

Integración de CSM TACACS con ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Procedimiento de autenticación](#)

[Configuración de ISE](#)

[Configuración de CSM](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el procedimiento para integrar Cisco Security Manager (CSM) con Identity Services Engine (ISE) para la autenticación de usuarios administradores con el protocolo TACACS+.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor CSM versión 4.22
- ISE versión 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

De forma predeterminada, Cisco Security Manager (CSM) utiliza un modo de autenticación denominado CiscoWorks para autenticar y autorizar a los usuarios de forma local, con el fin de disponer de un método de autenticación centralizado, puede utilizar Cisco Identity Service Engine a través del protocolo TACACS.

Configurar

Diagrama de la red



Procedimiento de autenticación

Paso 1. Inicie sesión en la aplicación CSM con las credenciales del usuario administrador.

Paso 2. El proceso de autenticación desencadena e ISE valida las credenciales localmente o a través de Active Directory.


Paso 3. Una vez que la autenticación se realiza correctamente, ISE envía un paquete de permiso para autorizar el acceso al CSM.

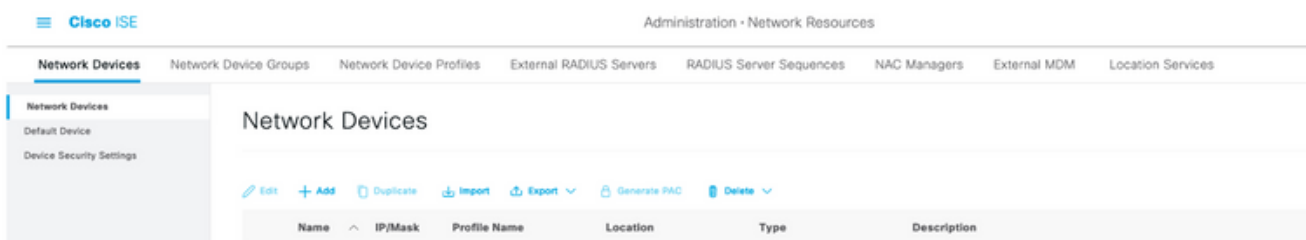
Paso 4. CSM asigna el nombre de usuario con la asignación de rol de usuario local.

Paso 5. ISE muestra un registro en directo de autenticación exitoso.

Configuración de ISE



Paso 1. Seleccione el icono de tres líneas  se encuentra en la esquina superior izquierda y navegue hasta **Administración > Recursos de red > Dispositivos de red.**



Paso 2. Seleccione el botón **+Add** e ingrese los valores adecuados para Network Access Device Name y IP Address, luego verifique la **casilla de verificación TACACS Authentication Settings** y defina un secreto compartido. Seleccione el botón **Enviar**.

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](#)



Paso 3. Seleccione el icono de tres líneas se encuentra en la esquina superior izquierda y navegue hasta **Administración > Administración de identidades > Grupos**.

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


Paso 4. Navegue hasta la carpeta **Grupos de identidad de usuario** y seleccione el botón **+Agregar** botón. Defina un nombre y seleccione el botón **Enviar**.

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 below the toolbar 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	

Nota: Este ejemplo crea grupos de administración CSM y de identidad Oper CSM. Puede repetir el paso 4 para cada tipo de usuarios de administración en CSM



Paso 5. Seleccione el icono de tres líneas  y navegue hasta **Administración > Administración de identidades > Identidades**. Seleccione el botón **+Agregar** y defina el nombre de usuario y la contraseña y, a continuación, seleccione el grupo al que pertenece el usuario. En este ejemplo, crea los usuarios **csmadmin** y **csmoper** y se asigna al grupo CSM Admin y CSM Oper respectivamente.

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 (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 ↻ ⚙

✎ 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	



Paso 6. Seleccionar y navegue hasta **Administración > Sistema > Implementación**. Seleccione el nodo de nombre de host y active **Device Admin Service**

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 ⓘ

Nota: En caso de implementación distribuida, seleccione el nodo PSN que gestiona las solicitudes TACACS

Paso 7. Seleccione el icono de tres líneas y navegue hasta **Administración > Administración de dispositivos > Elementos de políticas**. Vaya a **Resultados > Conjuntos de Comandos TACACS**. Seleccione +botón **Agregar**, defina un nombre para el conjunto de comandos y habilite la **casilla de verificación Permitir cualquier comando que no aparezca en la siguiente lista**. Seleccione **Enviar**.

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

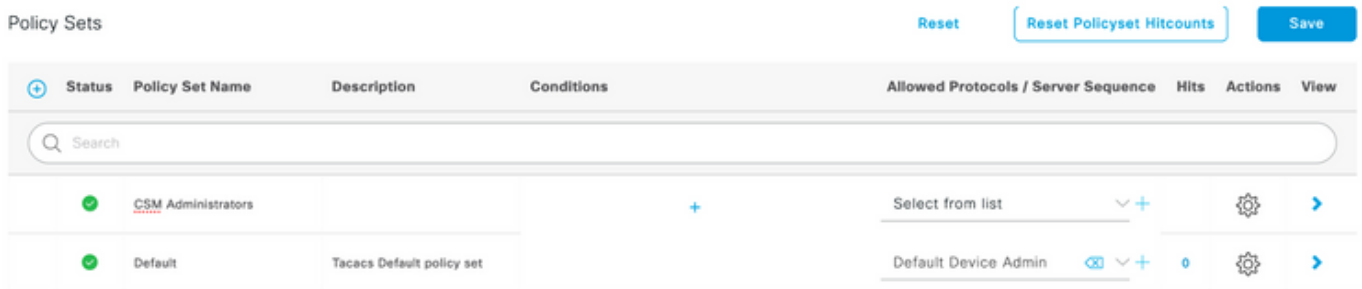
+ Add Trash Edit Move Up Move Down

Grant	Command	Arguments
No data found.		

