无线局域网控制器的 ISE TACACS+ 配置指南

安全访问操作指南用户系列

作者：Aruna Yerragudi（由 Hsing-Tsu Lai 编辑）

日期：2015 年 12 月

目录

指南简介

概述

增强型终端访问控制器访问控制系统 (TACACS+) 是为用户提供集中式安全控制来获取对路由器或任何网络访问设备的管理访问权限的客户端-服务器协议。TACACS+ 提供以下 AAA 服务：

- 身份验证 - 用户是谁
- 授权 - 允许用户执行什么操作
- 记帐 - 谁做过什么以及时间

本文档提供以思科身份服务引擎 (ISE) 作为 TACACS+ 服务器并以思科无线局域网控制器 (WLC) 作为 TACACS+ 客户端的 TACACS+ 配置示例。

使用本指南

本指南将活动划分为两个部分，以启用 ISE 来管理 WLC 的管理员访问权限。

- 第 1 部分 - 为设备管理配置 ISE
- 第 2 部分 - 为 TACACS+ 配置 WLC

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ISE 版本 2.0
- 使用 AireOS 软件版本 7.6 和 8.0 的 WLC

本文档中的信息是从实验室环境中的设备所创建。所有设备最初都采用出厂（默认）配置。

设备管理的 ISE 配置

在 ISE 上许可设备管理

设备管理根据部署获得许可，但是需要现有且有效的 ISE 库或移动许可证。

在 ISE 上启用设备管理

在 ISE 节点中，默认情况下未启用设备管理服务 (TACACS+)。第一步是启用该服务。

第 1 步： 使用其中一个受支持的浏览器登录到 ISE 管理 Web 门户。

第 2 步： 导航到**管理 (Administration) > 系统 (System) > 部署 (Deployment)**。选中 ISE 节点的对应复选框，然后点击**编辑 (Edit)**。

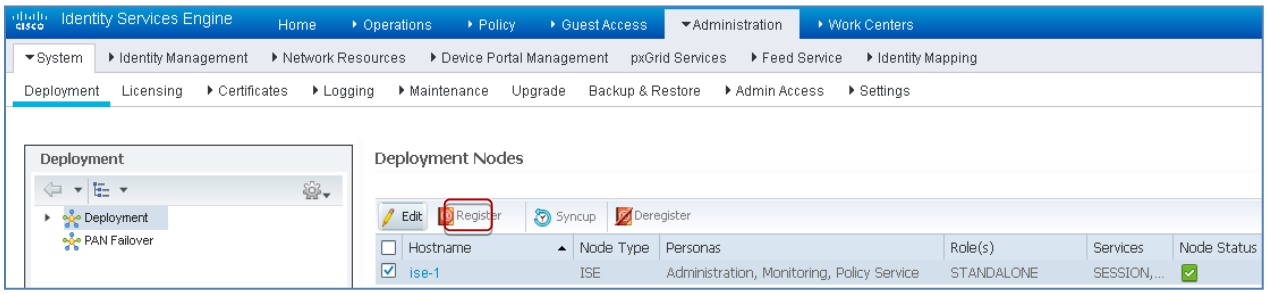

图 1. ISE 部署页面

第 3 步： 在**常规设置 (General Settings)** 下，向下滚动并选中**启用设备管理服务 (Enable Device Admin Service)** 的对应复选框。

