使用ISE(RADIUS)配置AsyncOS外部身份验证

目录

简介

先决条件

- 要求
- 使用的组件
- 相关产品

背景信息

配置

- 网络图
- 步骤1.创建身份验证身份组
- 步骤2.创建本地用户以进行身份验证
- 步骤3.创建授权配置文件
- 步骤4.创建授权策略
- 步骤5.在设备上启用外部身份验证

验证

故障排除

相关信息

简介

本文档介绍在思科安全邮件网关和思科身份服务引擎之间配置RADIUS外部身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 验证、授权和记帐 (AAA)
- RADIUS类属性。
- 思科ISE身份管理和授权策略。
- 思科安全邮件网关(ESA)和安全邮件和网络管理器(SMA)用户角色

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ISE 2.4
- 思科安全电子邮件网关(ESA)13.5.1、13.7.0
- 思科安全电子邮件和网络管理器(SMA)13.6.2

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。

相关产品

未测试“使用的组件”部分中列出的版本以外的版本。

背景信息

RADIUS类属性

Class属性是RADIUS服务器在Access-Accept响应中返回并包含在记帐数据包中的任意值。在思科ISE中按组进行配置。

当用户匹配绑定了属性25的ISE组时，ISE会返回Access-Accept上的Class值。然后，安全邮件网关读取该值并应用在其映射表中定义的本地角色。



注意：在ISE授权配置文件中，ASA VPN公用任务用作填充RADIUS属性25(Class)的容器。 此处输入的值是设备读取的角色映射值。

配置

网络图



思科身份服务引擎接受来自设备的身份验证请求，并将其与用户身份和组进行匹配。

步骤1.创建身份验证身份组

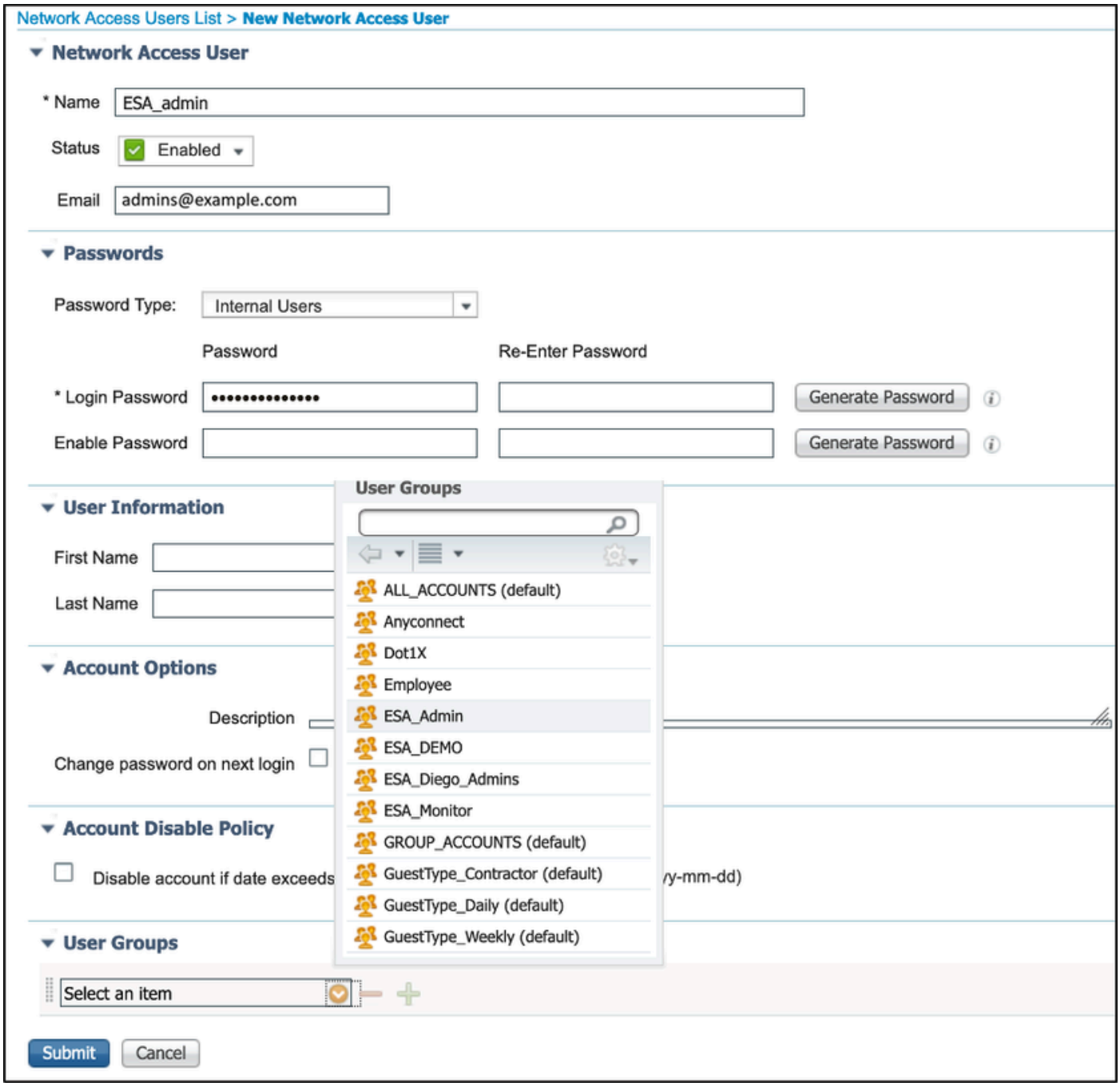
登录到ISE服务器。导航到Administration > Identity Management > Groups > User Identity Group并创建身份组。



