

Integração de TACACS CSM com ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Procedimento de autenticação](#)

[Configuração do ISE](#)

[Configuração do CSM](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve o procedimento para integrar o Cisco Security Manager (CSM) ao Identity Services Engine (ISE) para autenticação de usuários administradores com o TACACS+ Protocol.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CSM Server versão 4.22
- ISE versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Por padrão, o Cisco Security Manager (CSM) usa um modo de Autenticação chamado CiscoWorks para autenticar e autorizar usuários localmente, a fim de ter um método de autenticação centralizado, você pode usar o Cisco Identity Service Engine através do protocolo TACACS.

Configurar

Diagrama de Rede



Procedimento de autenticação

Etapa 1. Faça login no aplicativo CSM com as credenciais do Usuário Admin.

Etapa 2. O processo de autenticação dispara e o ISE valida as credenciais localmente ou através do Active Directory.

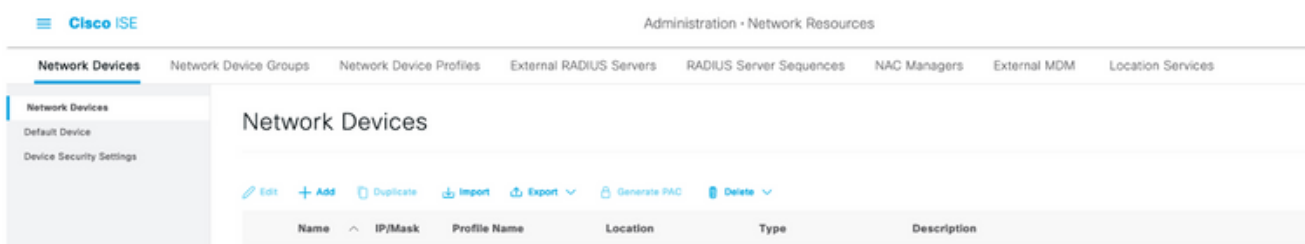
Etapa 3. Quando a autenticação for bem-sucedida, o ISE envia um pacote de permissão para autorizar o acesso ao CSM.

Etapa 4. O CSM mapeia o nome de usuário com a atribuição de função de usuário local.

Etapa 5. O ISE mostra um registro ao vivo de autenticação bem-sucedido.

Configuração do ISE

Etapa 1. Selecione o ícone de três linhas  localizado no canto superior esquerdo e navegue até **Administration > Network Resources > Network Devices (Administração > Recursos de rede > Dispositivos de rede)**.



Etapa 2. Selecione o botão **+Adicionar** e insira os valores corretos para Network Access Device Name (Nome do dispositivo de acesso à rede) e IP Address (Endereço IP), verifique a caixa de

seleção **TACACS Authentication Settings (Configurações de autenticação TACACS)** e defina um segredo compartilhado. Selecione o botão **Enviar**.

The screenshot displays the configuration interface for a network device. The main content area is titled "Network Devices" and includes the following sections:

- Name:** CSM422
- Description:** (empty field)
- IP Address:** 10.88.243.42 / 32
- Device Profile:** Cisco
- Model Name:** (empty field)
- Software Version:** (empty field)
- Network Device Group:**
 - Location: All Locations (Set To Default)
 - Is IPSEC Device: (Set To Default)
 - Device Type: All Device Types (Set To Default)
- Authentication Settings:**
 - RADIUS Authentication Settings
 - TACACS Authentication Settings
 - Shared Secret: (masked) (Show)
 - Enable Single Connect Mode:
 - Legacy Cisco Device:
 - TACACS Draft Compliance Single Connect Support:
 - SNMP Settings
 - Advanced TrustSec Settings

At the bottom right, there are **Submit** and **Cancel** buttons.



Etapa 3. Selecione o ícone de três linhas localizado no canto superior esquerdo e navegue até **Administration > Identity Management > Groups**.

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 |

Etapa 4. Navegue até a pasta **Grupos de Identidades do Usuário** e selecione o botão **+Adicionar**. Defina um nome e selecione o botão **Enviar**.

Identity Groups

EQ



> Endpoint Identity Groups

> **User Identity Groups**

User Identity Groups

Edit + Add Delete Import Export

Selected 0 Total 10

All

| | 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: Este exemplo cria grupos Admin CSM e Oper Identity CSM. Você pode repetir a Etapa 4 para cada tipo de usuário administrativo no CSM



Etapa 5. Selecione o ícone de três linhas e navegue até **Administration > Identity Management > Identities**. Selecione o botão **+Adicionar**, defina o nome de usuário e a senha e selecione o grupo ao qual o usuário pertence. Neste exemplo, cria os usuários **csmadmin** e **csmoper** e atribuídos ao CSM Admin e ao CSM Oper group 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 | |



Etapa 6. Selecionar  e navegue até **Administration > System > Deployment** (Administração > Sistema > Implantação). Selecione o nó do nome de host e ative o **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 ⓘ

Note: Em caso de implantação distribuída, selecione o nó PSN que lida com solicitações TACACS

Passo 7. Selecione o ícone de três linhas e navegue até **Administration > Device Administration > Policy Elements (Administração > Administração de dispositivo > Elementos de política)**. Navegue até **Results > TACACS Command Sets (Resultados > Conjuntos de comandos TACACS)**. Selecione **+Adicionar** botão, defina um nome para o conjunto de comandos e ative o **comando Permitir qualquer que não esteja listado abaixo** da caixa de seleção. Selecione **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

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

Etapa 8. Selecione o ícone de três linhas localizado no canto superior esquerdo e navegue até

Administration->Device Administration->Device Admin Policy Sets. Selecionar  localizado abaixo do título Conjuntos de políticas, defina um nome e selecione o + botão no meio para adicionar uma nova condição.



| 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 | ⚙️ | ➔ |

Etapa 9. Na janela Condição, selecione adicionar um atributo e selecione o ícone **Dispositivo de rede** seguido do endereço IP do dispositivo de acesso à rede. Selecione **Attribute Value** e adicione o endereço IP do CSM. Selecione **Usar** uma vez concluído.