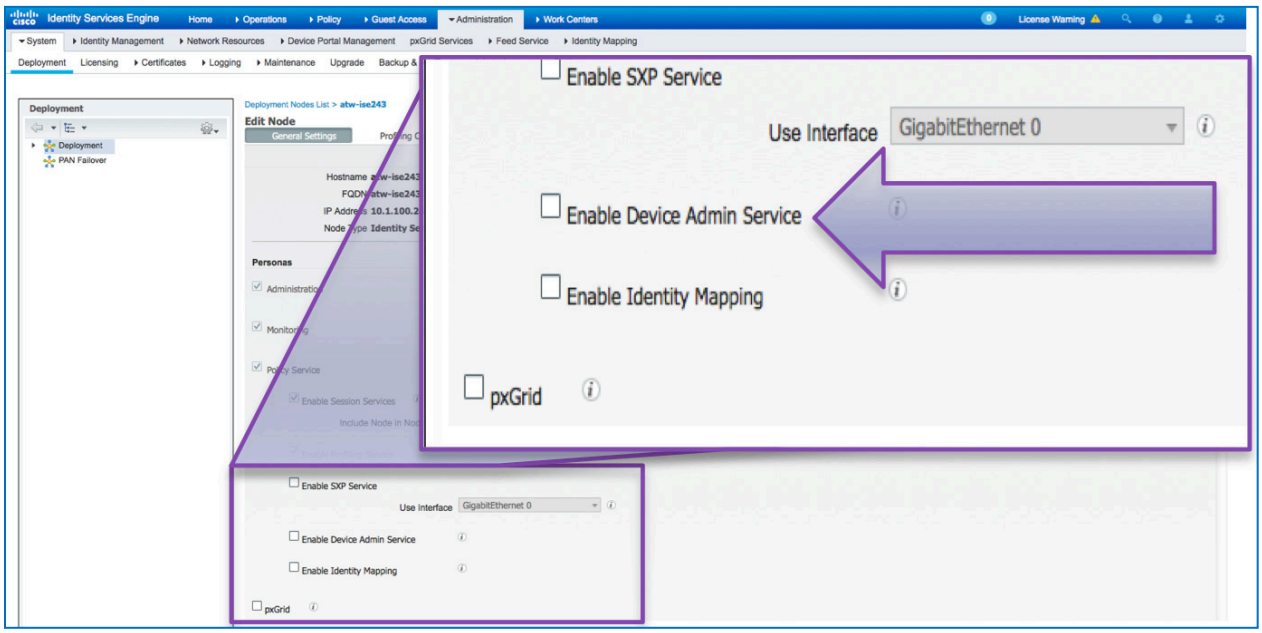

图 2. ISE 部署常规设置

第 4 步： **保存 (Save)** 配置。此时在 ISE 上已启用设备管理服务。

设备管理工作中心

ISE 2.0 引入了 TrutSec 和设备管理工作中心。工作中心包含特定功能的所有元素。

第 1 步： 转至**工作中心 (Work Centers) > 设备管理 (Device Administration) > 概述 (Overview)**

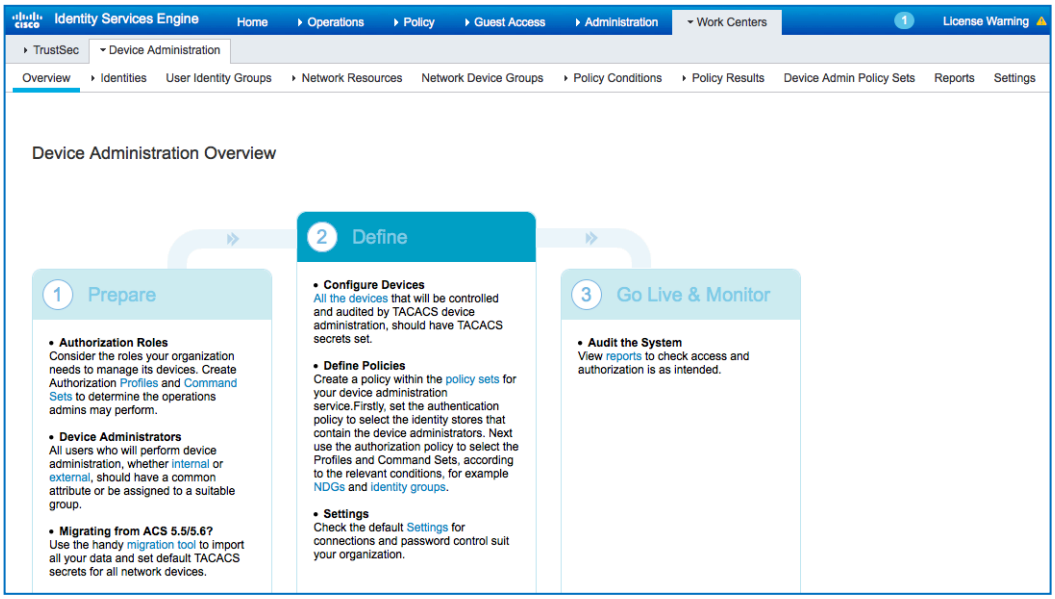

图 3. 设备管理概述

设备管理概述提供设备管理使用案例所需的高级步骤。

配置网络设备和网络设备组

现在，让我们来探索网络设备和网络设备分组。

ISE 以多个设备组层次结构的形式提供强大的设备分组。每个层次结构都表示一个不同且独立的网络设备分类。

第 1 步： 导航到**工作中心 (Work Centers) > 设备管理 (Device Administration) > 网络设备组 (Network Device Groups)**