Cancel Submit

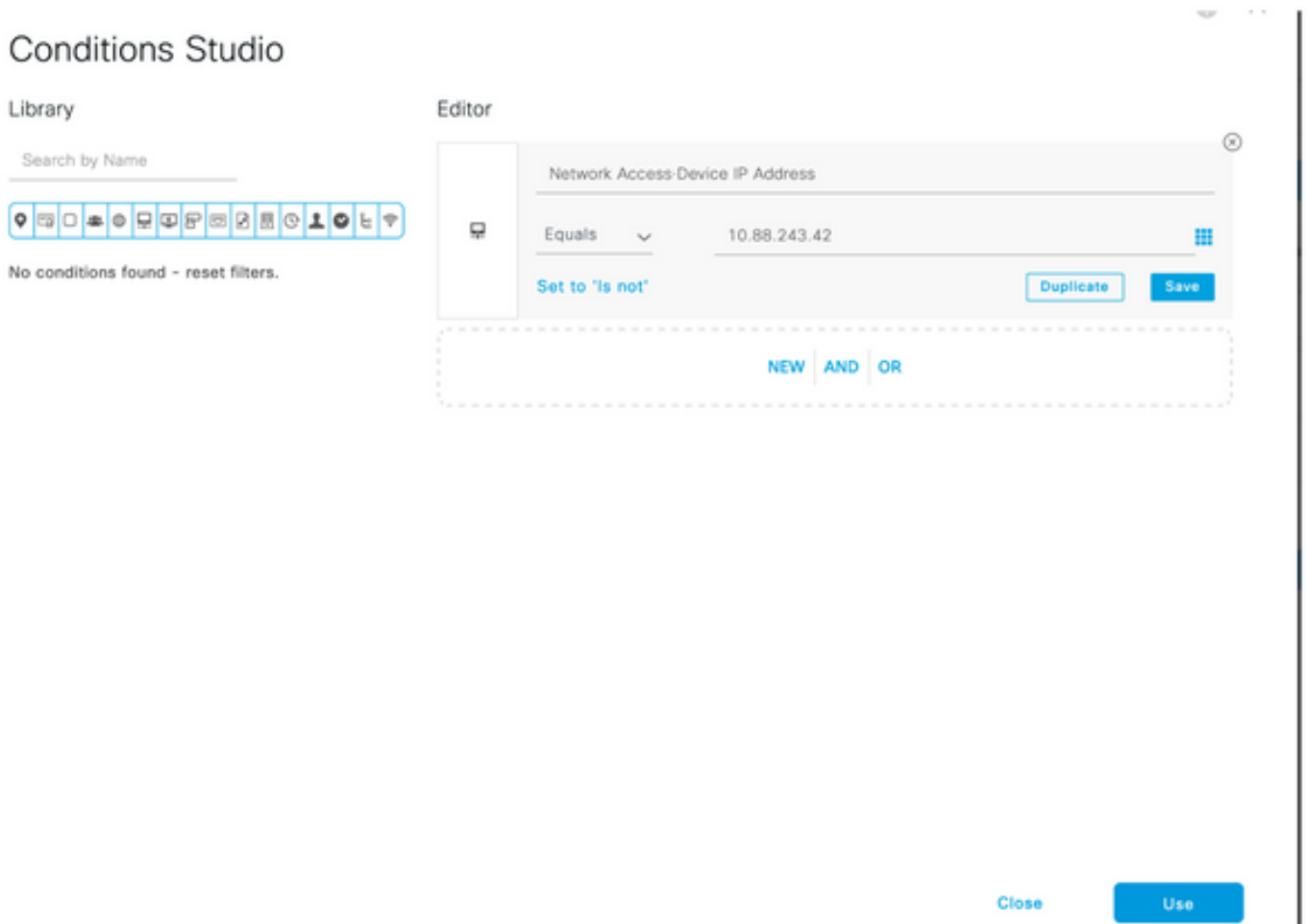
Paso 8. Seleccione el icono de tres líneas situado en la esquina superior izquierda y navegue hasta **Administración->Administración de dispositivos->Conjuntos de políticas de administración**

de dispositivos. Seleccione  situado debajo del título Conjunto de políticas, defina un nombre y seleccione el botón + en el centro para agregar una nueva condición.



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	⚙️	➔

Paso 9. En la ventana Condición, seleccione Add an attribute y luego seleccione **Network Device** Icon seguido de Network Access Device IP address. Seleccione **Valor de atributo** y agregue la dirección IP de CSM. Seleccione **Usar** una vez hecho.



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

Paso 10. En la sección Permitir protocolos, seleccione Device Default Admin. Seleccione Save (Guardar).

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		

Paso 11. Seleccione la flecha derecha  del conjunto de políticas para definir las políticas de autenticación y autorización

Paso 12. Seleccionar  situado debajo del título de la política de autenticación, defina un nombre y seleccione el + en el centro para agregar una nueva condición. En la ventana Condición, seleccione Add an attribute y luego seleccione **Network Device** Icon seguido de Network Access Device IP address. Seleccione **Valor de atributo** y agregue la dirección IP de CSM. Seleccione **Usar** una vez hecho


Paso 13. Seleccione **Usuarios Internos** como Almacén de Identidades y Seleccione **Guardar**

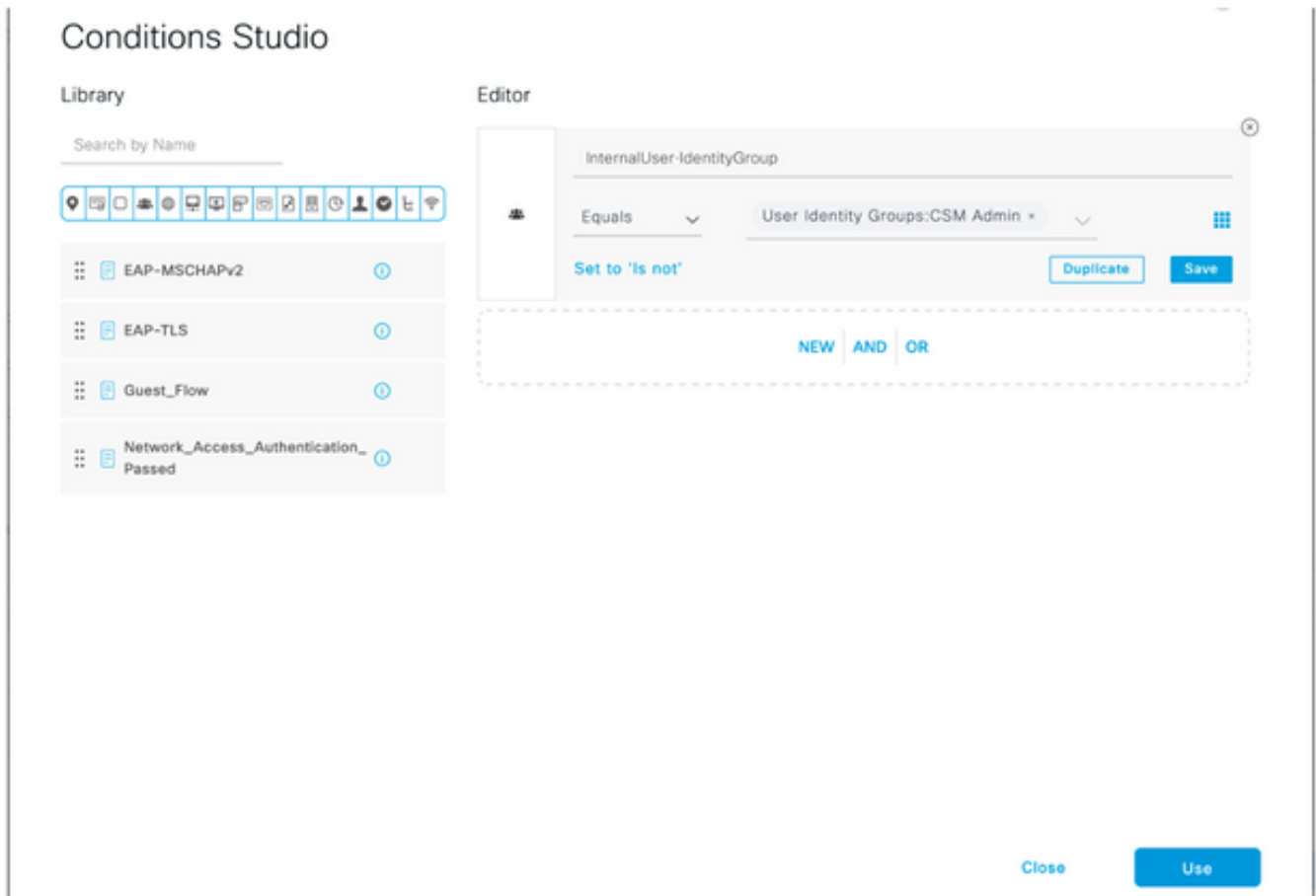
Authentication Policy (1)

