配置并且排除故障在ISE的外部TACACS服务器

目录

简介

本文描述功能使用在部署的外部TACACS+服务器使用身份服务Engine(ISE)作为代理。

先决条件

要求

- 设备管理基本的了解在ISE的。
- 本文根据身份服务引擎版本2.0，可适用在身份服务引擎的verison所有版本高于2.0。

使用的组件

> **Note**:对ACS的所有参考在本文可以interpretted是对任何外部TACACS+服务器的一参考。然而，在ACS的配置和在其他TACACS服务器的配置可能变化。

本文档中的信息基于以下软件和硬件版本：

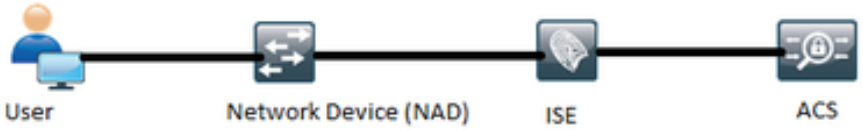
- 身份服务引擎2.0
- 访问控制系统(ACS) 5.7

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。如果您的网络实际，请确保您了解所有配置更改潜在影响。

配置

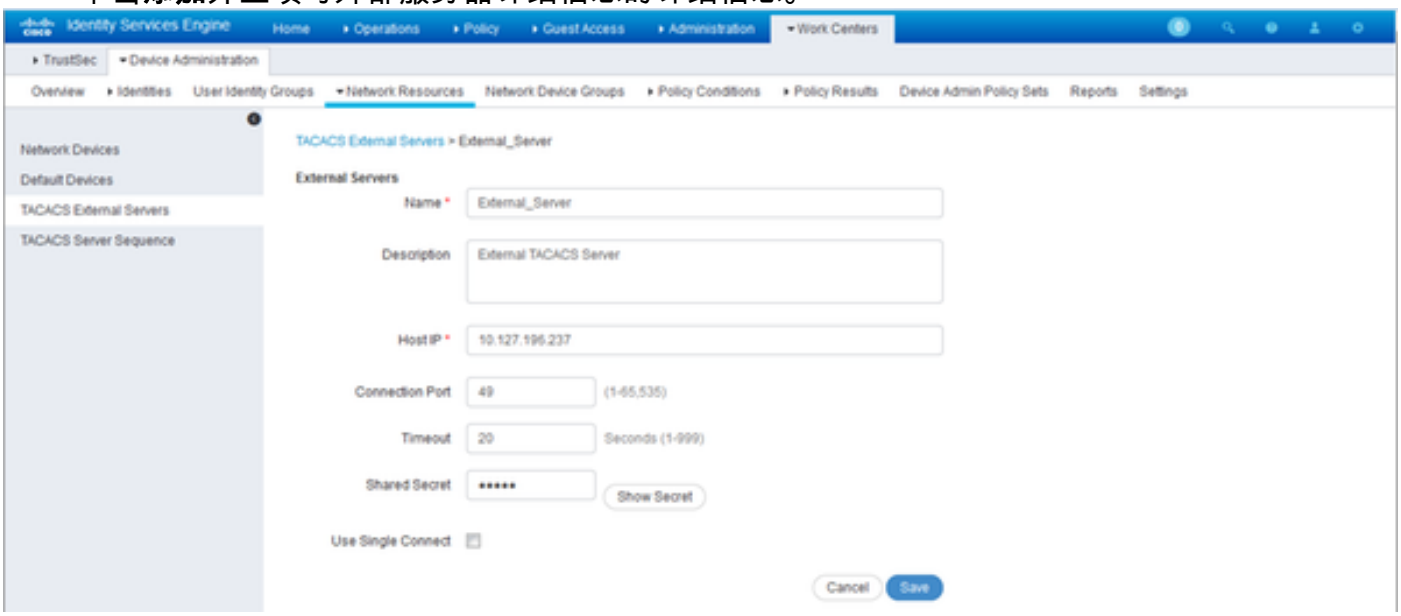
此部分帮助配置ISE到代理TACACS+请求到ACS。

网络图



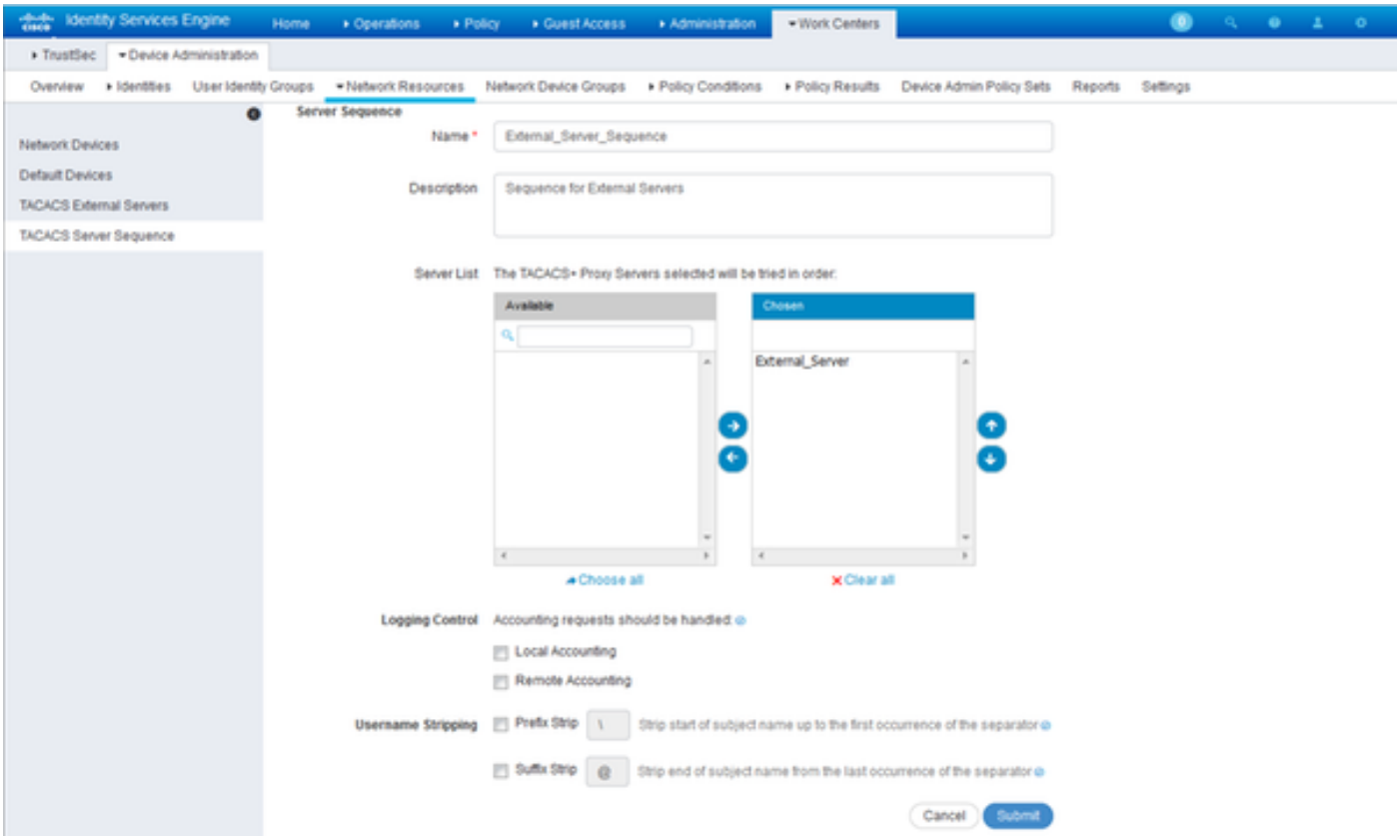
配置ISE

1. 多个外部TACACS服务器在ISE配置，并且可以使用验证用户。为了配置在ISE的外部TACACS+服务器，请导航到**工作区>设备Administration >网络资源> TACACS外部服务器。**单击**添加**并且填写外部服务器详细信息的详细信息。



在此部分提供的共享机密必须是用于ACS的同样机密。

2. 为了使用配置的外部TACACS服务器，在用于策略集的TACACS服务器顺序必须添加。我预定配置TACACS服务器顺序，导航对**工作区>设备Administration >网络资源> TACACS服务器顺序。**单击**添加，**填写详细信息并且选择是需要的使用在该顺序的服务器。

