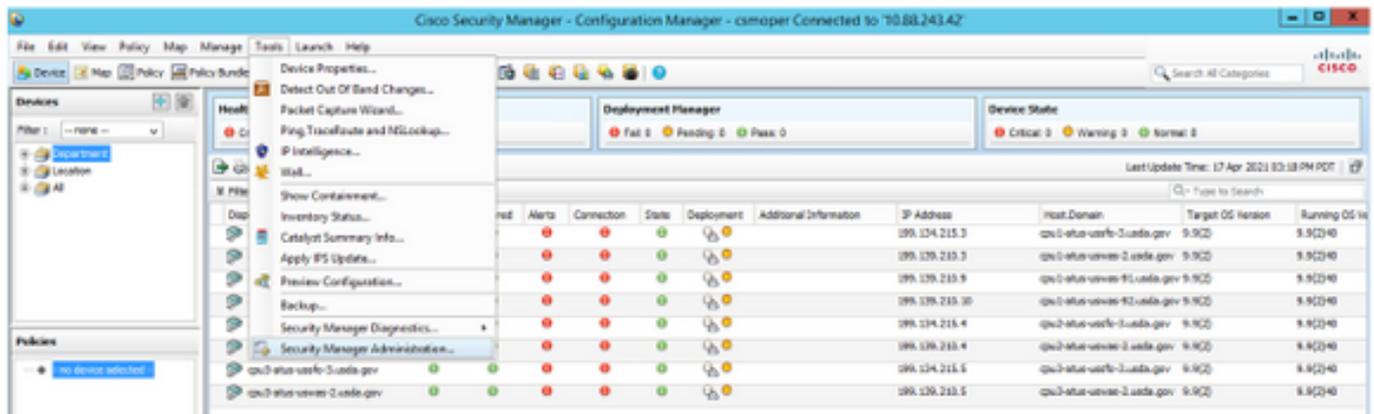
Sui log live ISE TACACS è possibile verificare l'esito del log nel tentativo

#### 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

**Passaggio 2.** Dal menu dell'applicazione client CSM selezionare **Strumenti > Amministrazione Security Manager**, deve essere visualizzato un messaggio di errore che indica la mancanza di privilegi.



**Passaggio 3.** Ripetere i passaggi da 1 a 3 con l'account **csmdadmin** per verificare che all'utente siano state fornite le autorizzazioni appropriate.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

### Convalida della comunicazione con lo strumento TCP Dump su ISE

**Passaggio 1.** Accedere ad ISE e selezionare l'icona con le tre righe nell'angolo superiore sinistro, quindi selezionare **Operations>Troubleshoot>Diagnostic Tools**.

**Passaggio 2.** In **Strumenti generali** selezionare **TCP Dump**, quindi selezionare **Add+**. Selezionare Nome host, Nome file interfaccia di rete, Repository e, facoltativamente, un filtro per raccogliere solo il flusso di comunicazione dell'indirizzo IP del CSM. Selezionare **Salva ed esegui**

**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

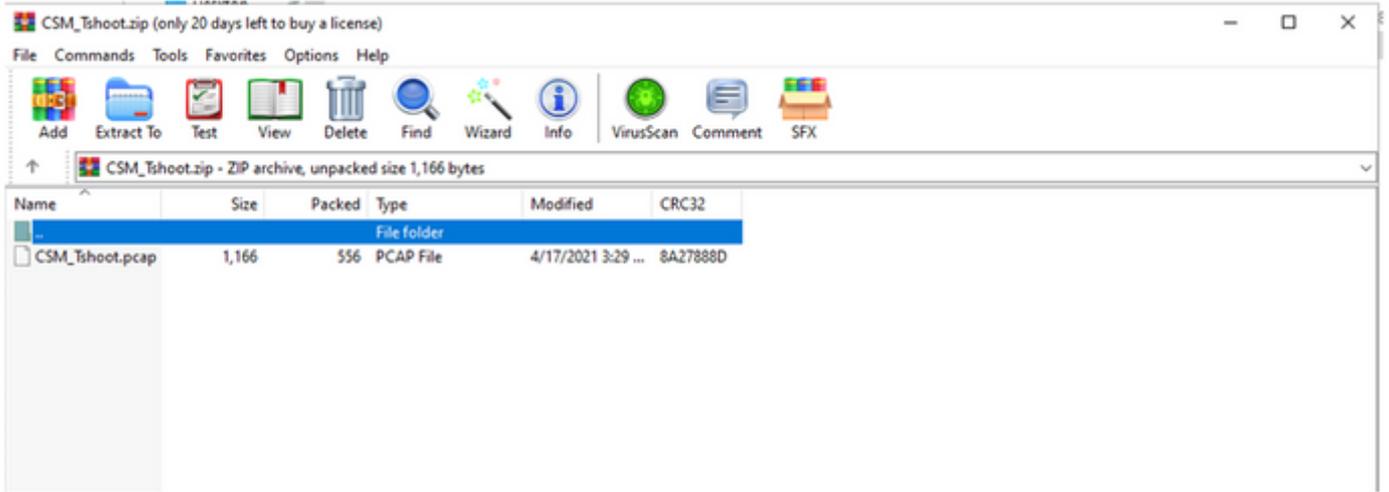
Cancel Save Save and Run

**Passaggio 3.** Accedere all'applicazione client CSM o all'interfaccia utente client e digitare le credenziali dell'amministratore.