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

> Options

Nota: El almacén de identidades se puede cambiar a almacén de AD si ISE se une a un directorio activo.

Paso 14. Seleccionar  situado debajo del título de la política de autorización, defina un nombre y seleccione el botón + en el centro para agregar una nueva condición. En la ventana Condición, seleccione agregar un atributo y, a continuación, seleccione el icono **Grupo de identidad** seguido por **Usuario interno: Grupo de identidad**. Seleccione el grupo de administración de CSM y seleccione **Usar**.



Paso 15. En Conjunto de comandos, seleccione Permitir todo el conjunto de comandos creado en el Paso 7 y, a continuación, seleccione **Guardar**

Repita los pasos 14 y 15 para el grupo CSM Oper

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
+	Search						
✓	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

Paso 16 (opcional). Seleccione el icono de tres líneas situado en la esquina superior izquierda y Seleccione **Administration>System>Maintenance>Repository**, seleccione **+Add** para agregar un repositorio que se utilice para almacenar el archivo de volcado TCP con fines de resolución de problemas.

Paso 17 (opcional). Defina un nombre de repositorio, protocolo, nombre de servidor, ruta y credenciales. Seleccione **Enviar** una vez hecho.

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

Configuración de CSM

Paso 1. Inicie sesión en la aplicación Cisco Security Manager Client con la cuenta de administrador local. En el menú, vaya a **Herramientas > Administración del Administrador de seguridad**

