

CSM TACACS与ISE集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[身份验证过程](#)

[ISE配置](#)

[CSM配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍将思科安全管理器(CSM)与身份服务引擎(ISE)集成的过程，以便管理员用户通过TACACS+协议进行身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全管理器(CSM)。
- 身份服务引擎(ISE)。
- TACACS协议。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CSM服务器版本4.22
- ISE版本3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

默认情况下，思科安全管理器(CSM)使用称为Ciscoworks的身份验证模式在本地对用户进行身份验

证和授权，以便采用集中式身份验证方法，您可以通过TACACS协议使用思科身份服务引擎。

配置

网络图



身份验证过程

步骤1.使用管理员用户的凭证登录CSM应用。

步骤2.身份验证过程触发，ISE在本地或通过Active Directory验证凭证。

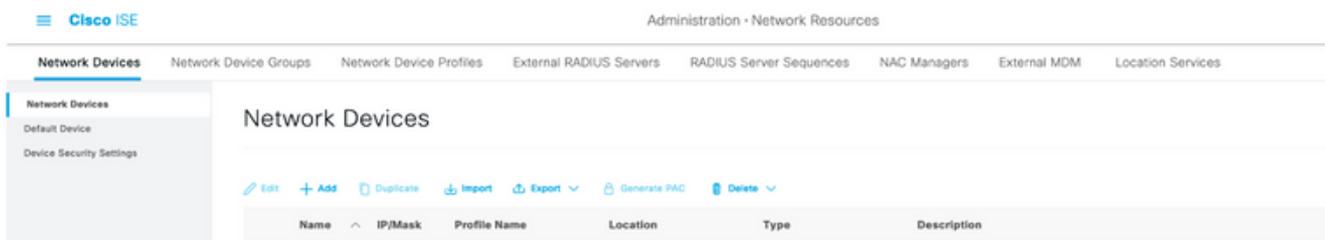
步骤3.身份验证成功后，ISE发送允许数据包以授权对CSM的访问。

步骤4. CSM将用户名与本地用户角色分配映射。

步骤5. ISE显示成功的身份验证实时日志。

ISE配置

步骤1.选择 位于左上角，导航至Administration > Network Resources > Network Devices。



步骤2.选择+Add按钮，为Network Access Device Name和IP Address输入正确的值，然后验证TACACS Authentication Settings复选框并定义共享密钥。选择“提交”按钮。

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](#)



步骤3.选择三行图标
Groups。

位于左上角，导航至Administration > Identity Management >

Cisco ISE Administration • Identity Management

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

Identity Groups

EQ

<

> Endpoint Identity Groups

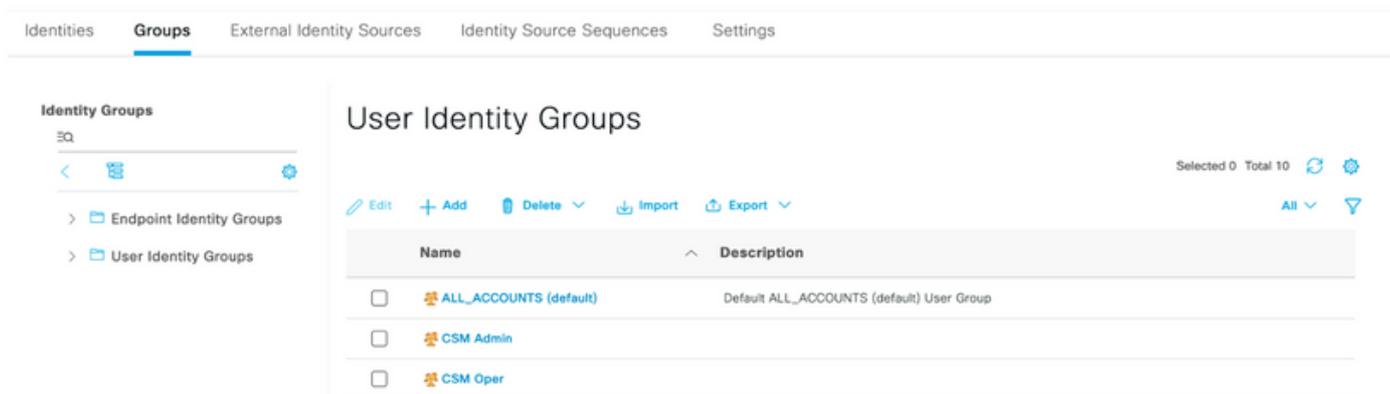
> **User Identity Groups**

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

步骤4.导航至“用户身份组”文件夹，然后选择+Add按钮。定义名称并选择“提交”按钮。



注意：此示例创建CSM Admin和CSM Oper Identity组。您可以对CSM上的每种类型的Admin Users重复步骤4



步骤5.选择三行图标 并导航至Administration > Identity Management > Identities。选择+Add按钮并定义用户名和密码，然后选择用户所属的组。在本示例中，分别创建csmadmin和csmoper 用户并分别分配给CSM Admin和CSM Oper组。

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: _____

These Password: _____

User Information

First Name: _____

Last Name: _____

Account Options

Description: _____

Change password on next login:

Account Disable Policy

Disable account if date exceeds: 2021-06-16 (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 checked="" type="checkbox"/>	Enabled	csmadmin				CSM Admin	
<input checked="" type="checkbox"/>	Enabled	csmoper				CSM Oper	

 **步骤6.选择** 并导航至**管理>系统>部署**。选择主机名节点并启用**设备管理服务**

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

> Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

注意：在分布式部署中，选择处理TACACS请求的PSN节点

步骤7.选择三行图标并导航至管理>设备管理>策略元素。导航至“结果”>“TACACS命令集”。选择+Add按钮,定义命令集的名称，并启用Permit any命令，该命令未列在复选框下。选择 Submit。

Work Centers - Device Administration

Policy Elements

TACACS Command Sets > New Command Set

Name: Permit all

Description:

Commands

Permit any command that is not listed below

Grant	Command	Arguments
No data found.		