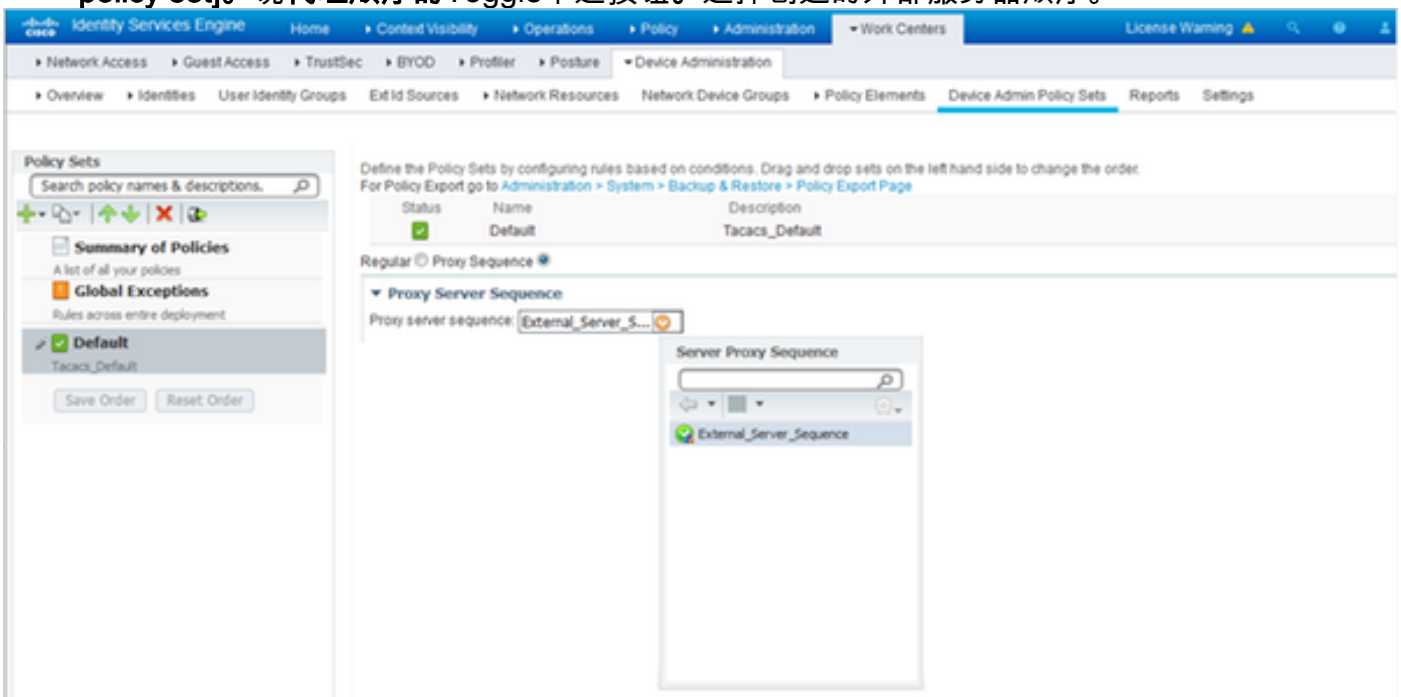


除服务器顺序之外，提供了两个其它选项。记录的控制和用户名剥离。

记录的控制给选项对日志核算请求本地在ISE或记录核算请求到处理验证的外部服务器。

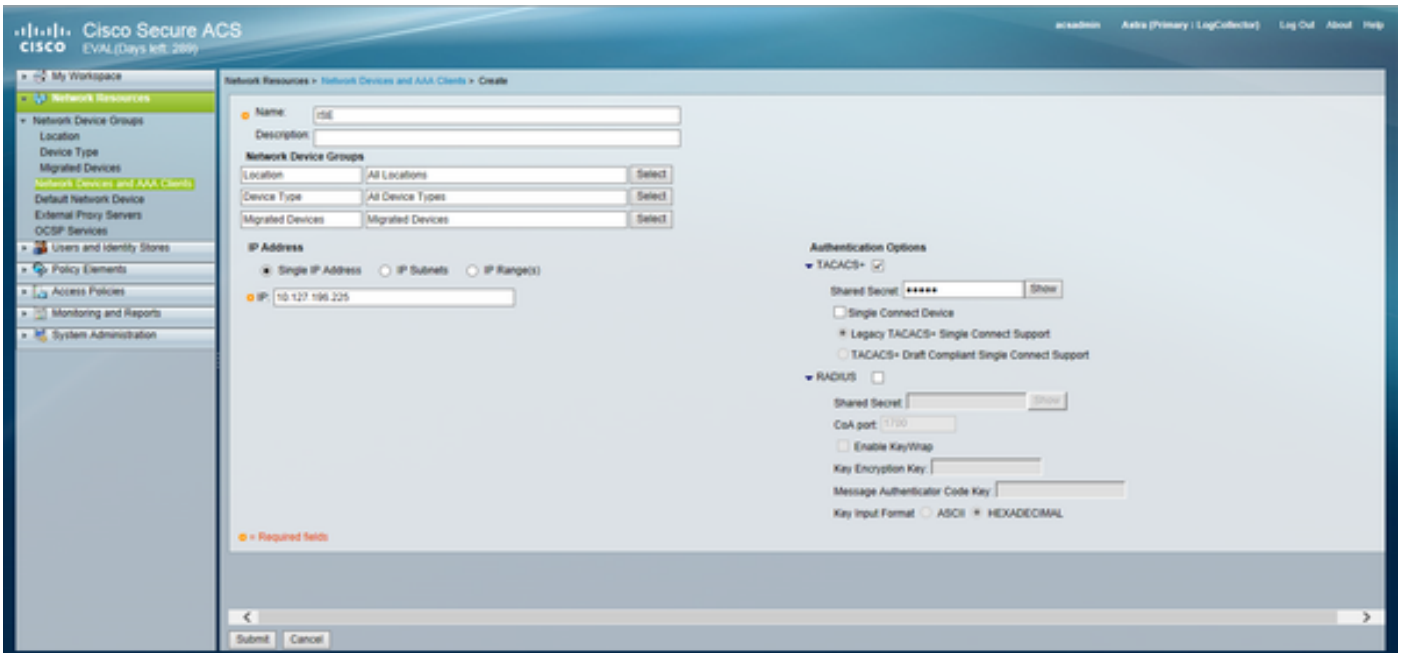
sepcifying分隔符用于用户名剥离在转发请求前剥离前缀或后缀到一个外部TACACS服务器。

3. 要使用配置的外部TACACS服务器顺序，必须配置策略集使用创建的顺序。为了配置策略集使用外部服务器顺序，请导航对**工作区>设备Administration >设备Admin策略集> [select the policy set]。**说**代理顺序的**Toggle单选按钮。选择创建的外部服务器顺序。