Cisco Security Manager
 Version 4.22.0 Service Pack 1

Server Name

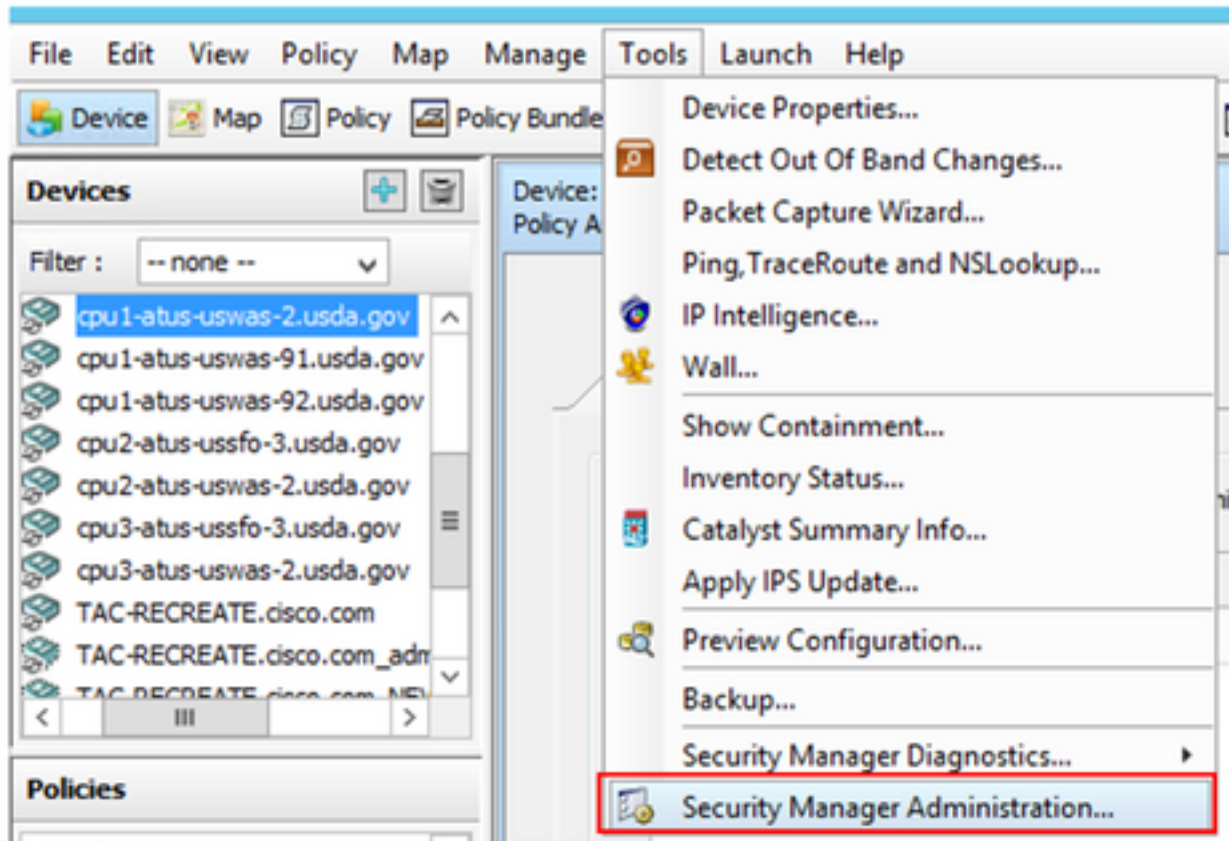
Username

Password

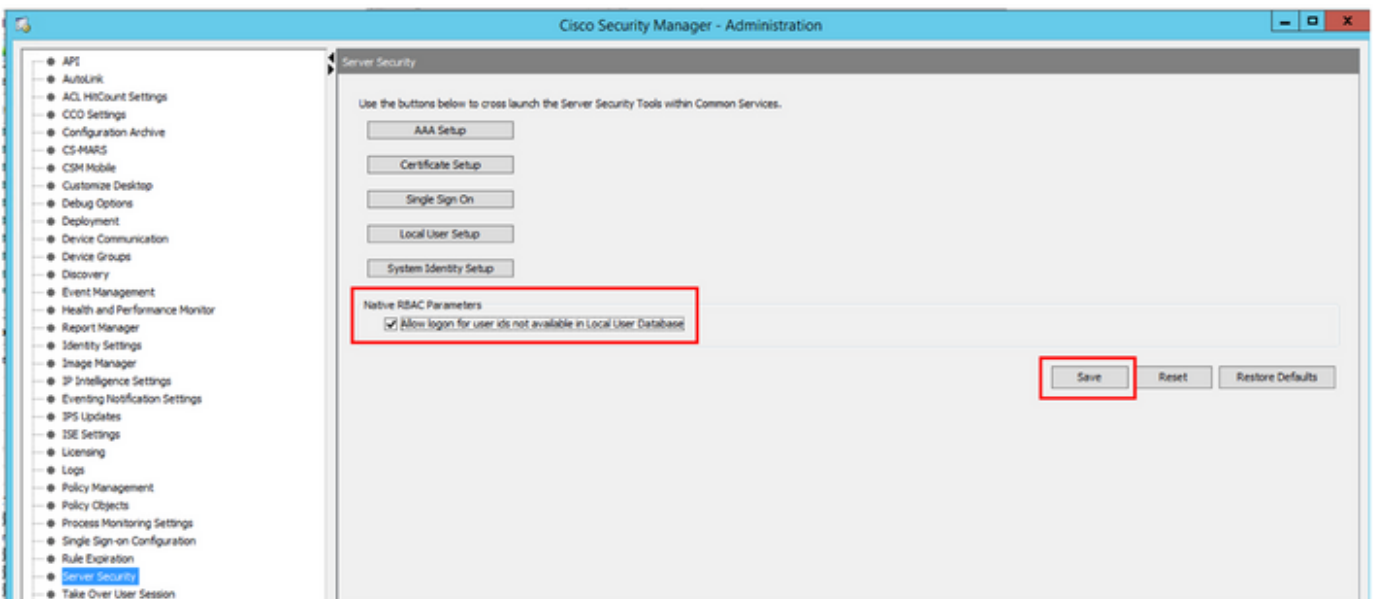
Default View

[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.



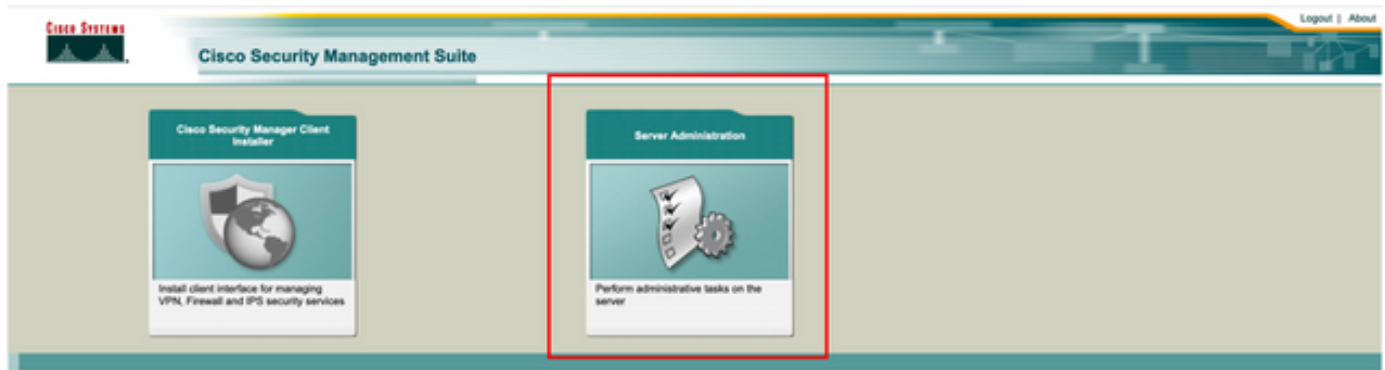
Paso 2. Marque la casilla en **Parámetros RBAC** nativos. Seleccione **Guardar y Cerrar**



Paso 3. En el menú seleccione **Archivo > Enviar**. **File > Submit (Archivo > Enviar)**.

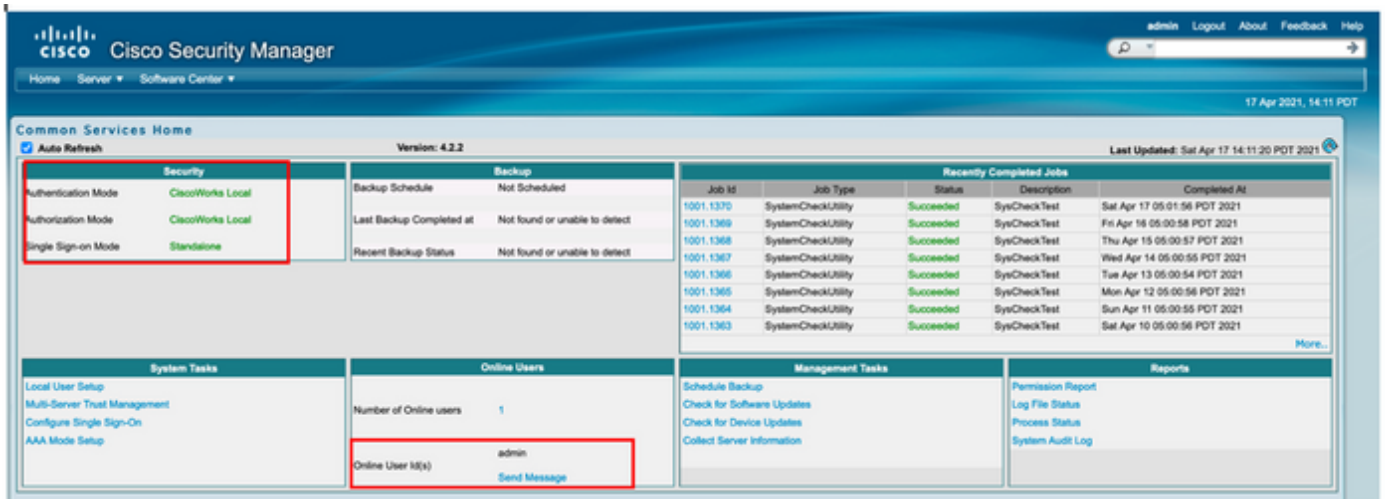
Nota: Todos los cambios se deben guardar, en caso de que se produzcan cambios en la configuración, es necesario enviarlos e implementarlos.