Cancel Submit

步骤8.选择左上角的三行图标，然后导航至Administration -> Device Administration -> Device

Admin Policy Sets。选择  位于“策略集”标题下，定义名称，然后选择中间的+按钮以添加新条件。

Policy Sets Reset Reset Policyset Hitcounts Save

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		

步骤9.在Condition窗口下，选择添加属性，然后选择**Network Device Icon**，后跟Network access device IP address。选择**Attribute Value**并添加CSM IP地址。选择“完成后使用”。

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

步骤10.在“允许协议”部分下，选择“设备默认管理”。选择保存

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		

步骤11.选择右箭头



“策略集”图标定义身份验证和授权策略

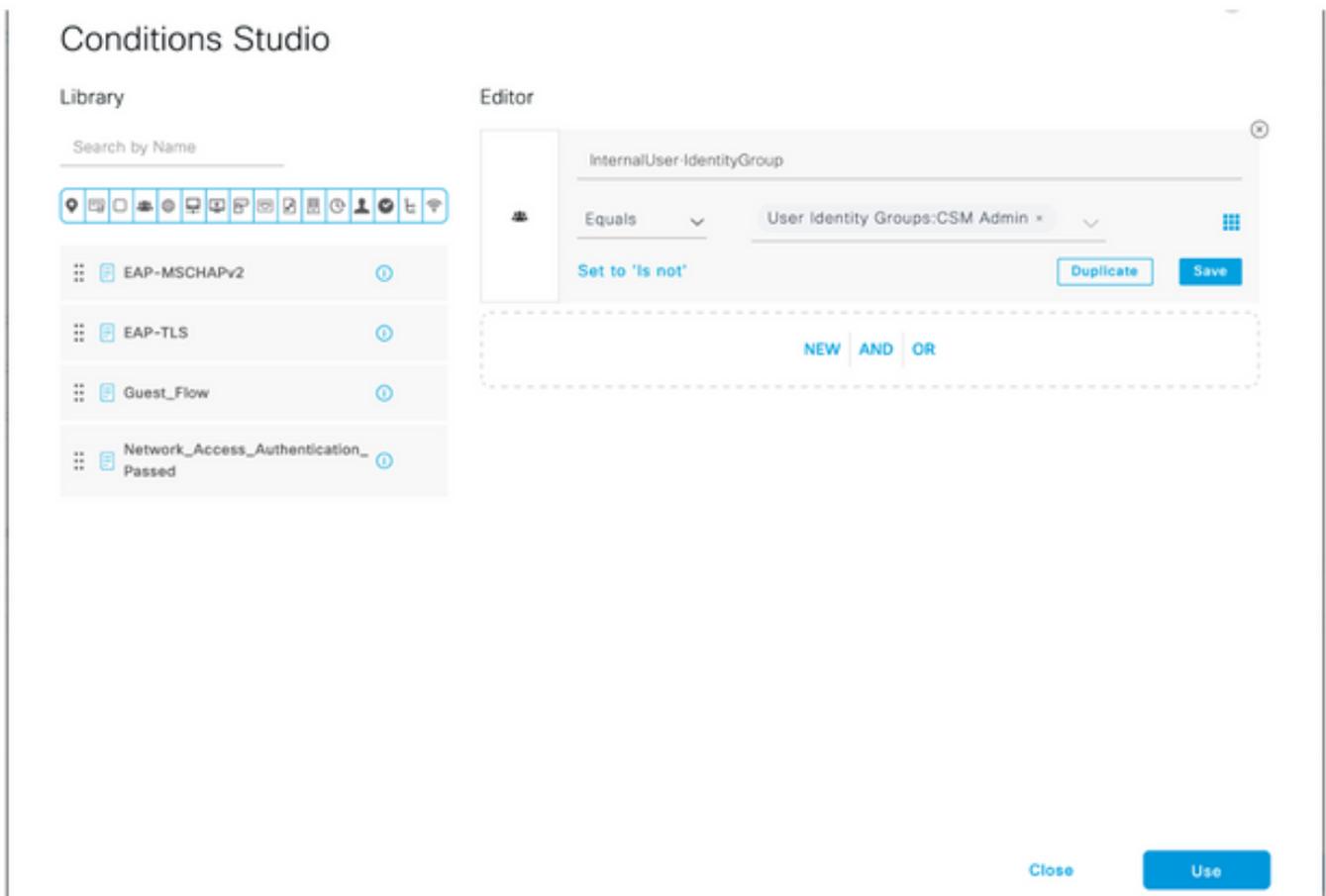
步骤12.选择  位于“身份验证策略”标题下，定义名称并选择中间的+以添加新条件。在“条件”窗口下，选择添加属性，然后选择**网络设备图标**，然后选择网络访问设备IP地址。选择**Attribute Value**并添加CSM IP地址。选择“完成后使用”

步骤13.选择Internal Users as the Identity Store并选择Save



注意：如果ISE加入Active Directory，则身份库可更改为AD库。

步骤14.选择  位于授权策略标题下，定义名称，**然后选择**中间的+按钮以添加新条件。在“条件”窗口下，选择添加属性，然后选择“**身份组**”图标，后跟“**内部用户：身份组**”。选择CSM Admin Group，然后选择**Use**。



步骤15.在“命令集”下，选择“允许在步骤7中创建的所有命令集”，然后选择“保存”

对CSM操作组重复步骤14和15

Authorization Policy (3)

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

步骤 16 (可选)。选择左上角的三行图标，然后选择 **Administration>System>Maintenance>Repository**，选择+Add以添加用于存储TCP转储文件以进行故障排除的存储库。