注意：思科建议为每个要分配的设备角色在ISE中分配一个身份组。

步骤2.创建本地用户以进行身份验证

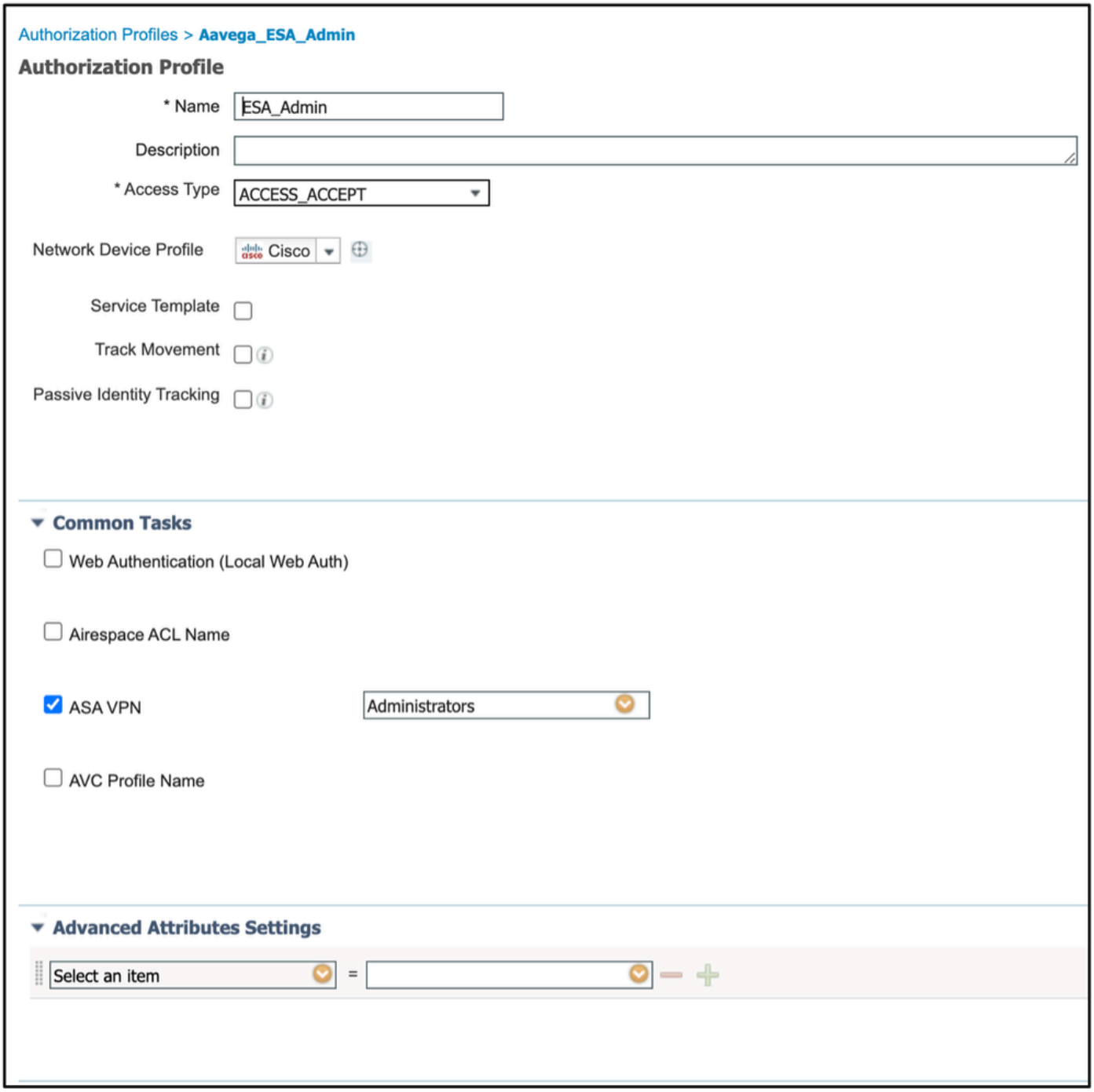
创建新用户或分配现有用户到步骤1中创建的身份组。导航到管理>身份管理>身份，然后创建或分配用户到该组。