Paso 4. Navegue hasta la interfaz de usuario de administración de CSM y escriba https://<enter_CSM_IP_Address> y seleccione **Administración del servidor**.

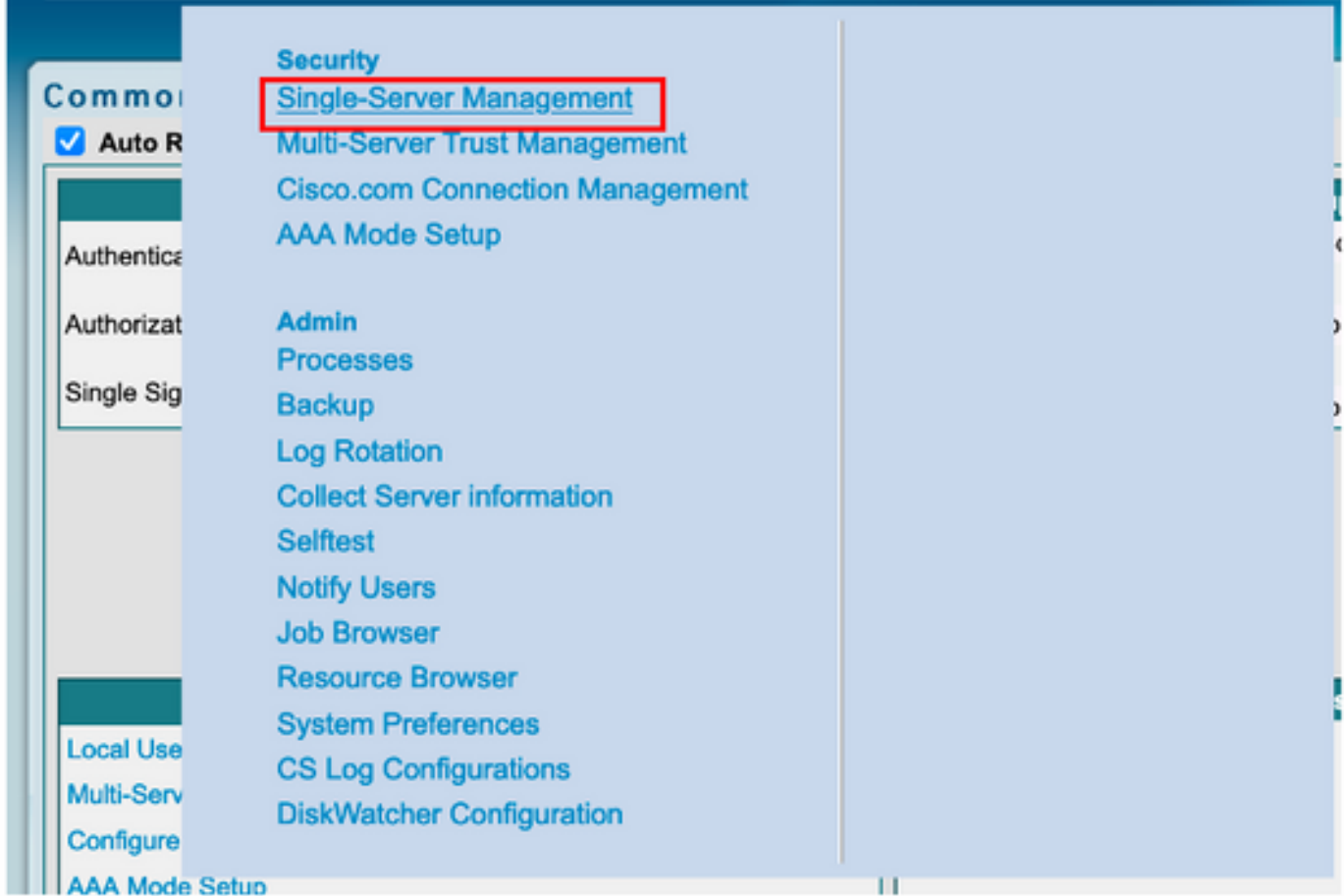


Nota: Los pasos 4 a 7 muestran el procedimiento para definir la función predeterminada para todos los administradores que no están definidos en ISE. Estos pasos son opcionales.

