使用ISE在Palo Alto上配置TACACS+设备管理

目录

简介

先决条件

使用的组件

网络图

- 身份验证流程

配置

- 第1部分：为TACACS+配置Palo Alto防火墙
- 第2部分：ISE上的TACACS+配置

验证

- ISE审核

故障排除

- 1个TACACS:无效的TACACS+请求数据包 — 可能共享密钥不匹配
  - 问题
  - 可能的原因
  - 解决方案
- 2.无ISE TACACS实时日志

简介

本文档介绍使用Cisco ISE在Palo Alto上的TACACS+配置。

先决条件

Cisco 建议您了解以下主题：

- Cisco ISE和TACACS+协议。
- Palo Alto防火墙。

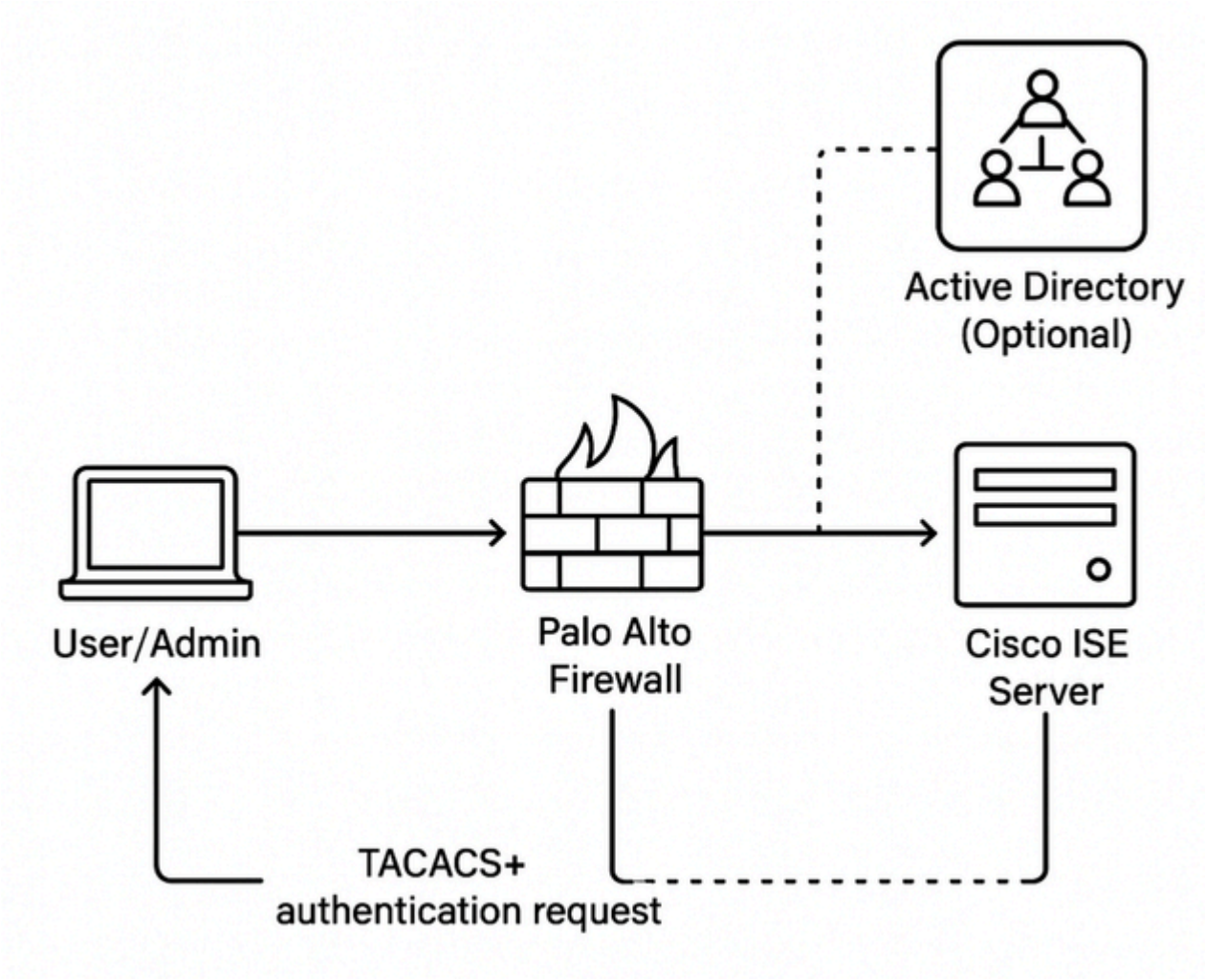
使用的组件

本文档中的信息基于以下软件和硬件版本：

- Palo Alto Firewall 10.1.0版
- 思科身份服务引擎(ISE)版本3.3补丁4

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。

网络图



身份验证流程

1.管理员登录Palo Alto防火墙。

2. Palo Alto向Cisco ISE发送TACACS+身份验证请求。

3.思科ISE:

- 如果AD已集成，它将查询AD进行身份验证和授权。
- 如果没有AD，则使用本地身份库或策略。
- 思科ISE根据配置的策略向Palo Alto发送授权响应。
- 管理员获得具有适当权限级别的访问权限。

配置

第1部分：为TACACS+配置Palo Alto防火墙

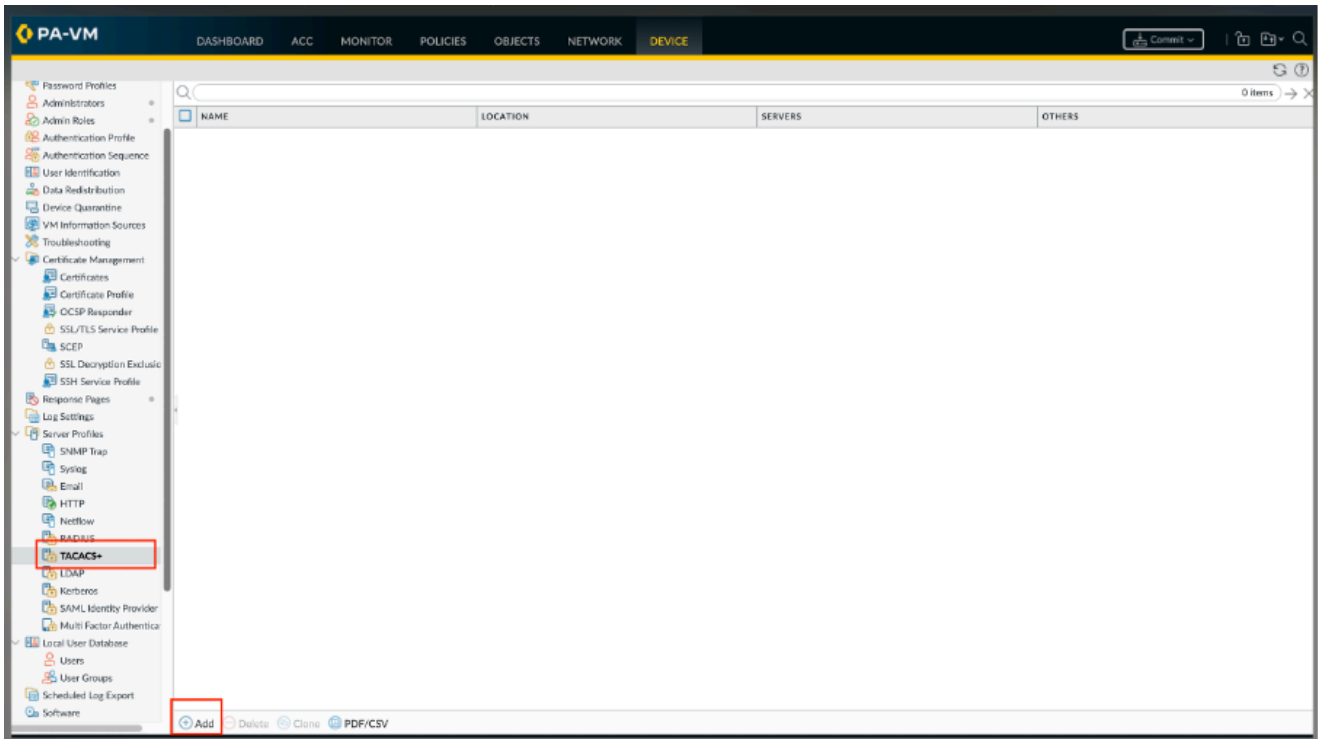
步骤1.添加TACACS+服务器配置文件。

配置文件定义防火墙如何连接到TACACS+服务器。

1. 选择Device > Server Profiles > TACACS+或Panorama > Server Profiles > TACACS+ on Panorama，然后添加配置文件。
2. 输入配置文件名称以标识服务器配置文件。
3. （可选）选择Administrator Use Only以限制管理员访问。
4. 输入身份验证请求超时前的超时间隔（以秒为单位）(默认值为3;范围为1-20)。
5. 选择Authentication Protocol（默认值为CHAP），防火墙使用该协议对TACACS+服务器进行身份验证。

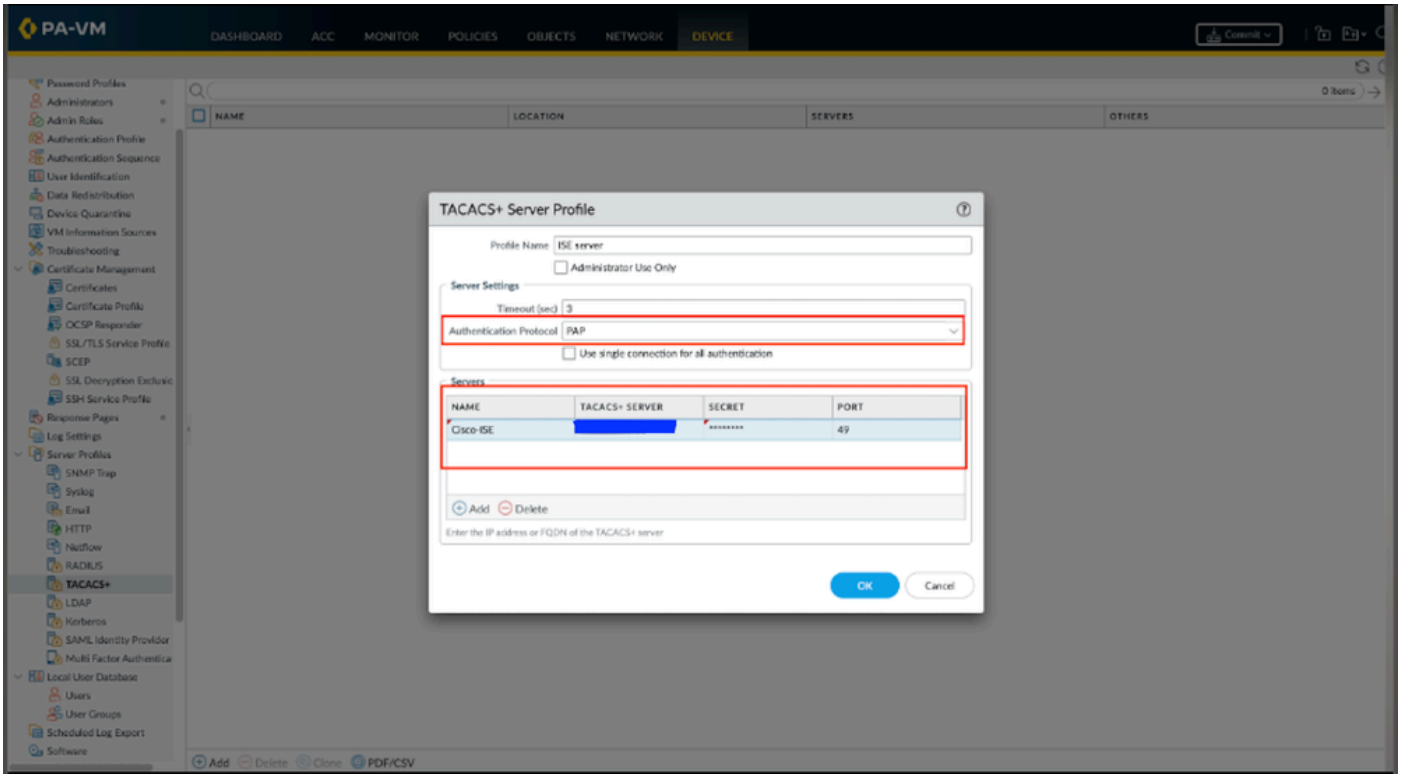
Palo Alto的默认TACACS+身份验证协议是CHAP(CHAP/MD5)。

当ISE根据外部身份库（如Active Directory）对用户进行身份验证时，无法使用CHAP/MD5，因为AD不向ISE提供CHAP验证所需的可逆密码信息。因此，对于AD支持的身份验证，请将Palo Alto TACACS+服务器配置文件配置为使用PAP，而不是CHAP

1. 