步骤3.创建授权配置文件

RADIUS身份验证可以在没有授权配置文件的情况下成功；但是，未分配任何角色。要分配角色，请导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。

注意：为每个要分配的角色创建一个授权配置文件。



注意：确保使用radius类属性25并指定名称。此名称必须与AsyncOS(ESA/SMA)上的配置匹配。 在图3中，管理员是CLASS属性名称。

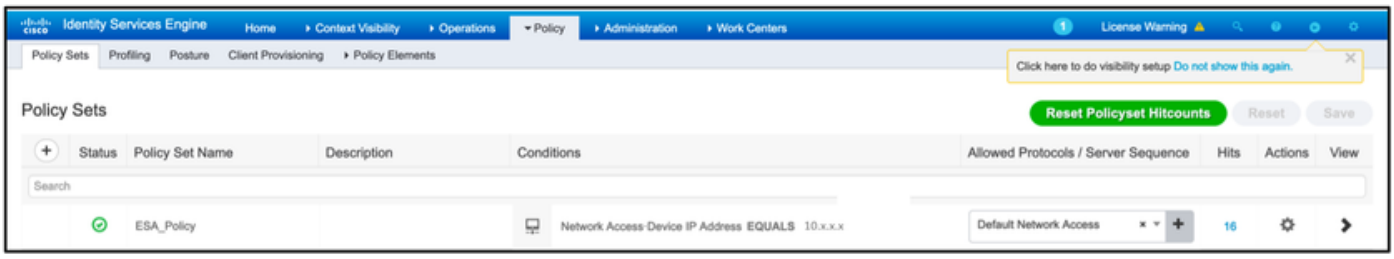
步骤4.创建授权策略

此步骤可让ISE识别登录尝试并将其映射到正确的授权配置文件。如果匹配成功，ISE会返回Access-Accept以及配置文件中定义的Class值。

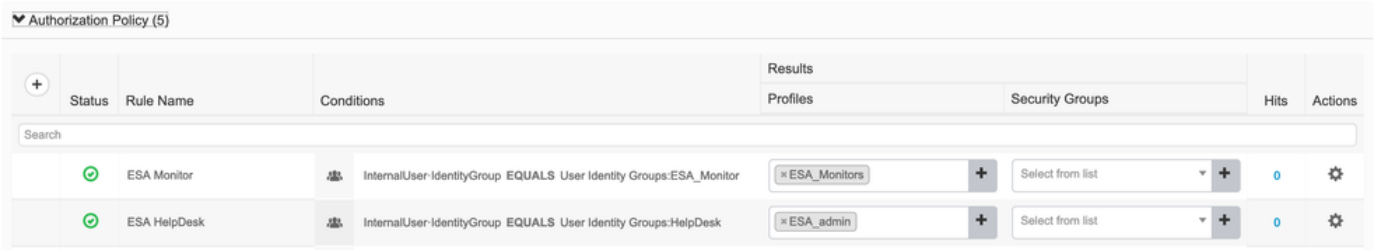
导航到Policy > Policy Sets，然后选择Add（+符号）。



指定名称并选择加号以添加所需的条件。本实验环境使用Radius NAS-IP-Address条件。保存新的策略。



要正确匹配授权请求，请添加条件。选择符号>并添加条件。本实验环境使用InternalUser-IdentityGroup并匹配每个授权配置文件。



步骤5.在设备上启用外部身份验证

登录设备。导航到System Administration > Users > External Authentication，然后选择Enable External Authentication。

