CSM TACACS与ISE集成

目录

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。

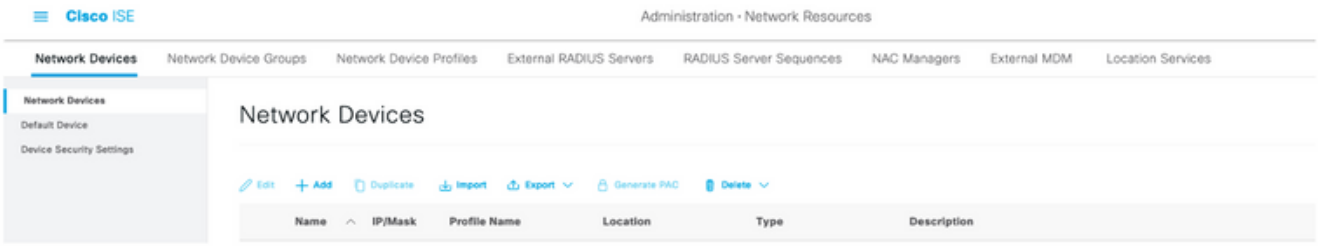
步骤3.身份验证成功后，ISE发送允许数据包以授权对CSM的访问。

步骤4. CSM将用户名与本地用户角色分配映射。

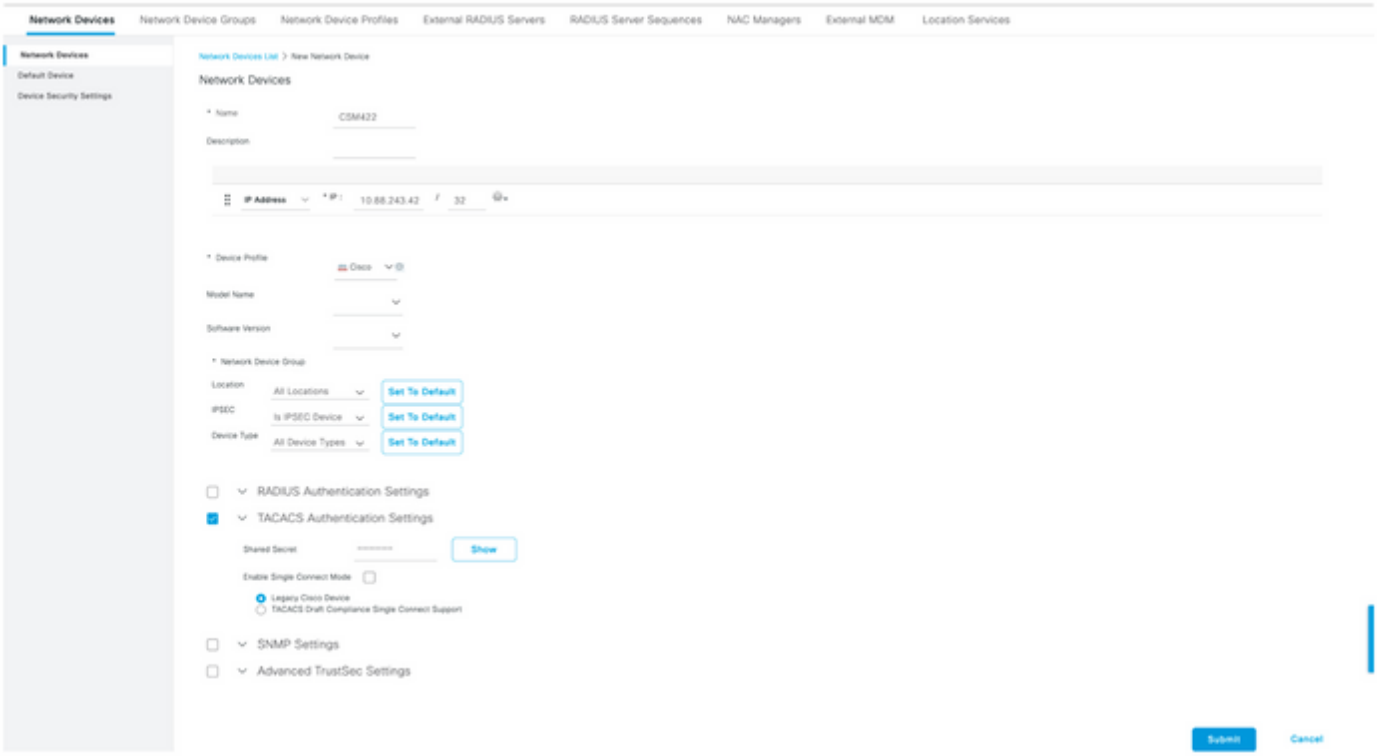
步骤5. ISE显示成功的身份验证实时日志。

ISE配置

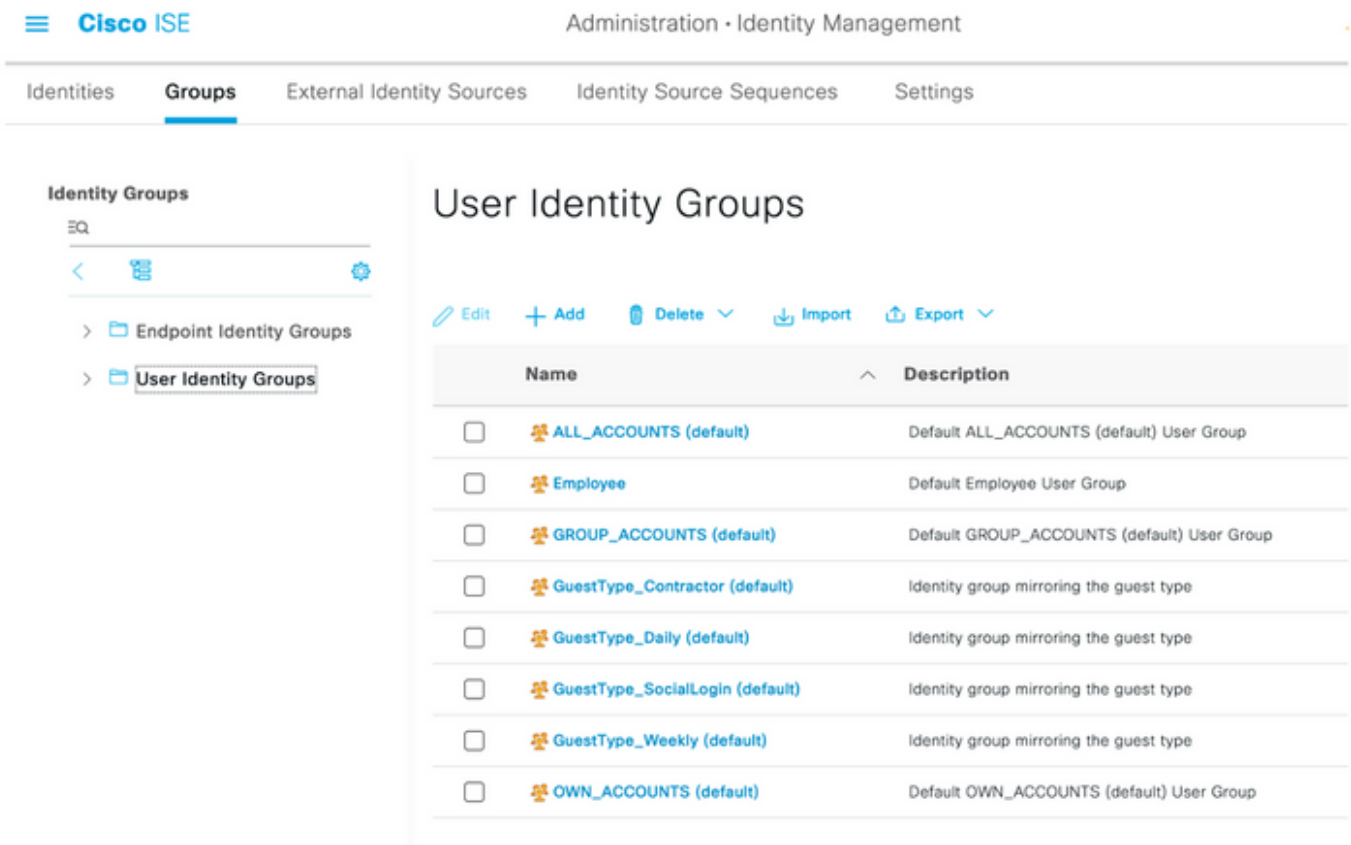
步骤1.选择三行图标 位于左上角，导航至**Administration > Network Resources > Network Devices。**



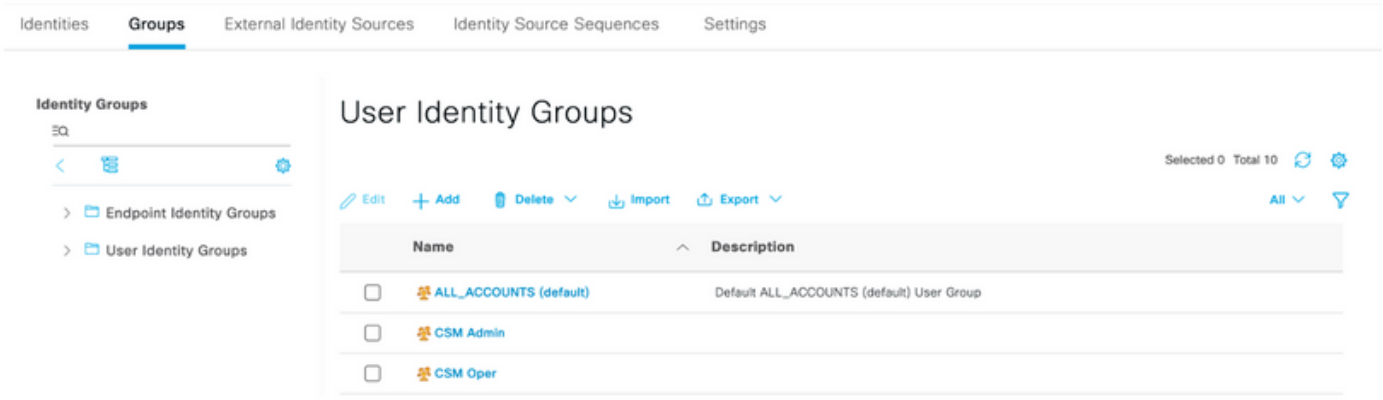
步骤2.选择**+Add**按钮，为Network Access Device Name和IP Address输入正确的值，然后验证**TACACS Authentication Settings**复选框并定义共享密钥。选择“**提交**”按钮。