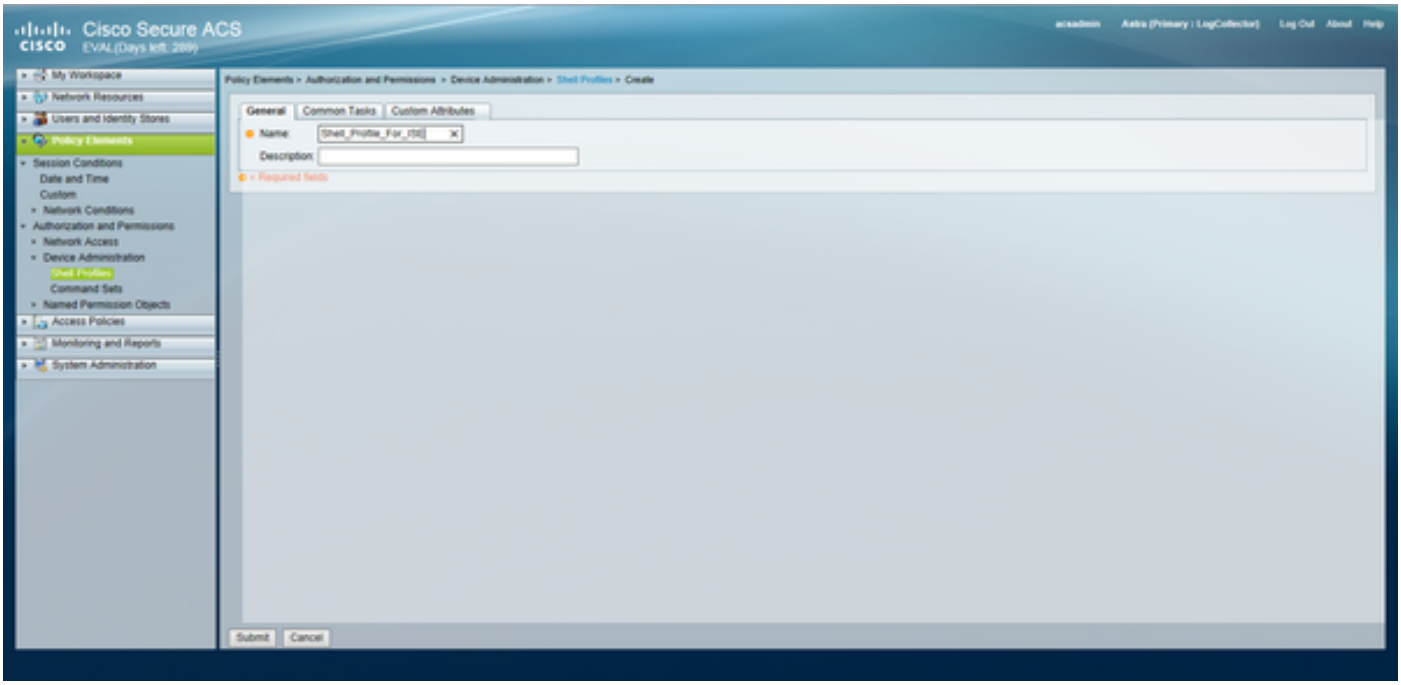


配置 ACS

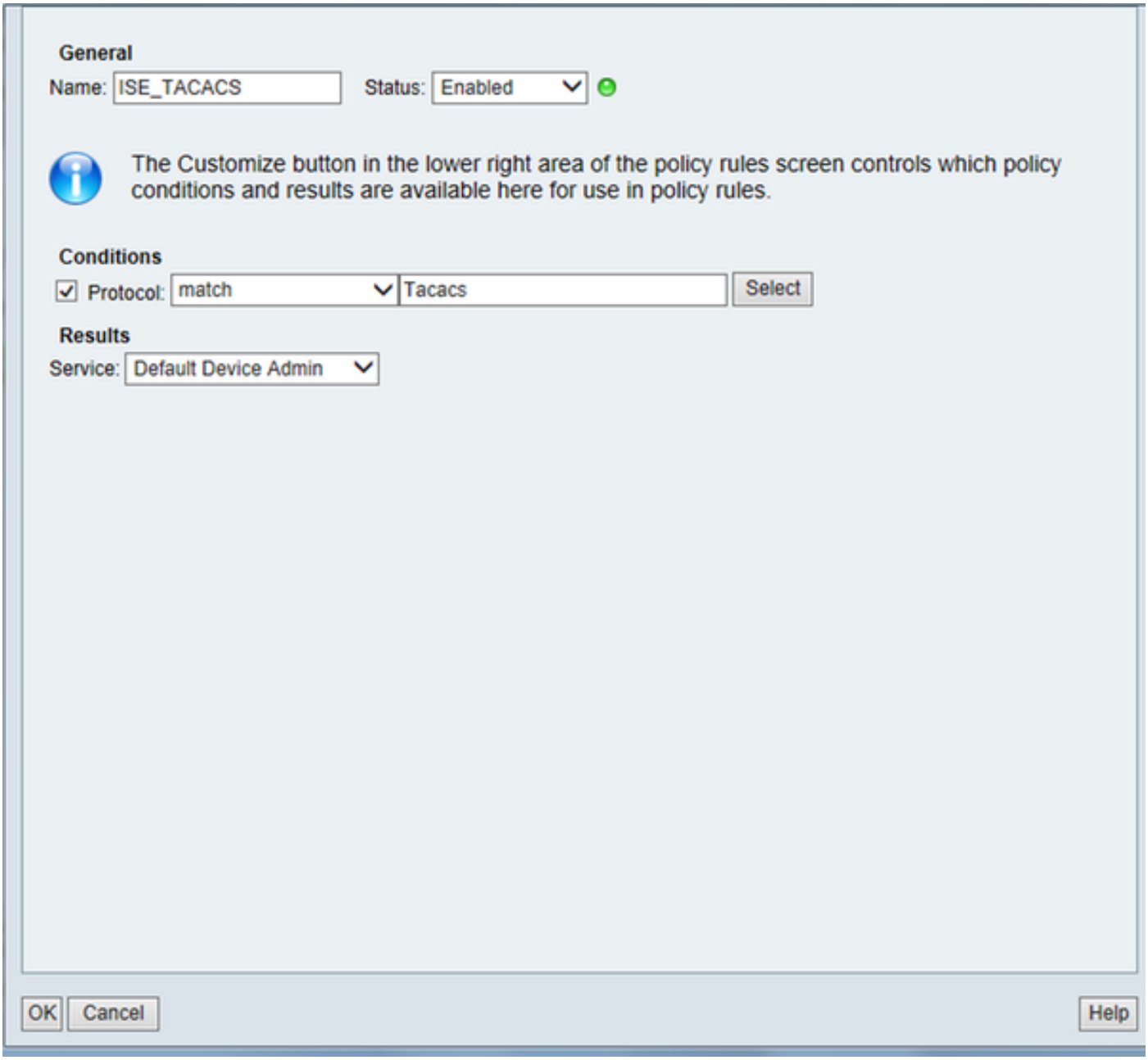
对于ACS， ISE是发送TACACS请求的另一个网络设备。为了配置ISE作为在ACS的一个网络设备，请导航给**网络资源>网络设备和AAA客户端。**单击**创建**并且填写ISE服务器的详细信息使用同样共享的机密象配置在ISE。