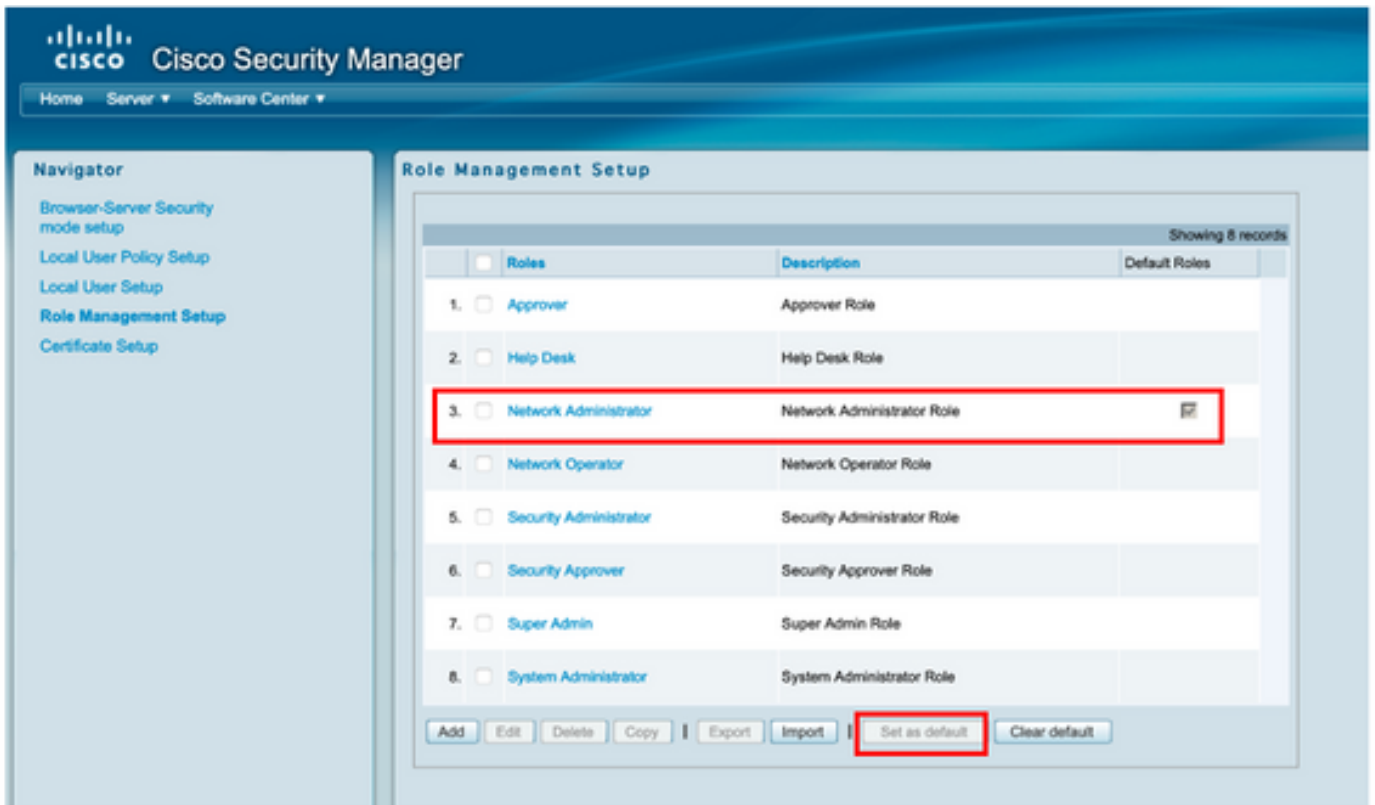
Paso 5. Validar el modo de autenticación se establece en CiscoWorks Local y Online userID es la cuenta de administración local creada en CSM.



Paso 6. Navegue hasta Servidor y seleccione Administración de Servidor Único



Paso 7. Seleccione Role Management Setup (Configuración de administración de funciones) y seleccione el privilegio predeterminado que reciben todos los usuarios administradores tras la autenticación. Para este ejemplo, se utiliza Network Administrator. Una vez seleccionado, seleccione **set as default** .



Paso 8. Seleccione **Servidor>Función de configuración del modo AAA** y luego seleccione la opción **TACACS+**, y finalmente seleccione **cambiar** para agregar información de ISE.





Paso 9. Defina la dirección IP y la clave de ISE; opcionalmente, puede seleccionar la opción para permitir a todos los usuarios de autenticación local o sólo a un usuario si falla el inicio de sesión. Para este ejemplo, se permite al único usuario administrador como método de reserva. Seleccione **Aceptar** para guardar los cambios.

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:**
 - 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.

Buttons for 'OK' and 'Cancel' are at the bottom right.

Login Module Change Summary

Login Module changes updated.

OK

Paso 10. Seleccione Server> Single Server Management, luego seleccione Local User Setup y seleccione add.



The screenshot shows the Cisco Security Manager interface. The top navigation bar includes 'Home', 'Server', and 'Software Center'. The left sidebar, titled 'Navigator', lists several setup options: '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 18 rows, each with a checkbox and a user name. The 'Add' button at the bottom right of the table is highlighted with a red box. The table also includes buttons for 'Import Users', 'Export Users', 'Edit', 'Delete', and 'Modify My Profile'.

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

Paso 11. En este ejemplo, se utilizan los mismos nombres de usuario y contraseña creados en ISE en el paso 5 de la sección de configuración de ISE, **csmoper** y **funciones de autorización de tareas de Help Desk**. Seleccione **OK** para guardar el usuario administrador.