2. 添加每个TACACS+服务器并执行以下步骤：
    1. 用于标识服务器的名称。
    2. TACACS+服务器IP地址或FQDN。如果使用FQDN地址对象标识服务器，并且随后更改了该地址，则必须提交更改，以使新服务器地址生效。
    3. 加密用户名和密码的加密和确认密钥。
    4. 用于身份验证请求的服务器端口（默认值为49）。 点击OK以保存服务器配置文件。

7.单击确定以保存服务器配置文件。



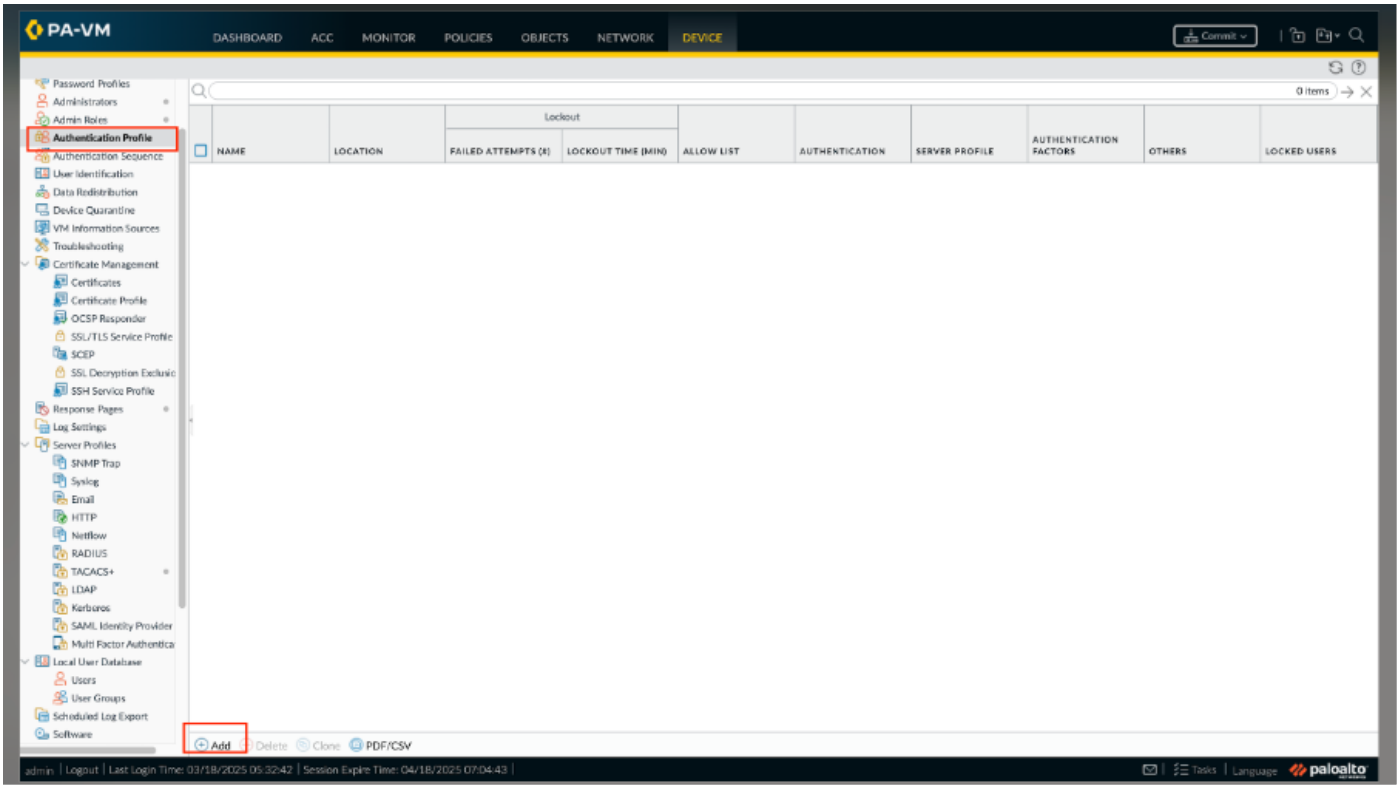
提示：使用Active Directory或其他外部身份库时选择PAP。

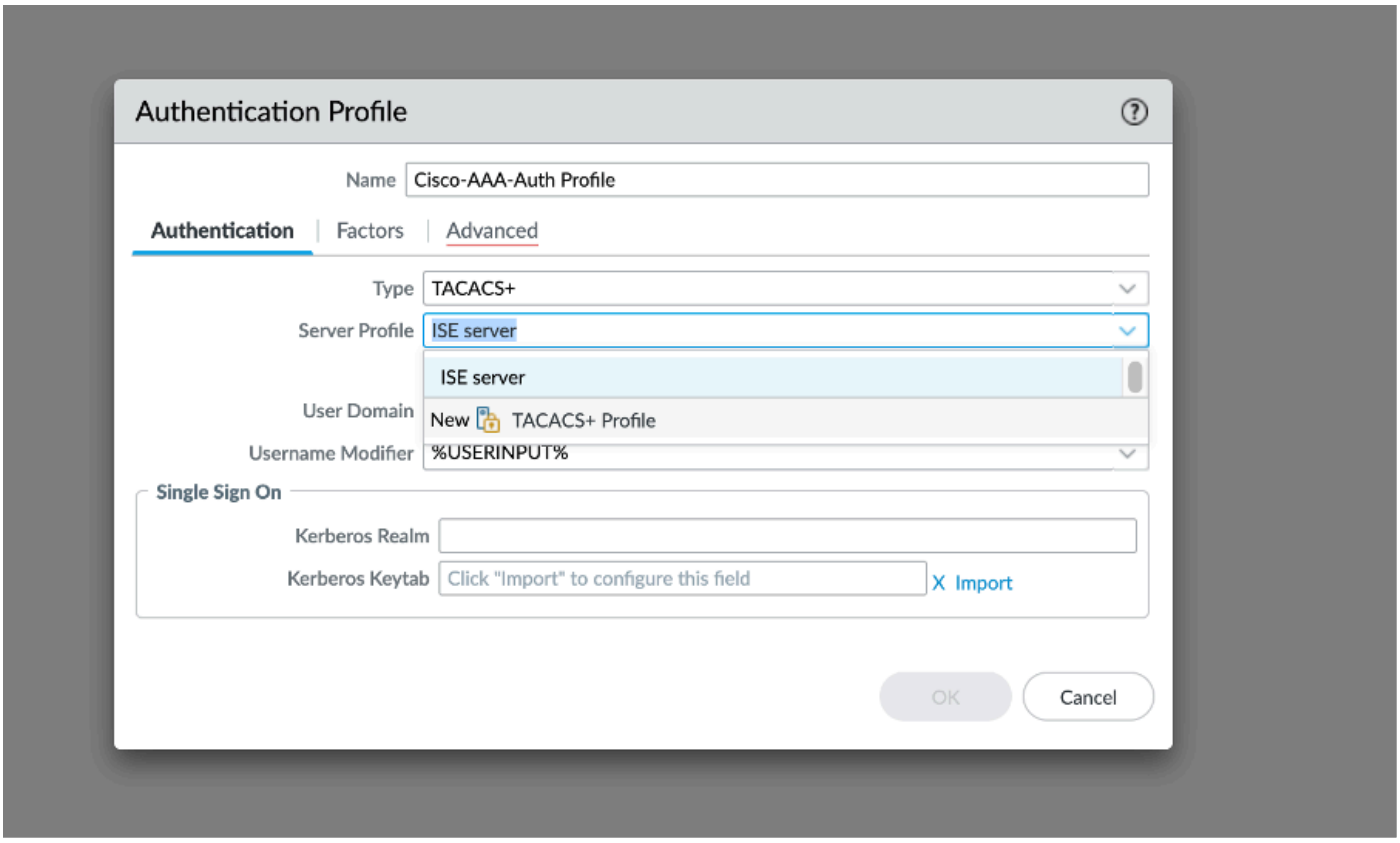
Palo Alto的CHAP选项使用CHAP/MD5。Cisco ISE无法针对Active Directory验证CHAP/MD5凭证，因为AD不公开所需的密码材料。将PAP用于支持AD的TACACS+管理员身份验证。只有在所选ISE身份源支持时（例如，适当配置的内部用户），才能使用CHAP。

步骤2.将TACACS+服务器配置文件分配到身份验证配置文件。

身份验证配置文件定义一组用户通用的身份验证设置。

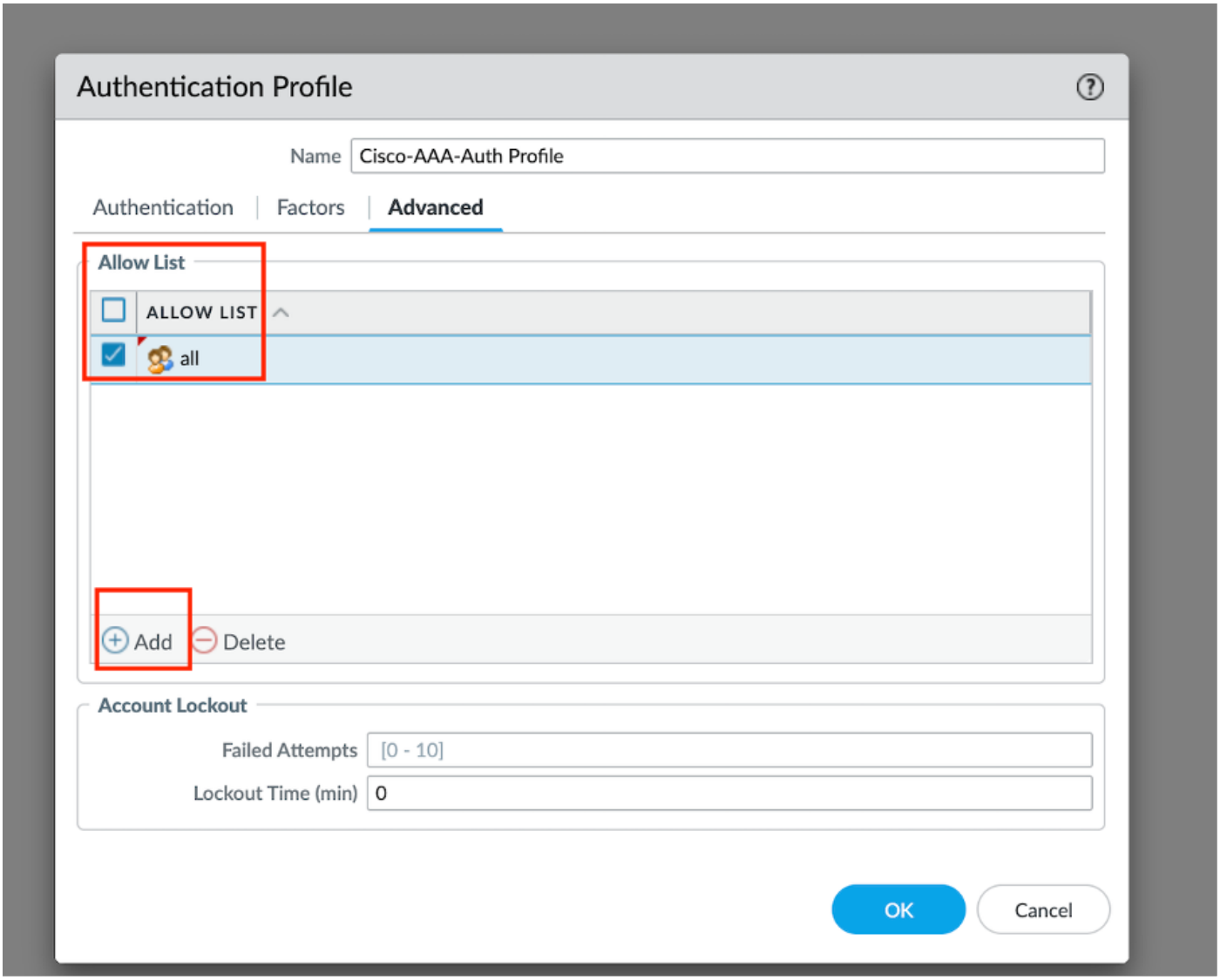
1. 选择Device > Authentication Profile和Add配置文件。
    1. 输入名称以标识配置文件
    2. 将Type（类型）设置为TACACS+。
    3. 选择您配置的服务器配置文件。
    4. 选择Retrieve user group from TACACS+，以从TACACS+服务器上定义的VSA收集用户组信息。