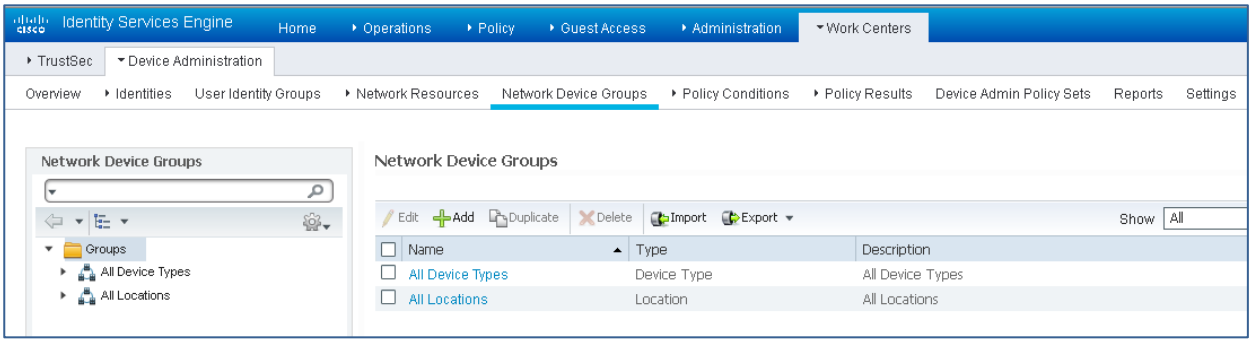

图 4. 网络设备组

“所有设备类型”(All Device Types) 和“所有位置”(All Locations) 是 ISE 提供的默认层次结构。您可以添加自己的层次结构或定义各种组件来识别稍后将在策略条件中使用的网络设备。

第 2 步： 在定义各种层次结构后，“网络设备组”(Network Device Groups) 将如下所示：

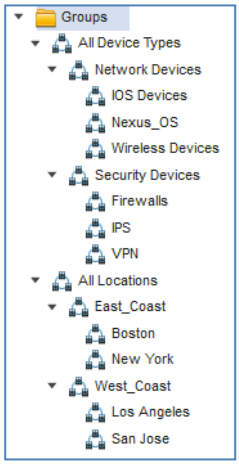

图 5. 网络设备组树状视图

我们在此处添加了各种设备类型以及位置。

第 3 步： 现在，请添加 WLC 作为网络设备。转至**工作中心 (Work Centers) > 设备管理 (Device Administration) > 网络资源 (Network Resources)**。点击**添加 (Add)** 以添加新的网络设备 **DMZ_BLDO_vWLC**。

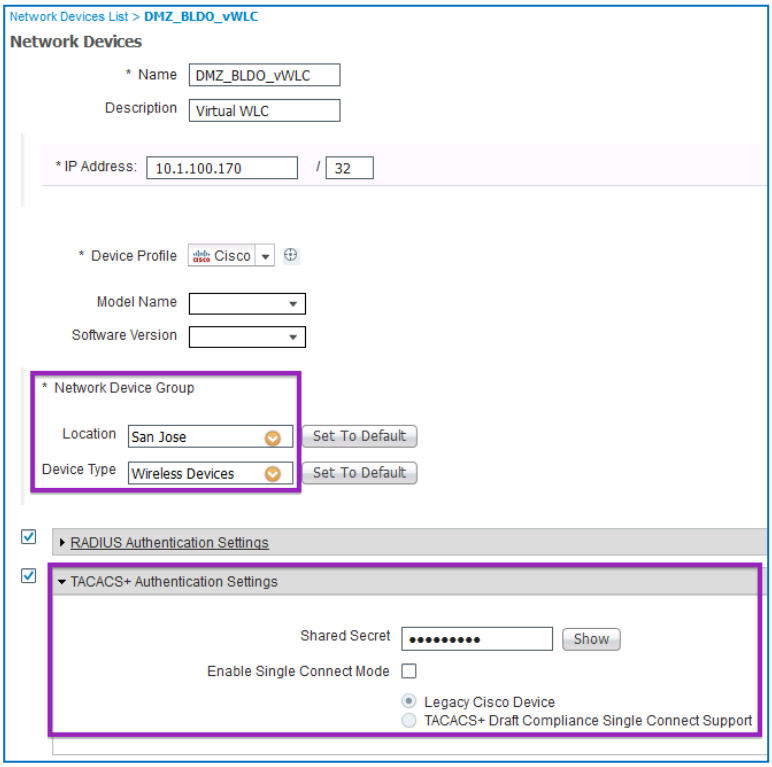

图 6. 添加网络设备

输入设备的 IP 地址并确保映射设备的位置和设备类型。最后，启用 **TACACS+ 身份验证设置 (TACACS+ Authentication Settings)** 并指定共享密钥。