步骤3.选择三行图标 位于左上角，导航至**Administration > Identity Management > Groups。**

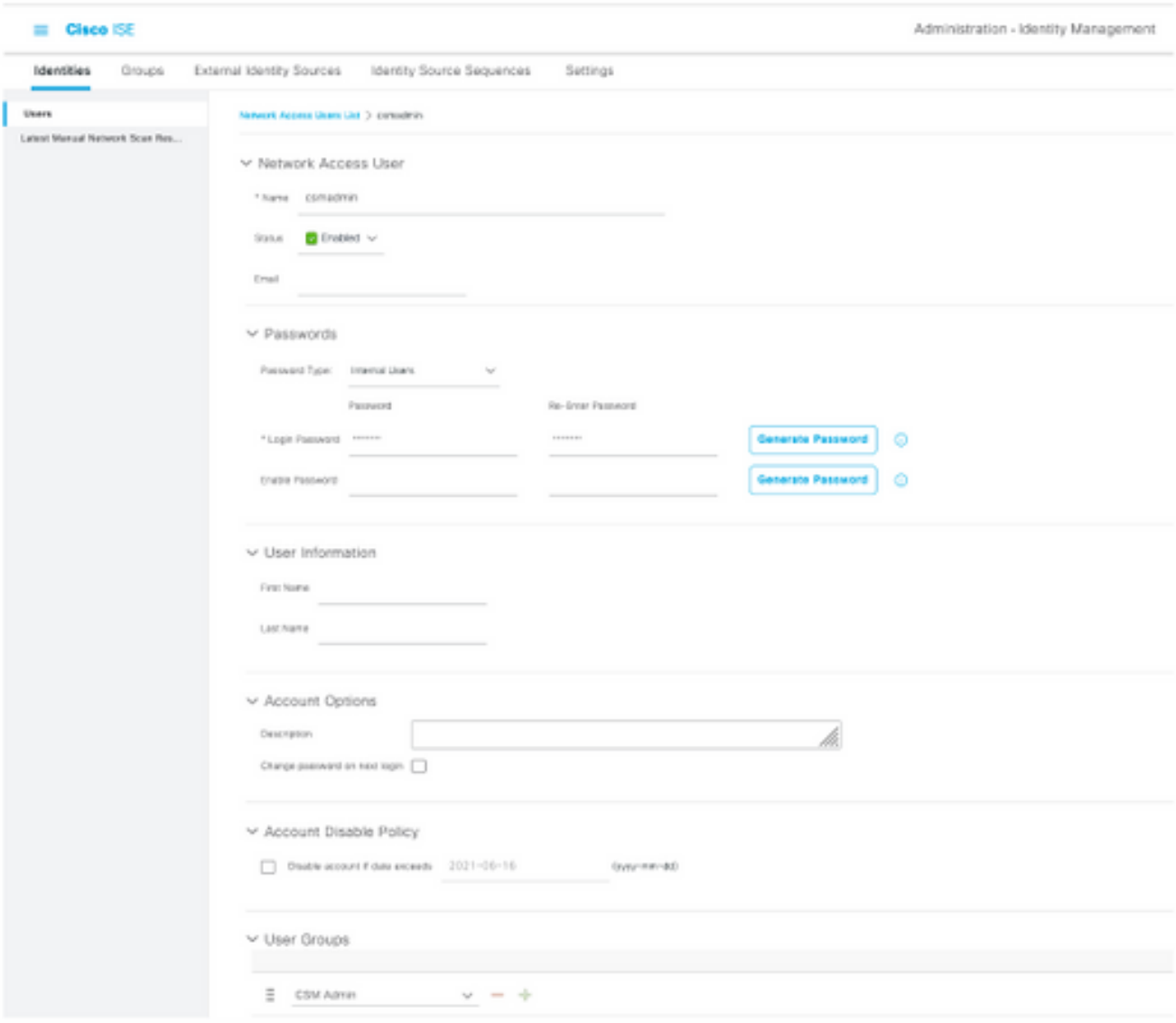


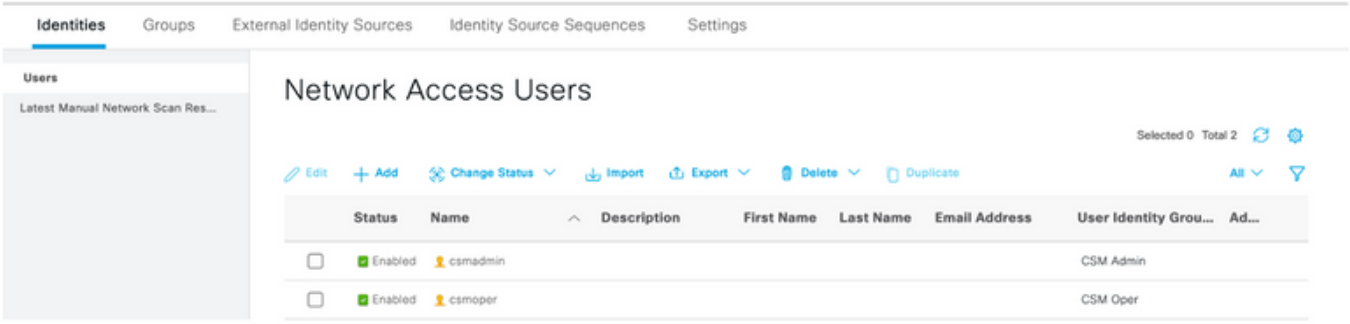
步骤4.导航至“**用户身份组**”文件夹，然后选**择+Add**按钮。定义名称并选择“提**交**”按钮。



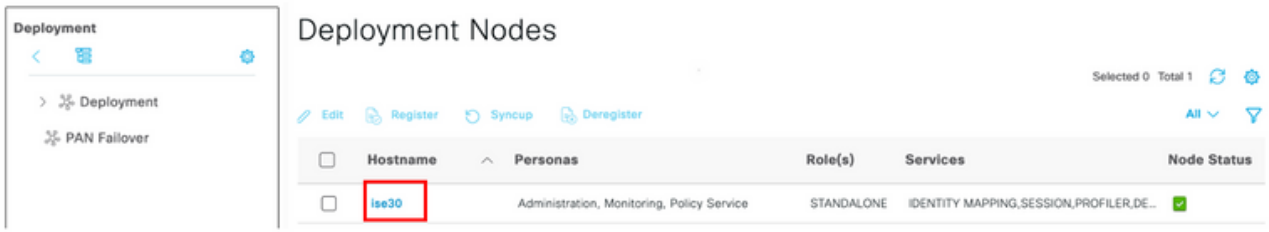
注意：此示例创建CSM Admin和CSM Oper Identity组。您可以对CSM上的每种类型的Admin Users重复步骤4

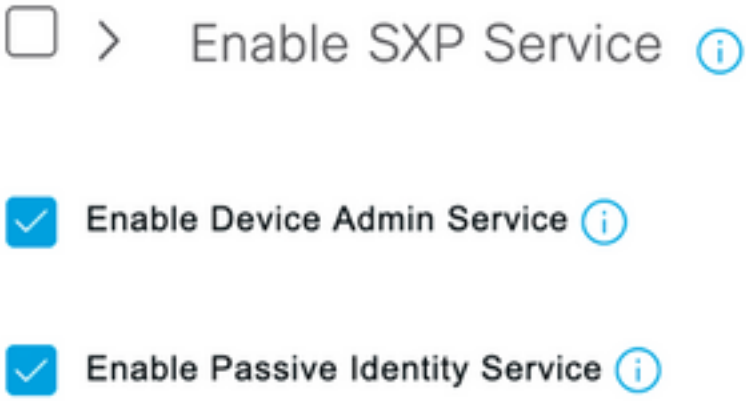
步骤5.选择三行图标 并导航至**Administration > Identity Management > Identities。**选择**+Add**按钮并定义用户名和密码，然后选择用户所属的组。在本示例中，分别创建**csmadmin**和**csmoper** 用户并分别分配给CSM Admin和CSM Oper组。





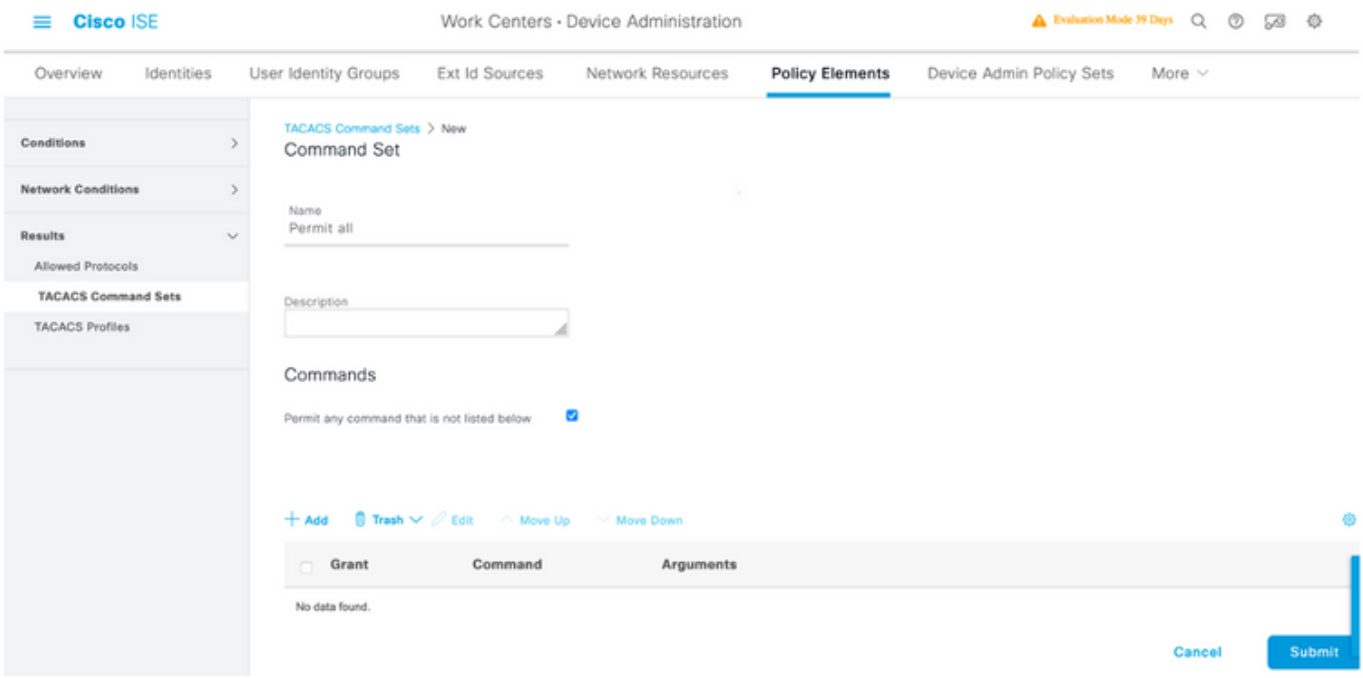
步骤6.选择 并导航至**管理>系统>部署。**选择主机名节点并启用设**备管理服务**



