使用TACACS+管理Cisco WLC的设备

目录

简介

本文档介绍如何使用身份服务引擎(ISE)配置TACACS+，以管理思科无线局域网控制器(WLC)的设备。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)的基本知识
- 思科无线局域网控制器(WLC)的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

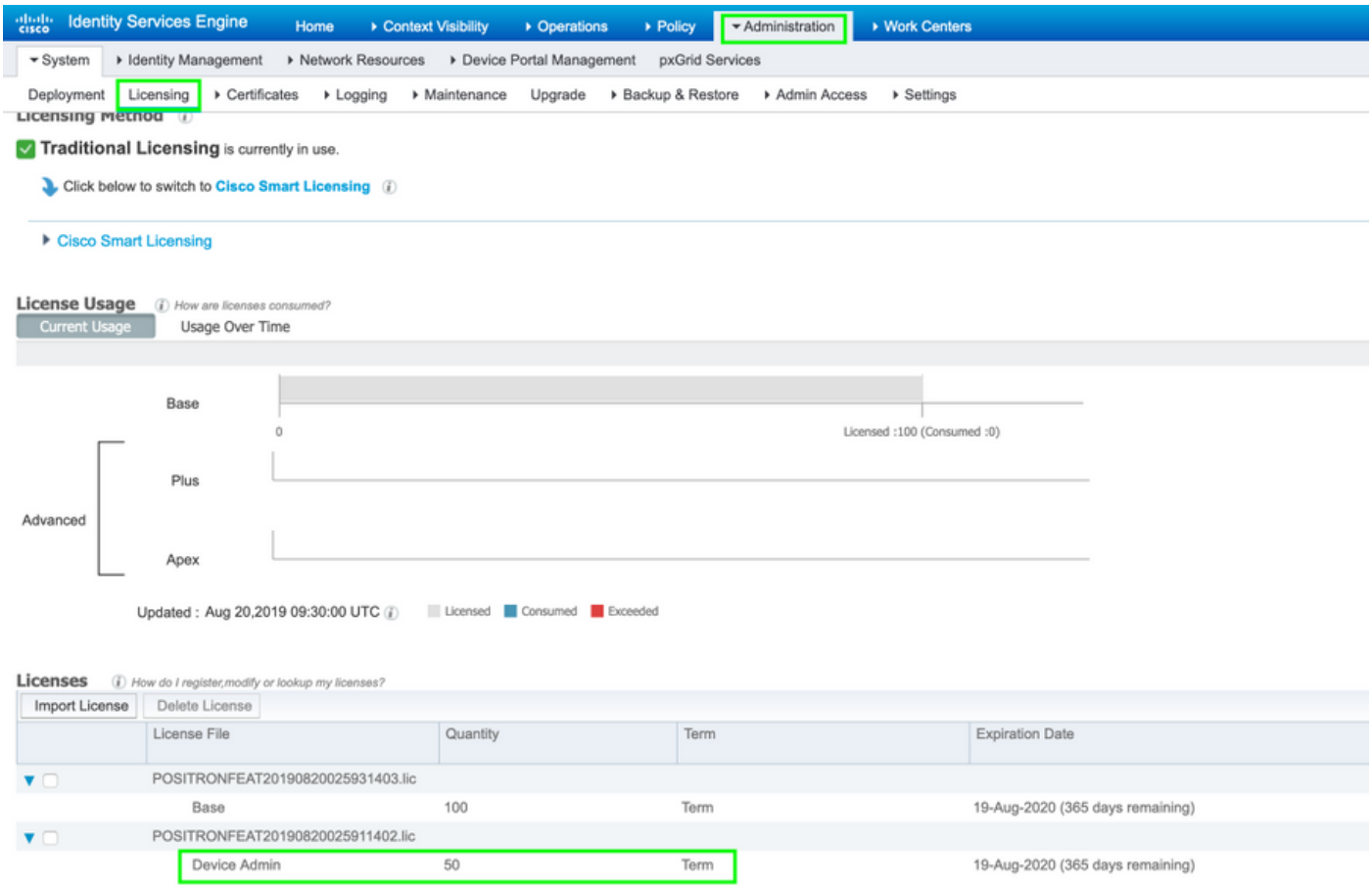
- 思科身份服务引擎2.4
- 思科无线局域网控制器8.5.135

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

步骤1.检查Device Administration License。

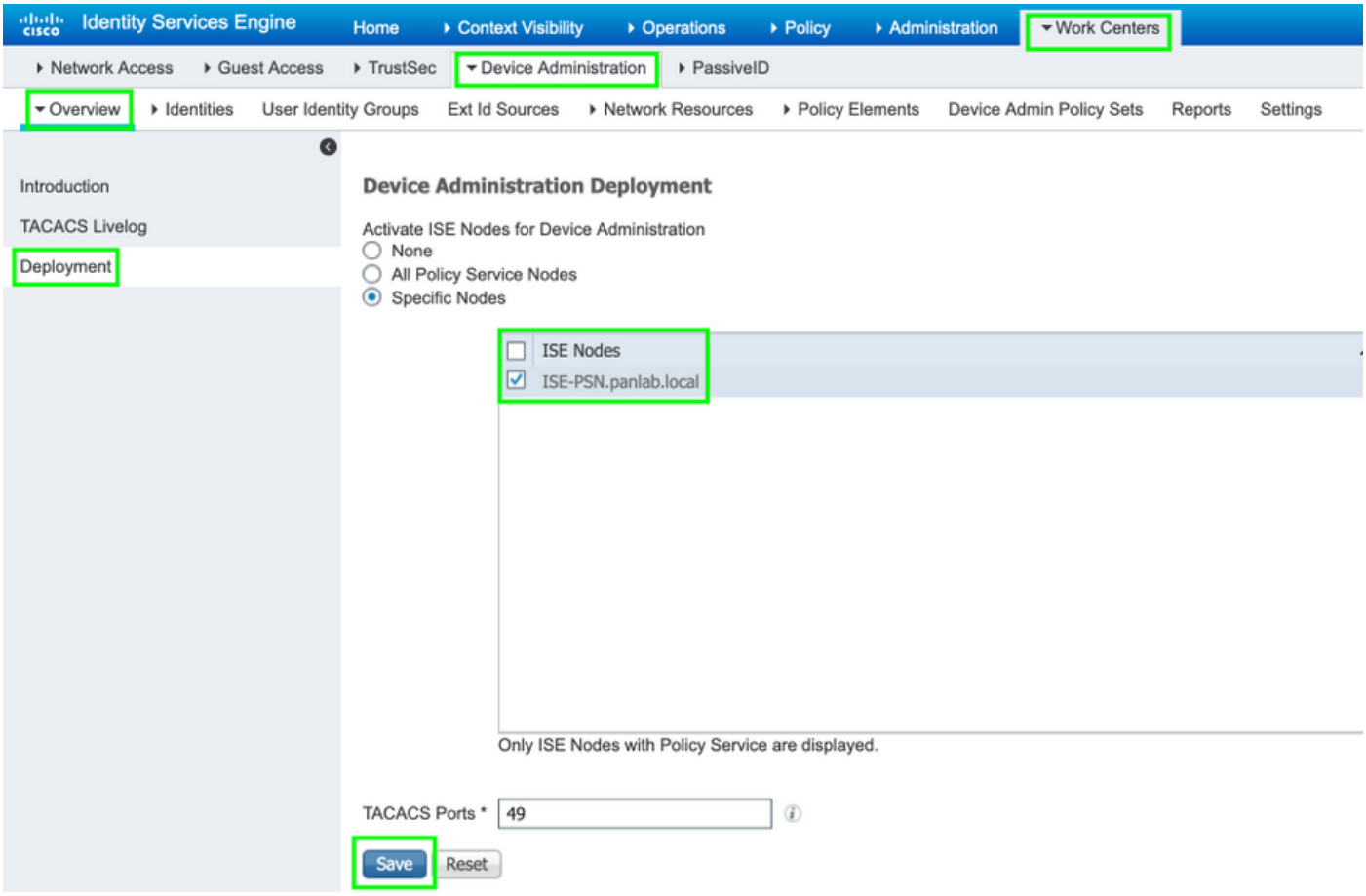
导航至**管理>系统>许可**选项卡并验**证设**备管理许可证是否已安装，如图所示。