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

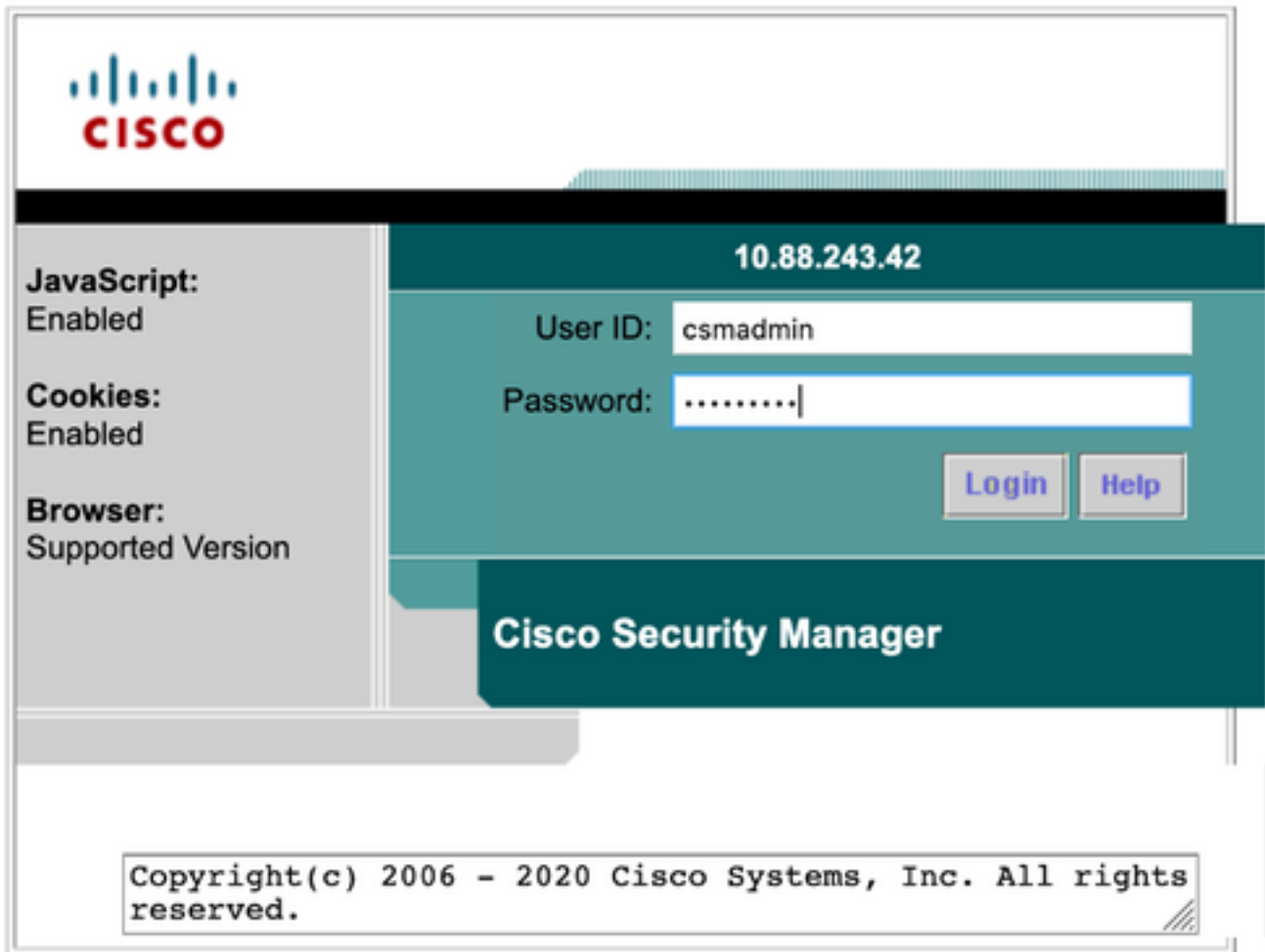
Device level Authorization

Not Applicable

Verificación

Interfaz de usuario del cliente de Cisco Security Manager

Paso 1. Abra un nuevo navegador de ventanas y escriba https://<enter_CSM_IP_Address>, utilice el nombre de usuario y la contraseña `csmadmin` creados en el paso 5 en la sección de configuración de ISE.



El inicio de sesión exitoso se puede verificar en los registros en vivo de 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		ise30	CSM422

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

aplicación Cisco Security Manager Client

Paso 1. Inicie sesión en la aplicación Cisco Security Manager Client con la cuenta de administrador del soporte técnico.



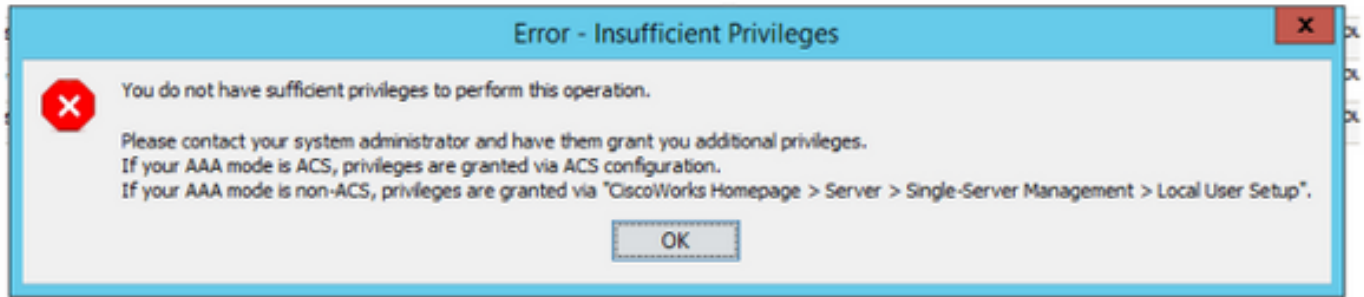
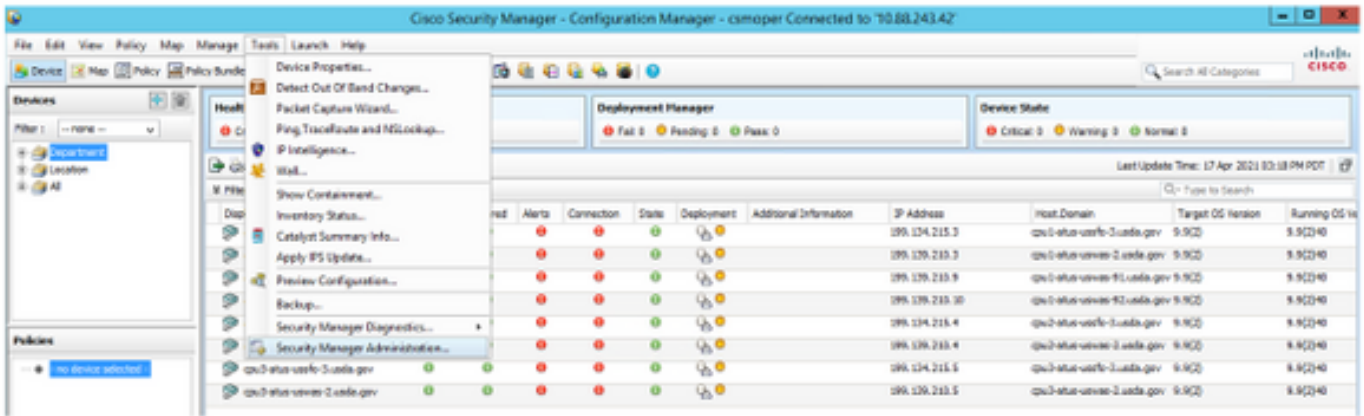
El inicio de sesión exitoso se puede verificar en los registros en vivo de ISE TACACS

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

Paso 2. En el menú de aplicación del cliente CSM seleccione **Herramientas > Administración del administrador de seguridad**, un mensaje de error indica que debe aparecer la falta de privilegio.



Paso 3. Repita los pasos 1 a 3 con la cuenta **csadmin** para validar los permisos adecuados que se han proporcionado a este usuario.

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Validación de la comunicación con la herramienta TCP Dump en ISE

Paso 1. Inicie sesión en ISE y desplácese al icono de tres líneas situado en la esquina superior izquierda y seleccione **Operaciones>Solución de problemas>Herramientas de diagnóstico**.