步骤 17 (可选)。定义存储库名称、协议、服务器名称、路径和凭证。完成后选择“提交”。

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

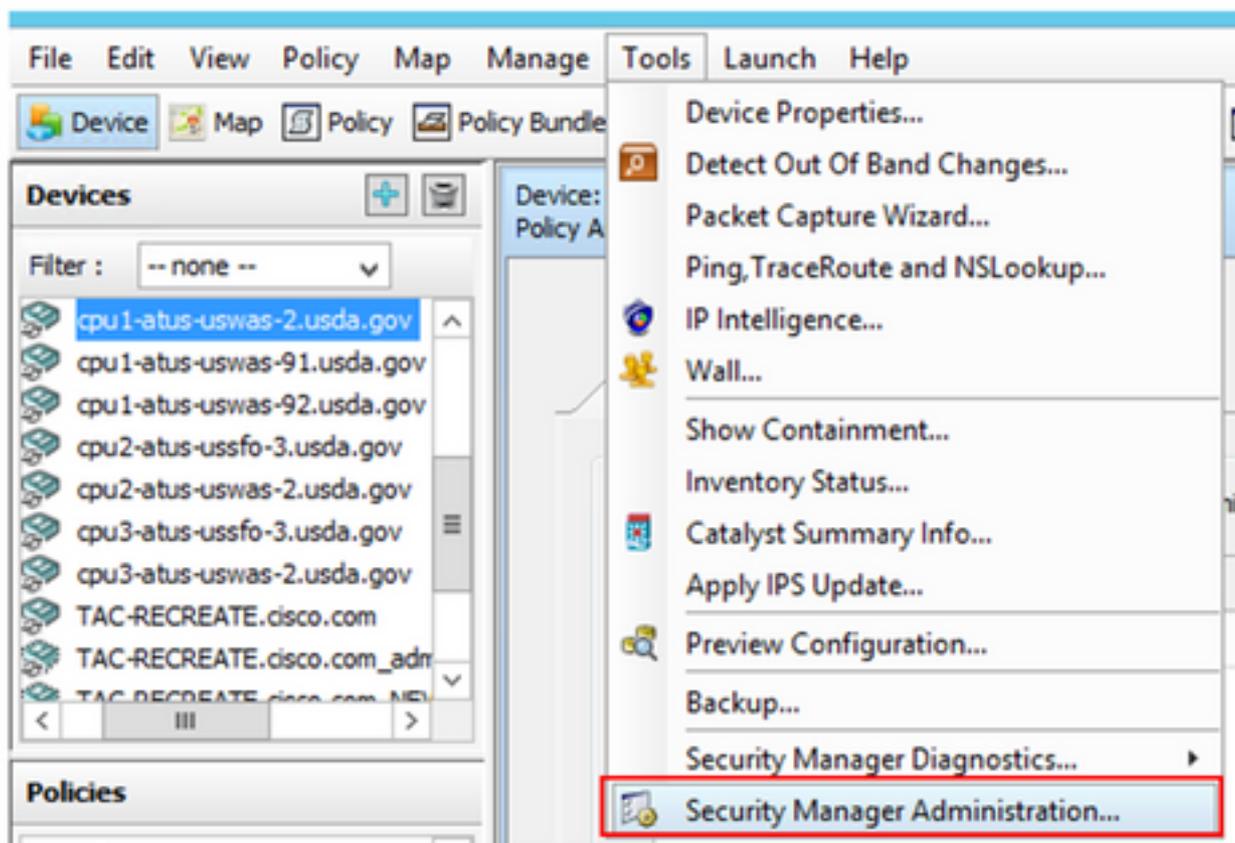
Credentials

* User Name

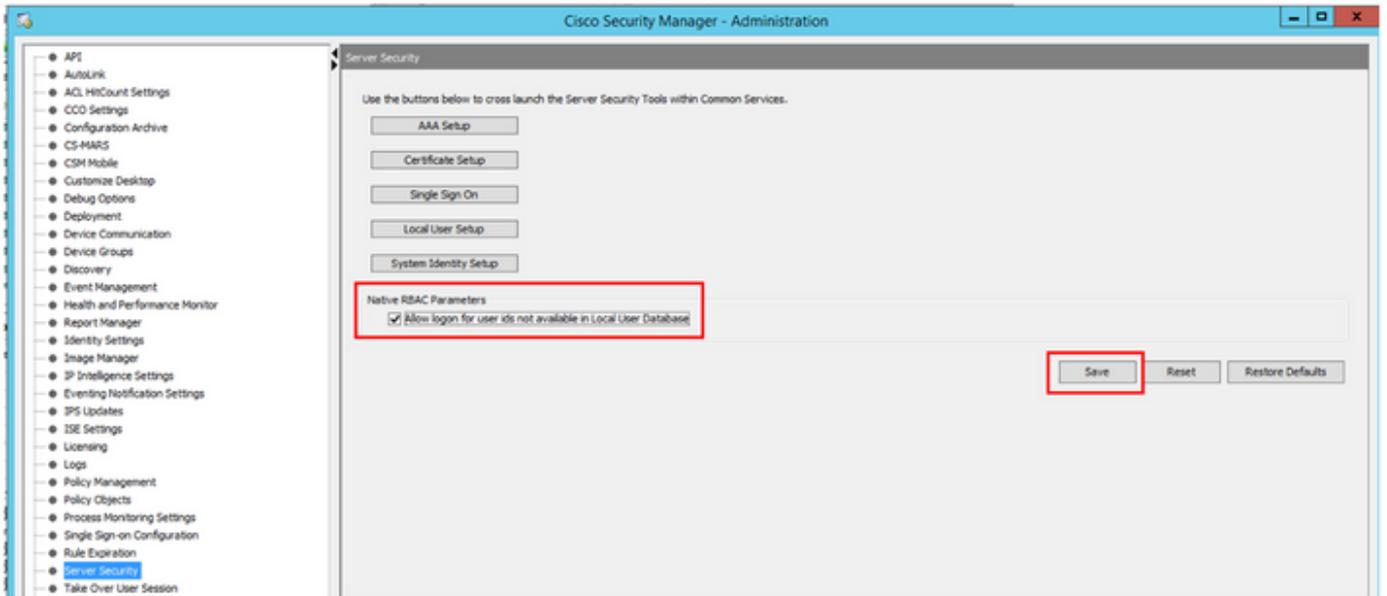
* Password

CSM配置

步骤1.使用本地管理员帐户登录到Cisco Security Manager客户端应用。从菜单导航到工具>安全管理器管理



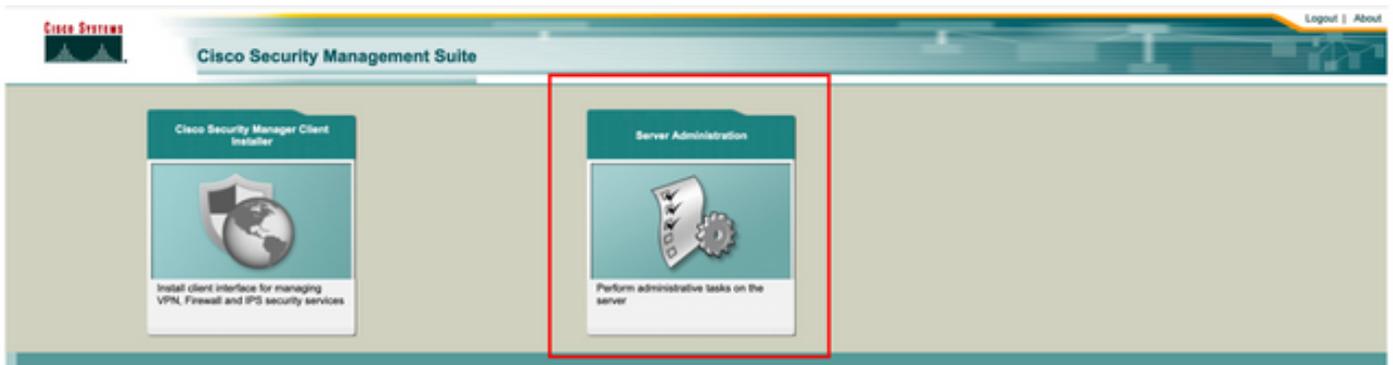
步骤2.选中Native RBAC Parameters下的复选框。选择保存并关闭