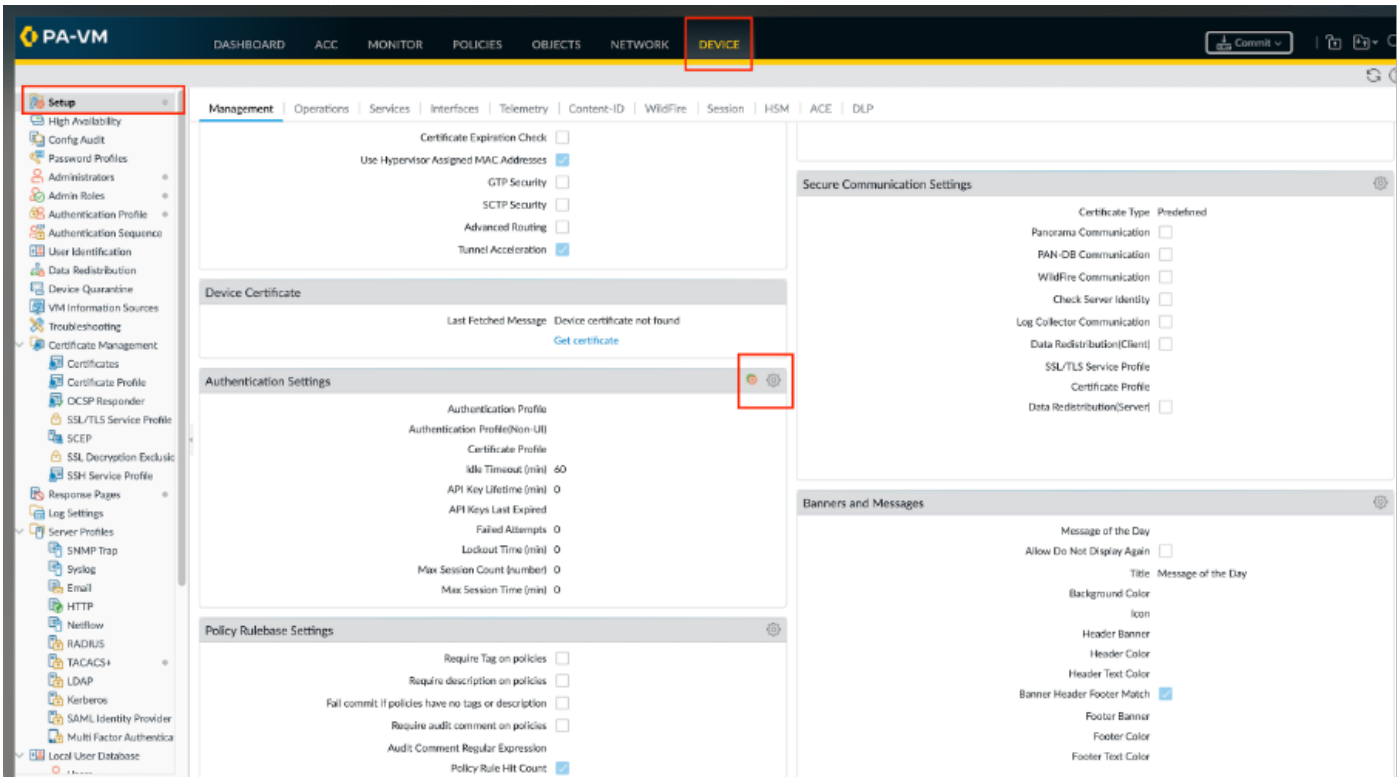
防火墙使用您在身份验证配置文件的Allow List中指定的组匹配组信息。

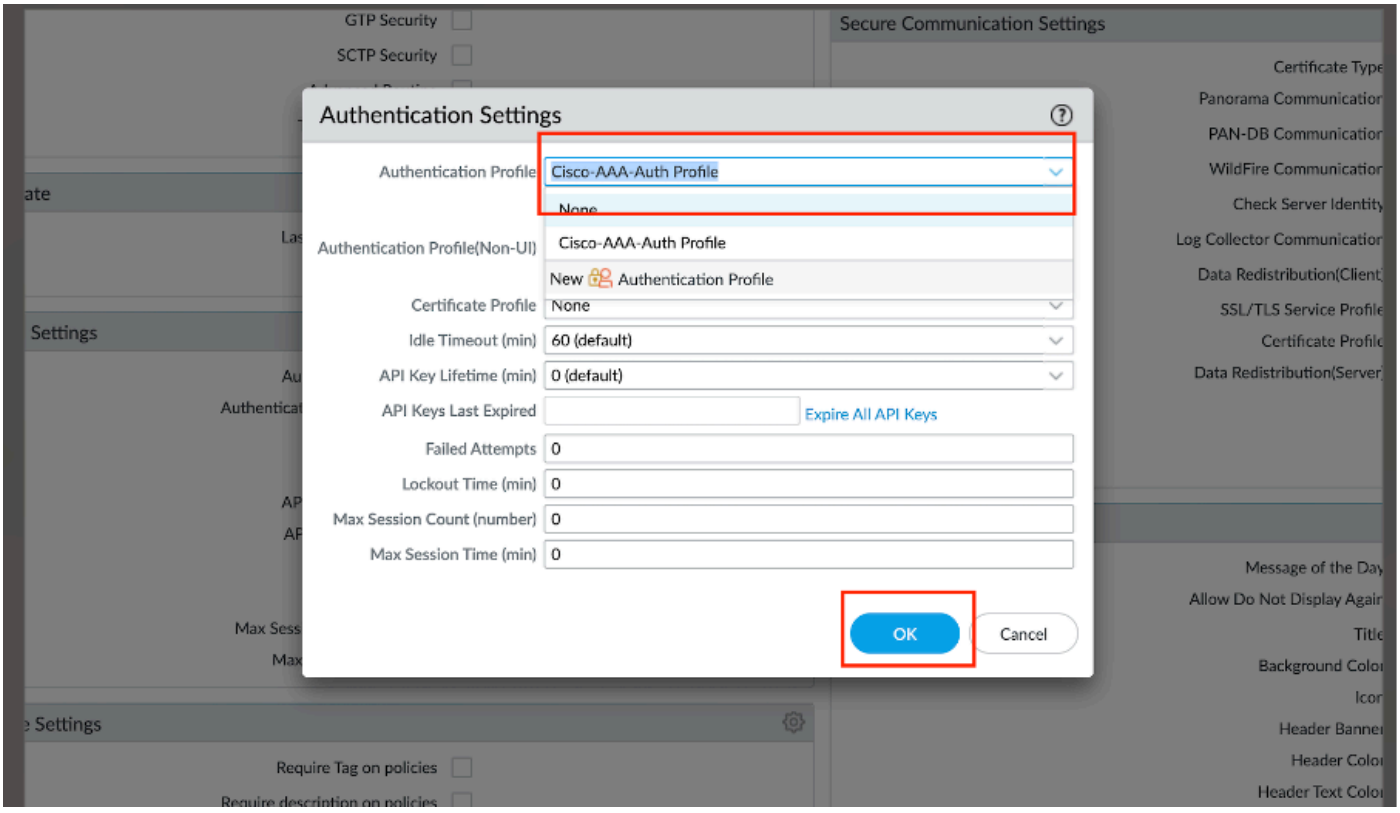
1. 选择Advanced，并在Allow List中Add可使用此身份验证配置文件进行身份验证的用户和组。
2. 单击OK保存身份验证配置文件。



步骤3.配置防火墙，使其使用面向所有管理员的身份验证配置文件。

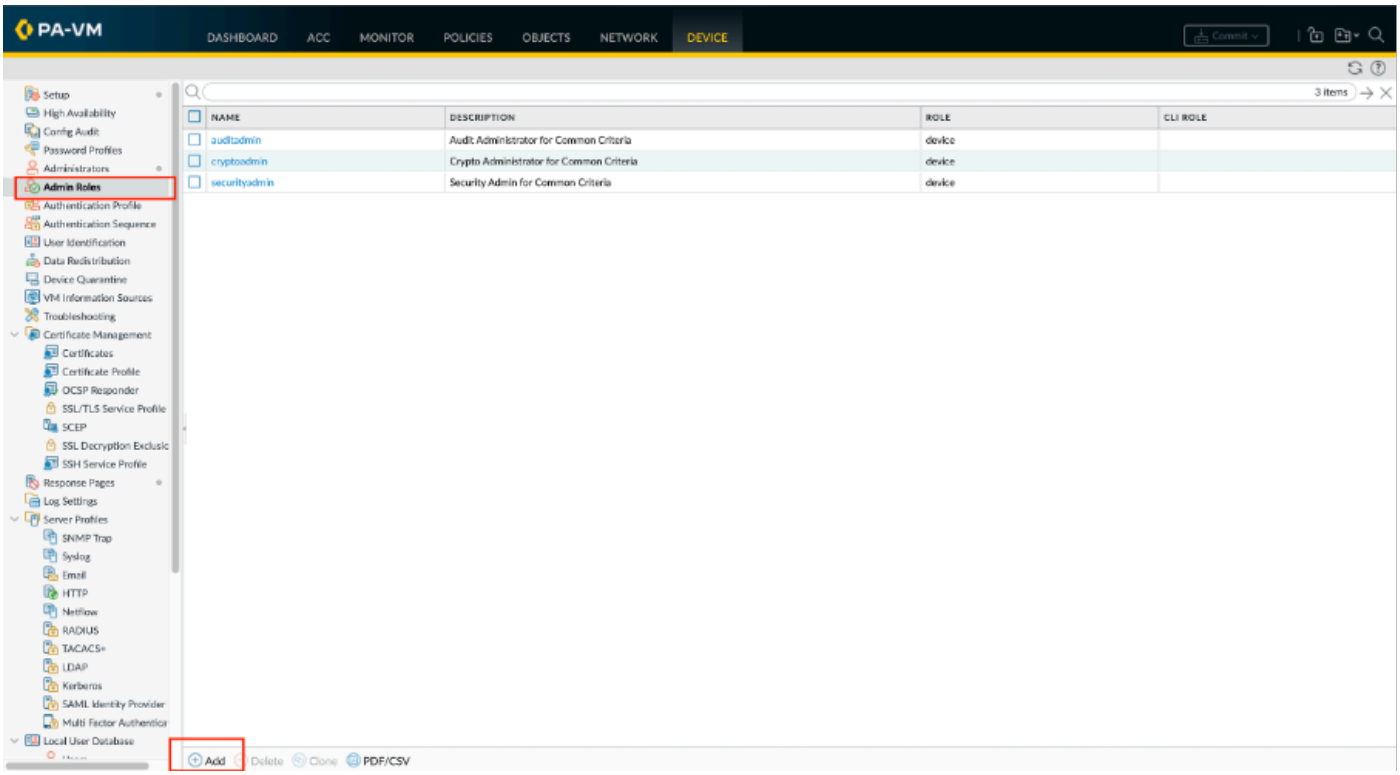
1. 选择Device > Setup > Management并编辑Authentication Settings。
2. 选择已配置的身份验证配置文件，然后点击OK。