定义身份库

本节旨在定义设备管理员的身份库。身份库可以是 ISE 内部用户和/或任何受支持的外部身份源。对于此配置，我们将使用外部身份源 Active Directory (AD)。

第 1 步： 导航到**管理 (Administration) > 身份管理 (Identity Management) > 外部身份库 (External Identity Stores) > Active Directory**。点击**添加 (Add)** 以定义新的 Active Directory 加入点。指定加入点名称和 AD 域名，然后点击**提交 (Submit)**。

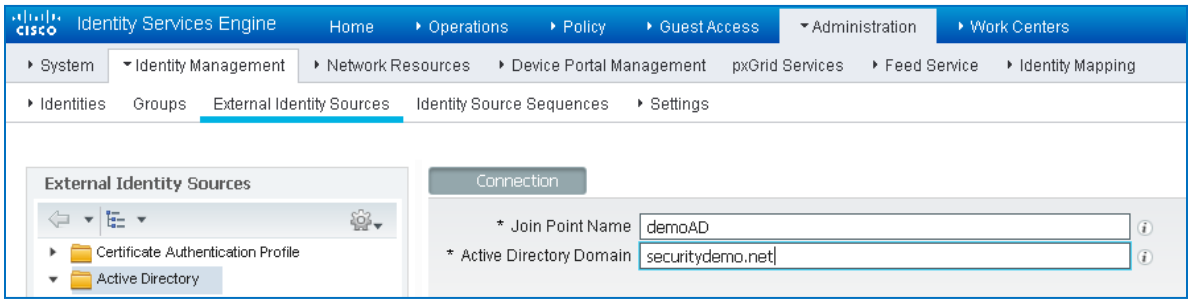

图 3. 添加 AD 加入点

第 2 步： 当提示“是否要将所有 ISE 节点都加入到此 Active Directory 域？”(Would you like to Join all ISE Nodes to this Active Directory Domain?) 时点击**是** (Yes)
输入具有 AD 加入权限的凭证，然后将 ISE **加入**到 AD。检查状态以验证其是否可操作。

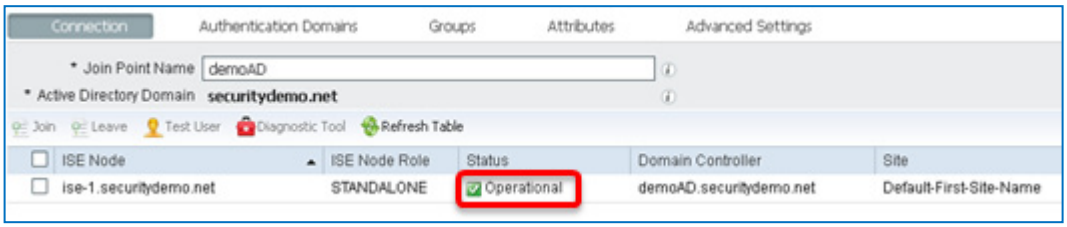

图 4. 将 ISE 加入到 AD

第 3 步： 转至**组 (Groups)** 选项卡，然后点击**添加 (Add)** 以获取需要的所有组，基于这些组可授权用户进行设备访问。下面显示本指南的授权策略中使用的组