步骤3.从菜单中选择“文件”>“提交”。文件>提交。

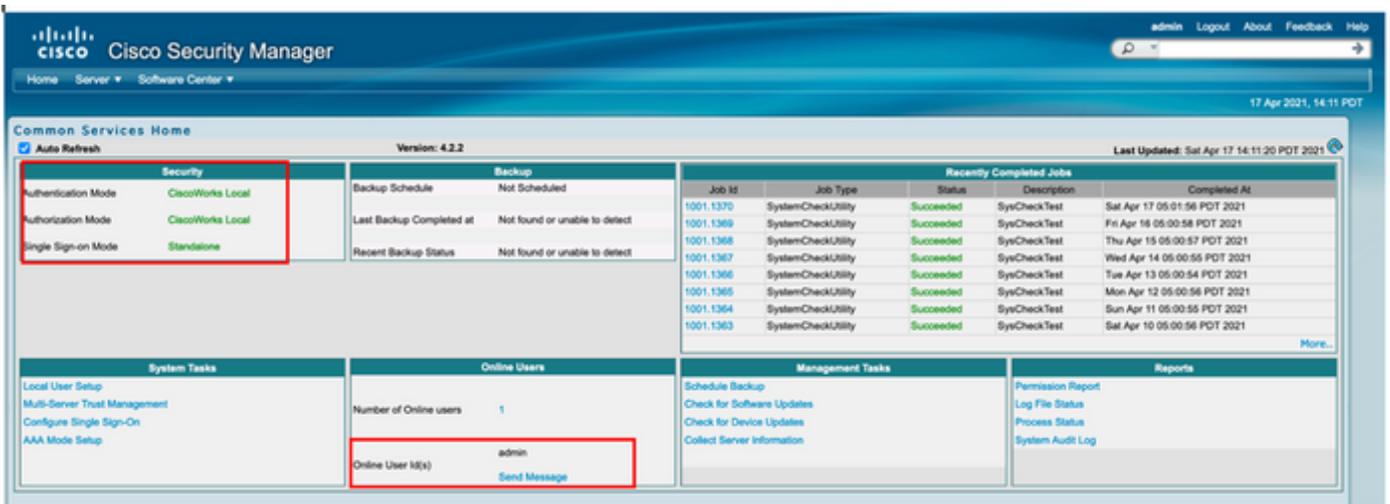
注意：在配置更改时，必须保存所有更改，这些更改需要提交和部署。

步骤4.导航至CSM Management UI并键入<https://<enter CSM IP Address>>，然后选择**Server Administration**。



注意：第4步到第7步显示了定义所有未在ISE上定义的管理员的默认角色的过程。这些步骤是可选的。

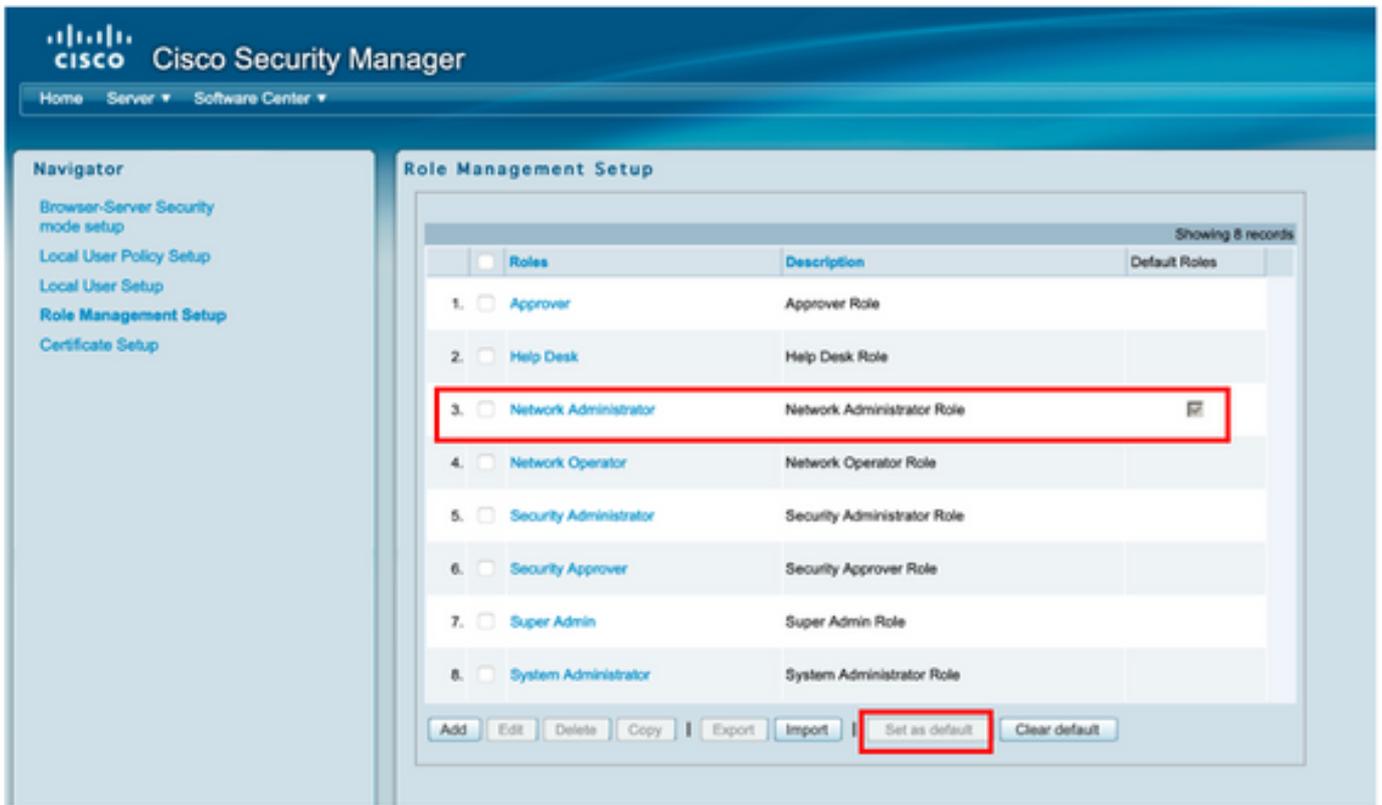
步骤5.验证身份验证模式设置为CiscoWorks Local，**Online** userID是在CSM上创建的本地管理员帐户。