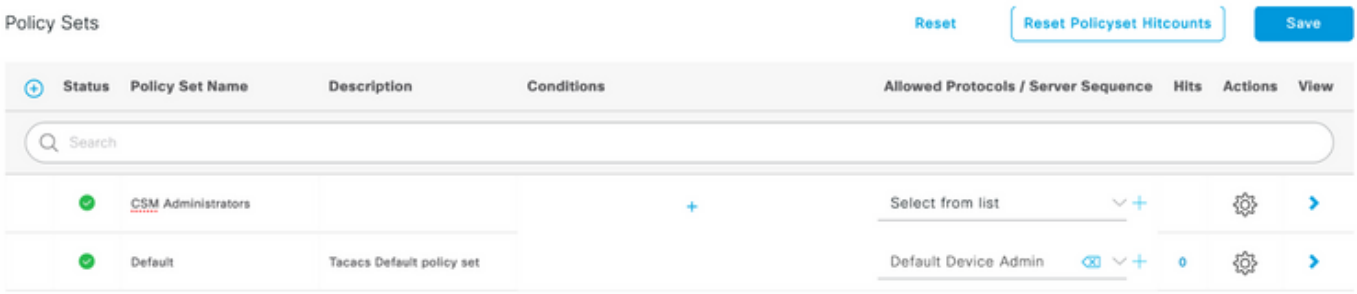


注意：在分布式部署中，选择处理TACACS请求的PSN节点

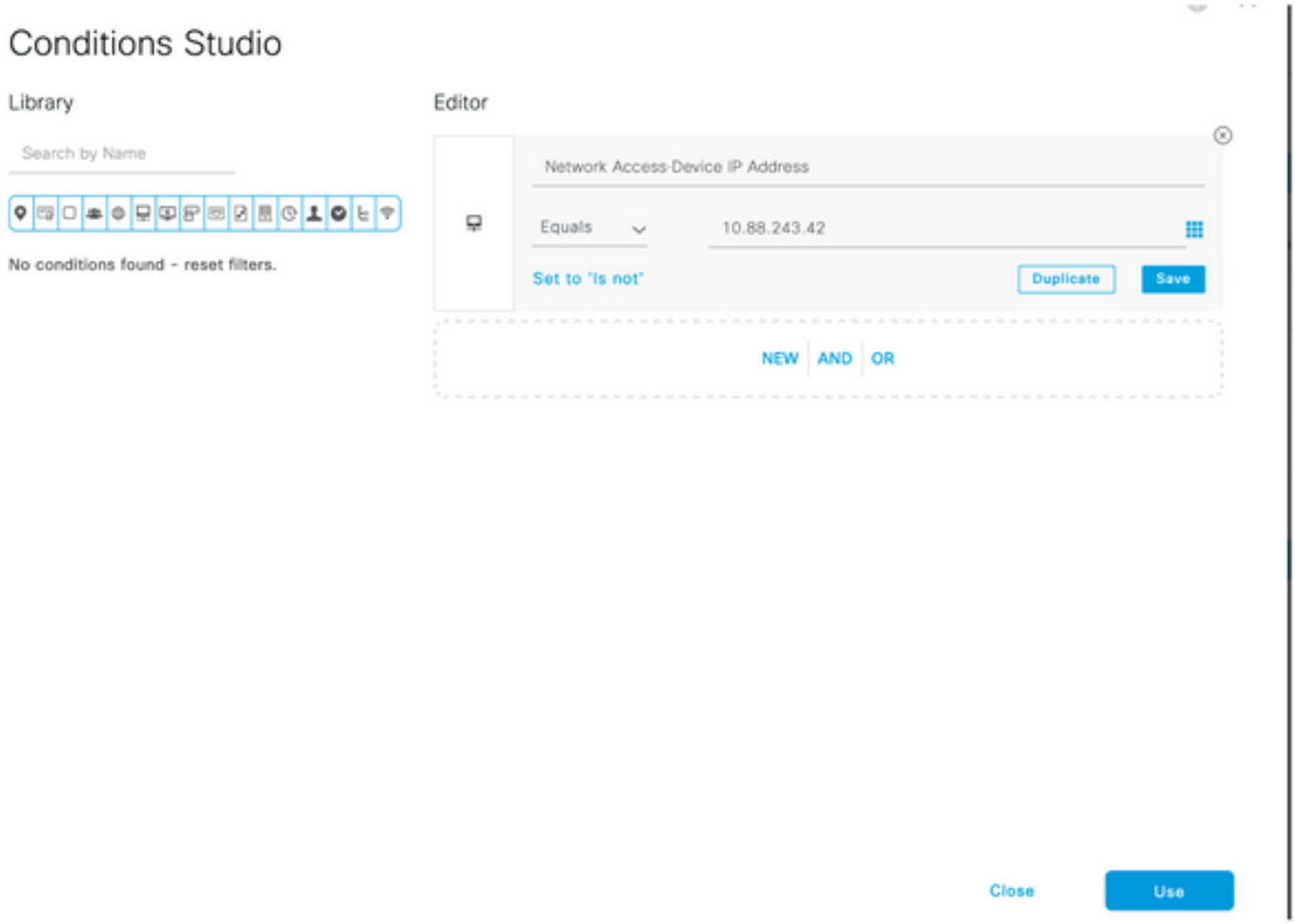
步骤7.选择三行图标并导航至管理**>设备管理>策略元素。**导航至“**结果”>“TACACS命令集”。**选择**+Add**按钮,定义命令集的名称，并启用**Permit any**命令，该命令未列在复选框下。选择 **Submit。**