Paso 2. En **General tools** seleccione **TCP Dumps** y luego **Add+**. Seleccione Nombre de host, Nombre de archivo de interfaz de red, Repositorio y opcionalmente un filtro para recopilar sólo el flujo de comunicación de dirección IP de CSM. Seleccione **Guardar y ejecutar**

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

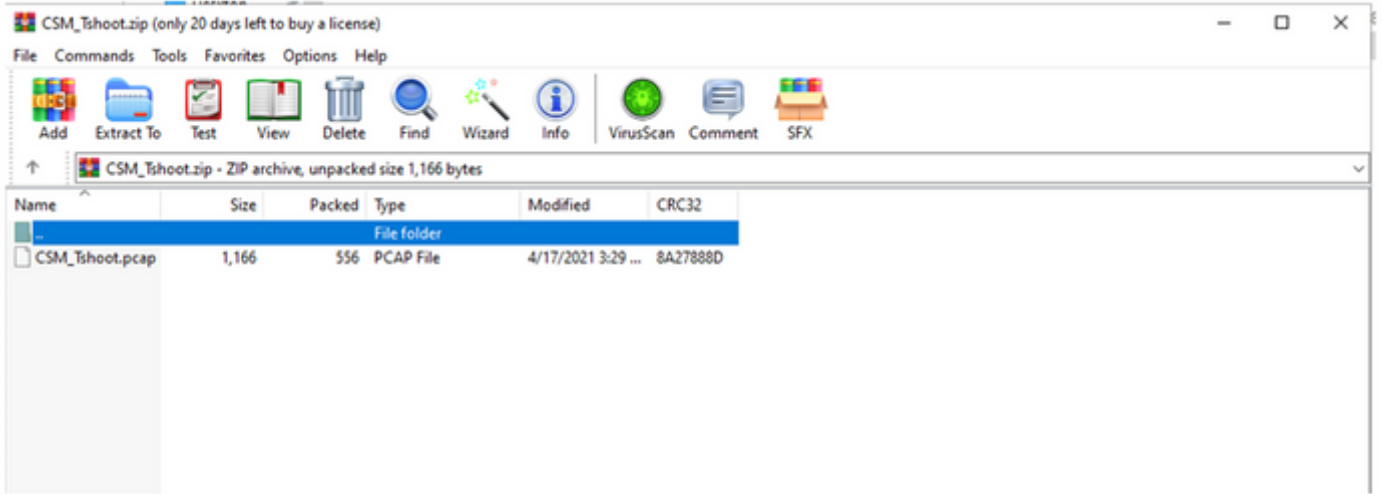
Cancel Save Save and Run

Paso 3. Inicie sesión en la aplicación cliente CSM o en la interfaz de usuario del cliente y escriba las credenciales de administrador.

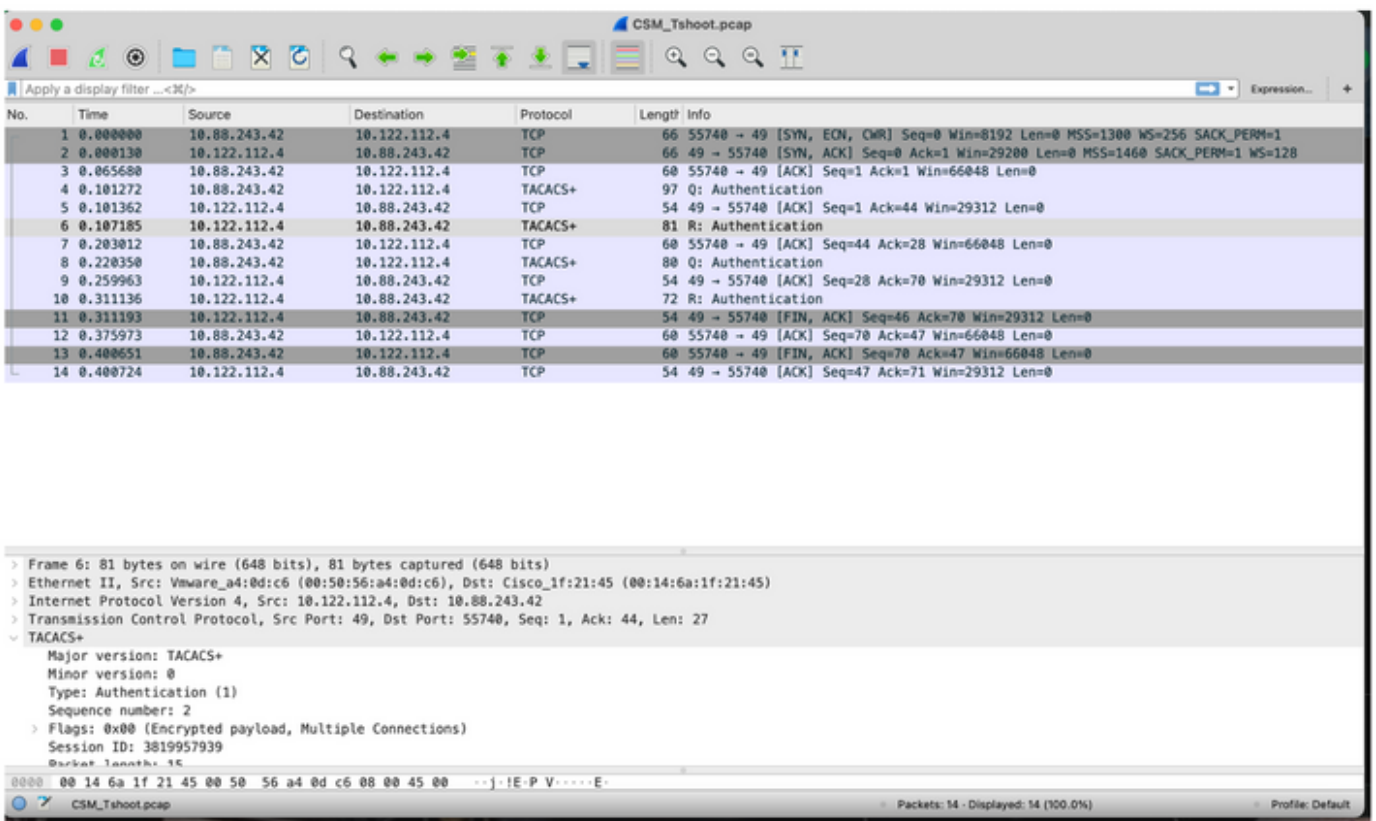
Paso 4. En ISE, seleccione el botón **Detener** y verifique que el archivo pcap haya sido enviado al repositorio definido.

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



Paso 5. Abra el archivo pcap para validar la comunicación correcta entre CSM e ISE.



Si no se muestra ninguna entrada en el archivo pcap, valide lo siguiente:

1. El servicio de administración de dispositivos está habilitado en el nodo ISE
2. La dirección IP de ISE correcta se ha agregado en la configuración de CSM
3. En el caso de un firewall se permite el puerto de verificación intermedio 49 (TACACS).