步骤6. 导航至服务器并选择单服务器管理



步骤7. 选择Role Management Setup并选择所有管理员用户在身份验证时接收的默认权限。在本例中，使用网络管理员。选中后，选择set作为默认值。

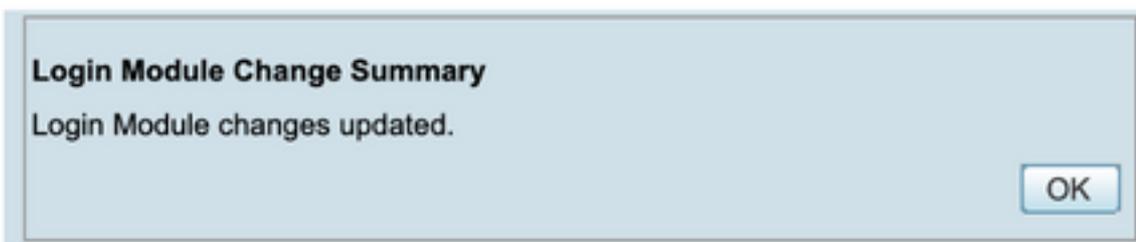
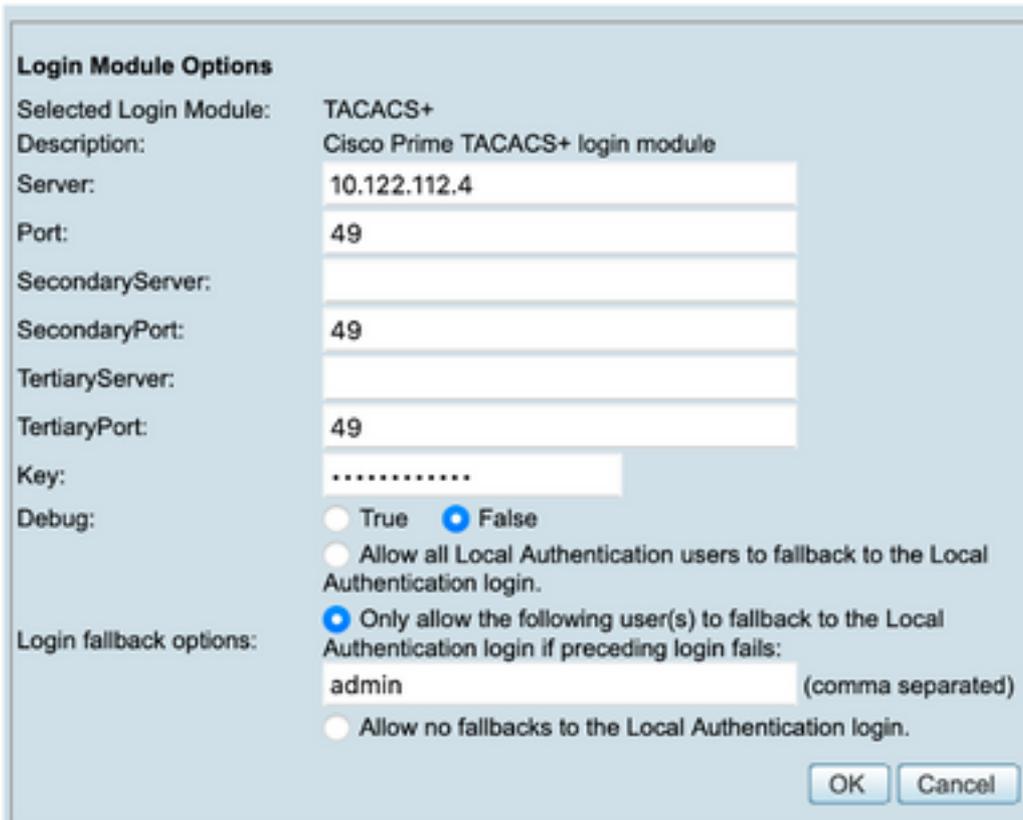