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。



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”。



步骤10.在“允许协议”部分下，选择“设**备默认管理”**。选择保存

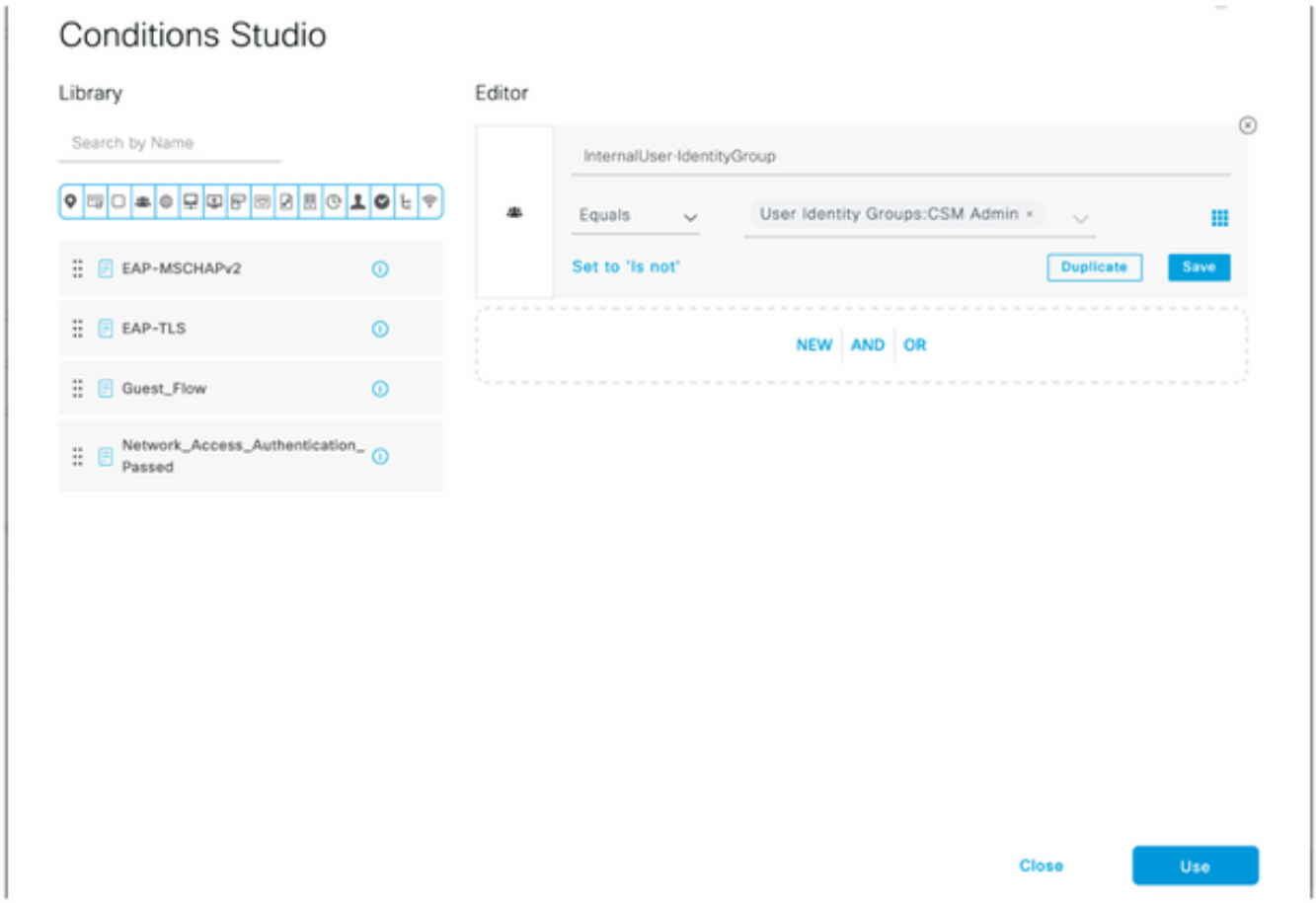
步骤11.选择右箭头 “策略集”图标定义身份验证和授权策略

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**

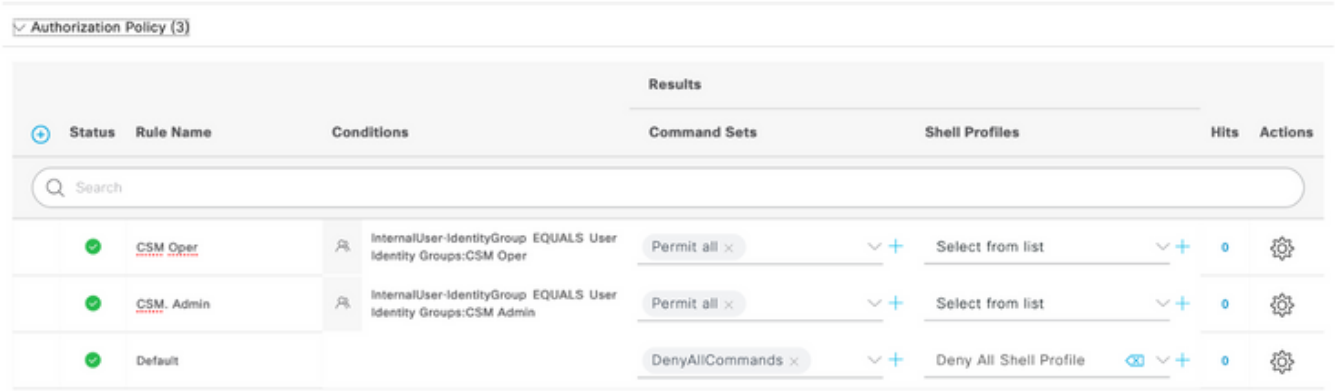
注意：如果ISE加入Active Directory，则身份库可更改为AD库。

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**。



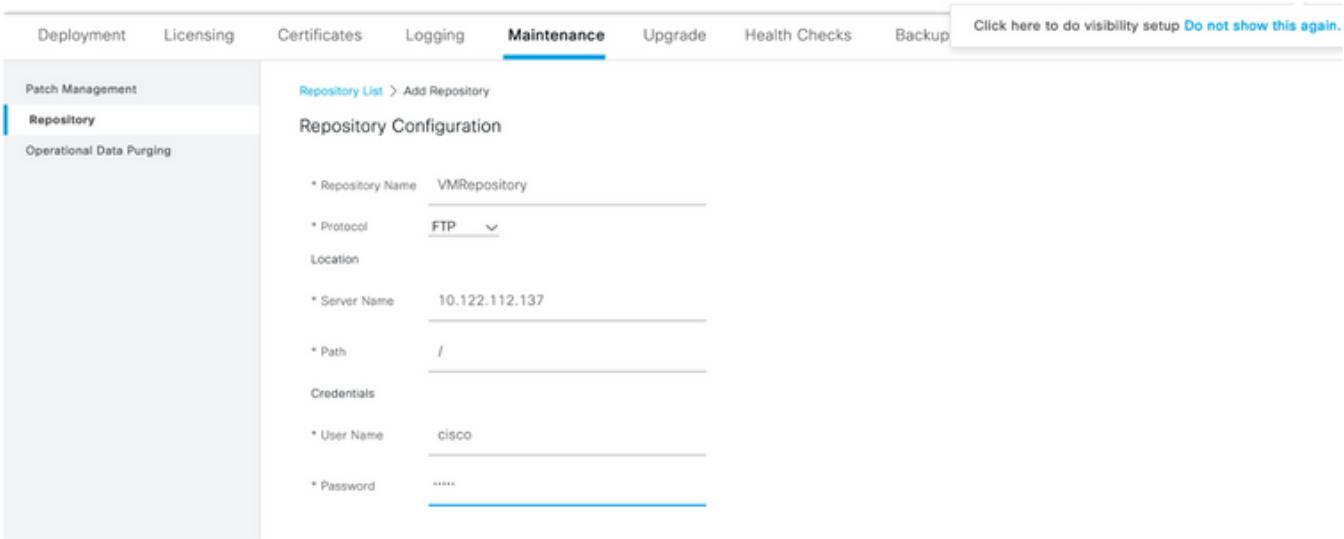
步骤15.在“命令集”下，选择“允许在步骤7中创建的所有命令集”，然后选择“保**存”**

对CSM操作组重复步骤14和15



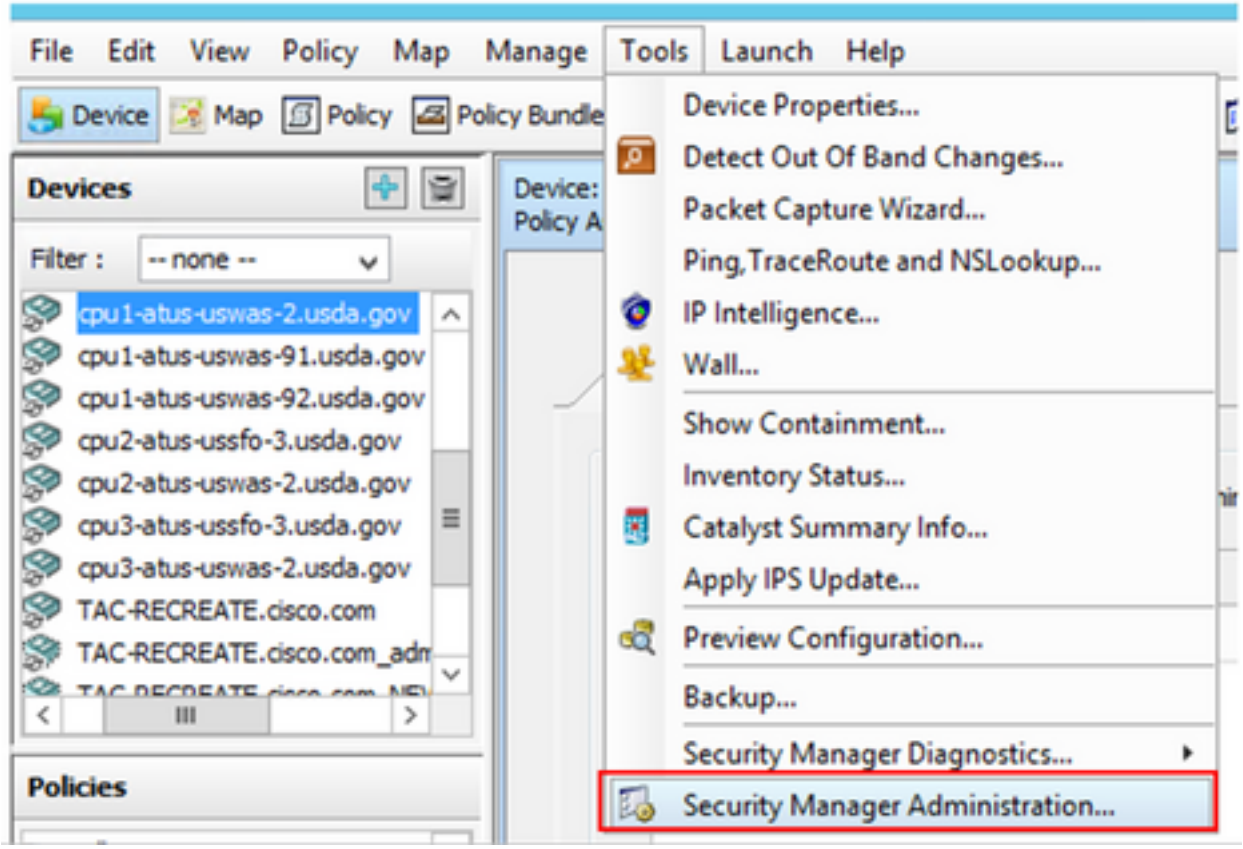
步骤 16（可选）。 选择左上角的三行图标，然后选择**Administration>System>Maintenance>Repository**，选择**+Add**以添加用于存储TCP转储文件以进行故障排除的存储库。