Conditions Studio

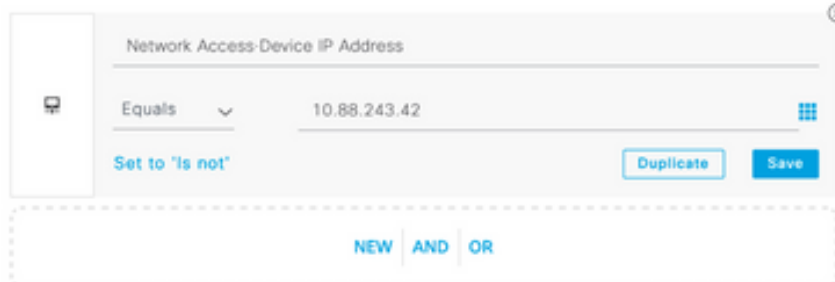
Library

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

Etapa 10. Na seção permitir protocolos, selecione **Device Default Admin**. Selecione Salvar


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 | | |

Etapa 11. Selecione a seta para a direita



ícone do Conjunto de políticas para definir políticas de autenticação e autorização

Etapa 12. Selecionar  localizado abaixo do título da política de autenticação, defina um nome e selecione o + no meio para adicionar uma nova condição. Na janela Condição, selecione adicionar um atributo e selecione o ícone **Dispositivo de rede** seguido do endereço IP do dispositivo de acesso à rede. Selecione **Attribute Value** e adicione o endereço IP do CSM. Selecione **Usar** uma vez concluído


Etapa 13. Selecione **Usuário interno** como o repositório de identidade e selecione **Salvar**

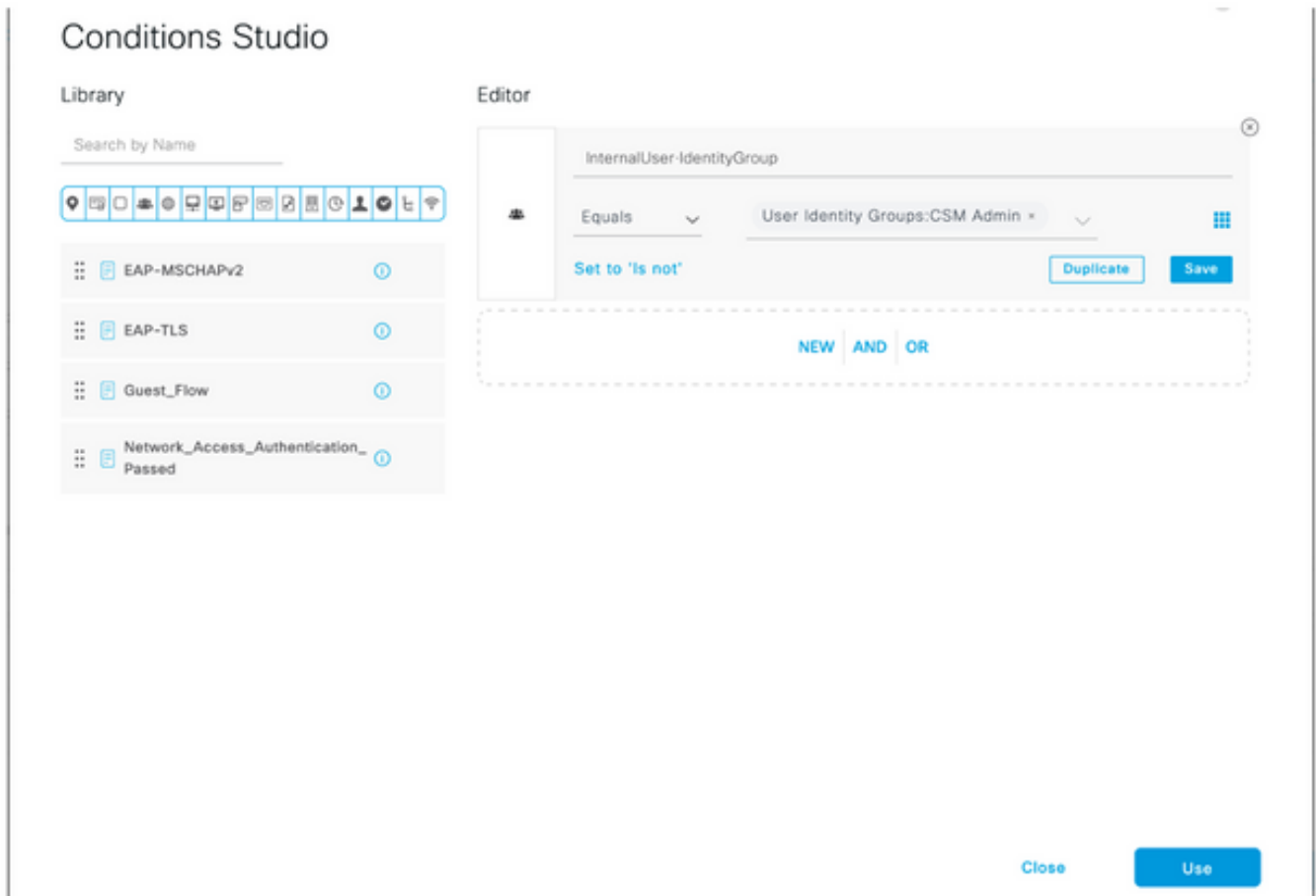
Authentication Policy (1)

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

Options

Note: O repositório de identidades pode ser alterado para o repositório do AD se o ISE estiver associado a um Active Directory.

Etapa 14. Selecionar  localizado abaixo do título da política de autorização, defina um nome e selecione o + botão no meio para adicionar uma nova condição. Na janela Condição, selecione adicionar um atributo e selecione o ícone **Grupo de Identidade** seguido por **Usuário Interno: Grupo de Identidades**. Selecione o grupo de administração do CSM e selecione **Usar**.