步骤8.选择服务器> AAA模式设置角色，然后选择TACACS+选项，最后选择更改以添加ISE信息。



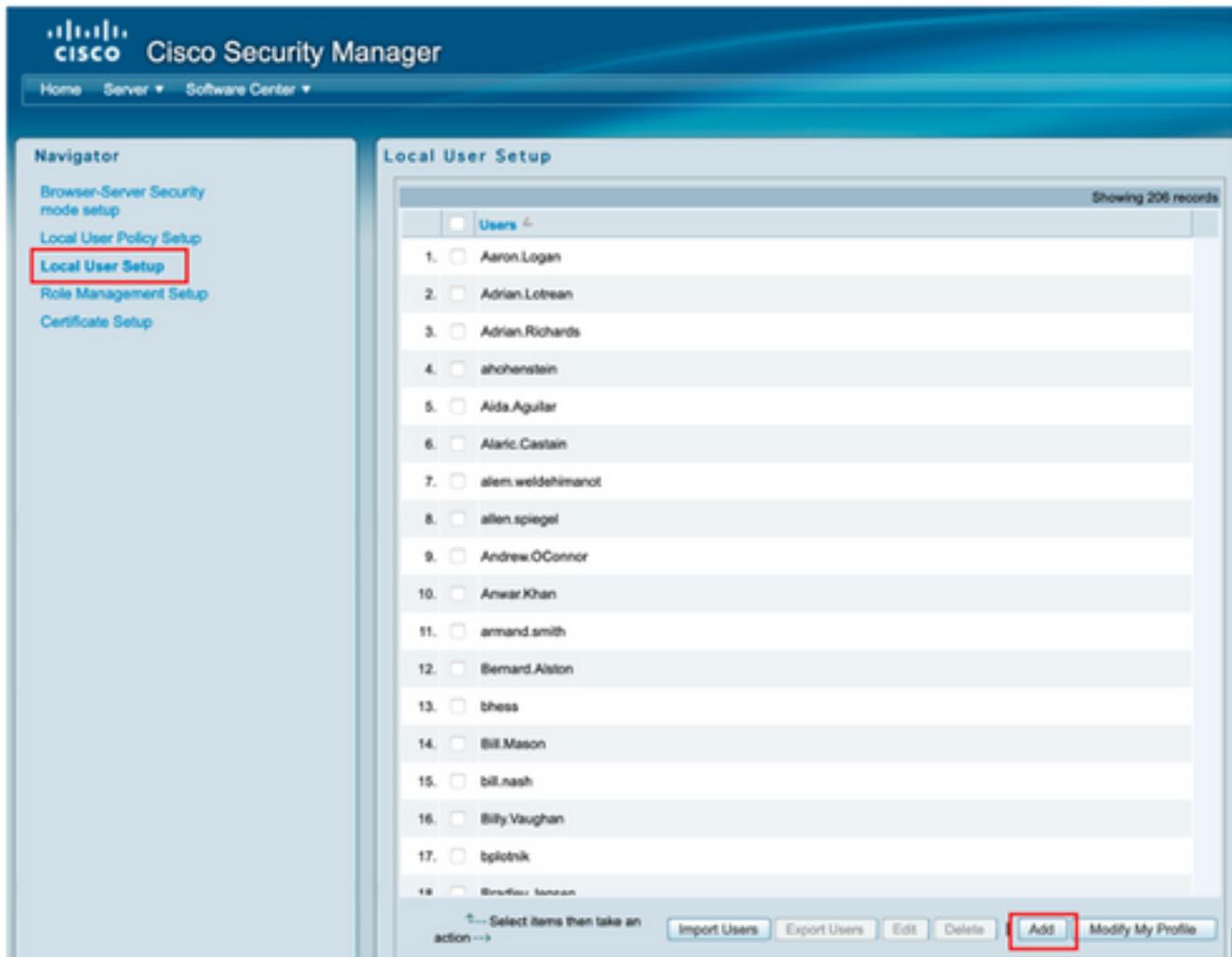


步骤9.定义ISE IP地址和密钥，或者，您可以选择允许所有本地身份验证用户或仅允许一个用户登录失败的选项。在本例中，仅允许管理员用户作为回退方法。选择**确定**以保存更改。



步骤10.选择Server> Single Server Management , 然后选择Local User Setup并选择Add。





步骤11.在ISE配置部分下定义步骤5中ISE上创建的相同用户名和密码，**csmpoper**和**帮助台任务授权**角色在本示例中使用。选择**OK**以保存管理员用户。