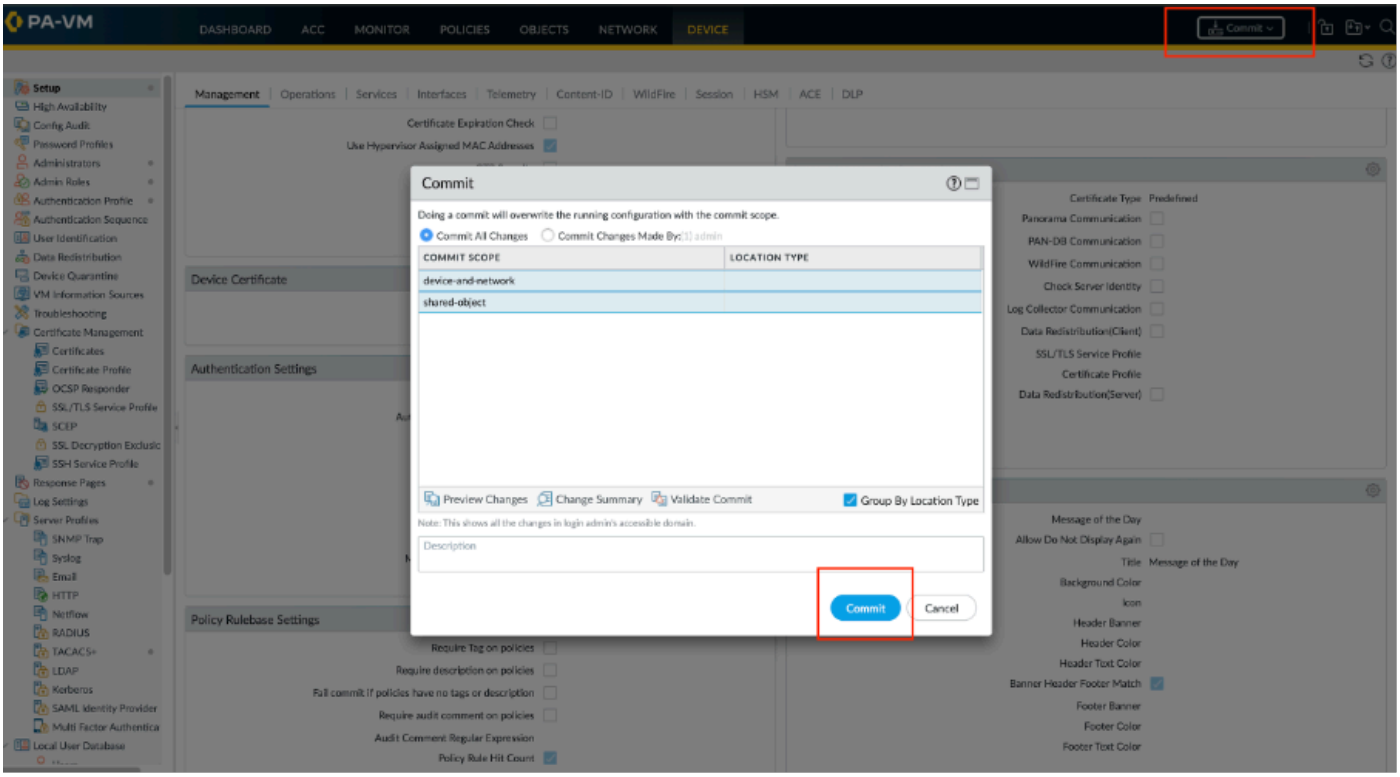


步骤4.配置管理员角色配置文件。

选择Device > Admin Roles，然后单击Add。输入Name以标识角色。



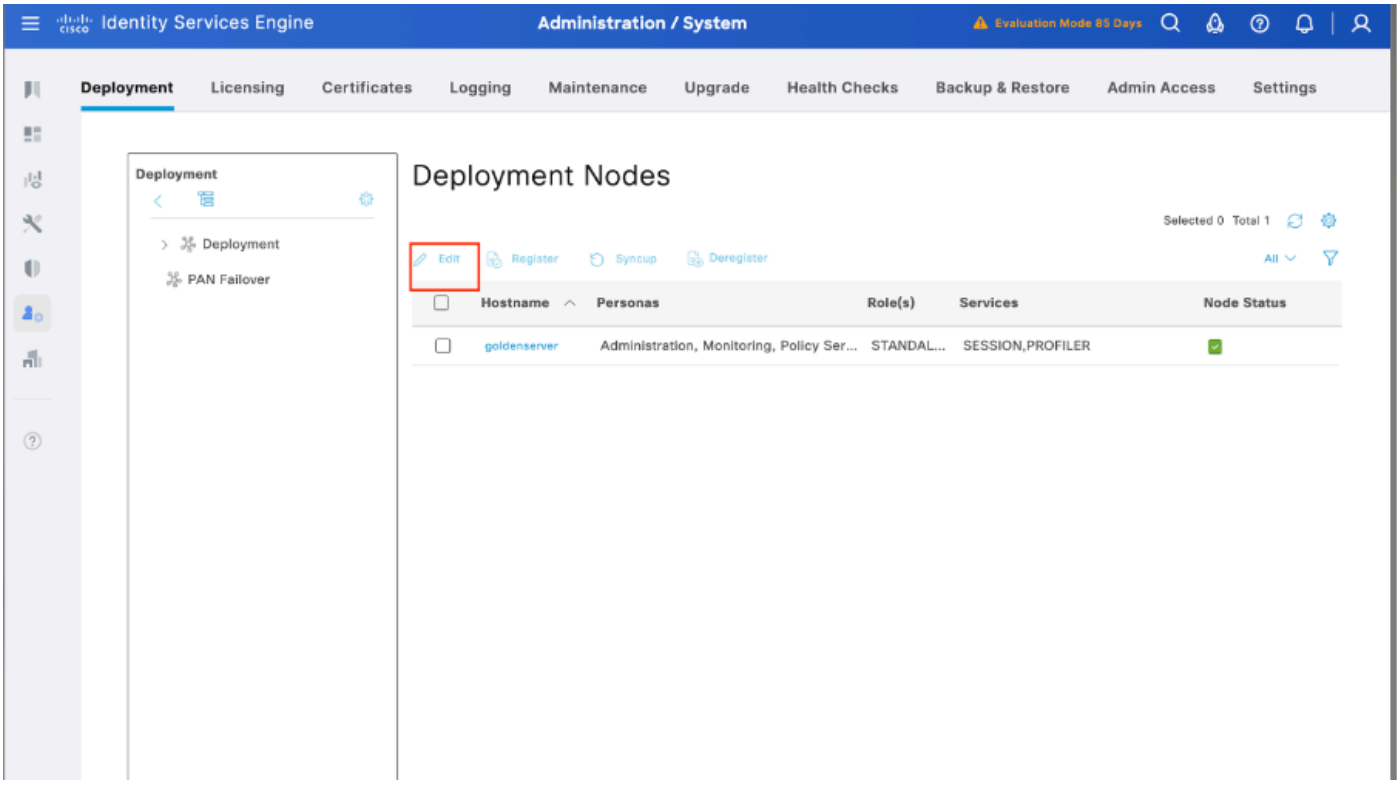
步骤5.提交更改以在防火墙上激活它们。



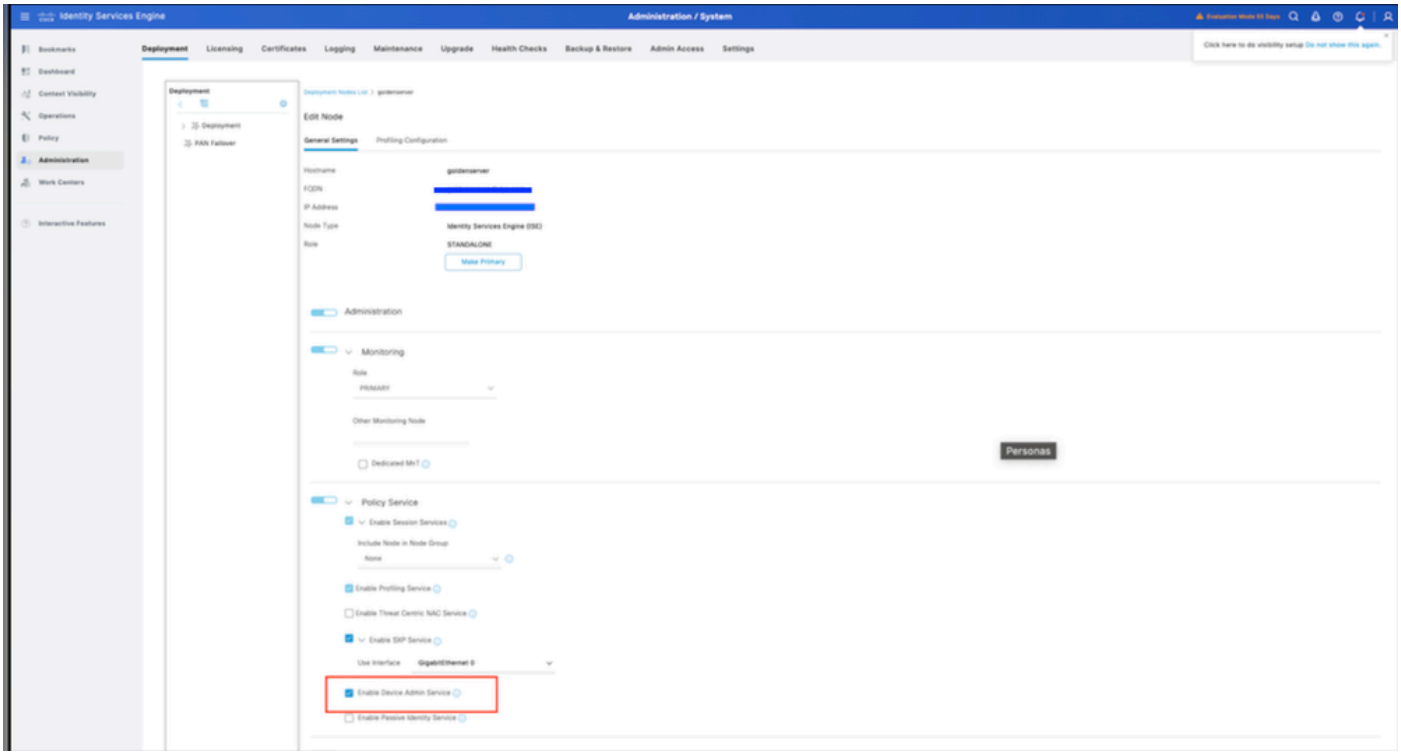
第2部分：ISE上的TACACS+配置

步骤1.初始步骤是验证思科ISE是否具有处理TACACS+身份验证的必要功能。为此，请确认所需的

策略服务节点(PSN)已启用设备管理服务功能。导航到Administration > System > Deployment，选择ISE处理TACACS+身份验证的相应节点，然后点击Edit以查看其配置。

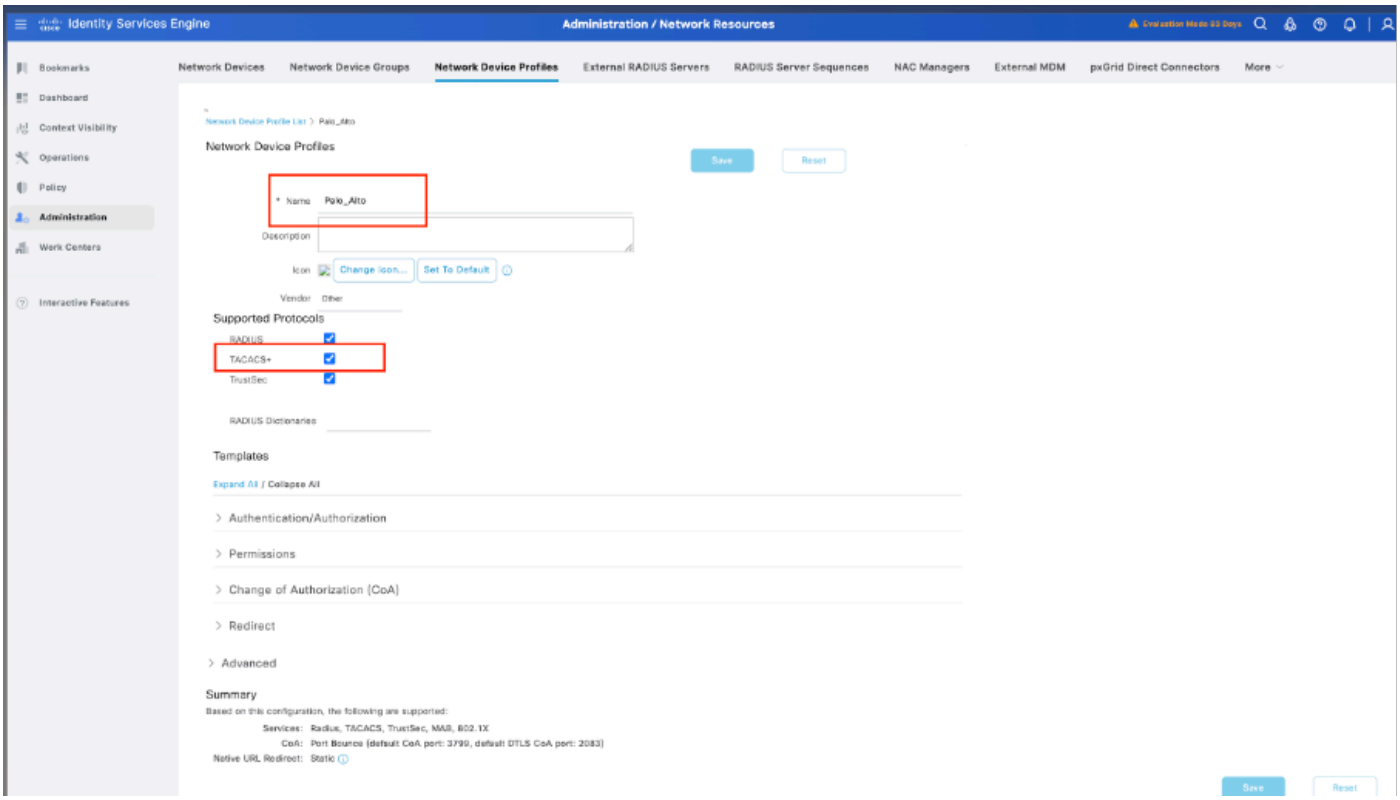


步骤2.向下滚动以查找Device Administration Service功能。请注意，启用此功能需要策略服务角色在节点上处于活动状态，并且部署中需要可用的TACACS+许可证。选中此复选框可启用该功能，然后保存配置。



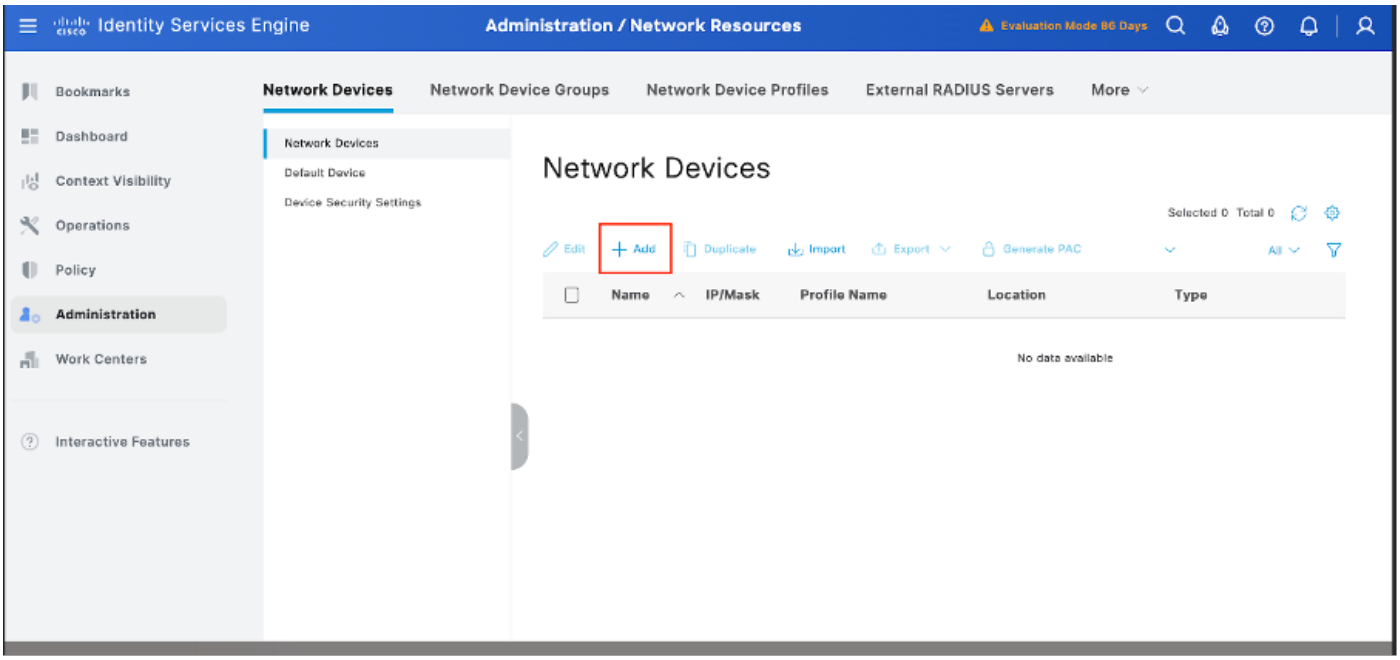
步骤3.为Cisco ISE配置Palo Alto网络设备配置文件。

导航到Administration > Network Resources > Network device profile。单击Add并提及名称(Palo Alto)，然后在支持的协议下启用TACACS+。