注意：在ISE上使用TACACS+功能需要设备管理许可证。

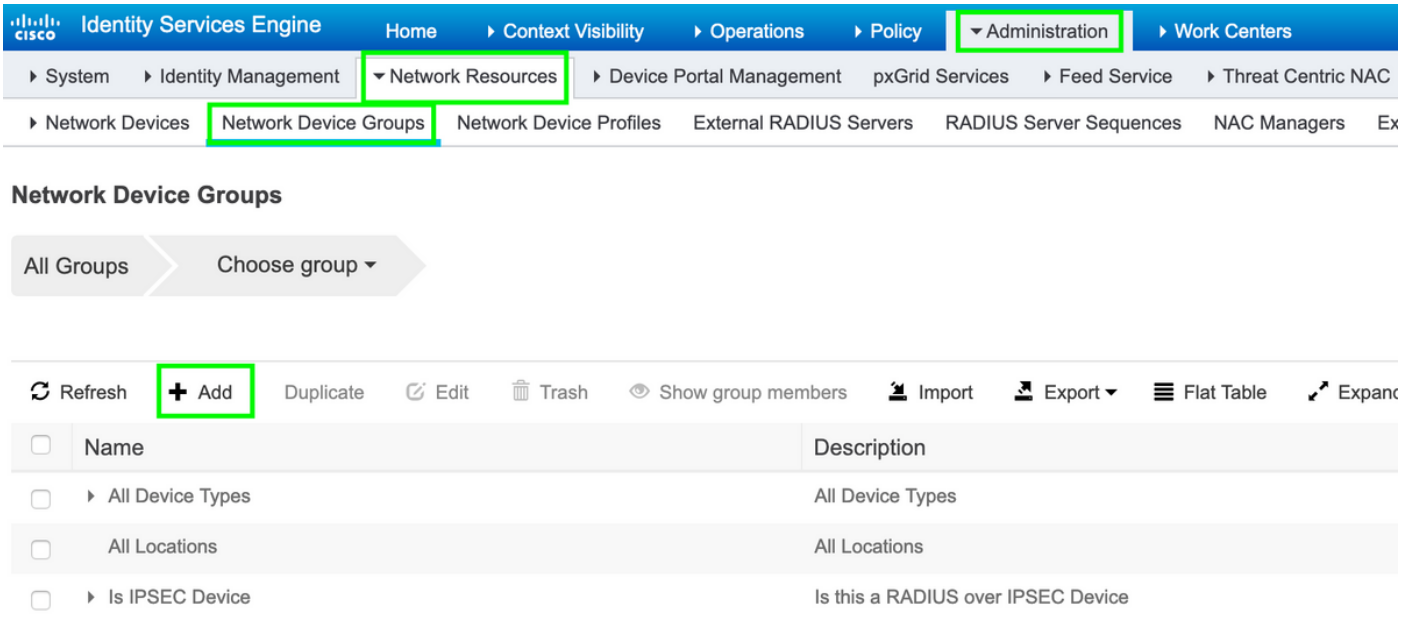
步骤2.在ISE PSN节点上启用设备管理。

导航至工**作中心>设备管理>概述**，单击**部署**选项卡，**选**择**特定PSN节点单选按钮。通**过选中复选框并单击**保存**，在ISE节点上启用设备管理：