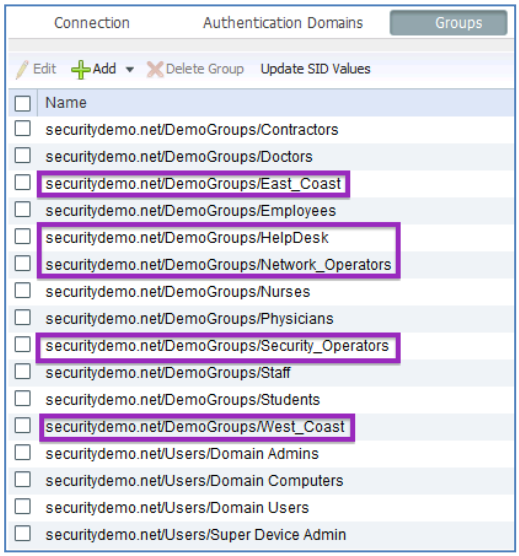

图 5. AD 组

配置 TACACS 配置文件

我们将定义要在授权策略中使用的三个 TACACS 配置文件 -

- WLC_Monitor_Only：具有“监控”(Monitor) 选项卡访问权限的服务中心
- WLC_Security_Access：具有“安全”(Security) 和“命令”(Commands) 选项卡访问权限的安全操作员
- WLC_Admin：具有完全访问权限的管理员。

WLC 使用需要定义为 role1、role2 等的 TACACS+ 自定义属性。可用角色为 MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、COMMAND、ALL 和 LOBBY。前七个角色对应于 WLC 管理 Web UI 上的菜单选项。您可以输入一个或多个角色来允许对特定功能进行读写访问，并对其余功能进行只读访问。

要向 WLAN、SECURITY 和 CONTROLLER 授予读写访问权限，请输入以下文本：

```
role1=WLAN
role2=SECURITY
role3=CONTROLLER
```

第 1 步： 在 ISE GUI 上，转至**工作中心 (Work Centers) > 设备管理 (Device Administration) > 策略结果 (Policy Results) > TACACS 配置文件 (TACACS Profiles)**。添加新的 TACACS 配置文件（称为 **WLC_Monitor_Only**）。向下滚动到**自定义属性 (Custom Attributes)** 部分以仅定义对 MONITOR 的访问权限。

图 6. WLC_Monitor_Only 的 TACACS 配置文件

点击**保存 (Save)** 以保存配置文件。

第 2 步： 添加另一个配置文件（称为 **WLC_Security_Access**）以提供对 SECURITY 和 COMMANDS 的访问权限。

图 7. WLC_Security_Access 的 TACACS 配置文件

点击**保存 (Save)** 以保存配置文件。

第 3 步： 添加第三个配置文件（称为 **WLC_Admin**），通过以 role1=ALL 为属性来提供对所有选项卡的访问权限。

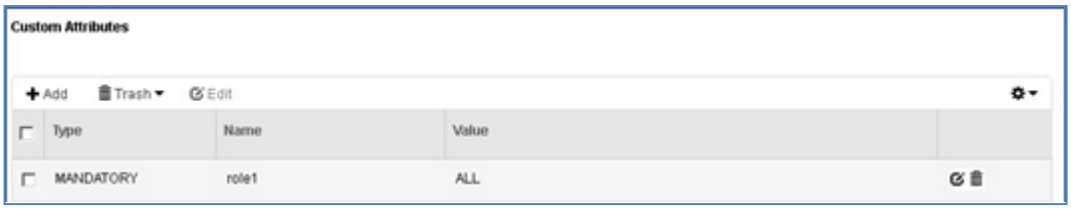

图 8. WLC_Admin 的 TACACS 配置文件

设备管理策略集

对于设备管理，默认情况下会启用策略集。策略集可以根据设备类型划分策略，从而轻松应用 TACACS 配置文件。例如，Cisco IOS 设备使用权限级别和/或命令集，而 WLC 设备则使用自定义属性。

第 1 步： 导航到**工作中心 (Work Centers) > 设备管理 (Device Administration) > 设备管理策略集 (Device Admin Policy Sets)**。添加具有以下条件的新策略集（称为 **WirelessLanControllers**）
DEVICE:Device Type EQUALS Device Type#All Device Types#Network Device#Wireless Devices

图 9. 策略集条件

第 2 步： 创建身份验证策略。对于身份验证，我们将使用 Active Directory 作为 ID 库。

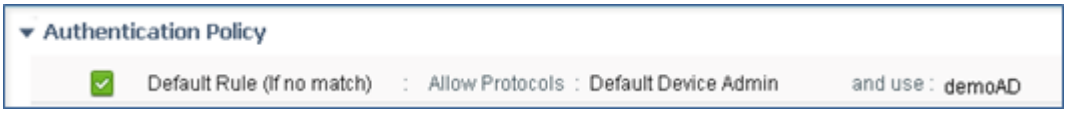

图 10. 身份验证策略

第 3 步： 定义授权策略。此处我们将根据 Active Directory 中的用户组和设备的位置来定义授权策略。例如，Active Directory 组 West Coast 中的用户只能访问位于 West Coast 的设备，而 Active Directory 组 East Coast 中的用户只能访问位于 East Coast 的设备。