Etapa 15. Em Conjunto de comandos, selecione Permitir todos os conjuntos de comandos criados na Etapa 7 e selecione **Salvar**

Repita as etapas 14 e 15 para o grupo de trabalho do 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 | ⚙️ | |

Etapa 16 (Opcional). Selecione o ícone de três linhas localizado no canto superior esquerdo e Selecione **Administração>Sistema>Manutenção>Repositório**, selecione **+Adicionar** para adicionar um repositório usado para armazenar o arquivo de despejo de TCP para fins de solução de problemas.

Etapa 17 (Opcional). Defina um nome de repositório, um protocolo, um nome de servidor, um caminho e credenciais. Selecione **Submit** quando terminar.

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

Configuração do CSM

Etapa 1. Faça login no aplicativo Cisco Security Manager Client com a conta de administrador local. No menu, navegue até **Ferramentas > Administração do Security Manager**

Cisco Security Manager
Version 4.22.0 Service Pack 1

Server Name

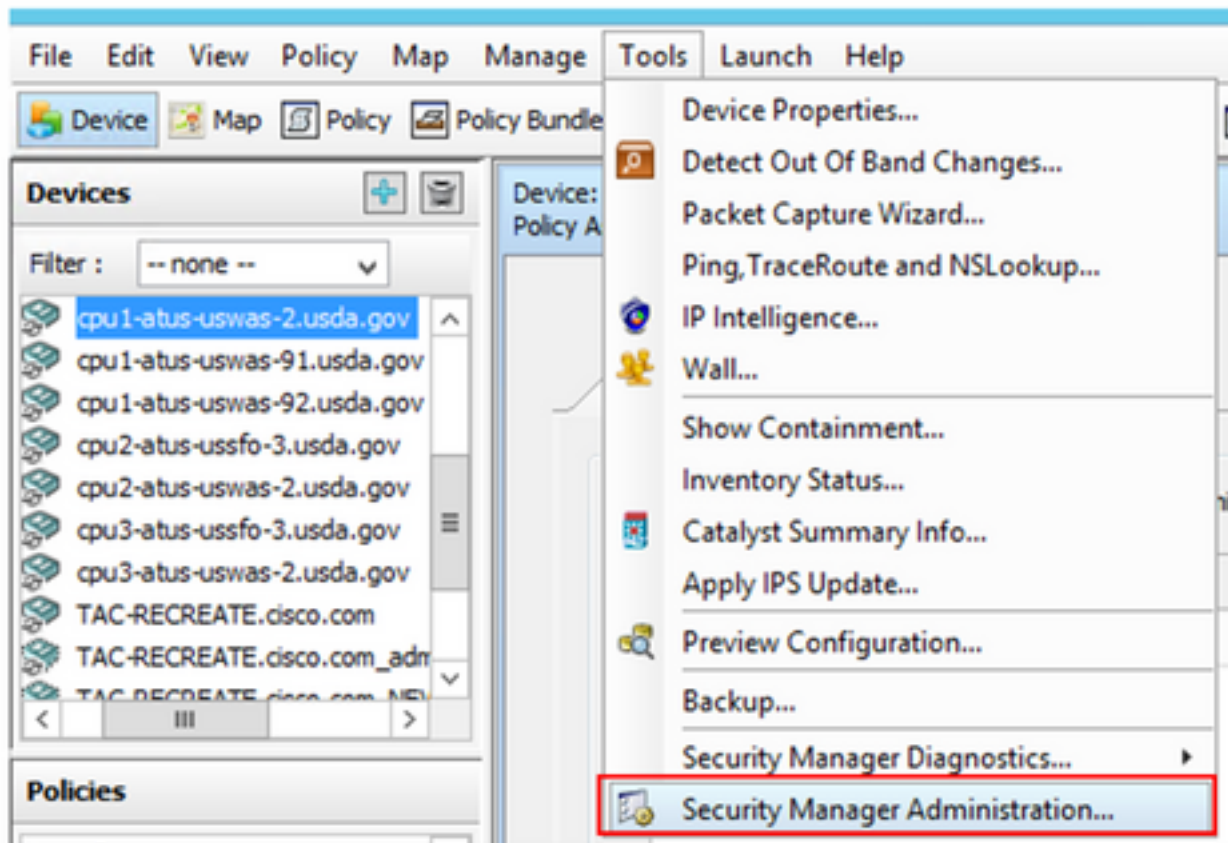
Username

Password

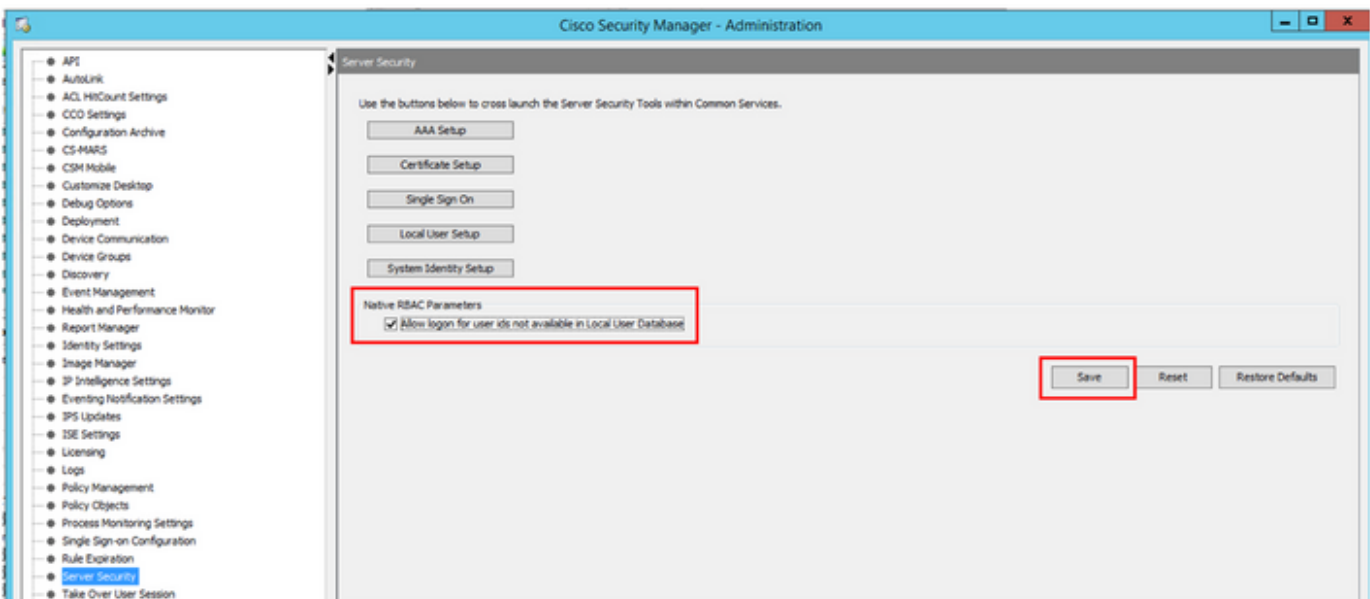
Default View

[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.



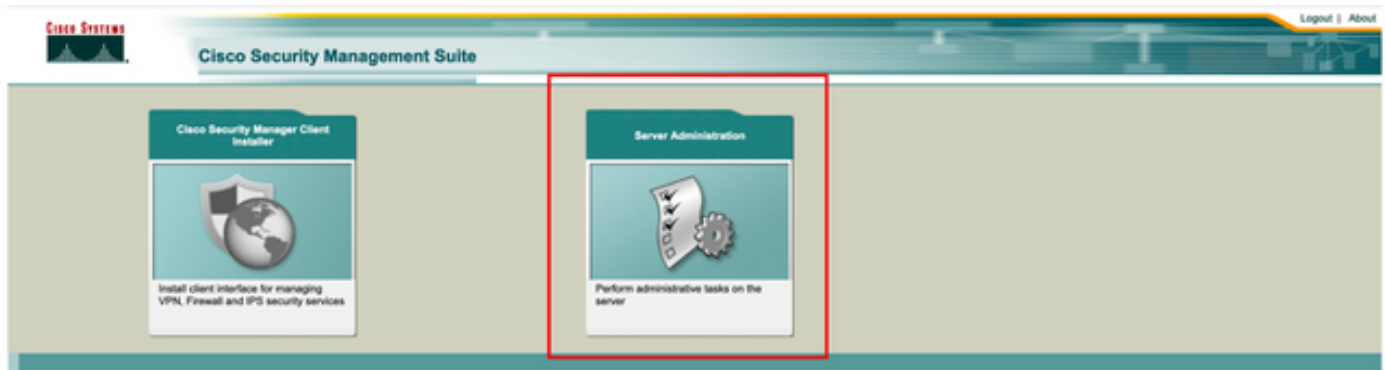
Etapa 2. Marque a caixa em Native RBAC Parameters. Selecione Salvar e Fechar



Etapa 3. No menu, selecione Arquivo > Enviar. Arquivo > Enviar.

Note: Todas as alterações devem ser salvas, caso sejam feitas alterações na configuração, elas precisam ser enviadas e implantadas.

Etapa 4. Navegue até CSM Management UI e digite https://<enter_CSM_IP_Address> e selecione Server Administration.



Note: As etapas 4 a 7 mostram o procedimento para definir a função padrão para todos os administradores que não estão definidos no ISE. Estas etapas são opcionais.

Etapa 5. Valide se o modo de autenticação está definido como **CiscoWorks Local** e **Online** userID é a conta de administrador local criada no CSM.