步骤4.添加Palo Alto作为网络设备。

1. 导航到管理>网络资源>网络设备> +添加。



2.单击Add并输入以下详细信息：

名称：帕洛阿尔托

IP Address:<Palo-Alto IP>

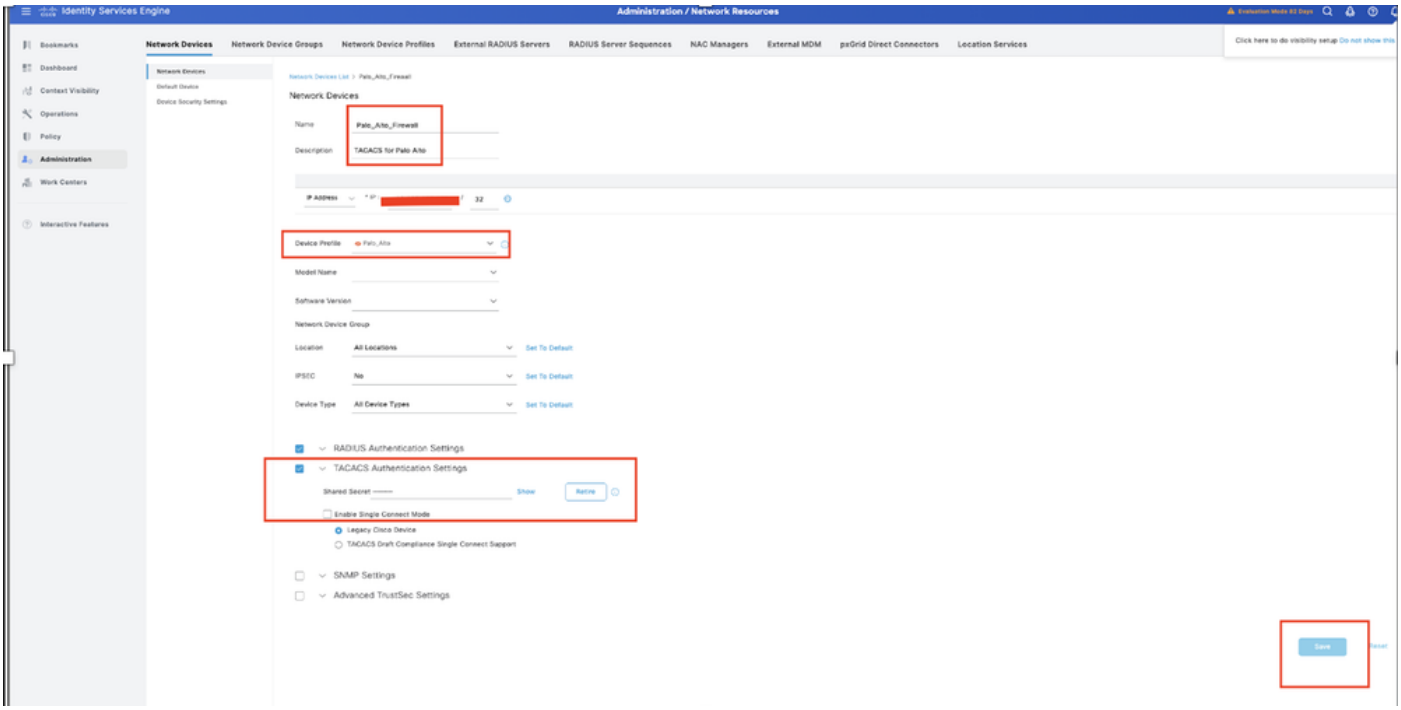
网络设备配置文件：选择Palo Alto

TACACS身份验证设置：

启用TACACS+身份验证

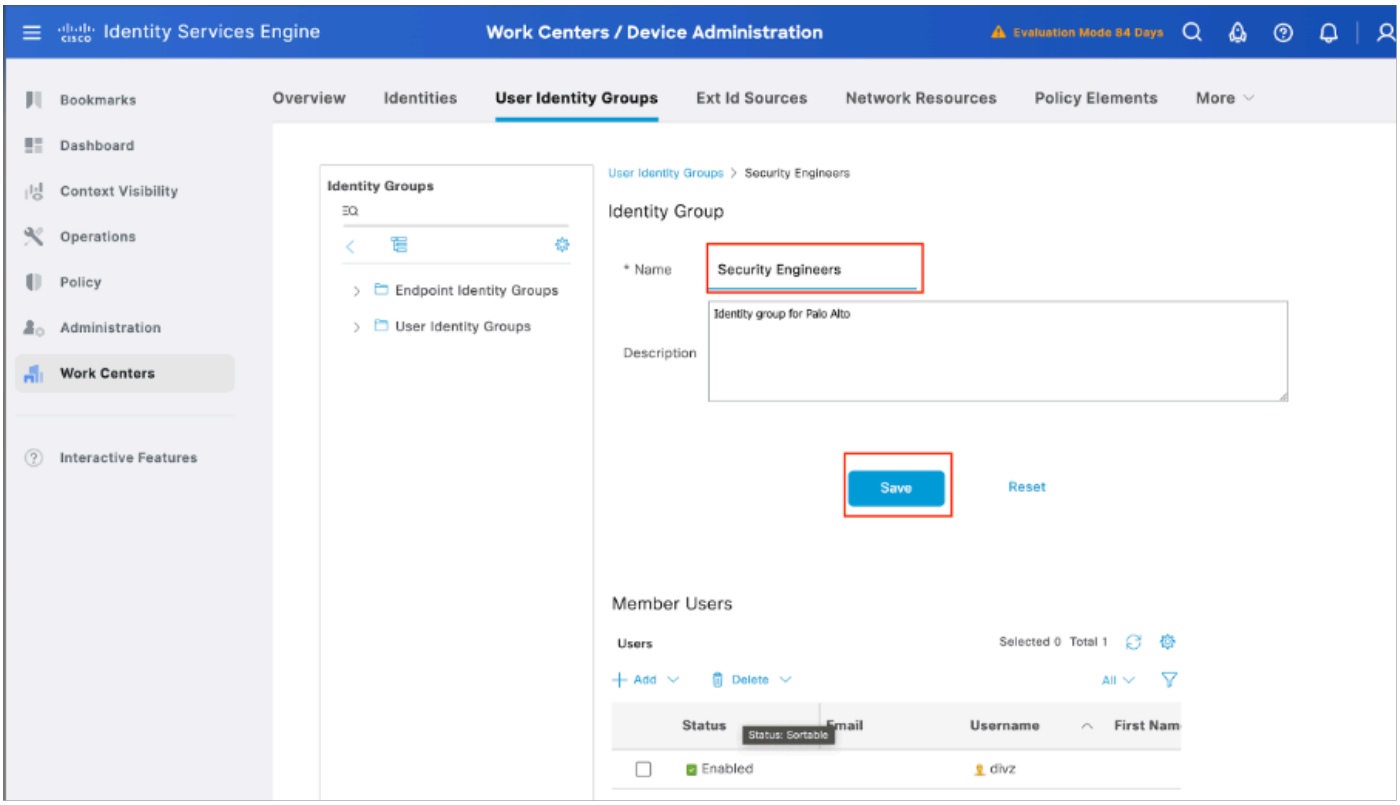
输入共享密钥（必须与Palo Alto配置匹配）

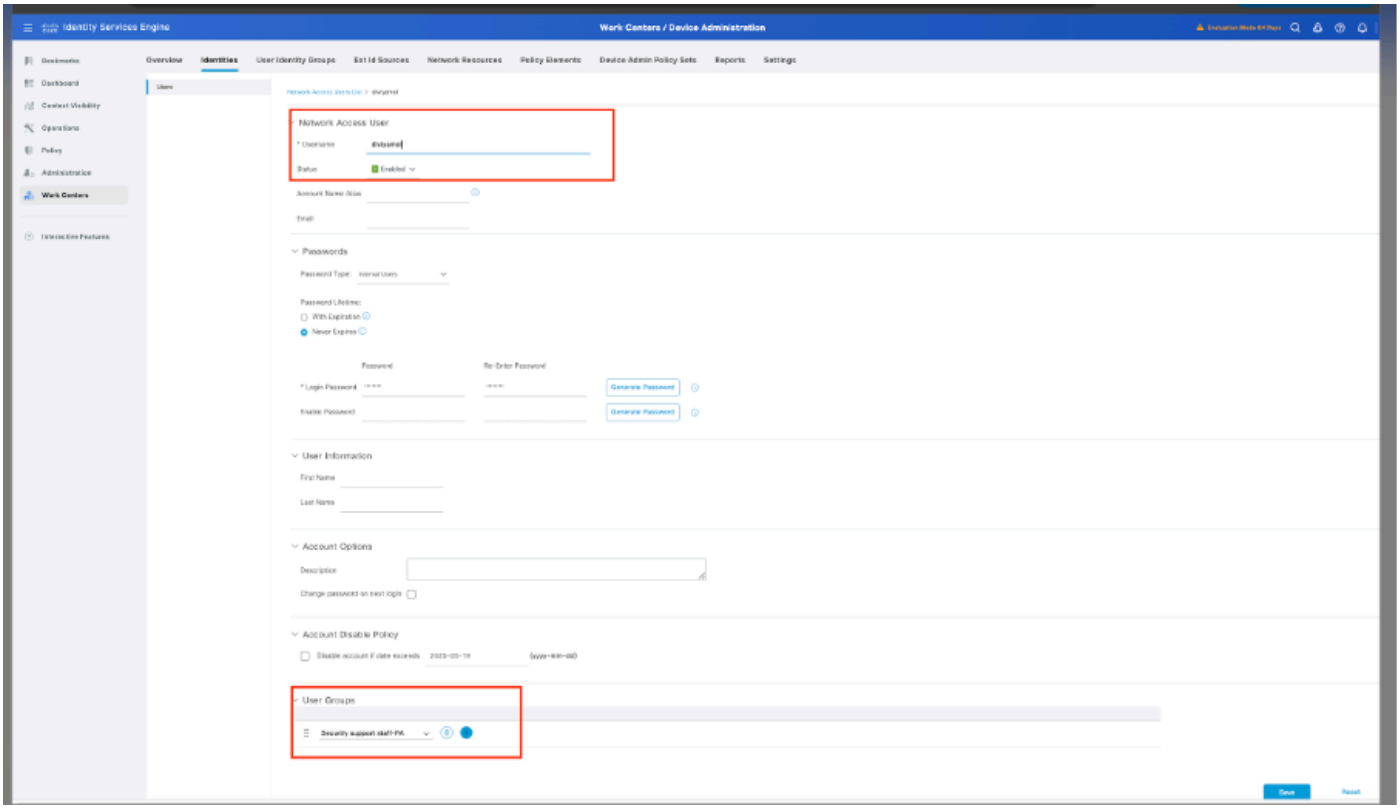
Click Save.

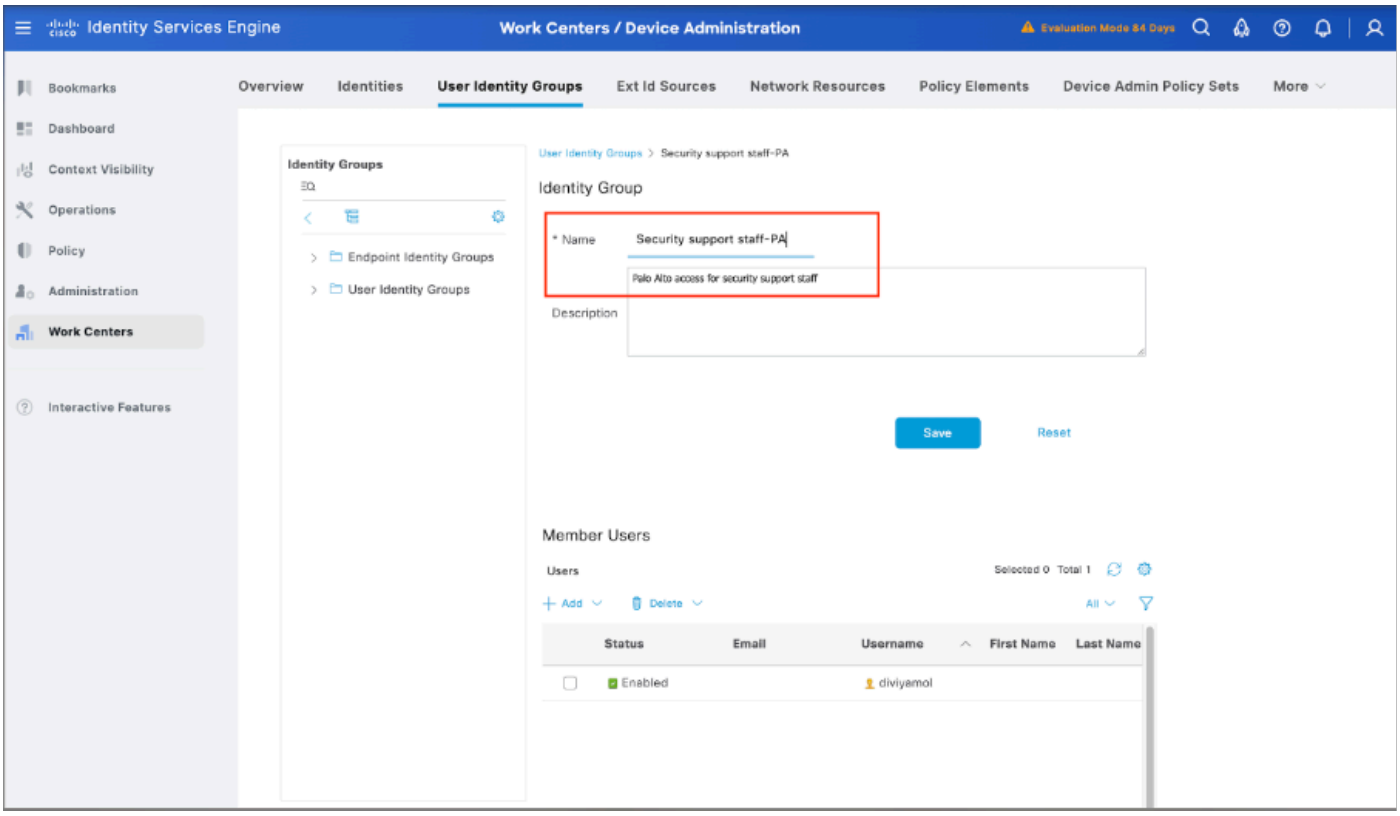


步骤5.创建用户身份组。

导航到工作中心(Work Centers)>设备管理(Device Administration)>用户身份组(User Identity Groups)，然后点击添加，然后指定用户组的名称。