配置设备是在ACS， shell配置文件和命令集的管理参数。为了配置Shell配置文件，请导航到**策略元素>授权和权限>设备Administration > Shell配置文件。**单击根据需求**创建**并且配置名称、普通的任务和自定义属性。



为了conofigure命令集，导航对**策略元素>授权，并且权限>设备Administration >命令设置。** 单击根据需求**创建**并且填写详细信息。



配置在服务选择规则选择的访问服务根据需求。为了配置访问服务规则，请导航到**访问策略>Access服务**标识存储需要使用可以为验证选择的**>Default设备Admin >标识**。授权规则可以通过导航配置对**访问策略>Access服务>Default设备Admin >授权。**

Note:授权策略和shell profles的配置特定设备的可能变化，并且那是超出本文的范围。

验证

请使用此部分确认配置适当地工作。

验证在ISE和ACS可以完成。所有错误在ISE的配置里或ACS将导致认证失败。ACS是将处理验证和授权请求的主服务器， ISE到/从ACS服务器承担责任并且作为请求的一个代理。因为数据包通过两个服务器横越，验证或授权请求的验证在两个服务器可以完成。

网络设备配置与ISE作为TACACS服务器而不是ACS。因此请求首先到达ISE，并且基于配置的规则，ISE决定请求是否需要转发到外部服务器。这在Live的TACACS可以验证注册ISE。

为了查看实际注册ISE，导航对**操作> TACACS > Live日志。**现场报告能被看到关于此页，并且一特定的请求的详细信息可以通过单击放大镜图标检查关于是利益的该特定请求。

为了查看关于ACS的验证报告，导航到**监控和报告>启动监听和报告查看器>监听和报告>报告>AAA协议> TACACS认证。** 类似ISE，一特定的请求的详细信息可以通过单击放大镜图标检查关于是利益的该特定请求