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

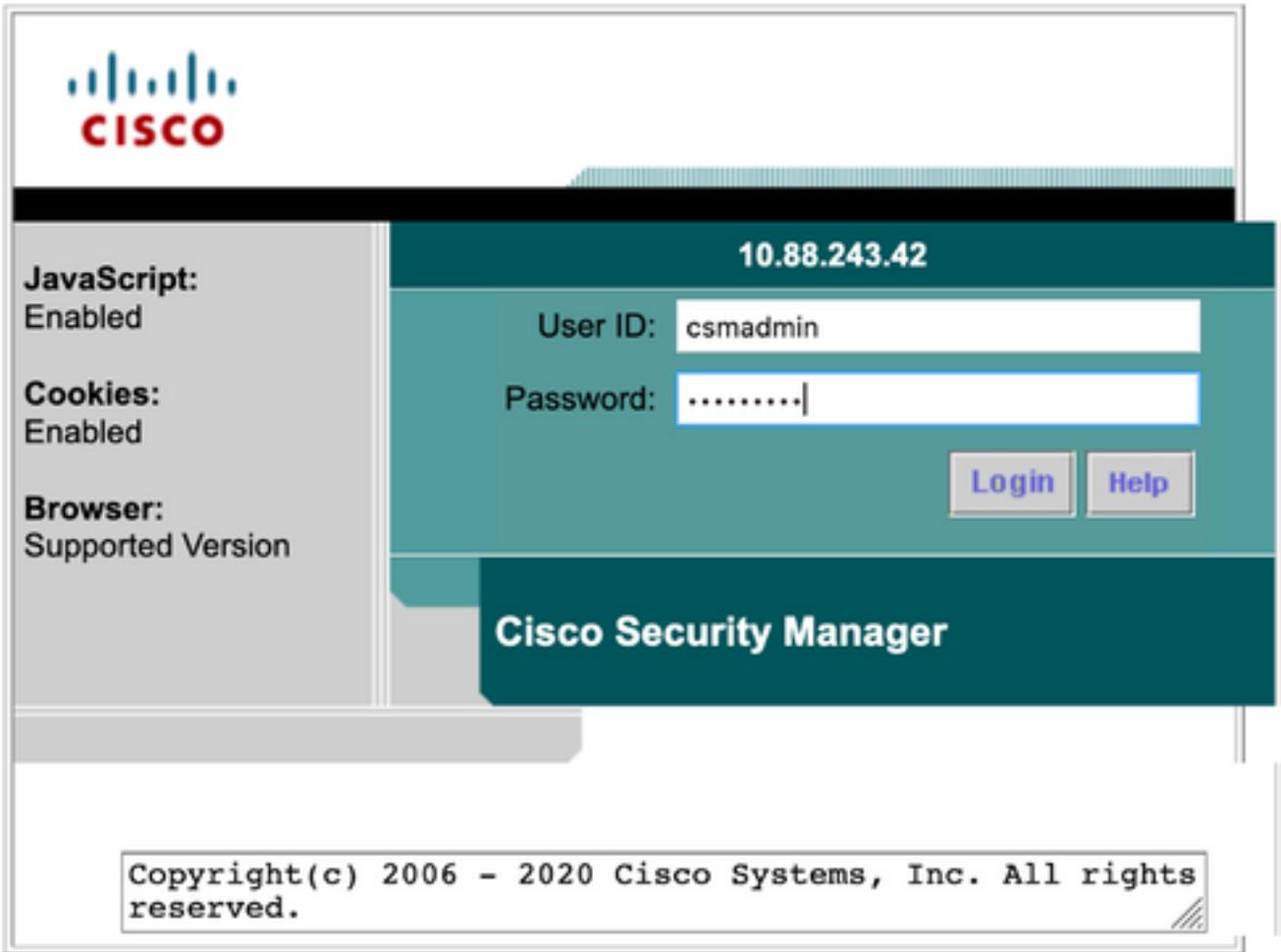
Device level Authorization

Not Applicable

验证

思科安全管理器客户端UI

步骤1. 打开新窗口浏览器并键入 https://<enter_CSM_IP_Address>，使用 **csmadmin** 用户名和密码在步骤5中在ISE配置部分下创建。



在ISE TACACS实时日志上验证尝试中的成功日志

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

思科安全管理器客户端应用

步骤1.使用帮助台管理员帐户登录到Cisco Security Manager客户端应用。



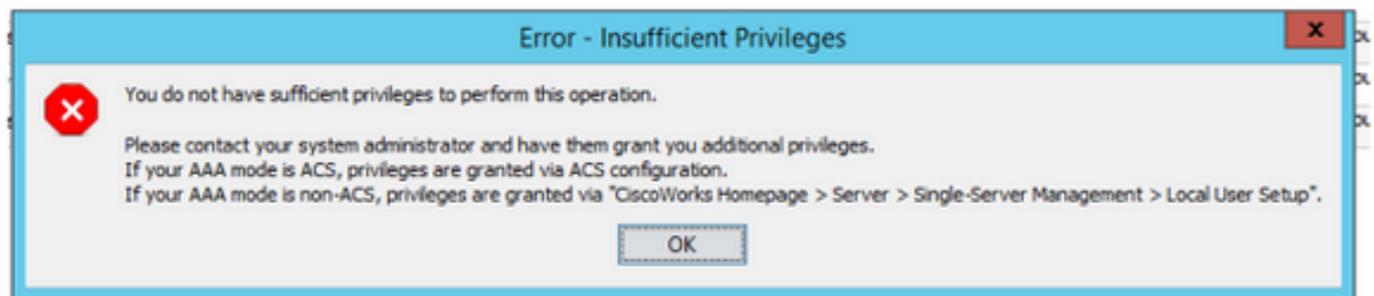
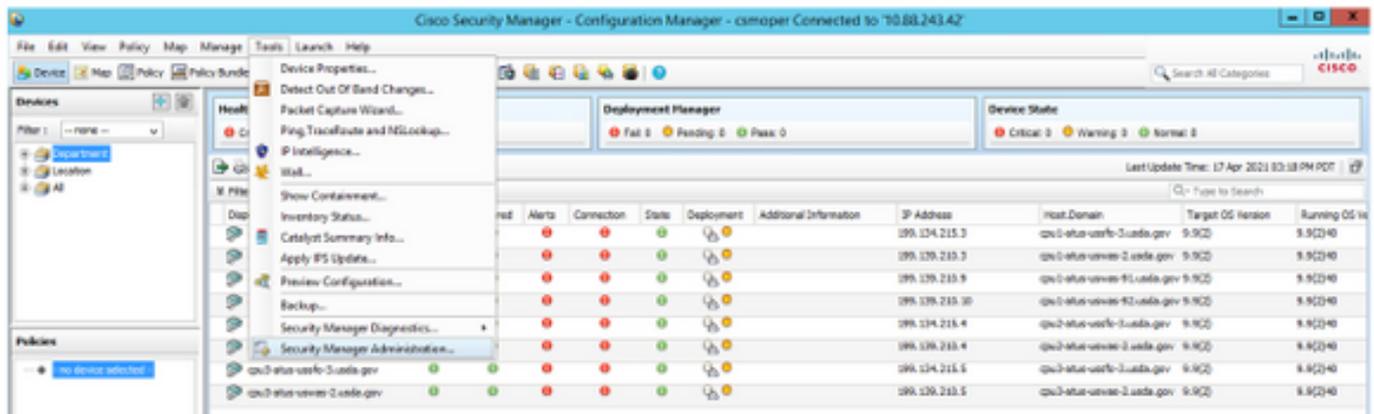
在ISE TACACS实时日志上验证尝试中的成功日志

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

步骤2.从CSM客户端应用程序菜单中选择**Tools > Security Manager Administration**，必须显示一条错误消息，指示权限不足。



步骤3.使用csmadmin帐户重复**步骤1**到**步骤3**，以验证是否向此用户提供了适当的权限。

故障排除

本节提供可用于排除配置故障的信息。

在ISE上使用TCP转储工具进行通信验证

步骤1.登录ISE并导航至左上角的三行图标，然后选择“操作”>“故障排除”>“诊断工具”。

步骤2.在“常规工具”下，选择“TCP转储”，然后选择“添加+”。选择Hostname、Network Interface File Name、Repository和过滤器（可选），以仅收集CSM IP地址通信流。选择**保存并运行**