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

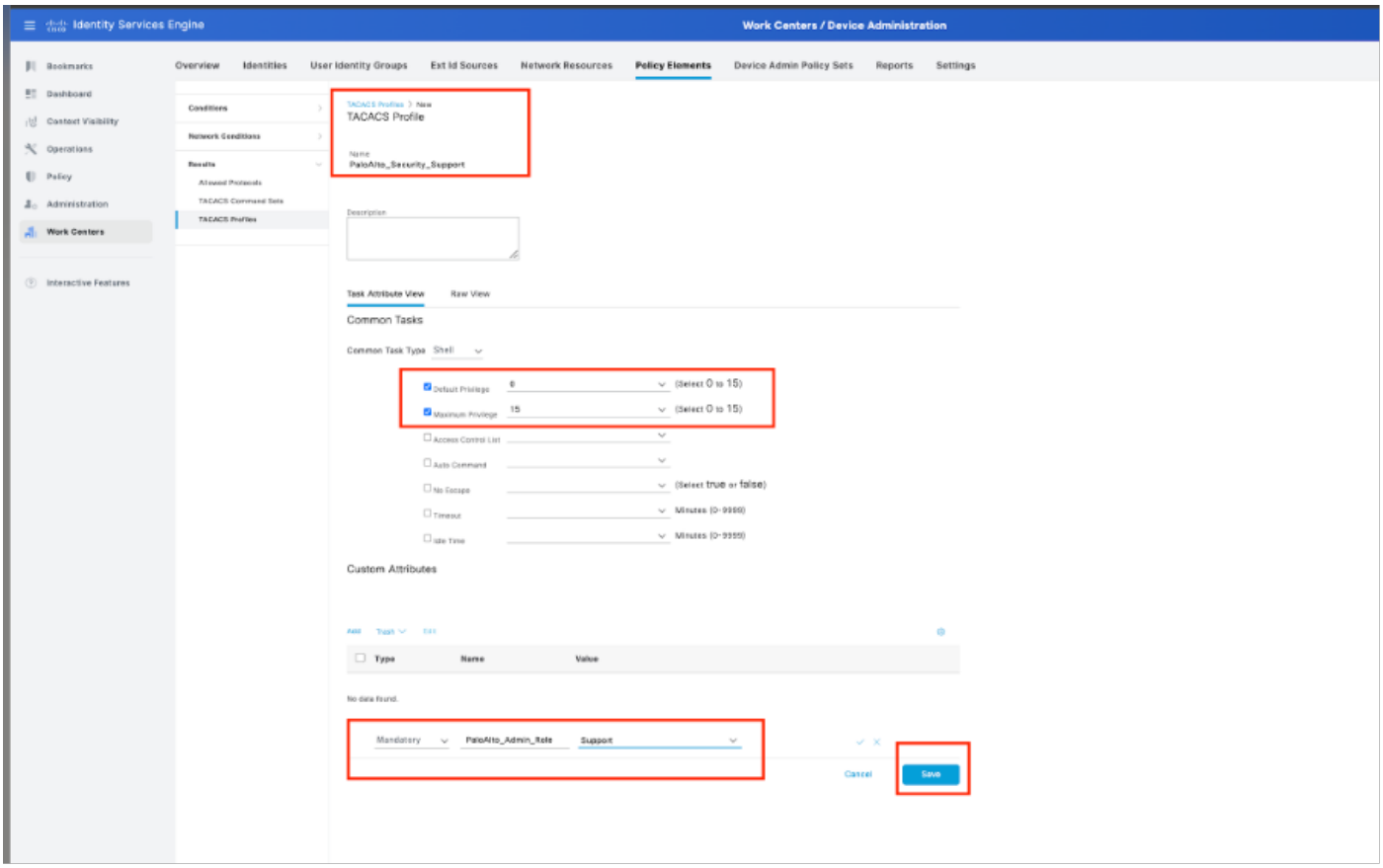


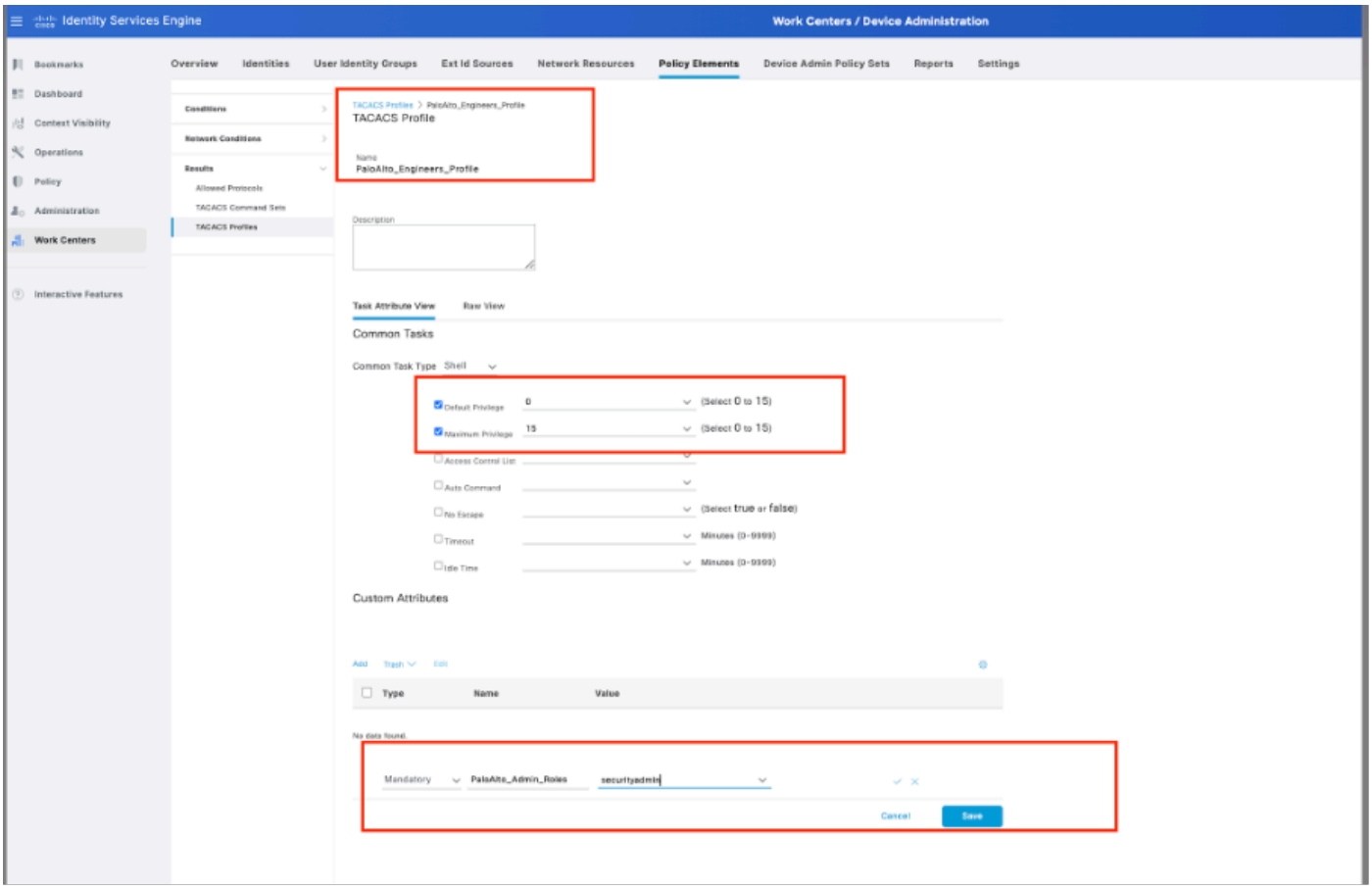


步骤6.配置TACACS配置文件。

下一步是配置TACACS配置文件，您可以在其中配置权限级别和超时设置等设置。导航至工作中心(Work Centers)>设备管理(Device Administration)->策略元素(Policy Elements)->结果(Results)->TACACS配置文件(TACACS Profiles)。

单击Add以创建新的TACACS配置文件。为配置文件命名。



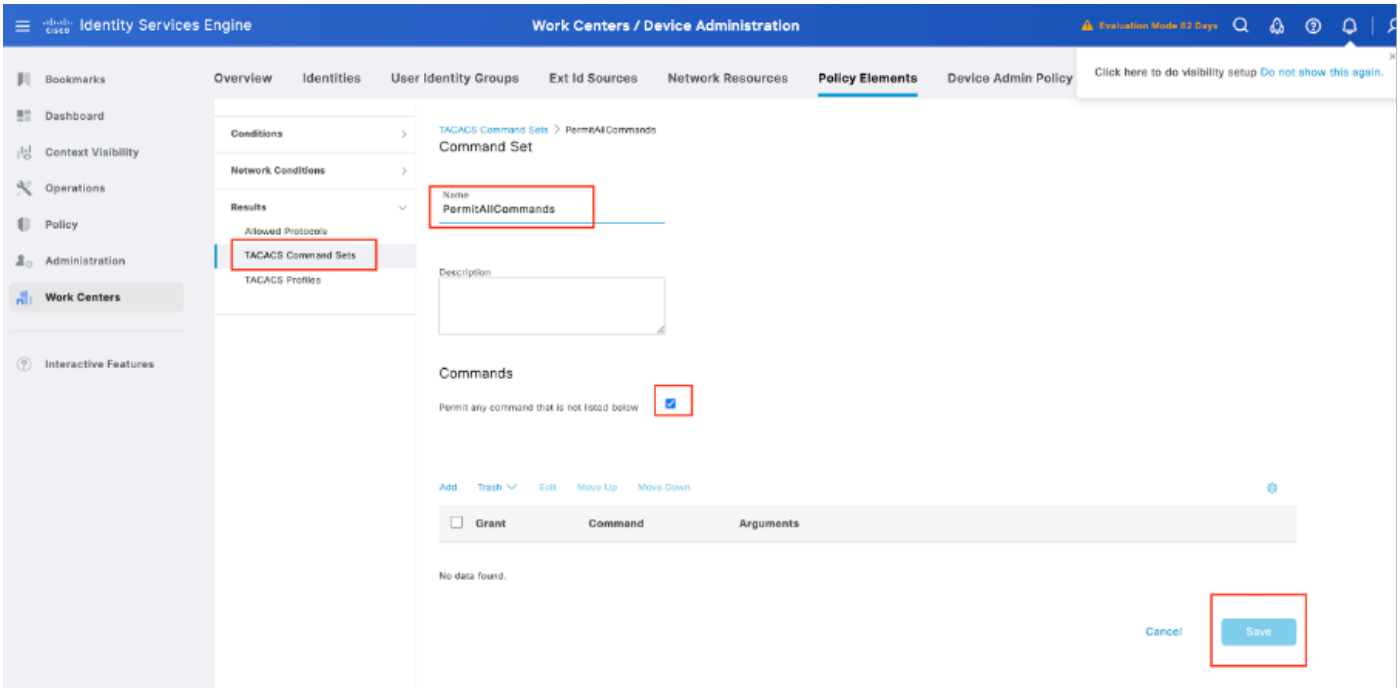


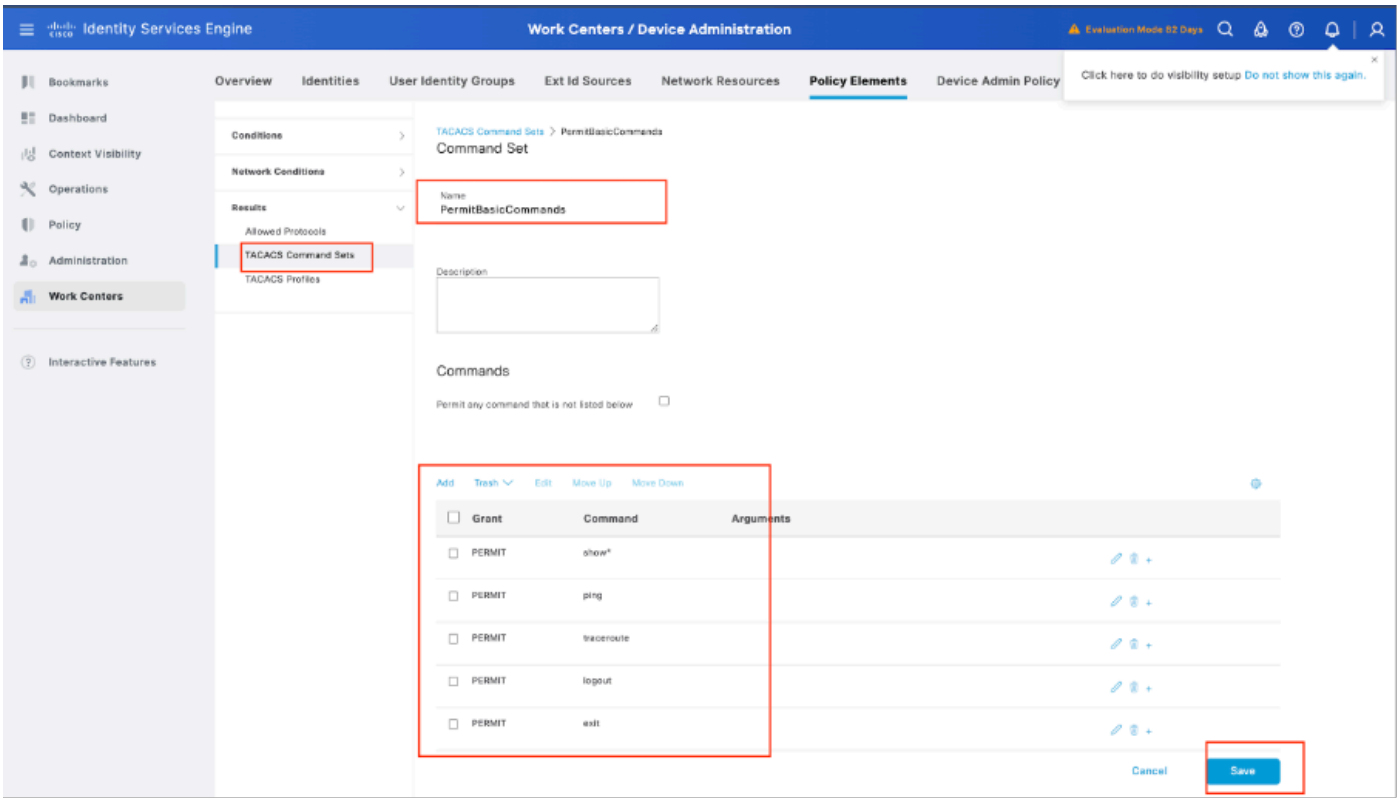
步骤6.配置TACACS命令集。

现在，是时候配置允许用户使用哪些命令了。由于您可以授予这两个使用案例权限级别15（用于访问每个可用的命令），因此请使用TACACS命令集来限制可以使用哪些命令。

导航到工作中心(Work Centers)>设备管理(Device Administration)>策略元素(Policy Elements)>结果(Results)-> TACACS命令集(TACACS Command Sets)。单击Add以创建新的TACACS命令集并将其命名为PermitAllCommands。将此TACACS命令集应用于安全支持。