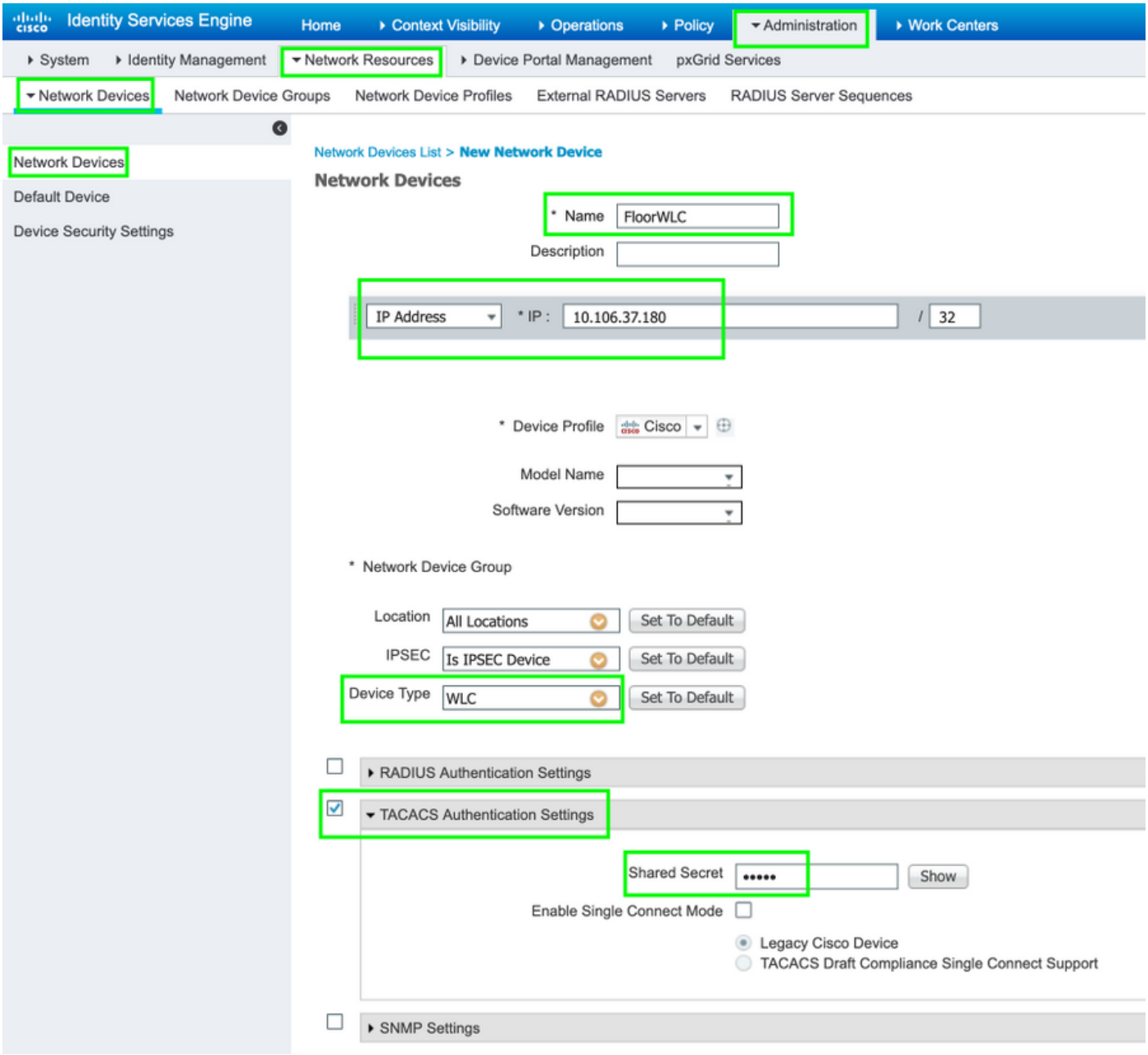
步骤3.创建网络设备组。

要在ISE上将WLC添加为网络设备，请导航到**管理>网络资源>网络设备组> 所有设备类**型，为WLC创建**新**组，如图所示：



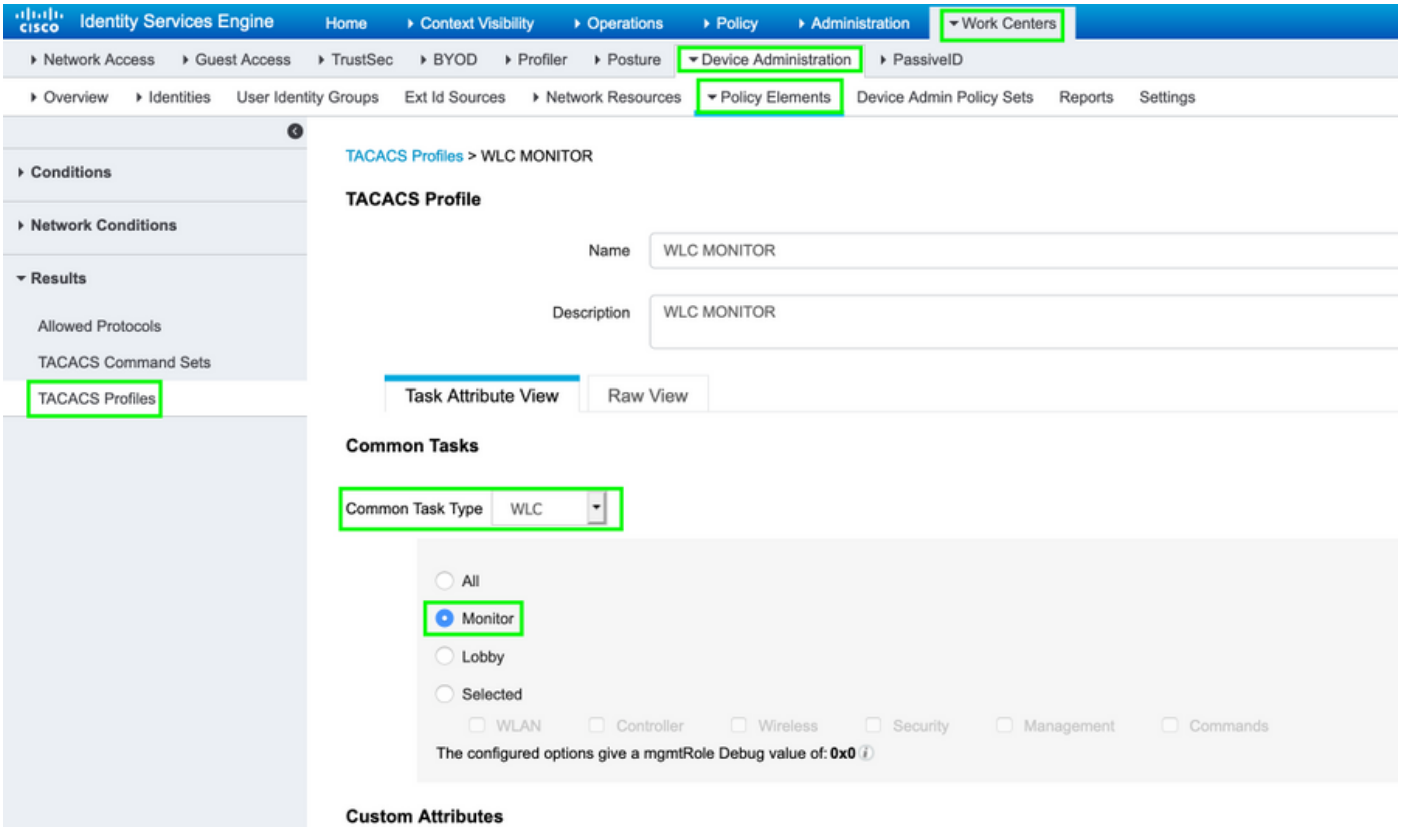
步骤4.将WLC添加为网络设备。

导航至工**作中心(Work Centers)>设备管理(Device Administration)>网络资源(Network Resources)>网络设备(Network Devices)**。单击Add，提供名称、IP地址并选择设备类型**为WLC**，选中TACACS+ Authentication Settings复选框并提供Shared Secret密钥，如图所示：