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”。

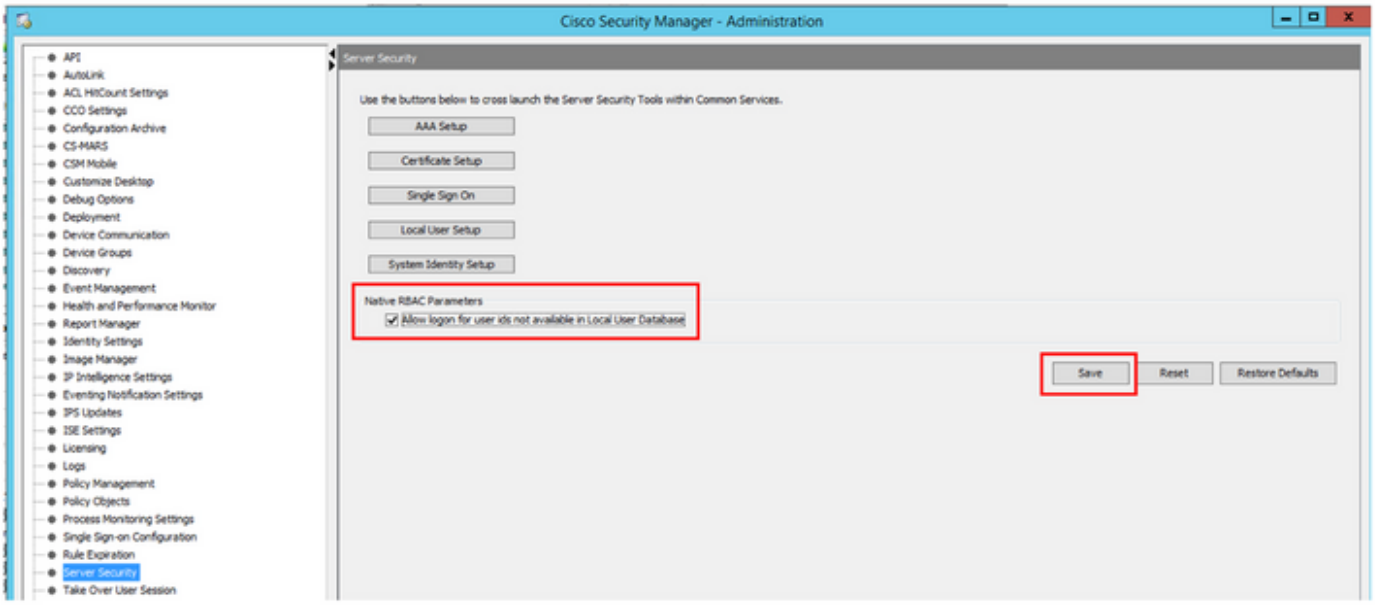


CSM配置

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**



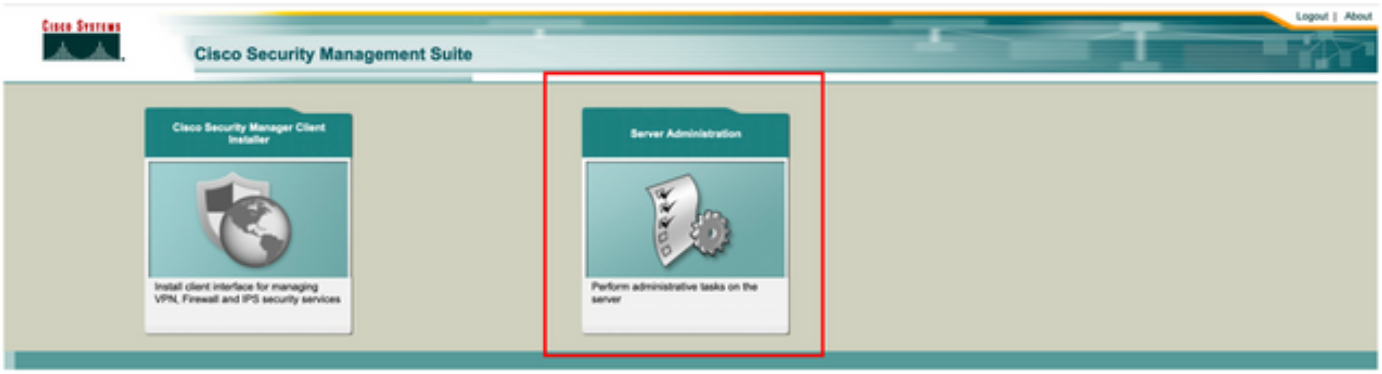
步骤2.选中Native RBAC Parameters下**的复选框。**选择**保存**并关**闭**



步骤3.从菜单中选择“文**件”>“提交”。文件>提交。**

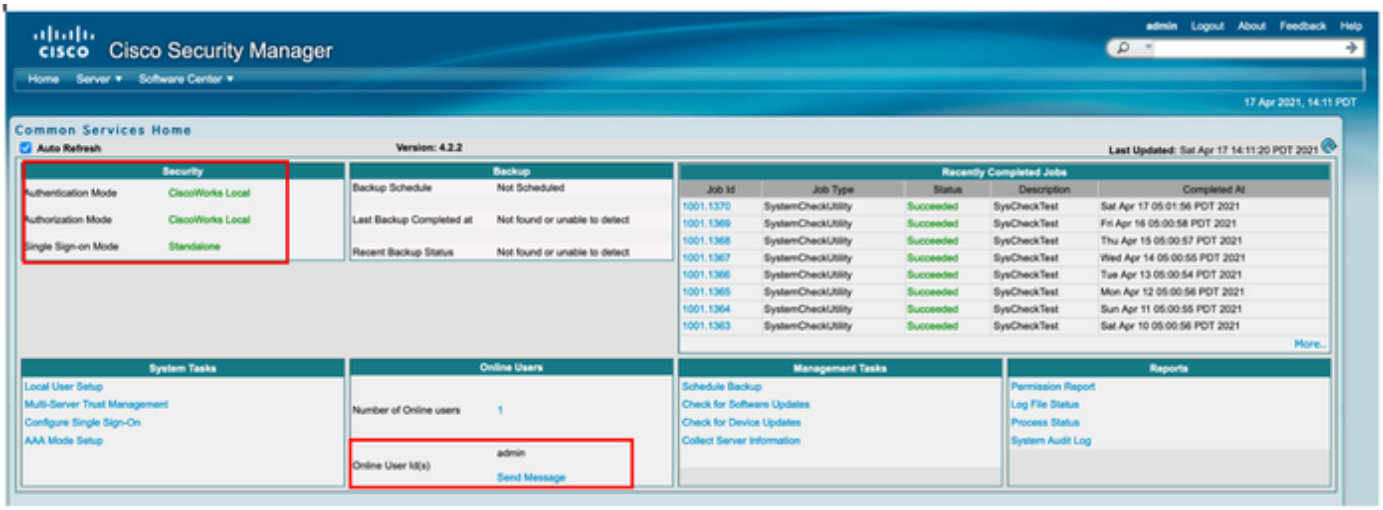
注意：在配置更改时，必须保存所有更改，这些更改需要提交和部署。

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



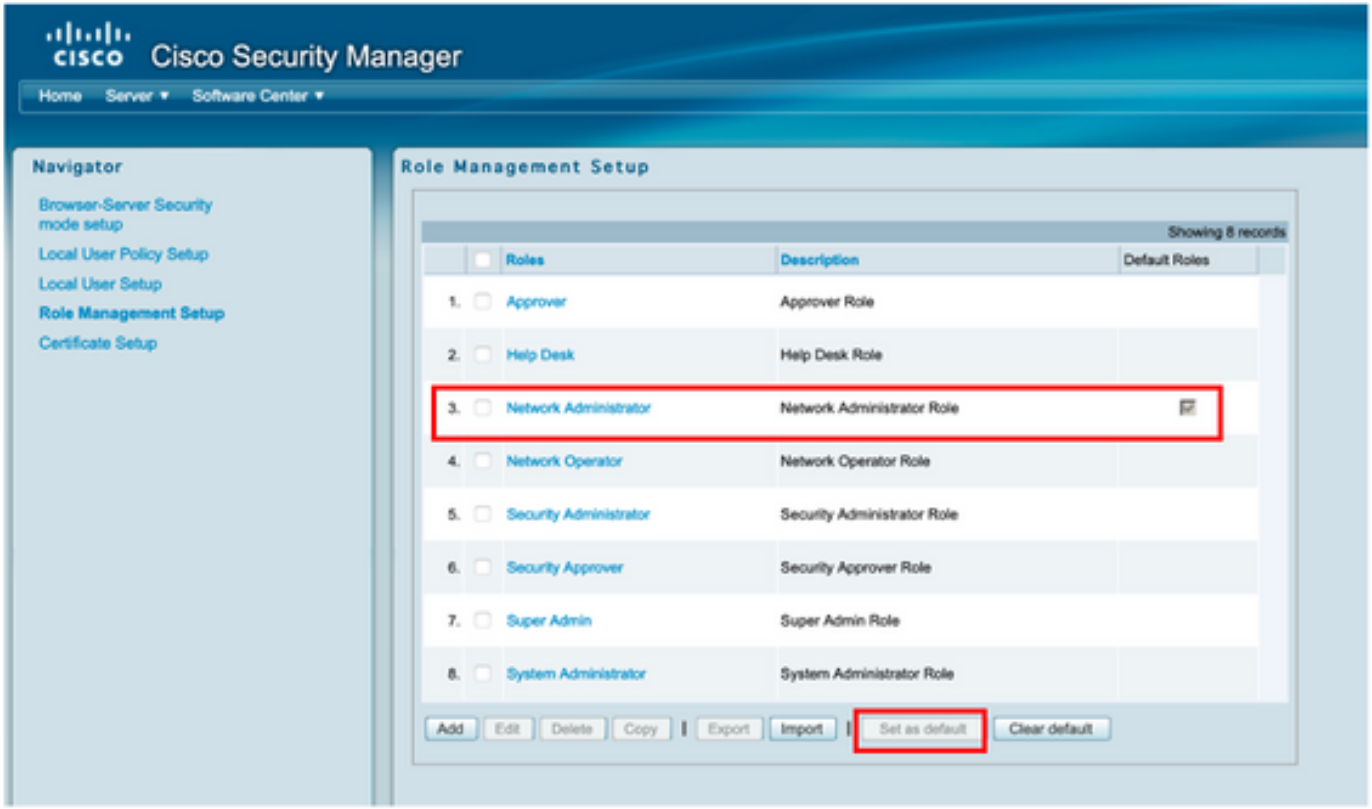
注意：第4步到第7步显示了定义所有未在ISE上定义的管理员的默认角色的过程。这些步骤是可选的。