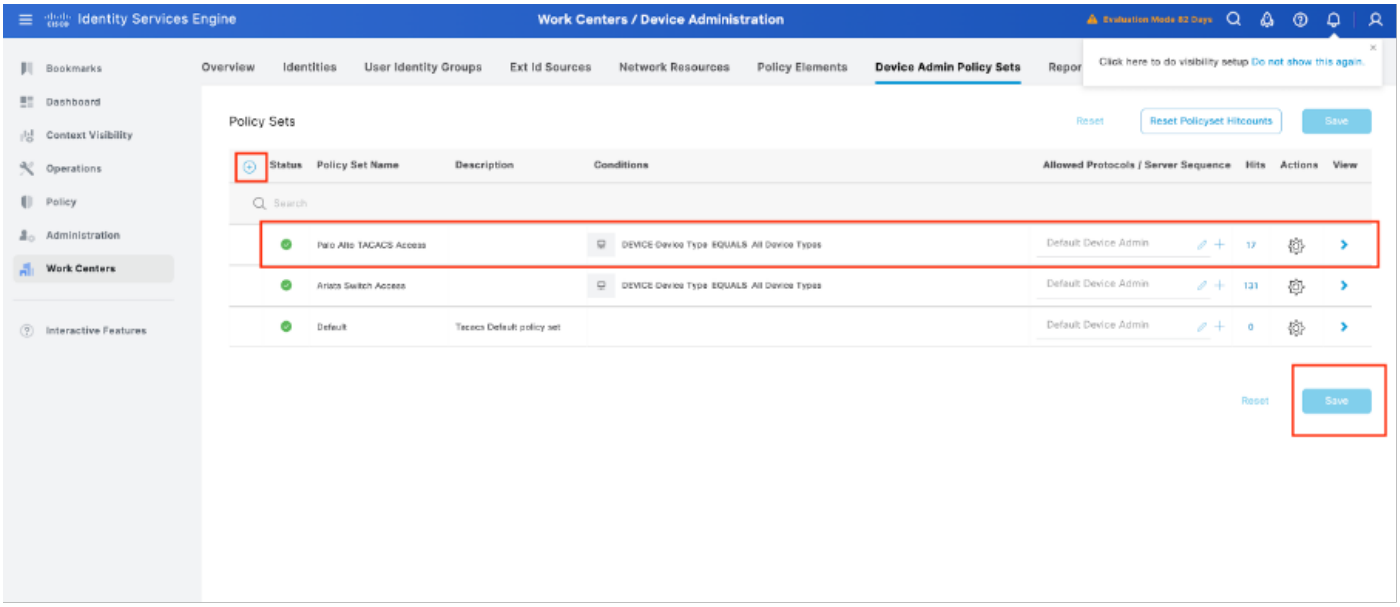
在此TACACS命令集中唯一需要配置的是选中Permit any command that is not listed below复选框。



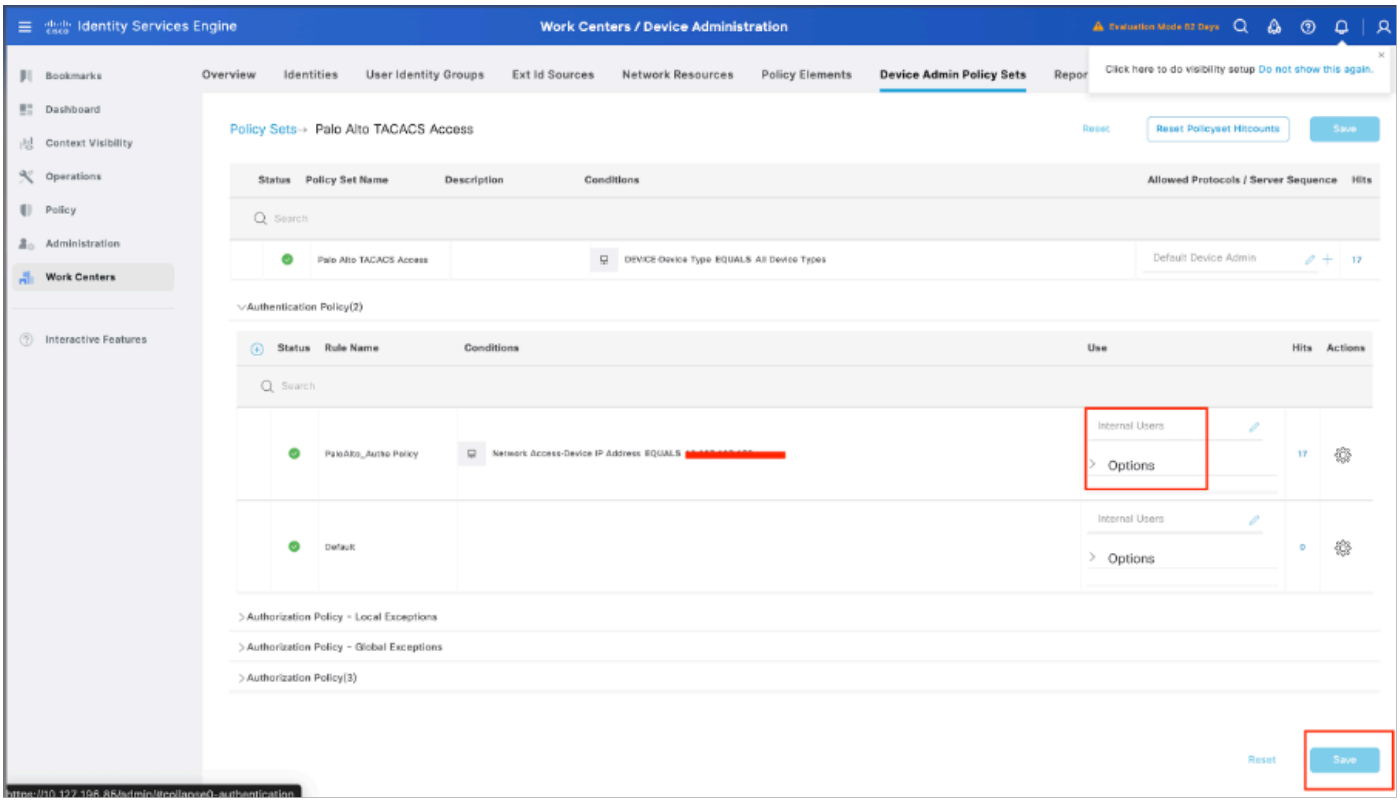


第7步：创建用于Palo Alto的设备管理策略集，导航菜单Work Centers > Device Administration > Device Admin Policy Sets，点击Add +图标。

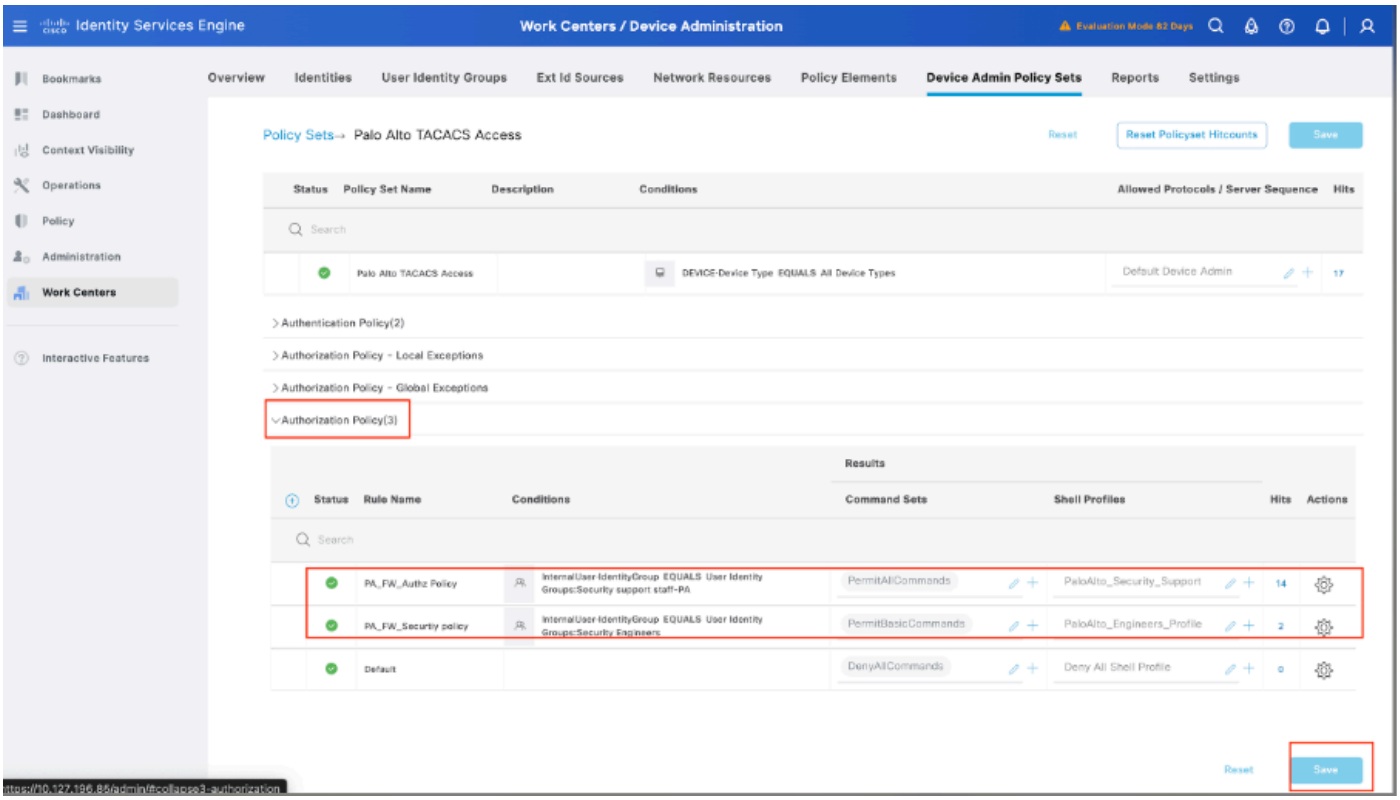
第8步：命名此新策略集，根据从Palo Alto防火墙进行中的TACACS+身份验证的特征添加条件，并选择为Allowed Protocols > Default Device Admin。保存配置。



第9步：在>视图选项中选择，然后在Authentication Policy部分，选择思科ISE用于在Palo Alto防火墙上查询身份验证的用户名和凭据的外部身份源。在本示例中，凭证对应于ISE中存储的内部用户。



步骤10.向下滚动至名为Authorization Policy的部分直到Default策略，选择齿轮图标，然后在上面插入一个规则。



第11步：命名新的授权规则，添加有关已通过身份验证的用户已作为组成员身份的条件，并在“外壳配置文件”部分添加您之前配置的TACACS配置文件，保存配置。

验证

ISE审核

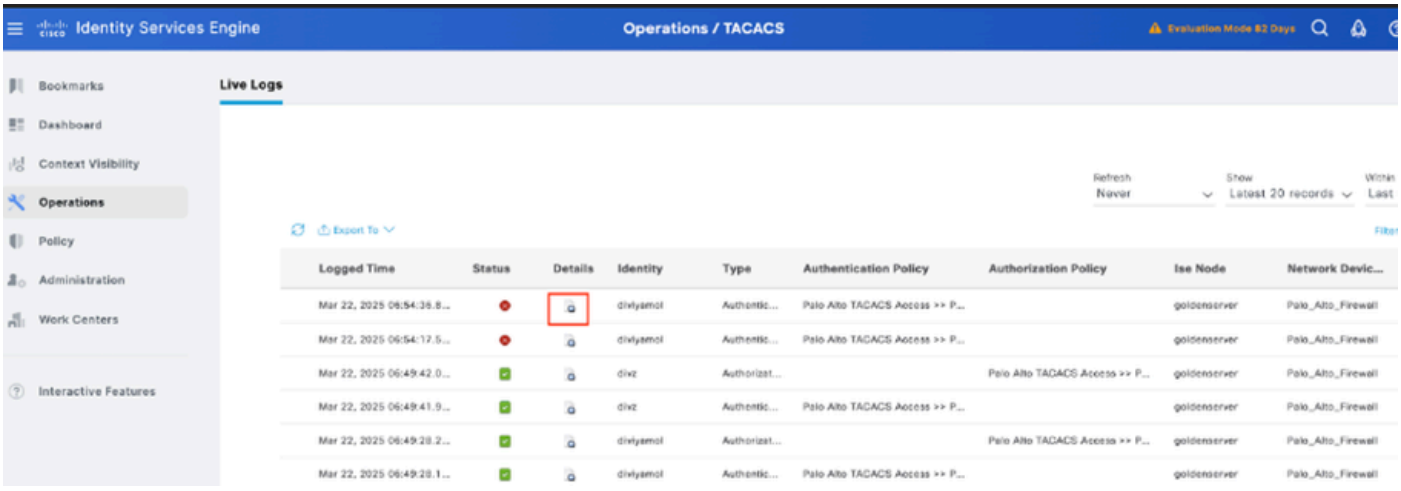
步骤1.检查TACACS+可维护性是否正在运行，可以将其检入：

- GUI:查看是否在Administration -> System -> Deployment中列出了DEVICE ADMIN服务节点。
- CLI：运行命令show ports | include 49以确认TCP端口中存在属于TACACS+的连接

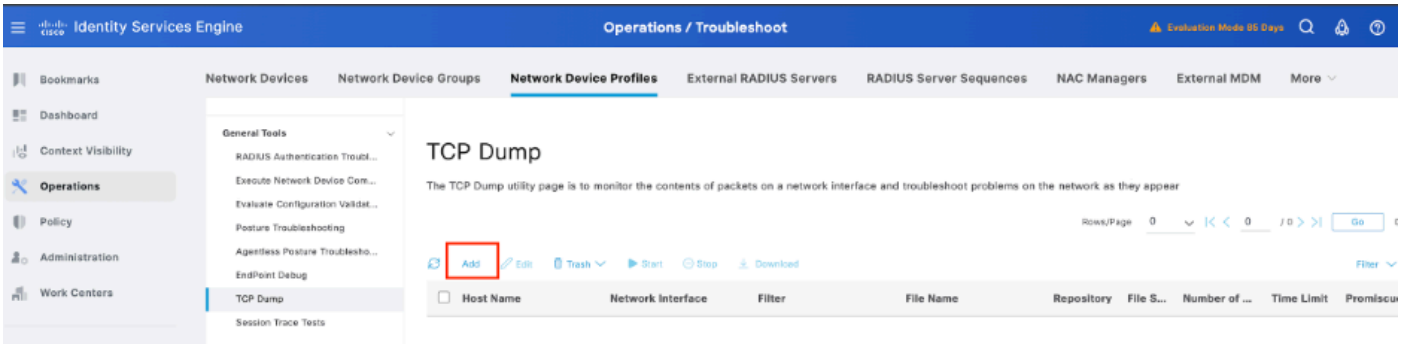
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