Common Services Home

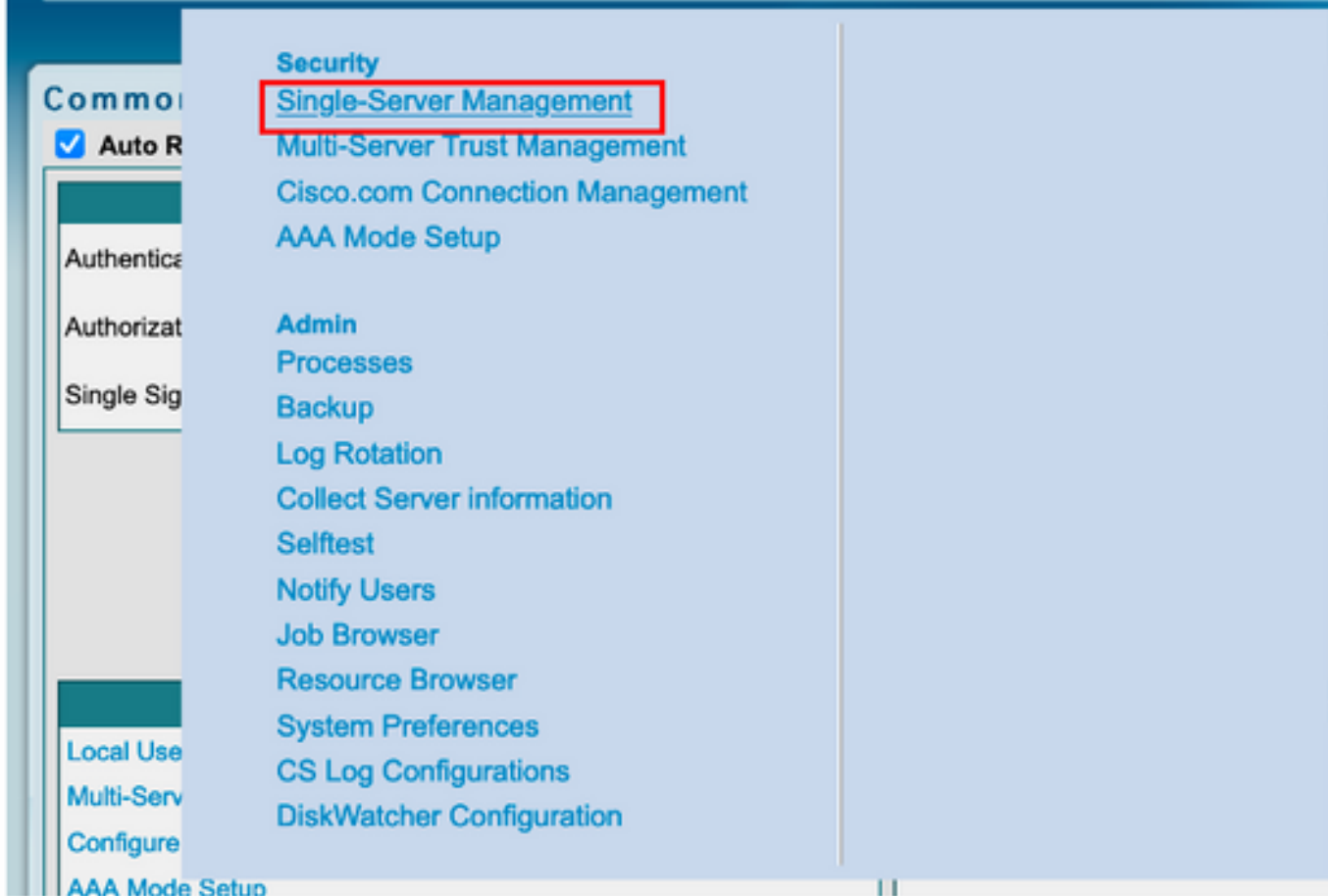
Version: 4.2.2

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

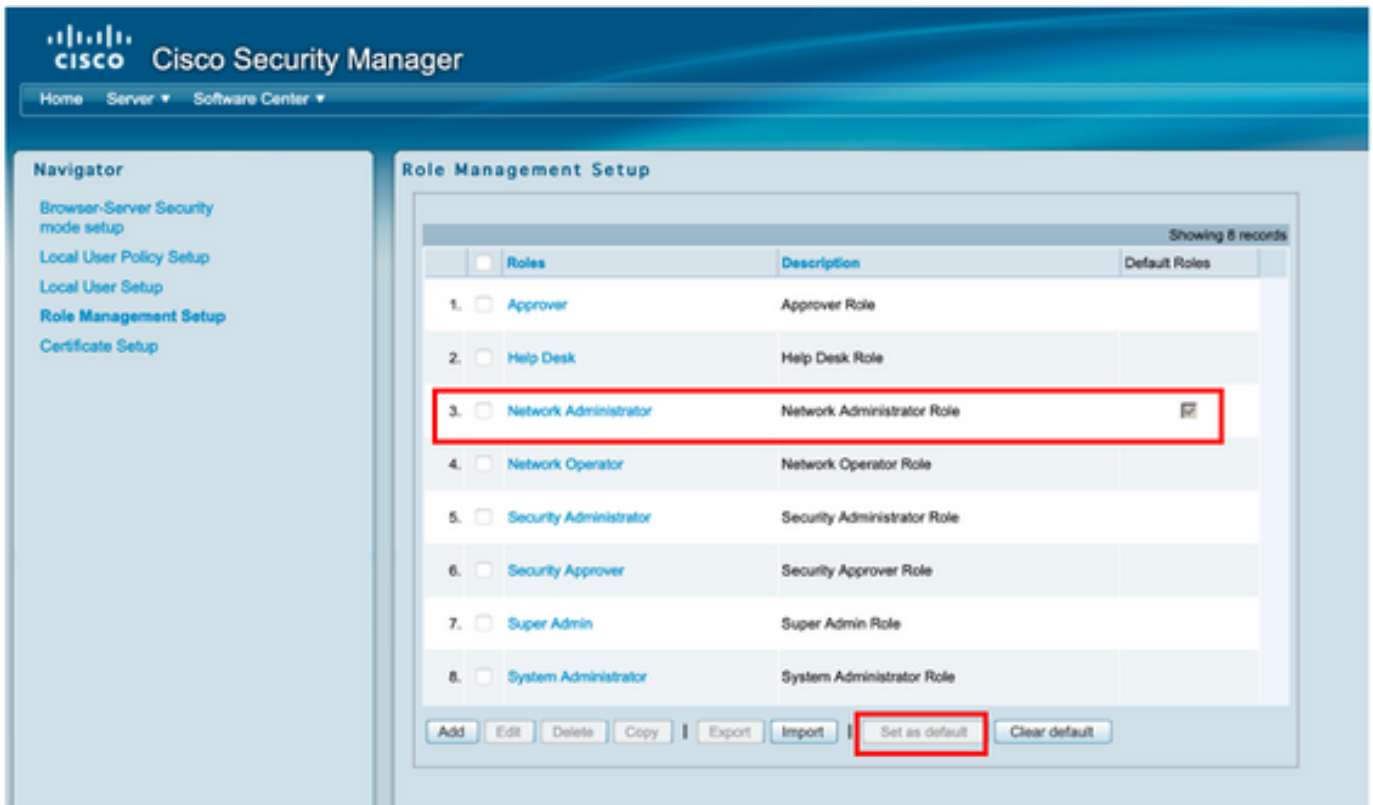
| Security | | Backup | | Recently Completed Jobs | | | | | |
|---------------------|------------------|--------------------------|-------------------------------|-------------------------|--------------------|-----------|--------------|------------------------------|--|
| Authentication Mode | CiscoWorks 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 | 1001.1369 | SystemCheckUtility | Succeeded | SysCheckTest | Fri Apr 16 05:00:58 PDT 2021 | |
| Single Sign-on Mode | Standalone | Recent Backup Status | Not found or unable to detect | 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 |

Etapa 6. Navegue até **Servidor** e selecione **Gerenciamento de servidor único**



Passo 7. Selecione Configuração de gerenciamento de função e selecione o privilégio padrão que todos os usuários admin recebem na autenticação. Para este exemplo, é usado o Network Administrator. Depois de selecionada, selecione **definir como padrão**.