S	规则名称	条件	Shell 配置文件
✓	WLC HelpDesk West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND DEVICE:Location CONTAINS All Locations#West_Coast	WLC_Monitor_Only
✓	WLC HelpDesk East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND DEVICE:Location CONTAINS All Locations#East_Coast	WLC_Monitor_Only
✓	WLC Security West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND DEVICE:Location CONTAINS All Locations#West_Coast	WLC_Security_Access
✓	WLC Security East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND DEVICE:Location CONTAINS All Locations#East_Coast	WLC_Security_Access
✓	WLC Admin E and W	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast	WLC_Admin

S	规则名称	条件	Shell 配置文件
✓	WLC Admin West	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND DEVICE:Location CONTAINS All Locations#West_Coast	WLC_Admin
✓	WLC Admin East	demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND DEVICE:Location CONTAINS All Locations#East_Coast	WLC_Admin
✓	Default	DenyAllCommands	

图 11. 授权策略

我们现在已完成 WLC 设备的设备管理的 ISE 配置

TACACS+ 的 WLC 配置

为在 WLC 控制器中配置 TACACS+，您需要完成下列步骤：

1. 添加 TACACS+ 身份验证服务器
2. 添加 TACACS+ 授权服务器
3. 添加 TACACS+ 记帐服务器
4. 配置管理用户身份验证的优先级顺序

添加 TACACS+ 身份验证服务器

完成下列步骤，以便添加 TACACS+ 身份验证服务器。

第 1 步： 从 WLC GUI 中，导航到**安全 (Security) > AAA > TACACS+ > 身份验证 (Authentication)**，然后点击**新建 (New)...**