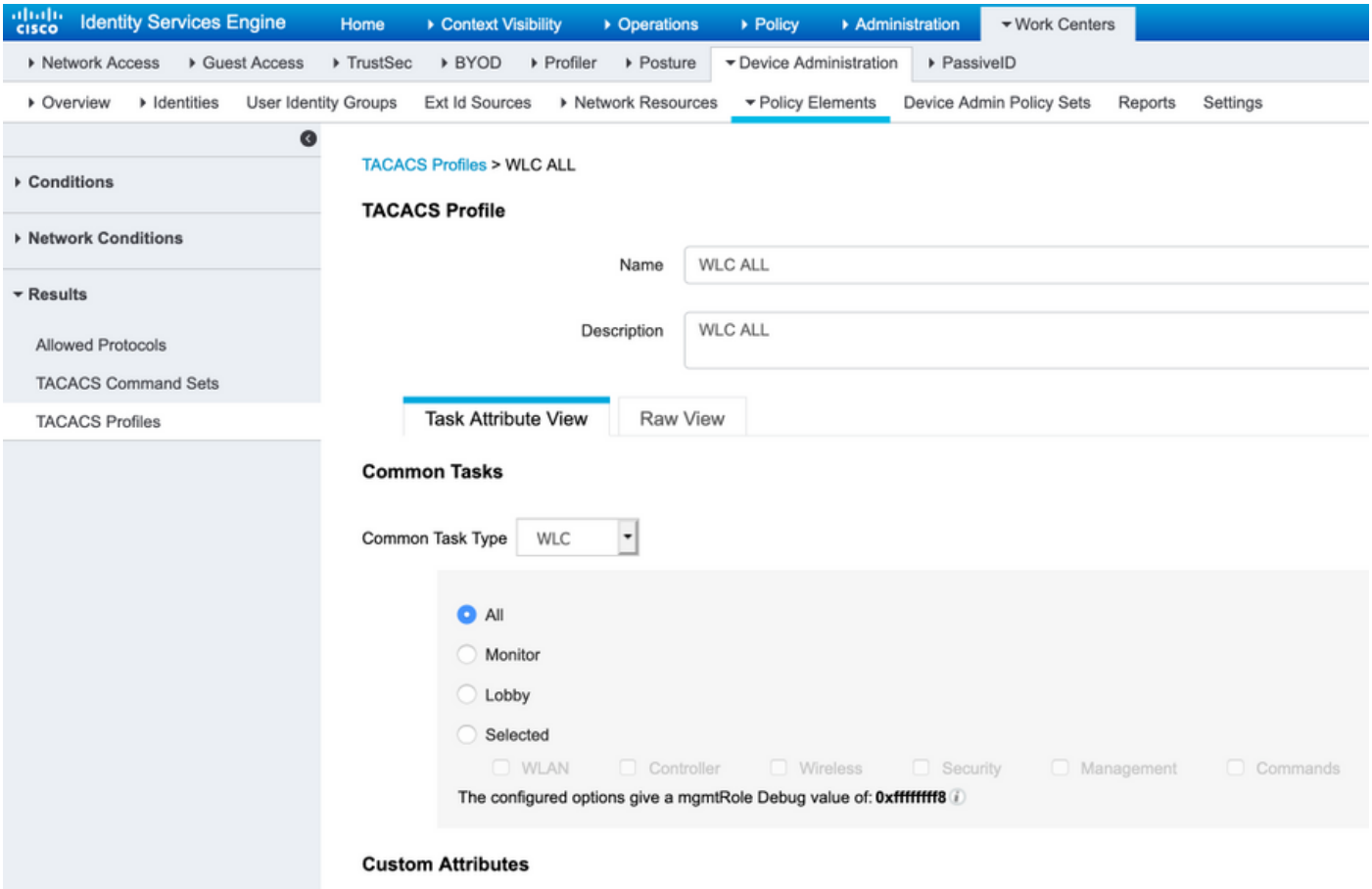


步骤5.为WLC创建TACACS配置文件。

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**并提供**Name。**在“任**务属性**视图”选项卡中，为**公用任务类型**选择**WLC。**存在默认配置文件，从中选择“监控”以允许对用户进行有限访问，如图所示。