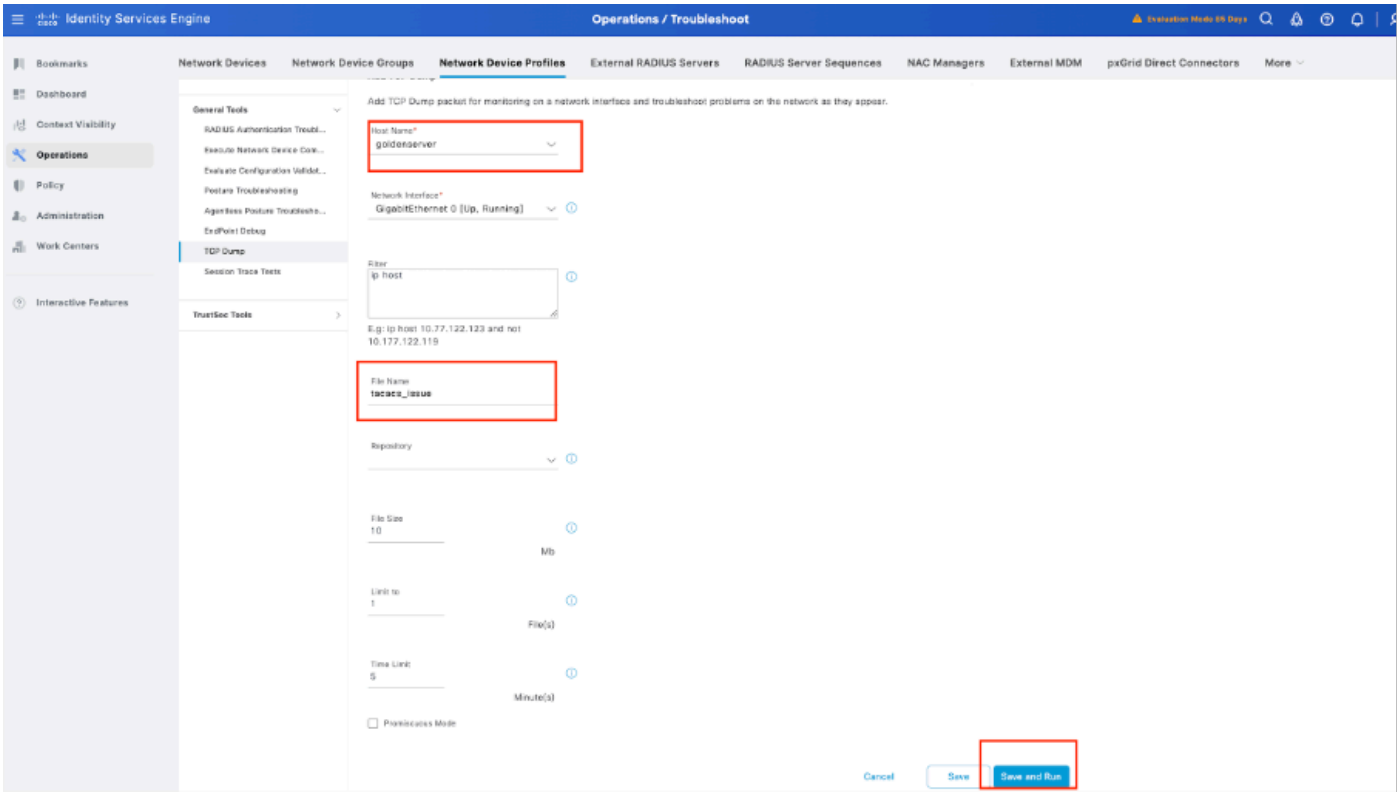
步骤2.确认是否存在有关TACACS+身份验证尝试的实时日志：可以在Operations -> TACACS -> Live logs菜单中选中此项。

根据故障原因，您可以调整配置或解决故障原因。

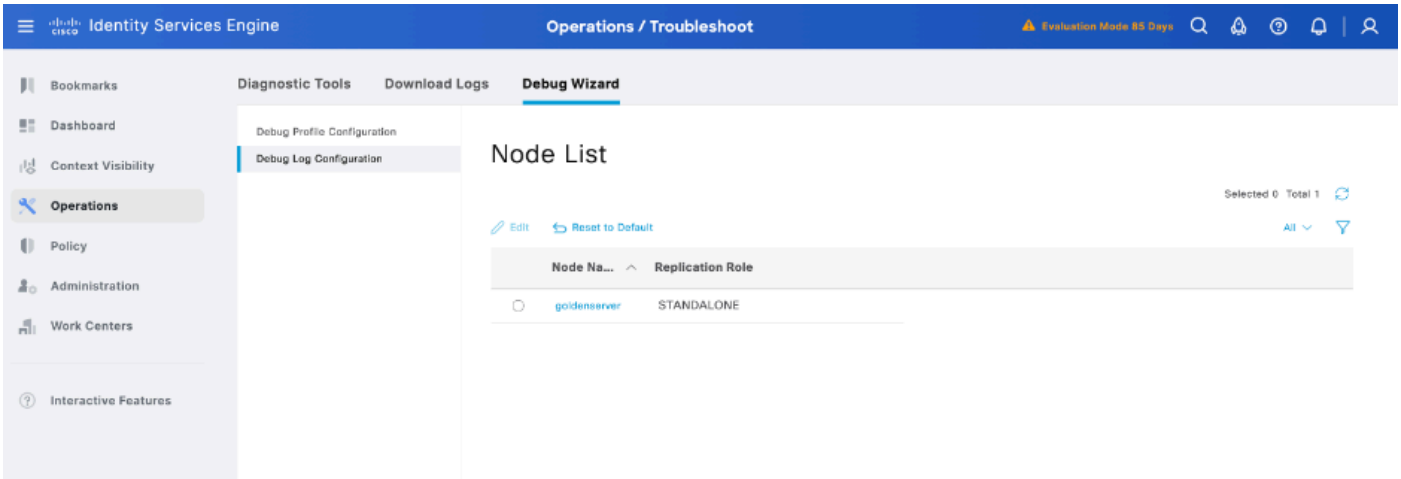


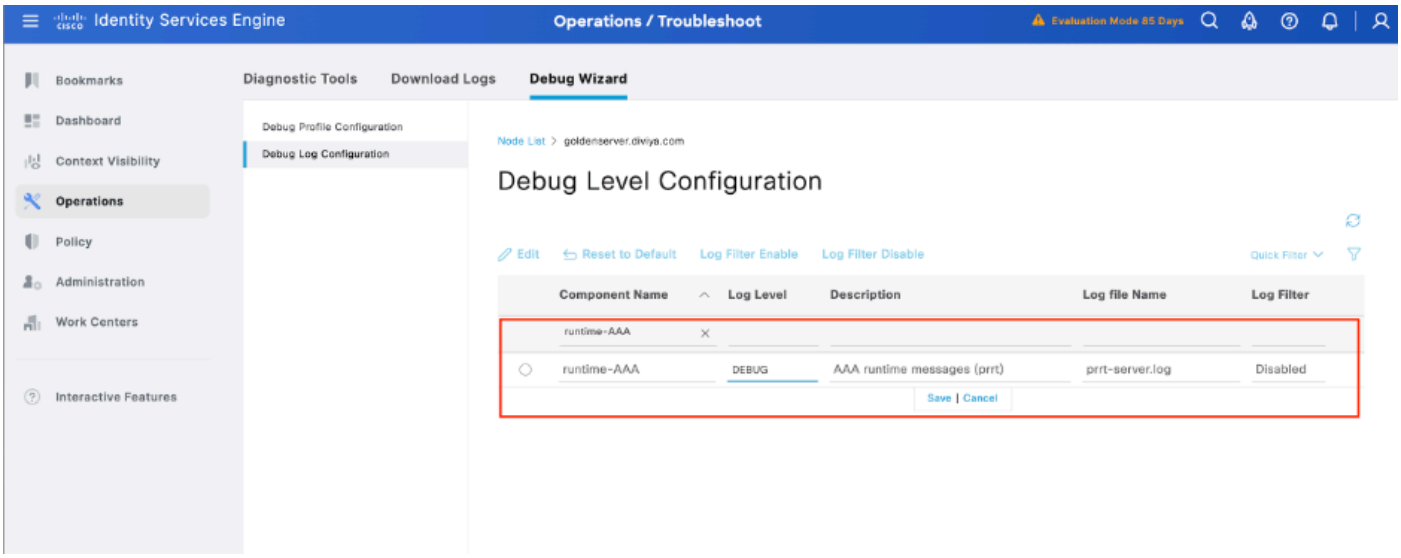
步骤3.如果没有看到任何实时日志，继续捕获数据包，导航到菜单Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump，选择Add。





步骤4.在操作>故障排除>调试向导>调试日志配置中执行身份验证的PSN内的debug中启用组件runtime-AAA，选择PSN节点，然后在“编辑”按钮中选择“下一步”。





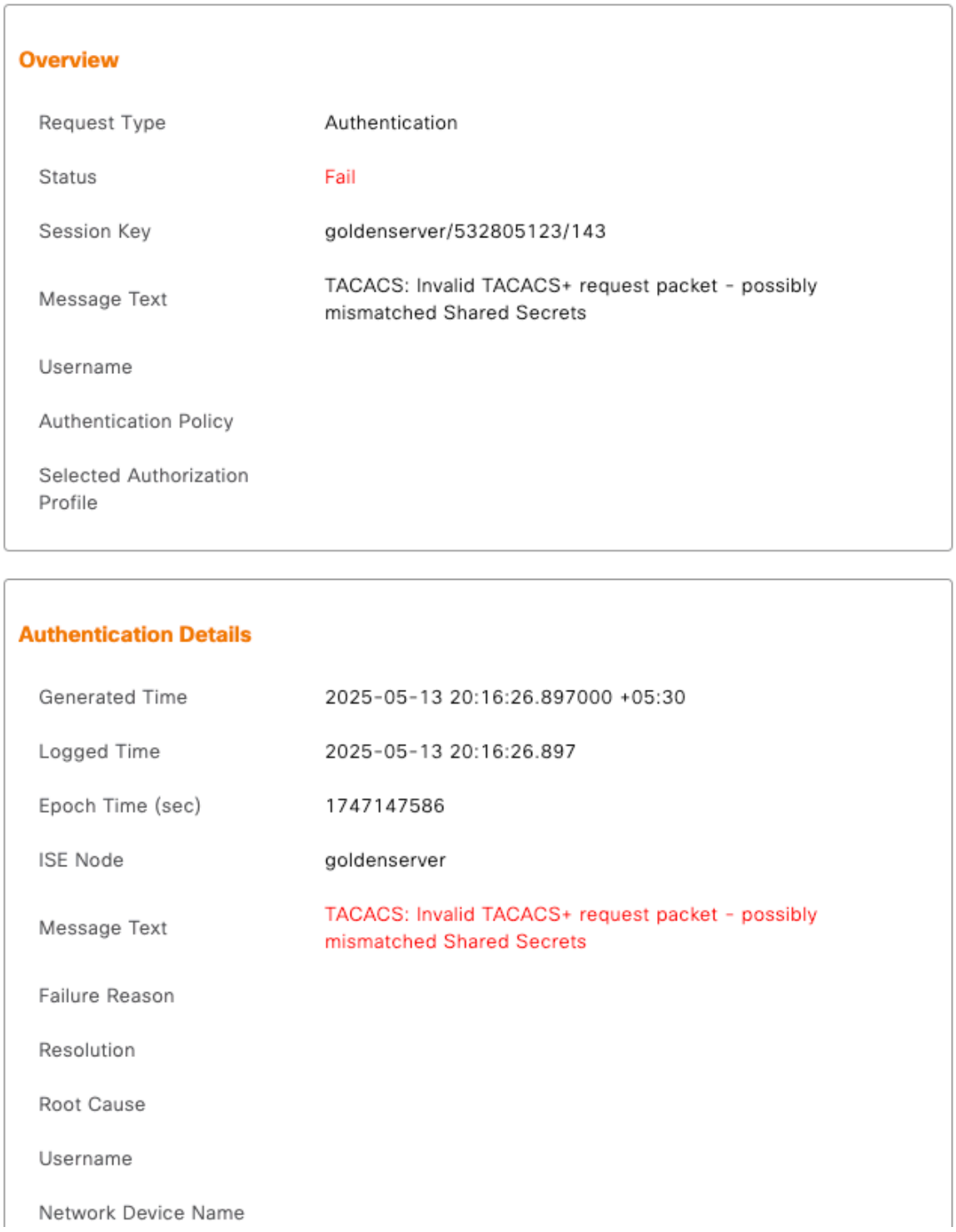
确定运行时AAA组件，将其日志记录级别设置为debug，重现问题，并分析日志以进一步进行调查。

故障排除

1个TACACS:无效的TACACS+请求数据包 — 可能共享密钥不匹配

问题

思科ISE和Palo Alto防火墙（或任何网络设备）之间的TACACS+身份验证失败，并显示以下错误消息：
"无效的TACACS+请求数据包 — 可能共享密钥不匹配"



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/532805123/143
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-05-13 20:16:26.897000 +05:30
Logged Time	2025-05-13 20:16:26.897
Epoch Time (sec)	1747147586
ISE Node	goldenserver
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Failure Reason	
Resolution	
Root Cause	
Username	
Network Device Name	

这可以防止成功的管理登录尝试，并可通过集中身份验证影响设备访问控制。

可能的原因

- 思科ISE和Palo Alto防火墙或网络设备配置的共享密钥不匹配。
- 设备上的TACACS+服务器配置不正确（例如，错误的IP地址、端口或协议）。

解决方案

此问题有几种可能的解决方案：

1.验证共享密钥：

- 在Cisco ISE上：
  导航到Administration > Network Resources > Network Devices，选择受影响的设备，并确认共享密钥。
- 在Palo Alto防火墙上：
  转至Device > Server Profiles > TACACS+，并确保共享密钥完全匹配，包括大小写和特殊字符。

2.检查TACACS+服务器设置：

- 确保在防火墙的TACACS+配置文件中配置思科ISE的正确IP地址和端口（默认值为49）。
- 确认协议类型为TACACS+（不是RADIUS）。

2.无ISE TACACS实时日志

·验证防火墙路由/源接口和TCP/49与已配置PSN的连接。

·验证防火墙是否使用预期的ISE IP/FQDN。

·确认已在目标PSN上启用设备管理服务。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。