Etapa 8. Selecione **Server>AAA Mode Setup Role** (Função de configuração do modo AAA) e selecione a opção **TACACS+**; finalmente selecione **change** (alterar) para adicionar informações do ISE.





Etapa 9. Defina o endereço IP e a chave do ISE, opcionalmente, você pode selecionar a opção para permitir todos os usuários de autenticação local ou apenas um usuário se o login falhar. Para este exemplo, o único usuário admin é permitido como método de fallback. Selecione **Ok** para salvar as alterações.

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

Etapa 10. Selezione **Server**> **Single Server Management**, seleccione **Local User Setup** e seleccione **add**.



Cisco Security Manager

Home Server Software Center

Navigator

- Browser-Server Security mode setup
- Local User Policy Setup
- Local User Setup**
- Role Management Setup
- Certificate Setup

Local User Setup

Showing 206 records

| | Users |
|-----|--|
| 1. | <input type="checkbox"/> Aaron.Logan |
| 2. | <input type="checkbox"/> Adrian.Lotreal |
| 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.weldehmanot |
| 8. | <input type="checkbox"/> allen.spiegel |
| 9. | <input type="checkbox"/> Andrew.OConnor |
| 10. | <input type="checkbox"/> Anwar.Khan |
| 11. | <input type="checkbox"/> amand.amith |
| 12. | <input type="checkbox"/> Bernard.Aiston |
| 13. | <input type="checkbox"/> bhess |
| 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.Sorenson |

Select items then take an action

Import Users Export Users Edit Delete **Add** Modify My Profile

Etapa 11. Defina o mesmo nome de usuário e senha criados no ISE na etapa 5 na seção de configuração do ISE, as funções de autorização de tarefas do Help Desk e do cliente são usadas neste exemplo. Selecione OK para salvar o usuário 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

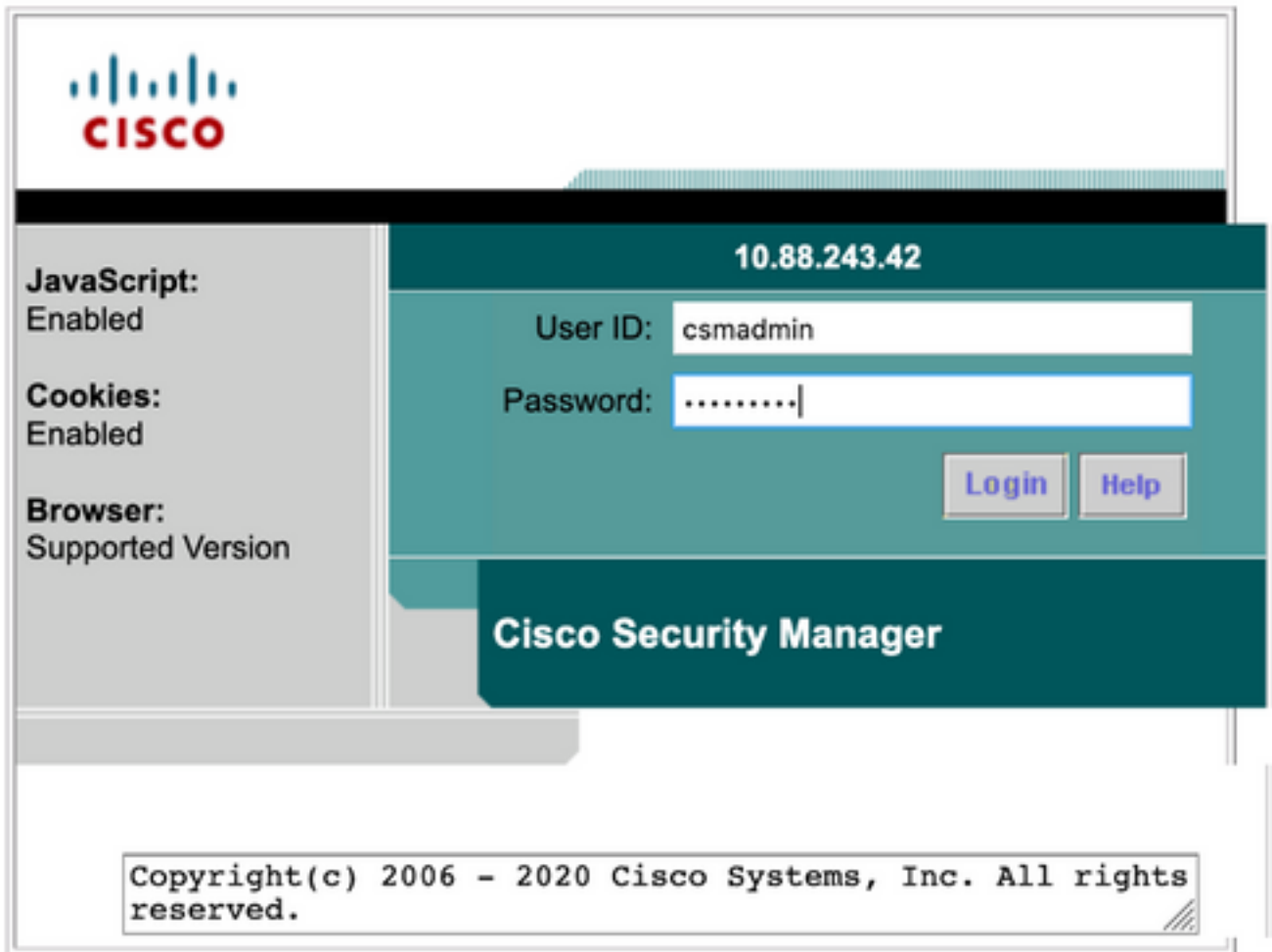
Device level Authorization

Not Applicable

Verificar

IU do cliente do Cisco Security Manager

Etapa 1. Abra um novo navegador de janela e digite https://<enter_CSM_IP_Address>, use csmadmin username e password criados na etapa 5 na seção de configuração do ISE.