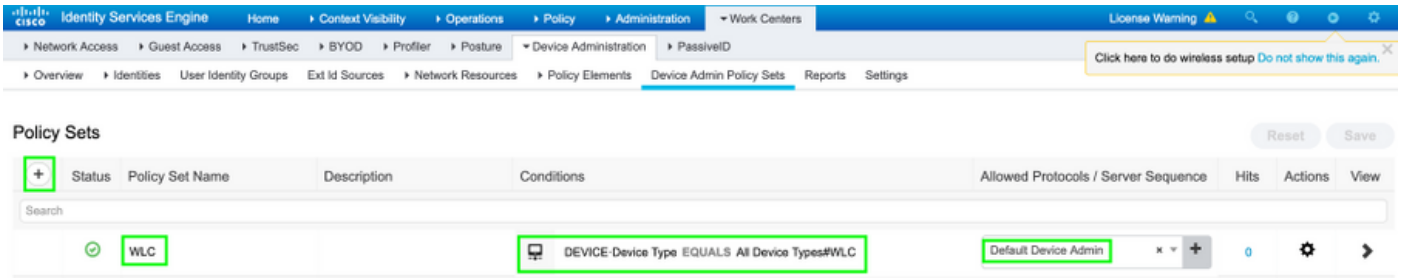


另有一个默认配置文件All，允许对用户进行完全访问，如图所示。



步骤6.创建策略集。

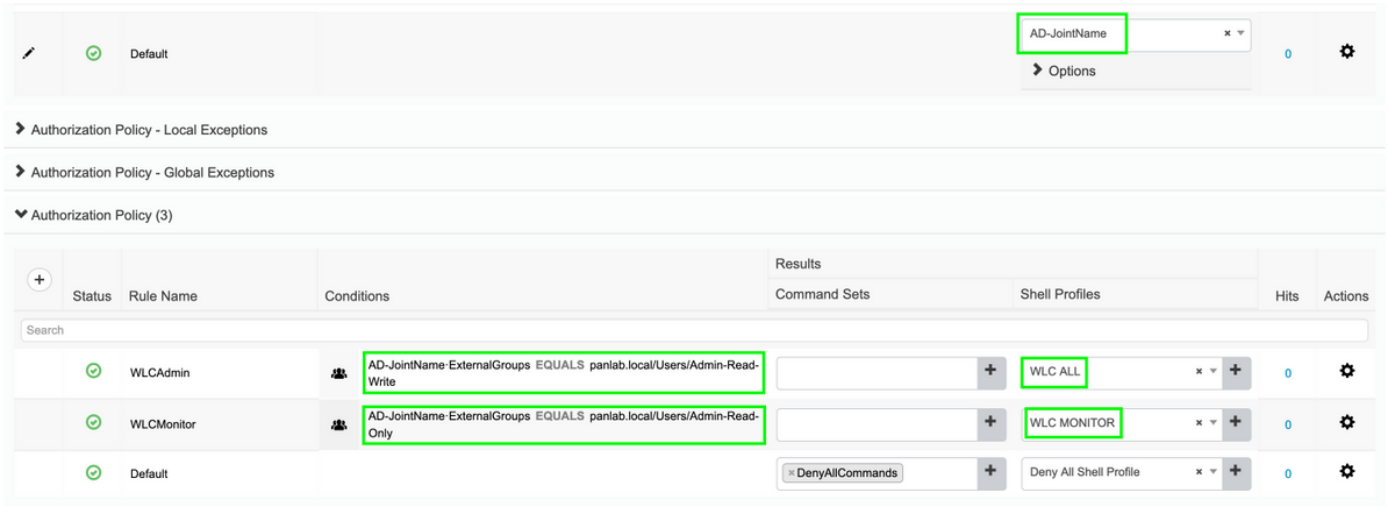
导航至**工作中心>设备管理>设备管理策略集。单**击**(+)**并为策略集指定名称。在策略条件中，选**择Device Type** as WLC，Allowed protocols可以**是Default Device Admin**，如图所示。



步骤7.创建身份验证和授权策略。

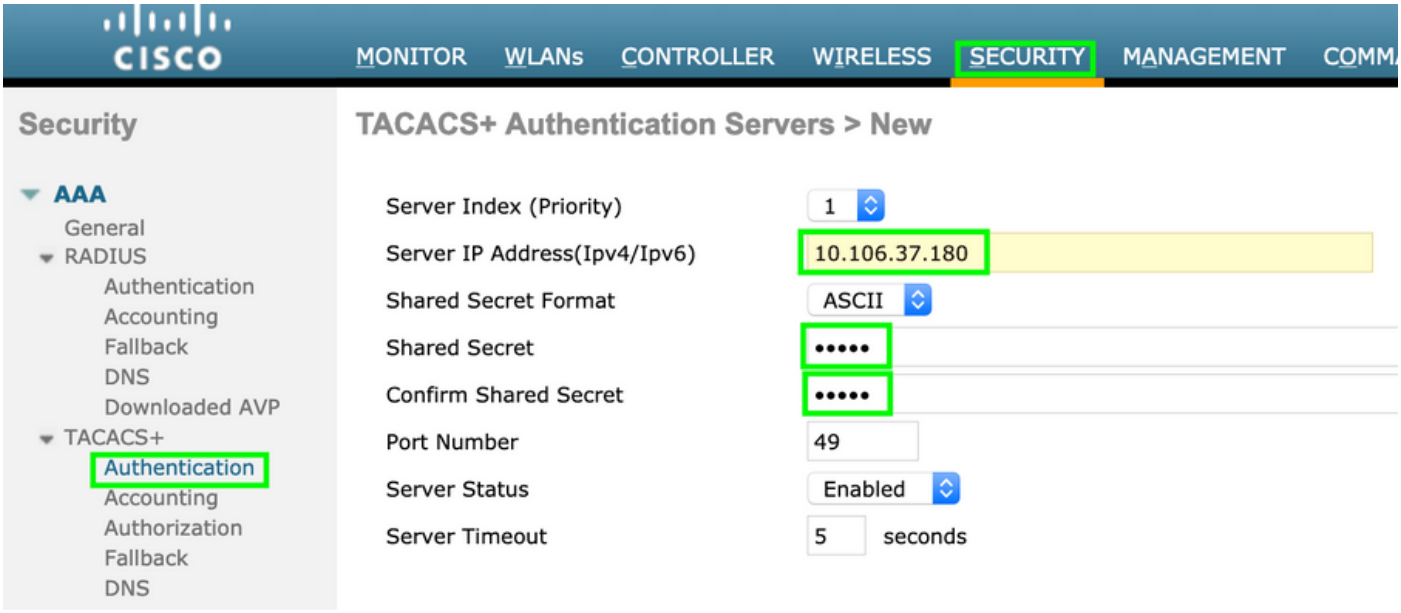
在本文档中，在Active Directory上配置了**Admin-Read-Write**和**Admin-Read-Only**两个示例组，每个组内分别配置了一个用户，每个组内分别配置了**admin1** 和**admin2**。Active Directory通过名为AD-JointName的加入点与**ISE集成。**