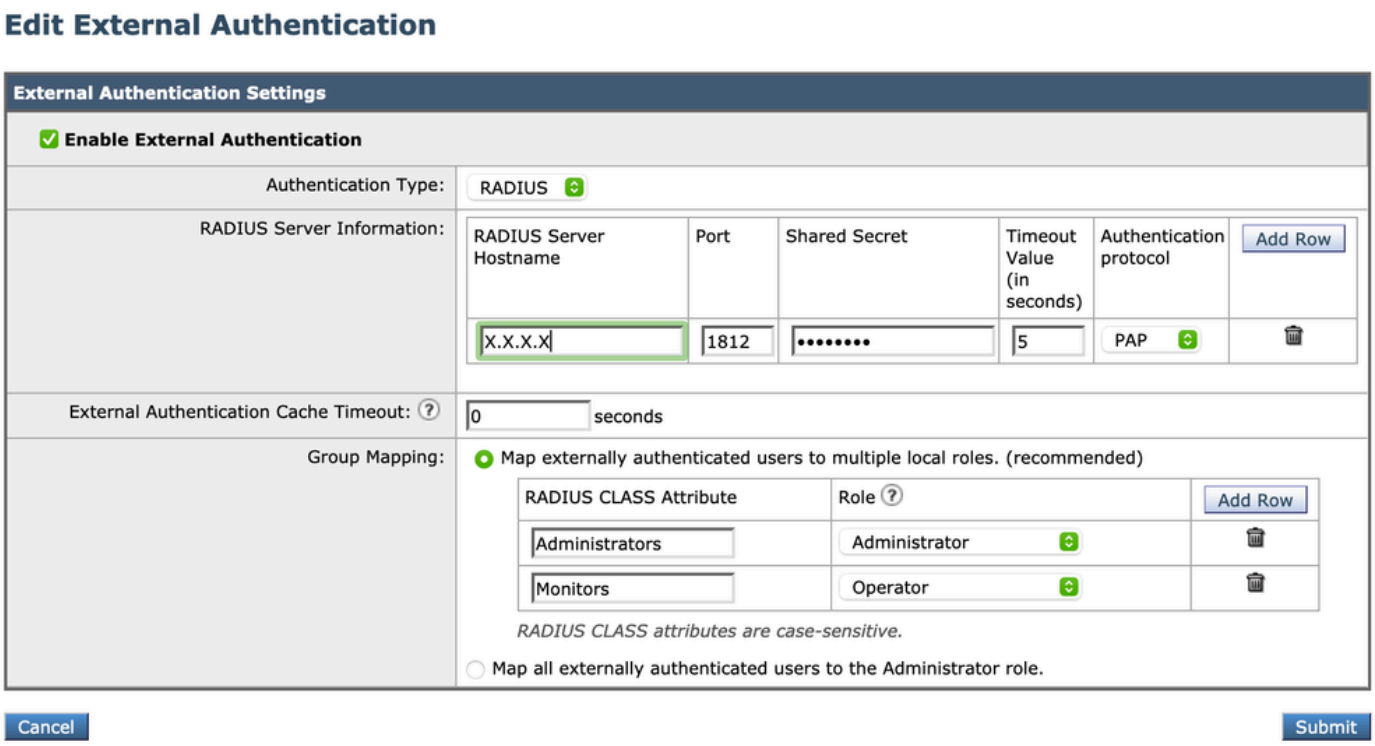


输入以下值：

- RADIUS服务器主机名
- 端口

- 共享密钥
- 超时值（以秒为单位）
- 身份验证协议

选择Map external authenticated users to multiple local roles(recommended)。



注意:RADIUS类值必须与步骤3中定义的值（在ASA VPN通用任务下输入）（包括大小写）匹配。

注意：此处选择的身份验证协议（例如，PAP）必须与ISE策略集中允许的协议匹配。不匹配导致身份验证失败。

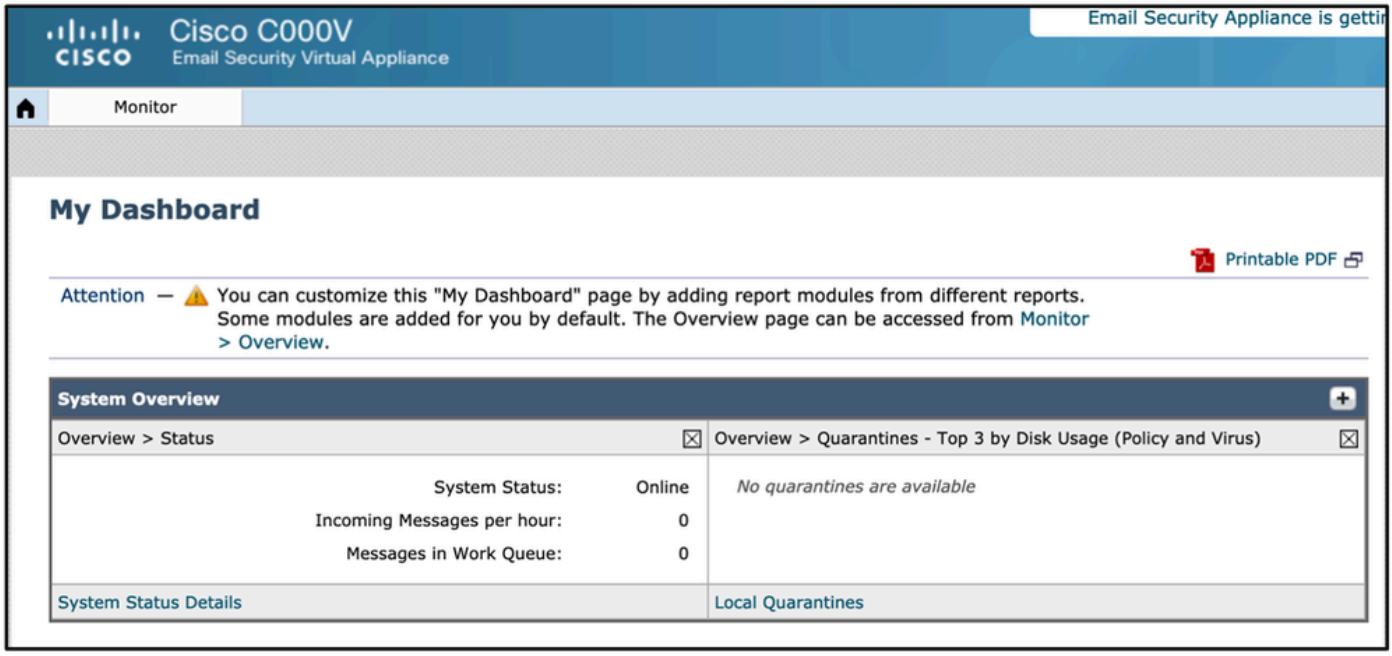
提交并确认更改。

验证

使用本部分可确定配置能否正常运行。

1. 使用外部身份验证的用户登录设备。
2. 确认访问权限已授予。

3. 确认分配的角色与返回的Class值中预期的角色匹配。
4. 在ISE中，确认已命中预期授权规则并返回正确的类值(操作> RADIUS >实时日志)。



故障排除