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

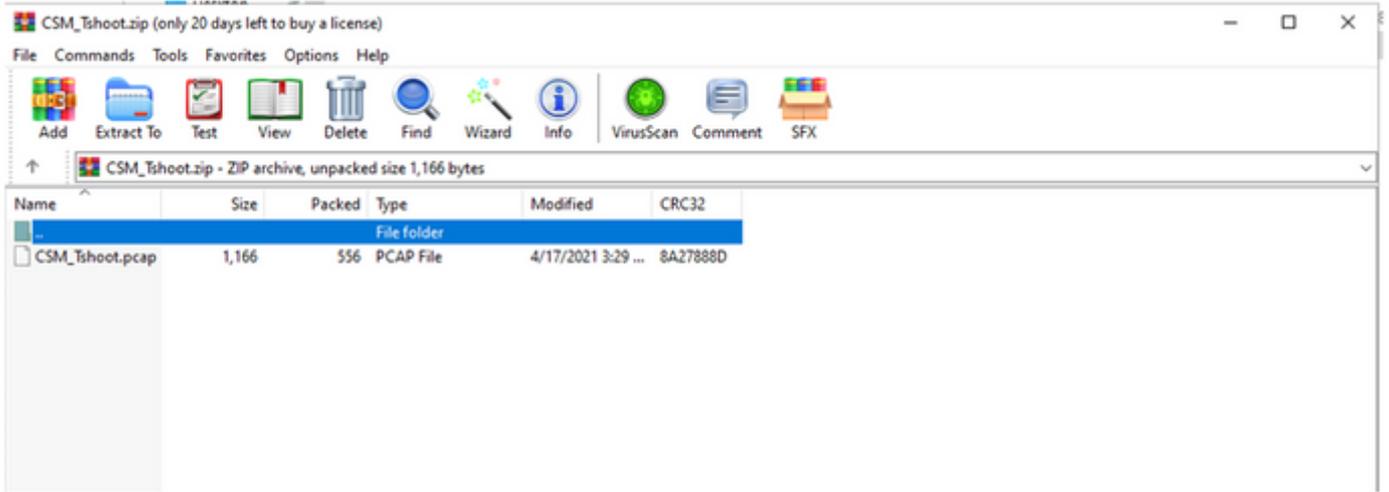
Cancel Save Save and Run

步骤3.登录CSM客户端应用或客户端UI并键入管理员凭证。

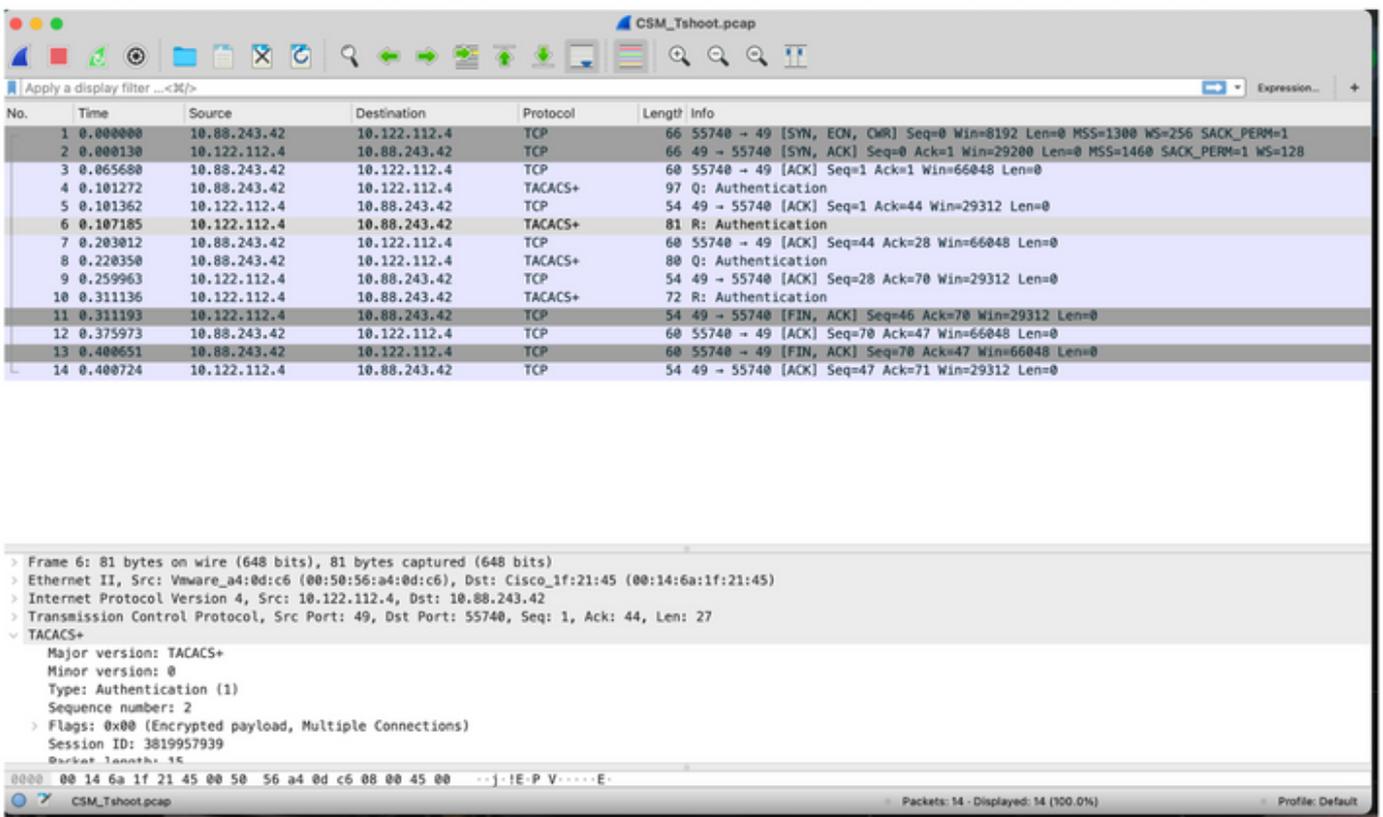
步骤4.在ISE上，选择**Stop**按钮并验证pcap文件是否已发送到定义的存储库。

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



步骤5.打开pcap文件以验证CSM和ISE之间的成功通信。



如果pcap文件上未显示任何条目，请验证以下内容：

1. 设备管理服务在ISE节点上启用
2. CSM配置中已添加正确的ISE IP地址
3. 如果防火墙位于中间，请验证端口49(TACACS)是否允许。