故障排除

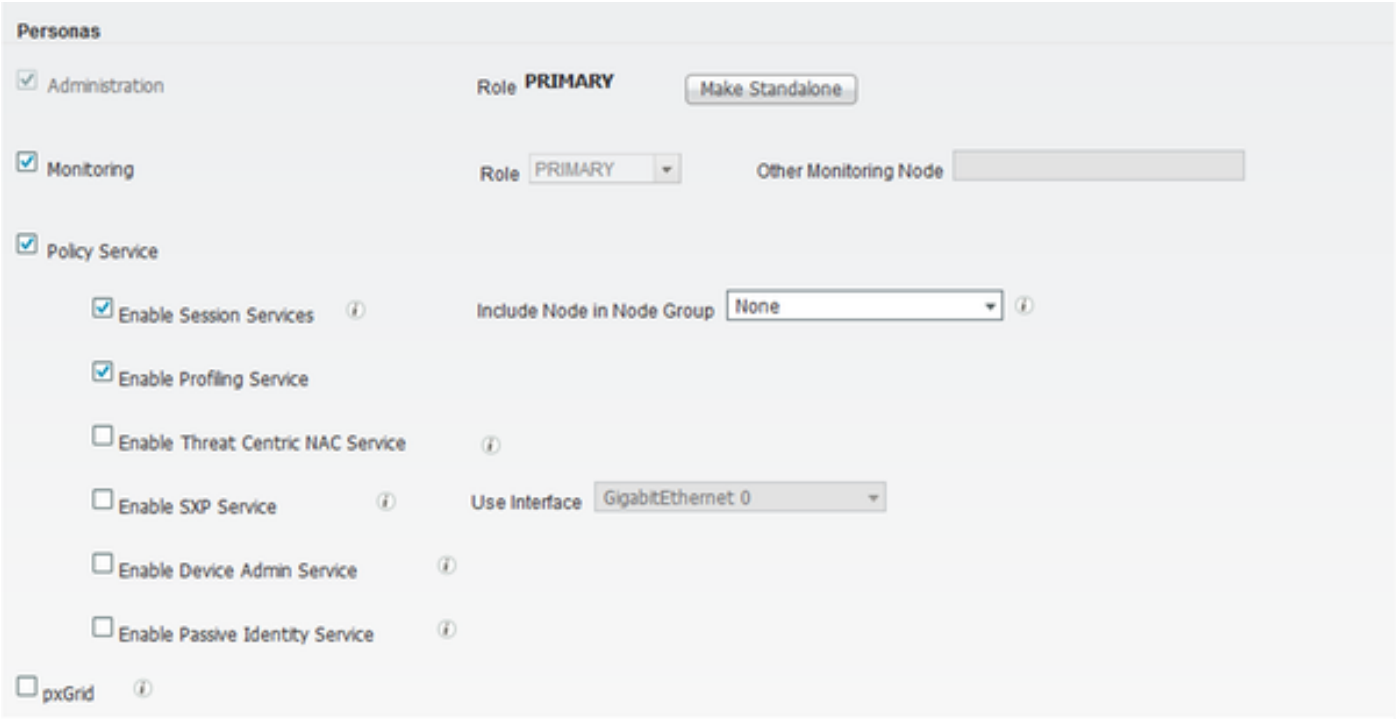
此部分提供您能使用排除故障您的配置的信息

1. 如果报告的详细信息关于ISE的表示在图表示的错误消息，则指示在ISE或Netowrk设备配置的一无效共享机密(纳季)。

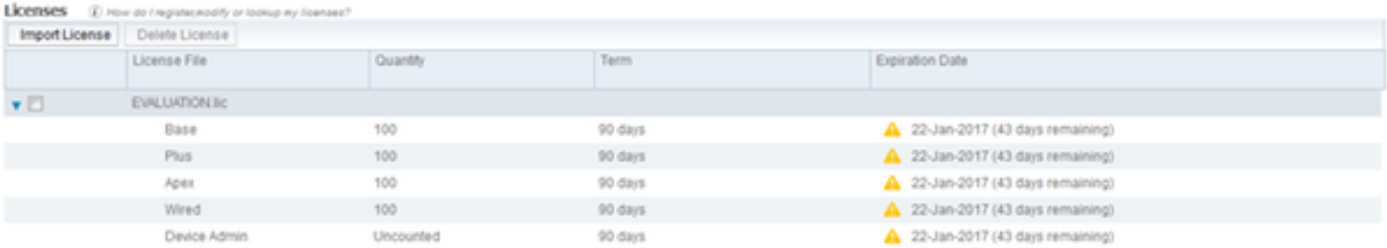
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. 如果没有请求的验证报告关于ISE，但是访问拒绝对最终用户对网络设备，这通常指示几件事。

- 请求没有执行伸手可及的距离ISE服务器。
- 如果设备管理角色在ISE禁用，则对ISE的所有TACACS+请求将静静地丢弃。指示同样的日志在报告或Live日志不会显示。要验证此，请导航对**管理>System >部署> [select the node]。**如图所显示，单击**编辑**并且注意“**以启用设备Admin服务**”复选框在**一般设置选项卡下**。复选框在ISE需要被检查设备管理工作。



- 如果设备管理许可证不是存在已到期，则所有TACACS+请求静静地丢弃。日志在同样的GUI没有显示。导航对**管理>System >许可授权**检查设备管理许可证。