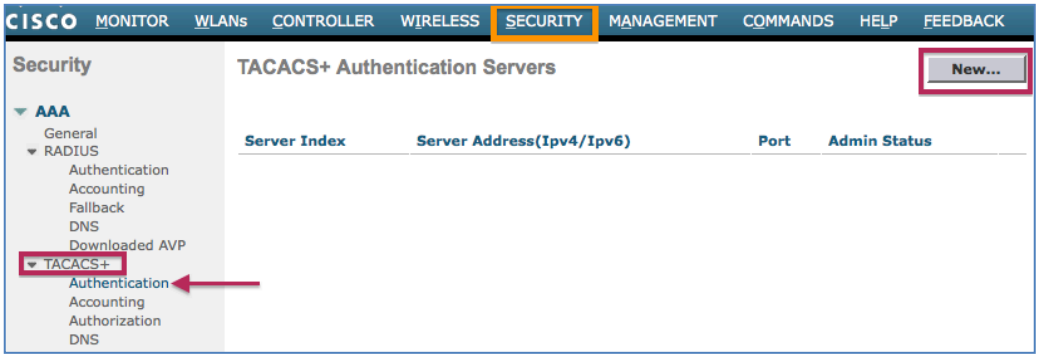

图 12. TACACS+ 身份验证服务器

第 2 步： 输入作为 TACACS+ 服务器的 ISE 服务器的 IP 地址，并输入共享密钥。

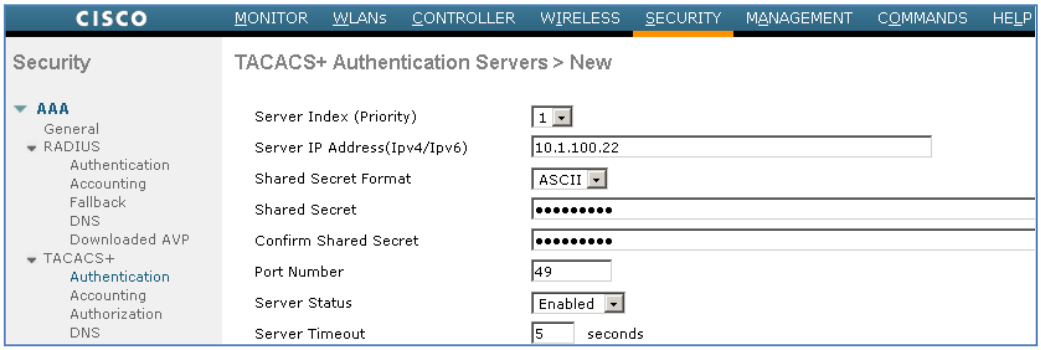

图 13. 添加 TACACS+ 身份验证服务器

第 3 步： 点击**应用 (Apply)**。

添加 TACACS+ 授权服务器

完成下列步骤，以便添加 TACACS+ 授权服务器。

第 1 步： 从 WLC GUI 中，导航到**安全 (Security) > AAA > TACACS+ > 授权 (Authorization)**，然后点击**新建 (New)...**

第 2 步： 添加 ISE 服务器的 IP 地址作为服务器 IP 地址，并输入共享密钥。

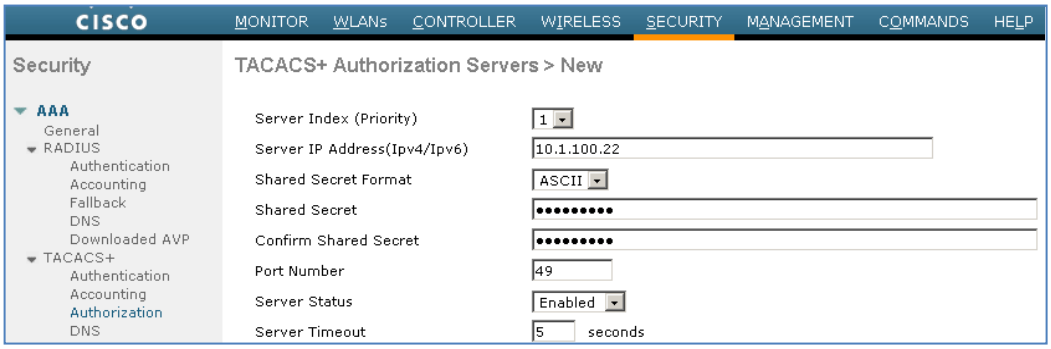

图 14. 添加 TACACS+ 授权服务器

第 3 步： 点击**应用 (Apply)**

添加 TACACS+ 记帐服务器

完成下列步骤，以便添加 TACACS+ 记帐服务器。

第 1 步： 从 WLC GUI 中，导航到**安全 (Security) > AAA > TACACS+ > 记帐 (Accounting)**，然后点击**新建 (New)...**

第 2 步： 输入 ISE 服务器的 IP 地址作为服务器 IP 地址，并输入共享密钥。

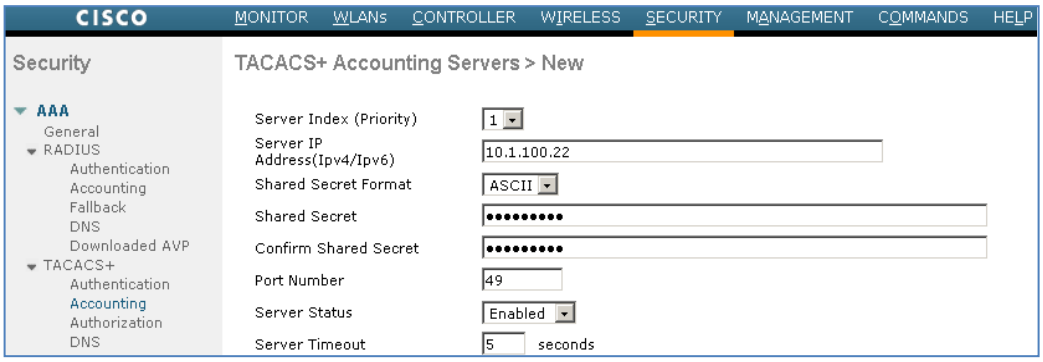

图 15. 添加 TACACS+ 记帐服务器

第 3 步： 点击**应用 (Apply)**

配置管理用户身份验证的优先级顺序

此步骤说明如何配置管理用户身份验证的优先级顺序。默认控制器配置为*本地和 RADIUS* (*local and RADIUS*)。使用 TACACS+，身份验证的顺序可以为 **TACACS+ 和本地 (TACACS+ and local)** 或**本地和 TACACS+ (local and TACACS+)**。