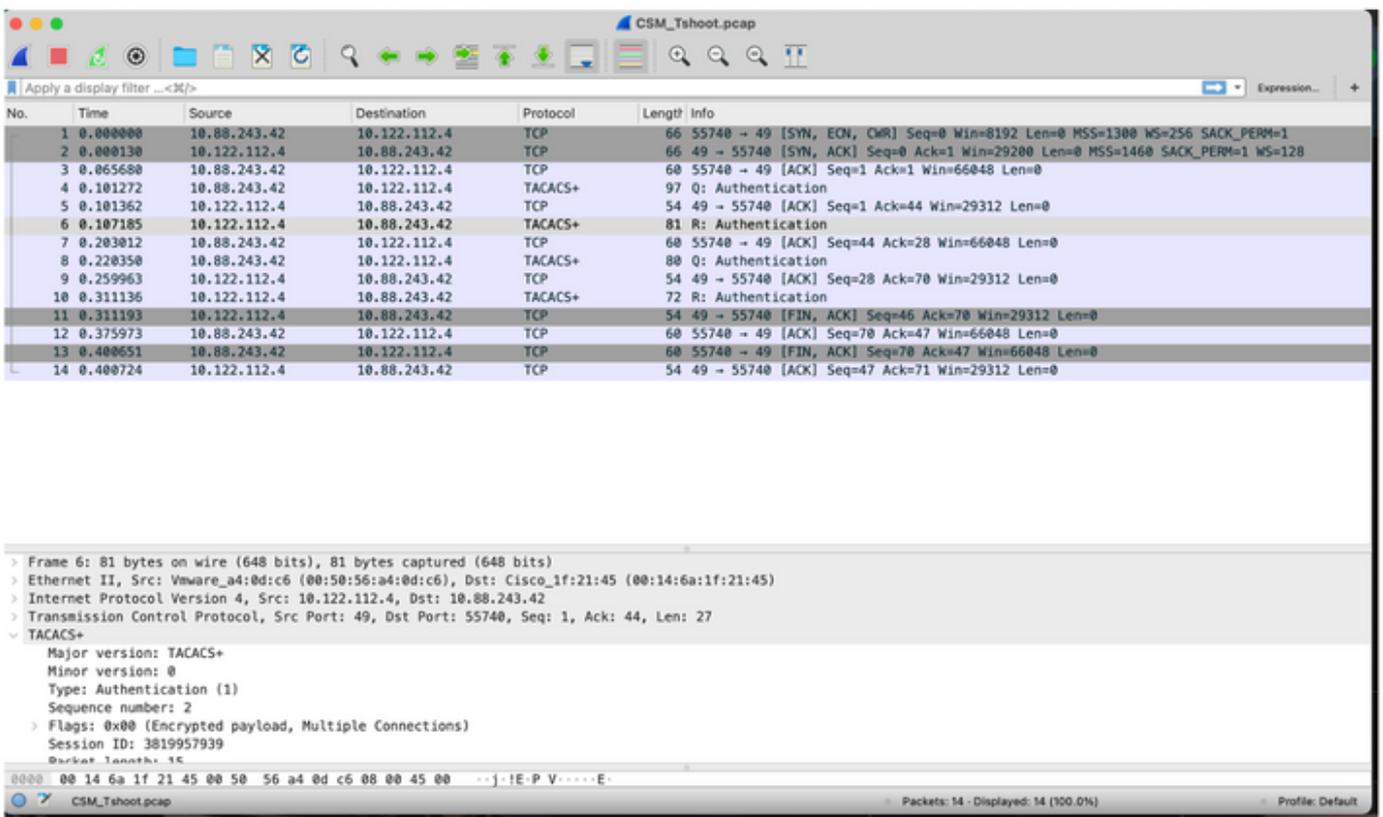
**Passaggio 4.** Su ISE, selezionare il pulsante **Stop** e verificare che il file pcap sia stato inviato al repository definito.

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



Passaggio 5. Aprire il file pcap per verificare la corretta comunicazione tra CSM e ISE.



Se nel file pcap non sono visualizzate voci, verificare quanto segue:

1. Il servizio Amministrazione dispositivi è abilitato sul nodo ISE
2. L'indirizzo IP ISE destro è stato aggiunto alla configurazione CSM
3. Se il firewall si trova nella parte centrale, verificare che la porta 49 (TACACS) sia autorizzata.