O login bem-sucedido na tentativa pode ser verificado nos registros ao vivo do ISE TACACS

| 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 |

aplicativo do Cisco Security Manager Client

Etapa 1. Faça login no aplicativo Cisco Security Manager Client com a conta de administrador do helpdesk.



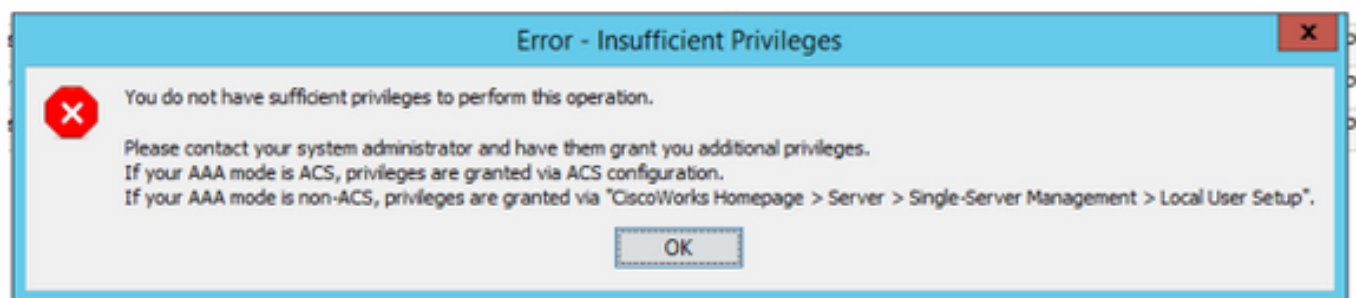
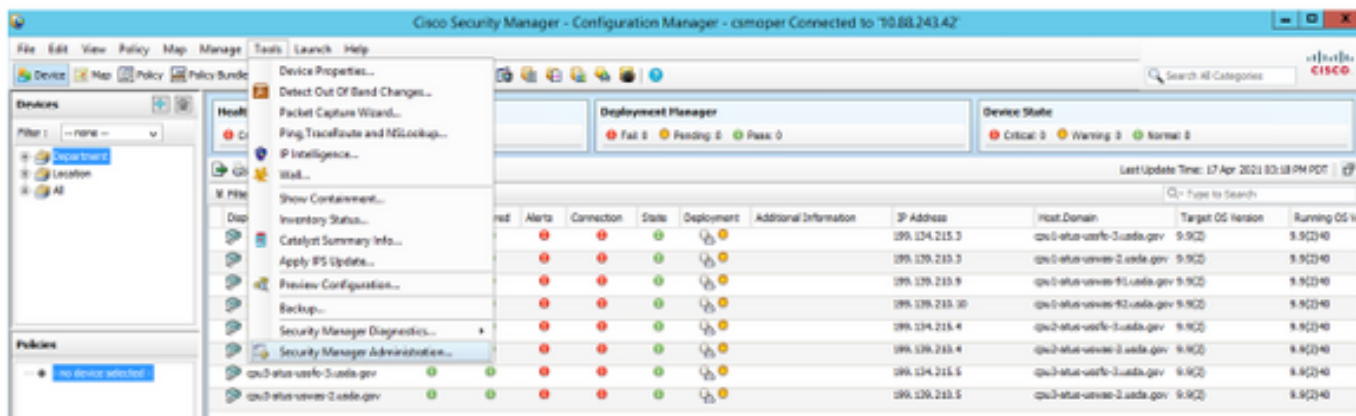
O login bem-sucedido na tentativa pode ser verificado nos registros ao vivo do ISE TACACS

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 |

Etapa 2. No menu do aplicativo cliente CSM, selecione **Tools > Security Manager Administration**, uma mensagem de erro indica que falta de privilégio deve aparecer.



Etapa 3. Repita as etapas 1 a 3 com a conta **csmadmin** para validar se as permissões apropriadas foram fornecidas a este usuário.

Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

Validação de comunicação com a ferramenta TCP Dump no ISE

Etapa 1. Faça login no ISE e navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione **Operations>Troubleshoot>Diagnostic Tools (Operações > Solucionar problemas > Ferramentas de diagnóstico)**.

Etapa 2. Em **Ferramentas gerais**, selecione **TCP Dumps** e selecione **Add+ (Adicionar+)**. Selecione o nome do host, o nome do arquivo da interface de rede, o repositório e, opcionalmente, um filtro para coletar somente o fluxo de comunicação do endereço IP do CSM. Selecione **Salvar e executar**