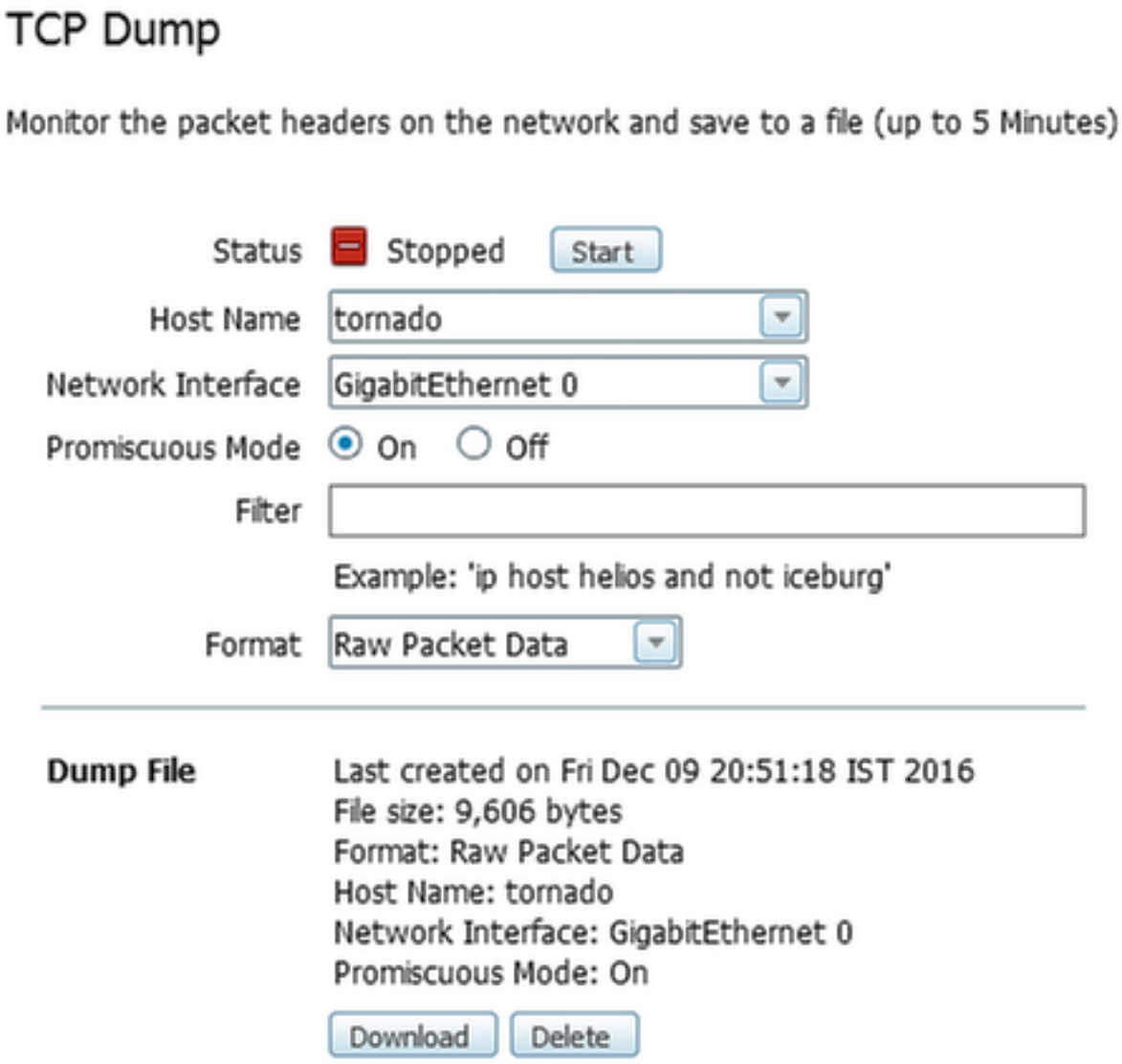


- 如果网络设备没有配置或，如果错误的网络设备IP在ISE配置，然后ISE将静静地丢弃数据包。无响应被退还的给客户端，并且日志在GUI没有显示。这是行为变化在TACACS+的ISE上，当与通知的那ACS比较请求自unkown网络设备或AAA客户端进来了。

- 请求到达了ACS，但是答复没有回来到ISE。如图所示，此方案可以从关于ACS的报告被检查。通常这是由于一无效共享机密在为ISE配置的ACS或在为ACS配置的ISE。

- 答复不会被发送，即使ISE没有配置或ISE管理接口的IP地址在ACS在网络设备配置里没有配置。在这样secario，在图的消息在ACS可以观察。

- 如果一成功认证报告被看到关于ACS，但是报告没有被看到关于ISE，并且用户拒绝，则它可能很好是在网络的一个问题。这可以由ISE的一数据包捕获验证用必要的过滤器。要收集ISE的一数据包捕获，请导航对**操作>排除故障>诊断工具>General工具> TCP转储。**



3. 如果报告能被看到关于ISE，但是不关于ACS，可能任一意味着请求未到达ACS由于策略集的误配置在可以排除故障根据详细的报告关于ISE或由于网络问题可以由ACS的一数据包捕获识别的ISE的。

4. 如果报告被看到关于两个ISE和ACS，但是用户仍然是拒绝访问，则它经常是一个问题在可以排除故障根据关于ACS的详细的报告的ACS的访问策略配置里。并且，必须允许从ISE的回程数据流到Netowork设备。