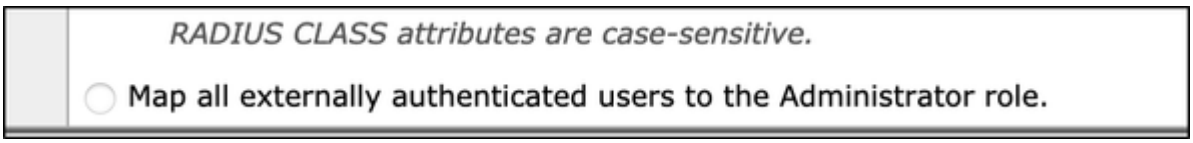
本节提供可用于对配置进行故障排除的信息。

症状：在设备上登录失败，并显示消息“用户名或密码无效”。

可能的原因：授权策略、返回的Class值或身份验证协议不匹配。

分辨率：

1. 在设备“外部身份验证”(External Authentication)设置中，临时选择“将所有外部身份验证的用户映射到管理员角色”(Map all external authenticated users to the Administrator role)。（映像11）
2. 提交并确认更改，然后尝试新登录。
3. 如果现在登录成功，则问题出在角色映射上。重新检查ISE授权配置文件（类别/属性25）和授权策略设置。
4. ReviewOperations > RADIUS > Live Login ISE，确认匹配的授权配置文件和返回的Class值。



相关信息

- ISE 2.4用户指南
- AsyncOS用户指南

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）。