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。



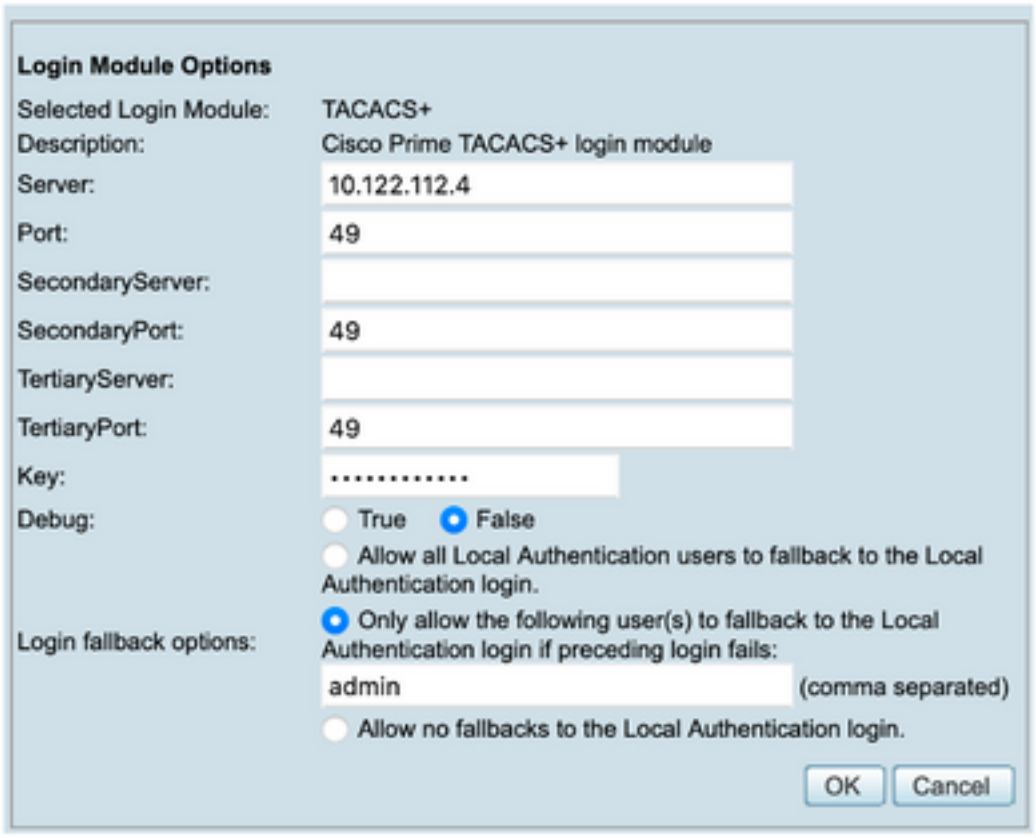
步骤6.导航至**服务器**并选择**单服务器管理**

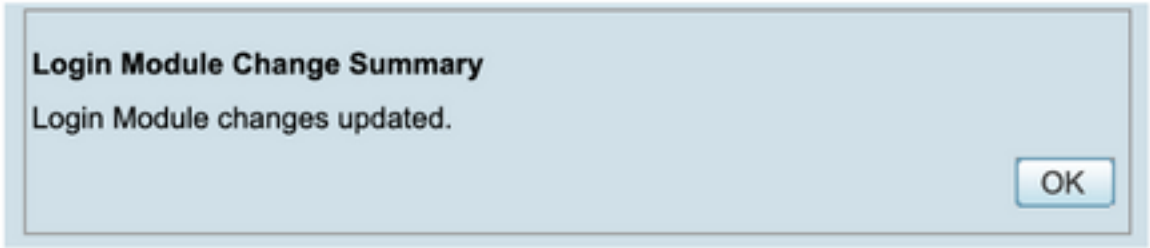
步骤7.选择Role Management Setup并选择所有管理员用户在身份验证时接收的默认权限。在本例中，使用网络管理员。选中后，选择**set作为默认值。**



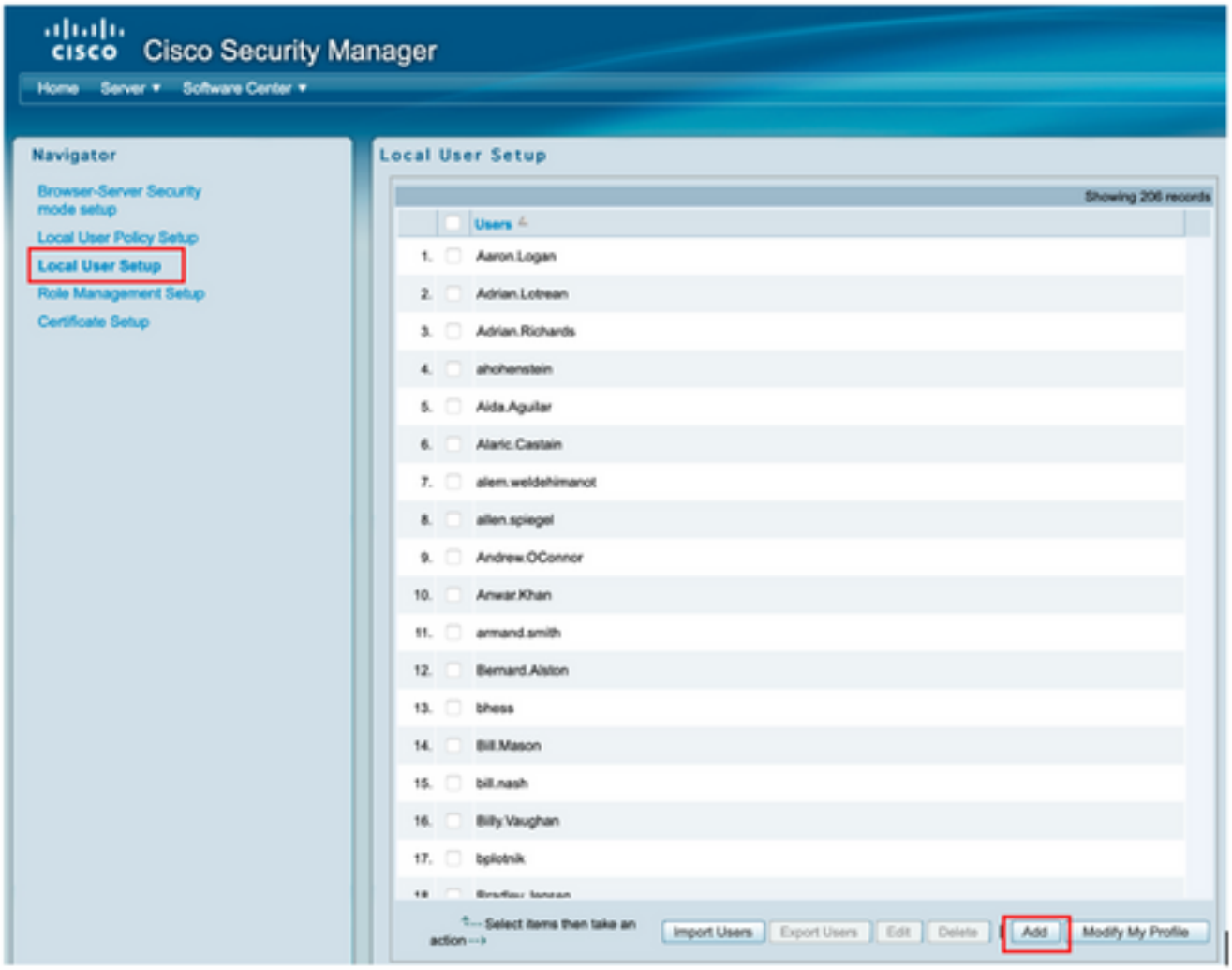
步骤8.选择服**务器> AAA模式设置角**色，然后**选择TACACS+**选项，最后选**择更改**以添加ISE信息。