第 1 步： 从 GUI 中，转至**安全 (Security) > 优先级顺序 (Priority Order) > 管理用户 (Management User)**。使用向上和向下箭头按钮，选择“身份验证”(Authentication) 并将其排序为 TACACS+ 后跟 LOCAL

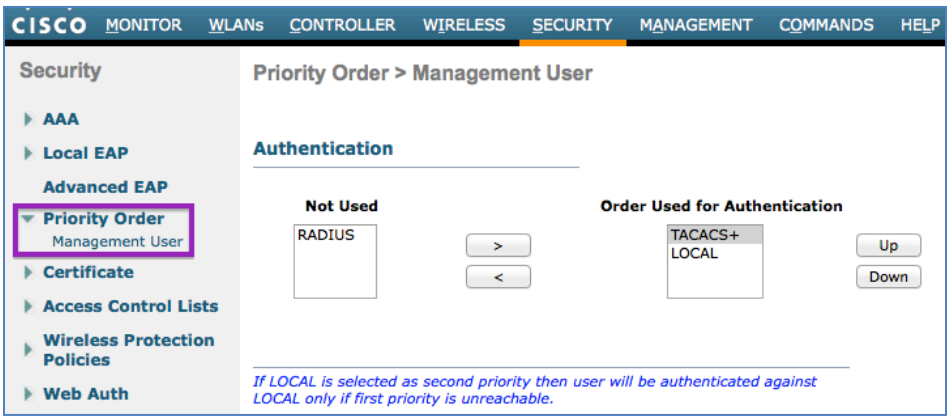

图 16. 配置身份验证顺序

第 2 步： 点击**应用 (Apply)**。

这将完成 TACACS+ 的 WLC 配置。

后续内容

此时，WLC 的设备管理所需的所有配置都已完成。您将需要验证配置。

第 1 步： 以属于不同组并访问不同设备的各种用户身份登录到 WLC。
第 2 步： 当登录时，请验证用户是否有权访问适当的选项卡。
第 3 步： 对于服务中心用户，请导航到不同的选项卡并尝试添加/修改/删除。例如，转至 WLAN 并尝试删除其中一个 WLAN。由于此用户仅有 MONITOR 访问权限，因此会因以下错误而拒绝操作

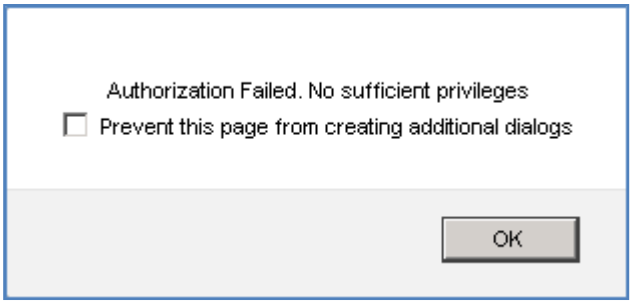

图 17. WLC 上授权失败的错误消息

第 4 步： 从 ISE GUI 中，导航到**操作 (Operations) > TACACS 实时日志 (TACACS Livelog)**。在此处捕获所有 TACACS 身份验证和授权请求，并且详细信息按钮将提供有关特定事务通过/失败的原因的详细信息。

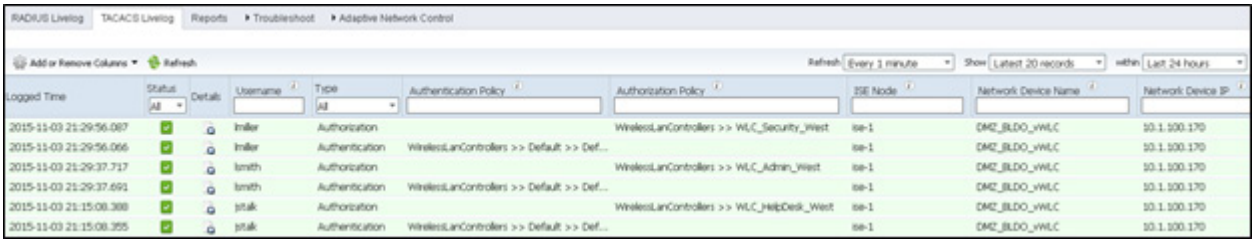

图 18. TACACS 实时日志

第 5 步： 对于历史报告，请在 ISE 上转至**工作中心 (Work Centers) > 设备管理 (Device Administration) > 报告 (Reports) > 设备管理 (Device Administration)** 以获取身份验证、授权和记帐报告。