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

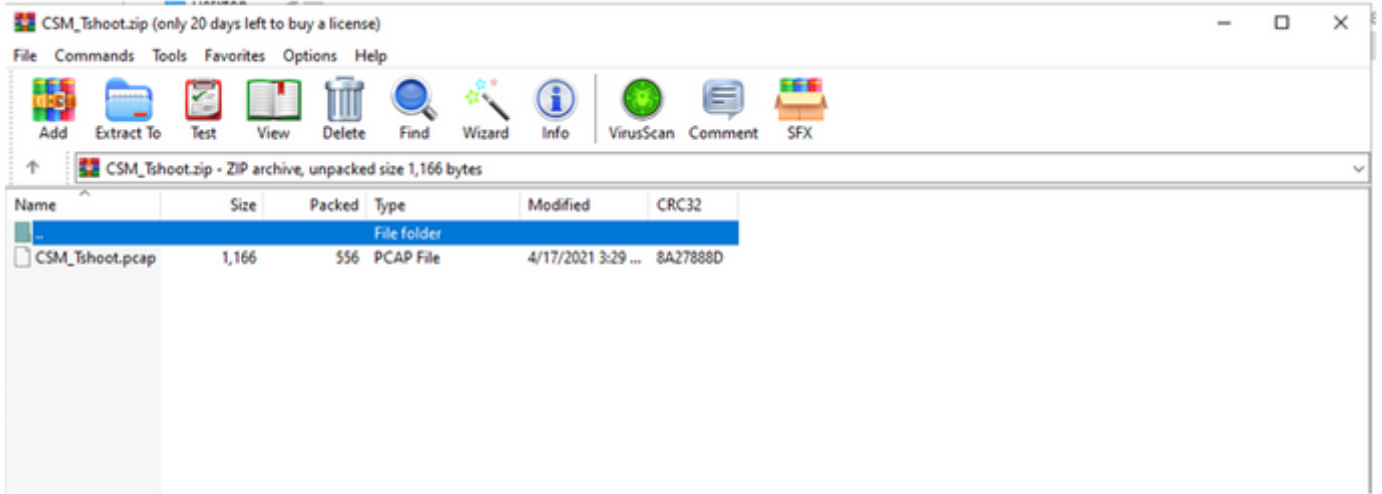
Cancel Save Save and Run

Etapa 3. Faça login no aplicativo cliente CSM ou na IU do cliente e digite as credenciais de administrador.

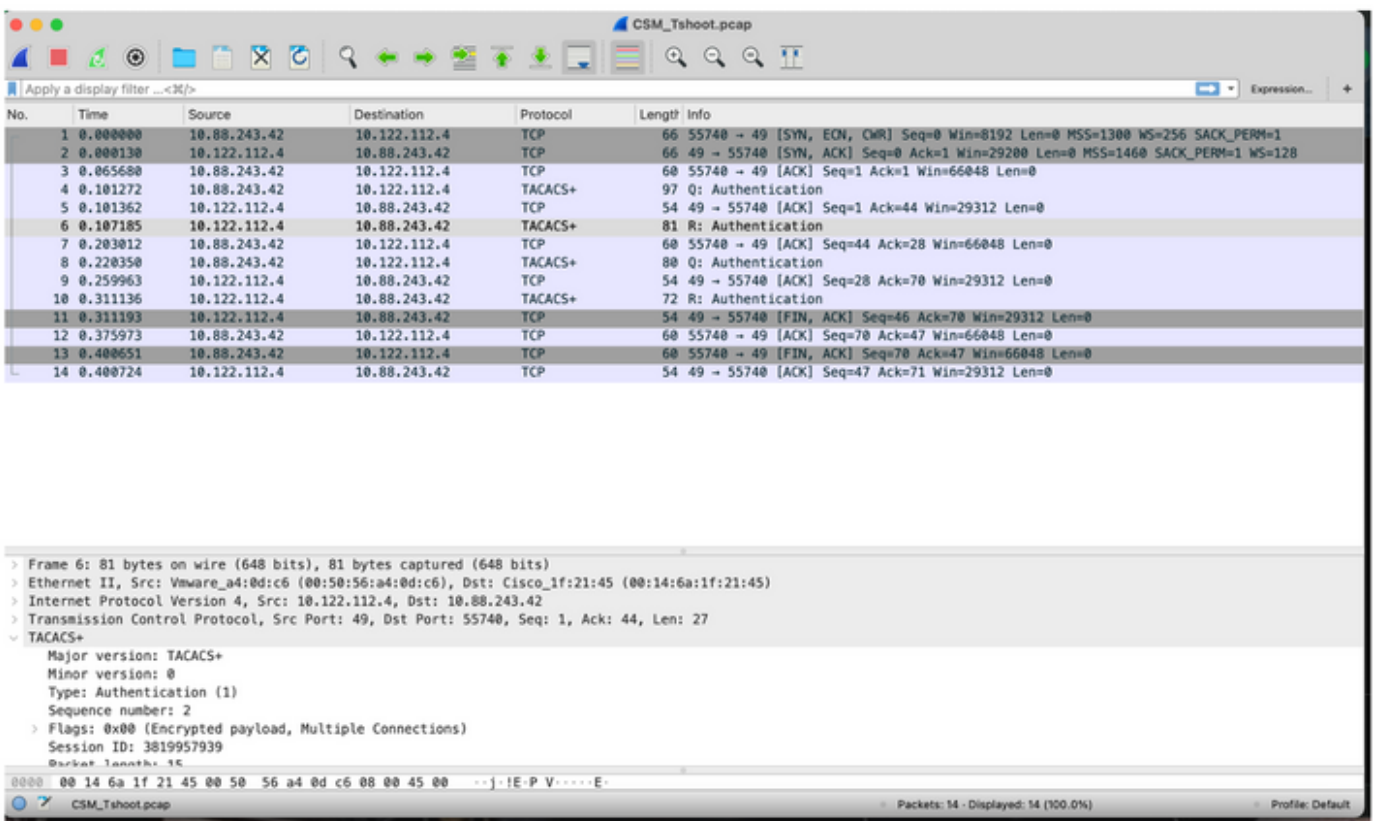
Etapa 4. No ISE, selecione o botão **Stop (Parar)** e verifique se o arquivo pcap foi enviado ao repositório definido.

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 |



Etapa 5. Abra o arquivo pcap para validar a comunicação bem-sucedida entre o CSM e o ISE.



Se nenhuma entrada for exibida no arquivo pcap, valide o seguinte:

1. O serviço de administração de dispositivos está ativado no nó ISE
2. O endereço IP correto do ISE foi adicionado na configuração do CSM
3. No caso de um firewall estar no meio, verifique se a porta 49 (TACACS) é permitida.