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。

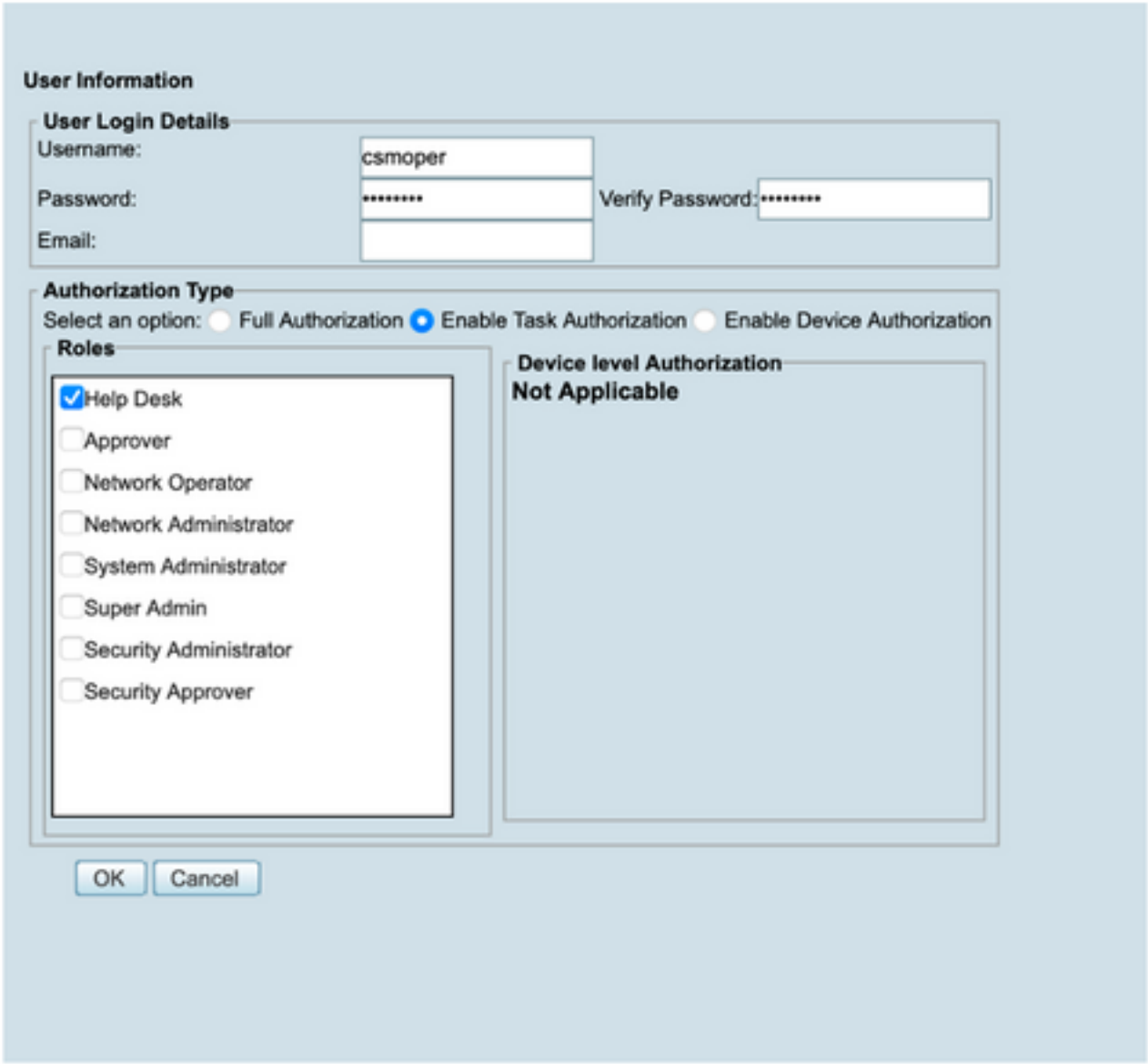




步骤10.选择Server> Single Server Management，然后选择Local User Setup并选择Add。



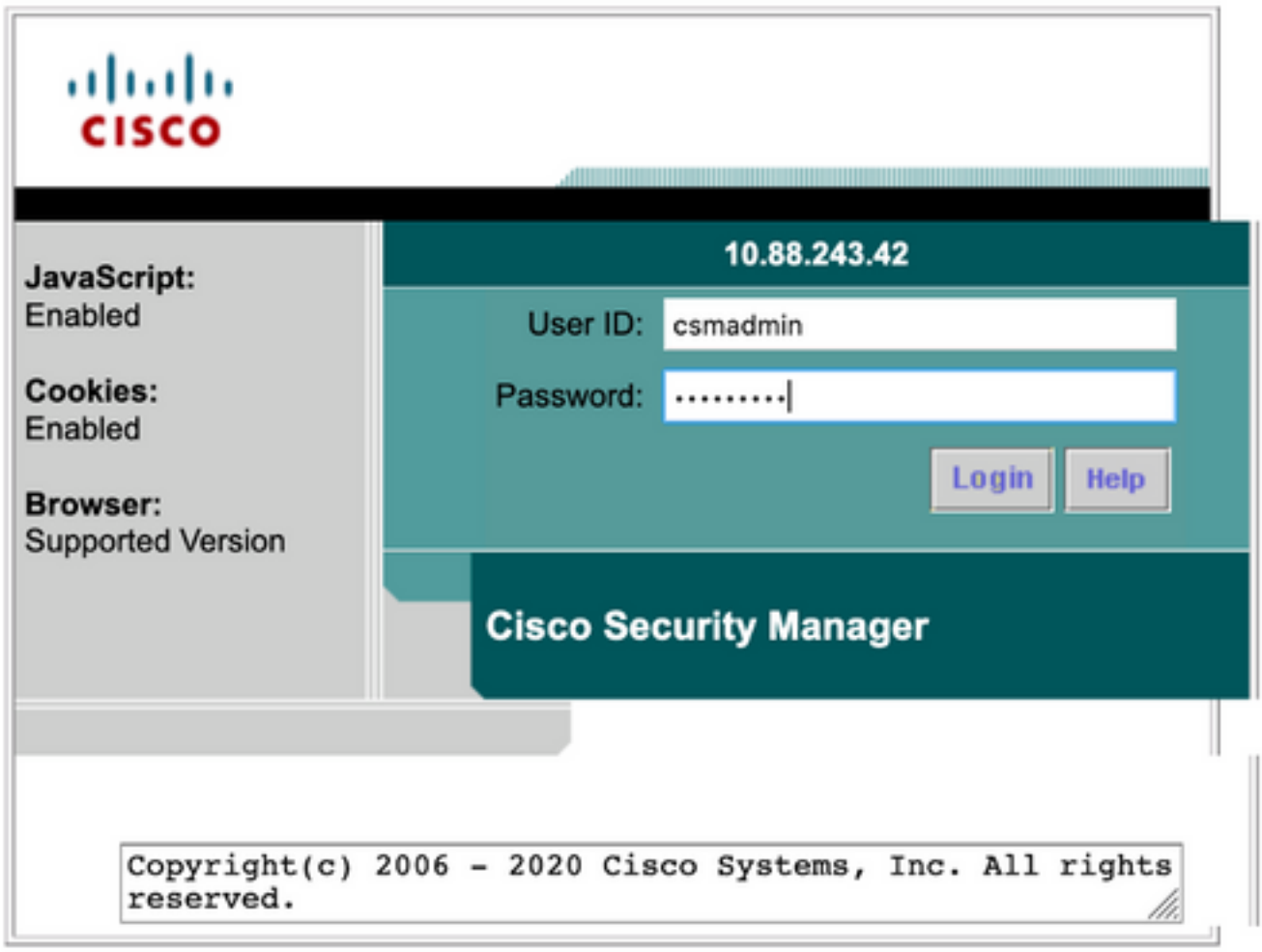
步骤11.在ISE配置部分下定义步骤5中ISE上创建的相同用户名和密码，**csmoper**和**帮助台任务授**权角色在本示例中使用。选择**OK**以保存管理员用户。