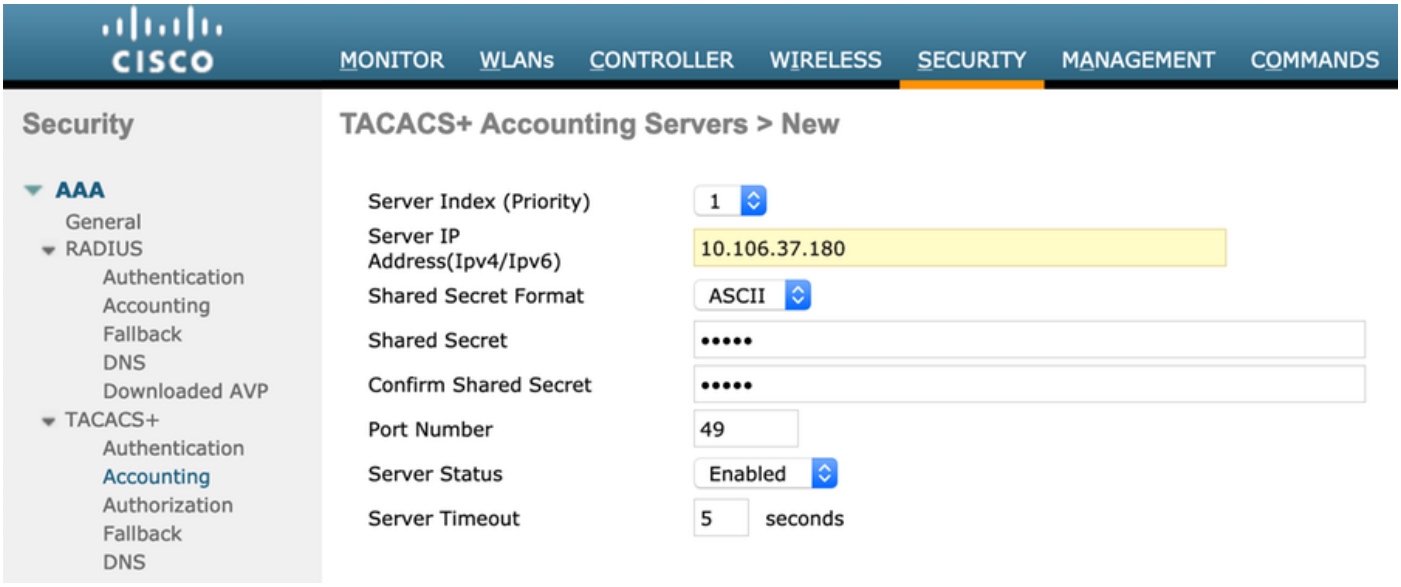
创建两个授权策略，如图所示：



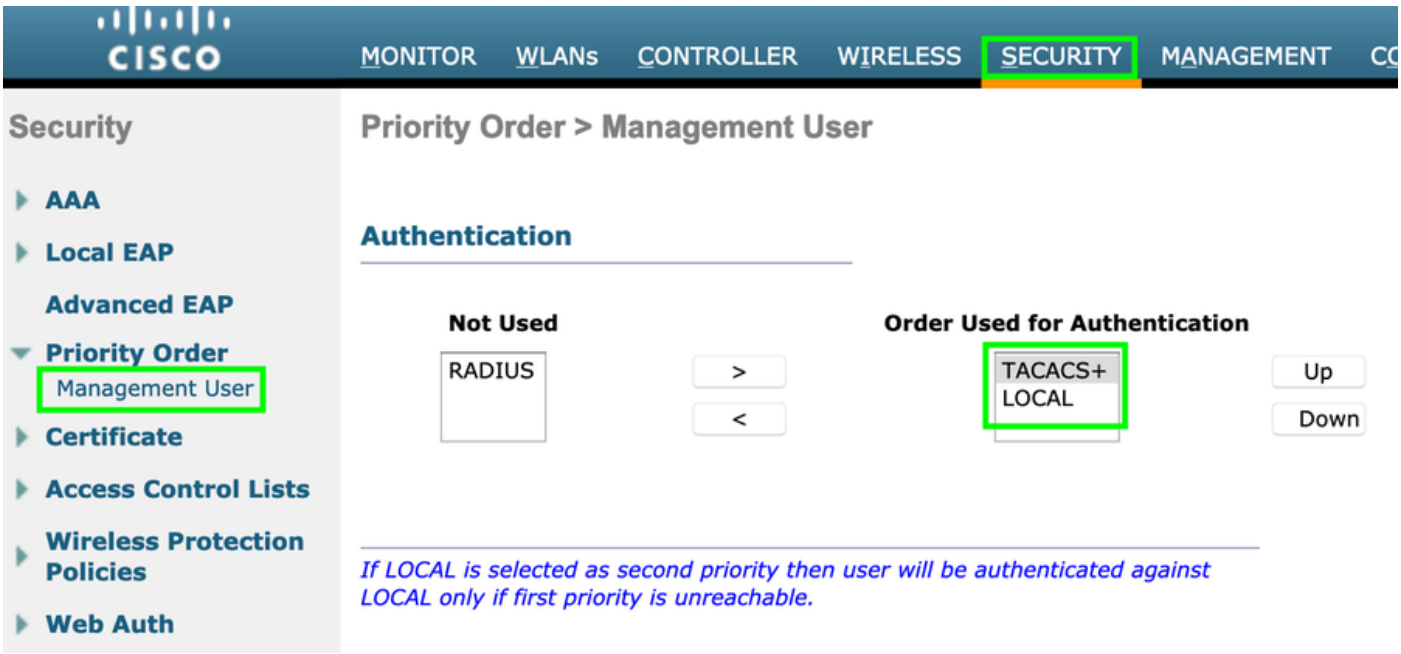
步骤8.为设备管理配置WLC。

导航至**Security > AAA > TACACS+**单击**New**并添加Authentication， Accounting server，如图所示。





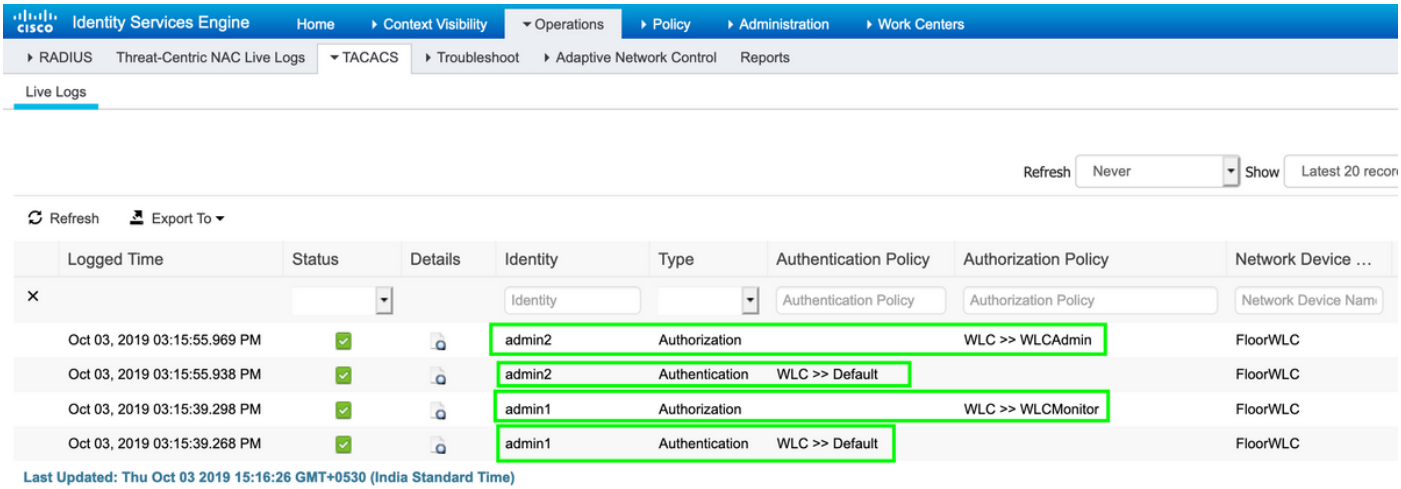
更改优先级顺序，使TACACS+位于顶部，使TACACS+位于本地到底部，如图所示：



警告：请勿关闭当前WLC GUI会话。建议在不同的Web浏览器中打开WLC GUI，并检查是否使用TACACS+凭证登录。否则，请检验TCP端口49上的配置和与ISE节点的连接。

验证

导航至**操作> TACACS >实时日志**并监控实**时日志**。打开WLC GUI并使用Active Directory用户凭证登录，如图所示



故障排除

目前没有针对此配置的故障排除信息。