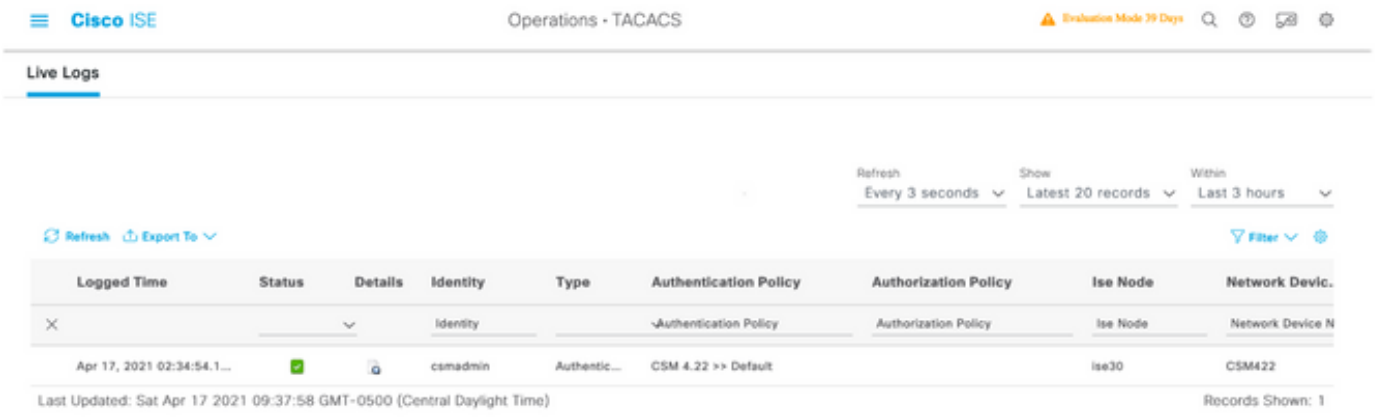
验证

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

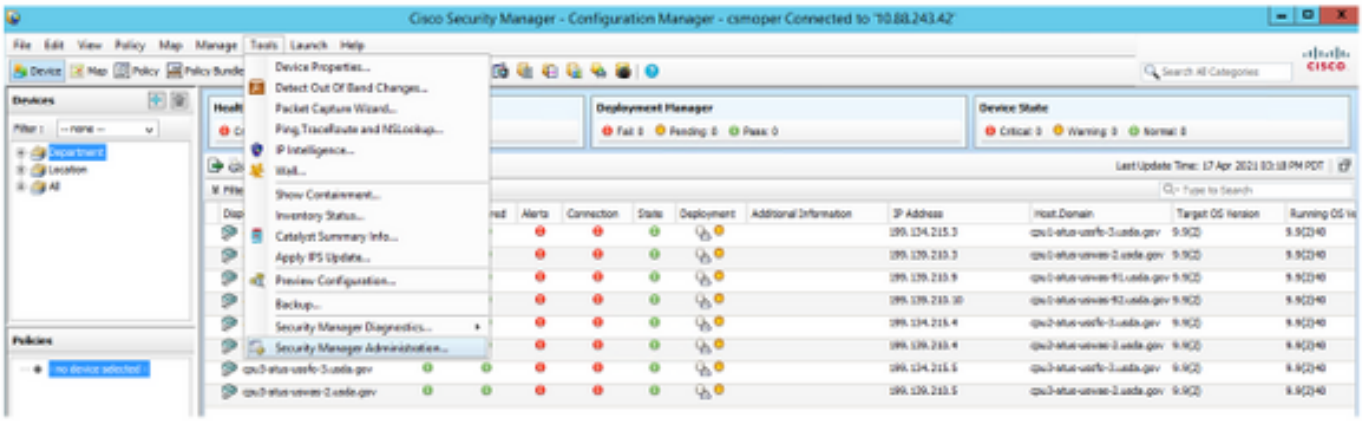


思科安全管理器客户端应用

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

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。

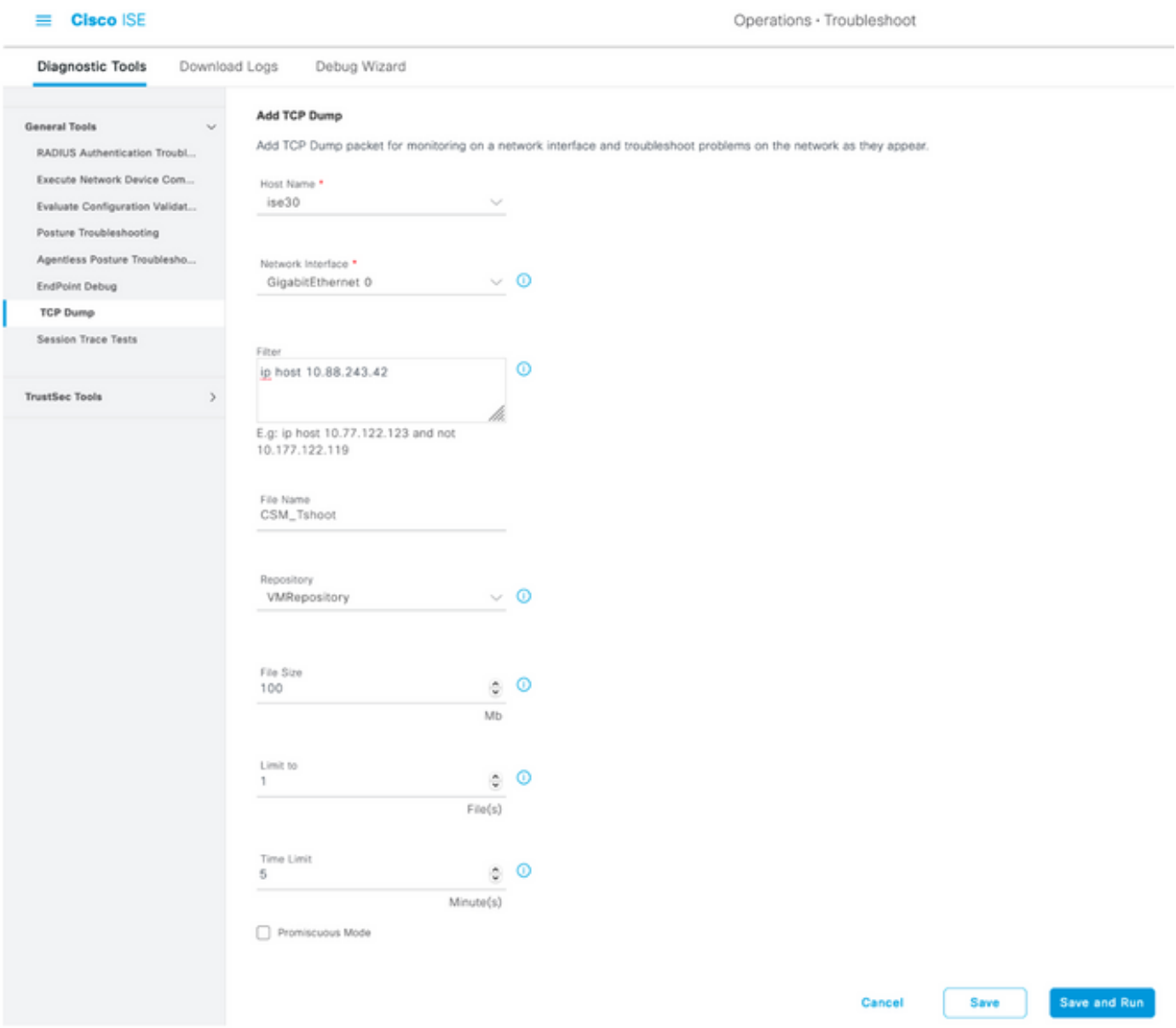
故障排除

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

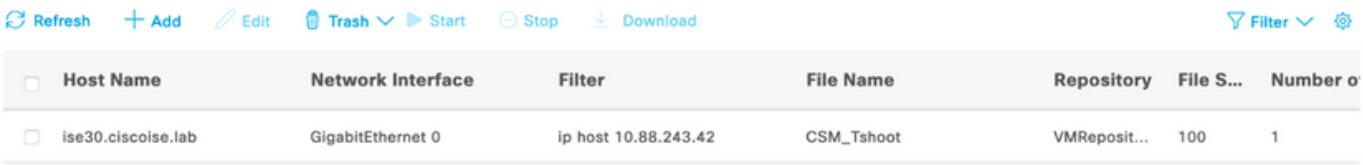
步骤1.登录ISE并导航至左上角的三行图标，然后选择“操作”>“故障排除”**>“诊断工具”。**

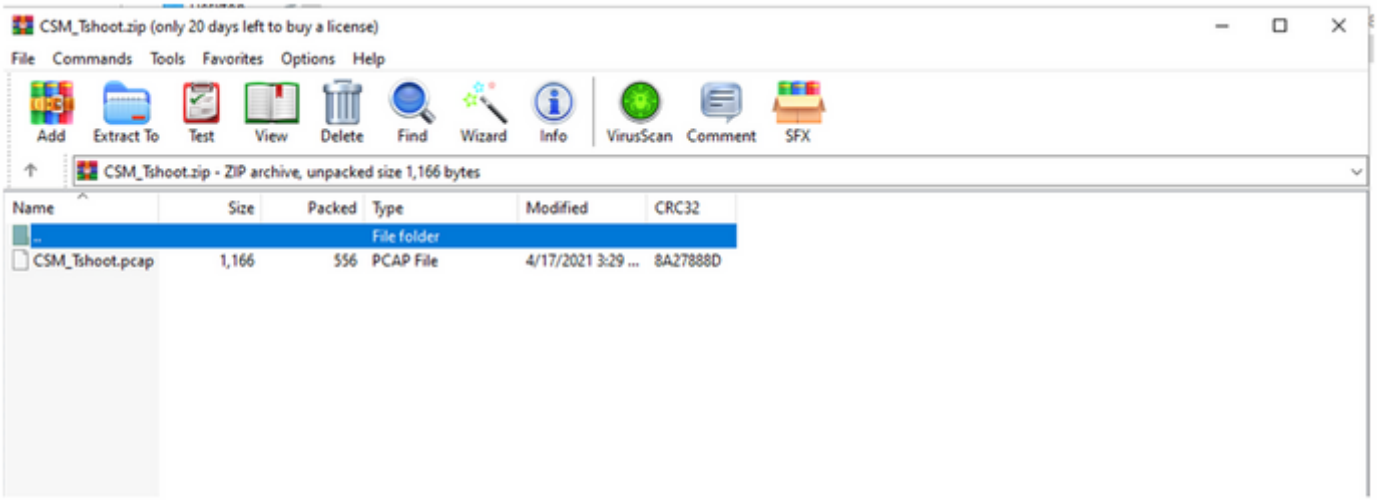
步骤2.在“常规**工具”**下，选**择“TCP转**储”，然后**选择“添加+”。**选择Hostname、Network Interface File Name、Repository和过滤器（可选），以仅收集CSM IP地址通信流。选择**保存并运行**



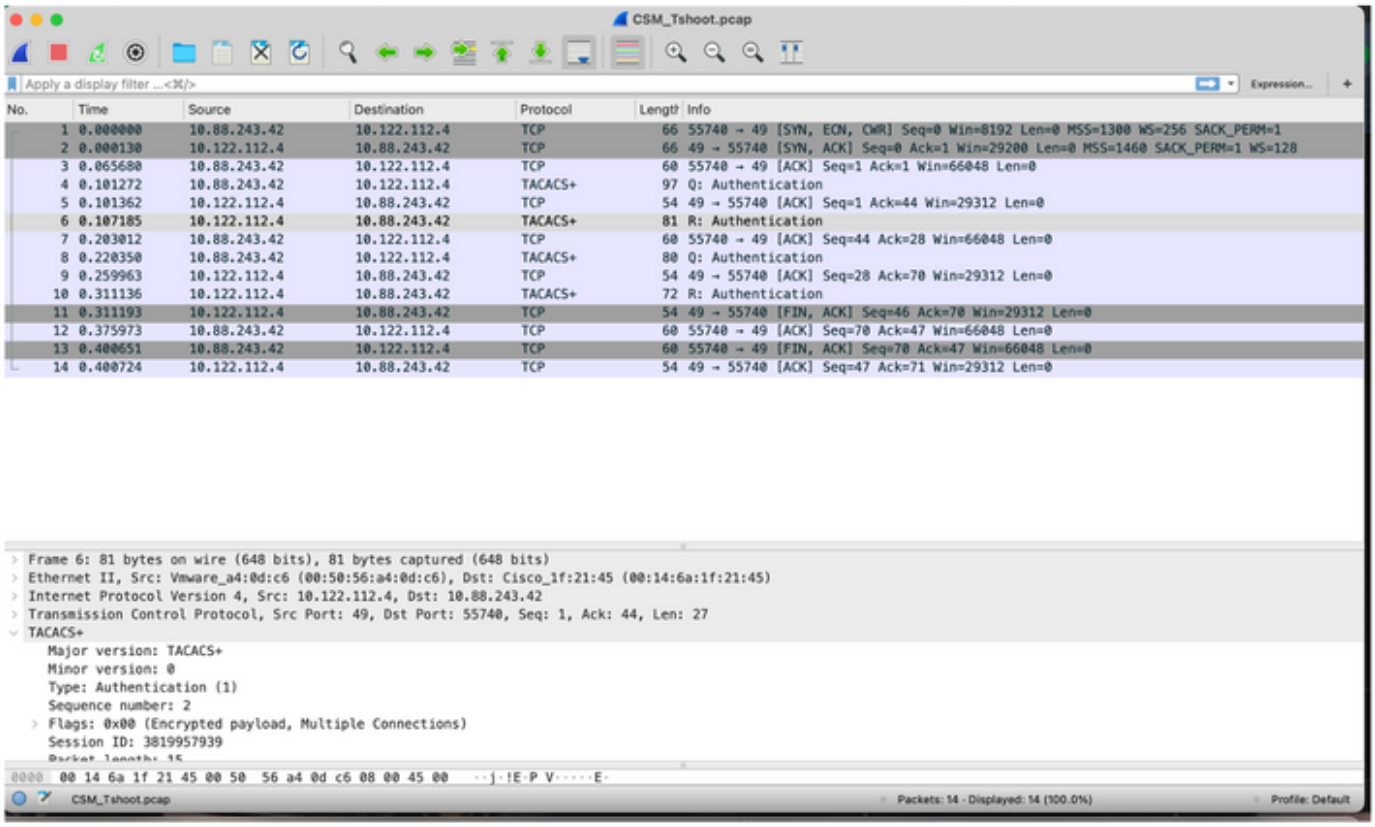
步骤3.登录CSM客户端应用或客户端UI并键入管理员凭证。

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。





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。