

使用TACACS+管理Cisco WLC的设备

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[步骤1.检查Device Administration License。](#)

[步骤2.在ISE PSN节点上启用设备管理。](#)

[步骤3.创建网络设备组。](#)

[步骤4.将WLC添加为网络设备。](#)

[步骤5.为WLC创建TACACS配置文件。](#)

[步骤6.创建策略集。](#)

[步骤7.创建身份验证和授权策略。](#)

[步骤8.为设备管理配置WLC。](#)

[验证](#)

[故障排除](#)

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。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. The main content area shows the 'Licensing' tab selected, indicating that 'Traditional Licensing' is currently in use. Below this, there is a section for 'License Usage' with a bar chart showing 'Licensed :100 (Consumed :0)'. The chart is categorized into 'Advanced' (Base, Plus, Apex) and 'Current Usage'. A legend at the bottom indicates 'Licensed' (gray), 'Consumed' (blue), and 'Exceeded' (red). The 'Licenses' section below the chart displays a table of installed licenses:

License File	Quantity	Term	Expiration Date
POSITRONFEAT20190820025931403.lic			
Base	100	Term	19-Aug-2020 (365 days remaining)
POSITRONFEAT20190820025911402.lic			
Device Admin	50	Term	19-Aug-2020 (365 days remaining)

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：

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

Device Administration Deployment

Activate ISE Nodes for Device Administration

None
 All Policy Service Nodes
 Specific Nodes

ISE Nodes
<input checked="" type="checkbox"/> ISE-PSN.panlab.local

Only ISE Nodes with Policy Service are displayed.

TACACS Ports *

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：

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > Ex

Network Device Groups

All Groups > Choose group ▾

Refresh Duplicate Edit Trash Show group members Import Export ▾ Flat Table Expand

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▶ All Device Types	All Device Types
<input type="checkbox"/>	All Locations	All Locations
<input type="checkbox"/>	▶ Is IPSEC Device	Is this a RADIUS over IPSEC Device

Add Group

Name *

WLC

Description

Parent Group *

All Device Types

Cancel

Save

步骤4.将WLC添加为网络设备。

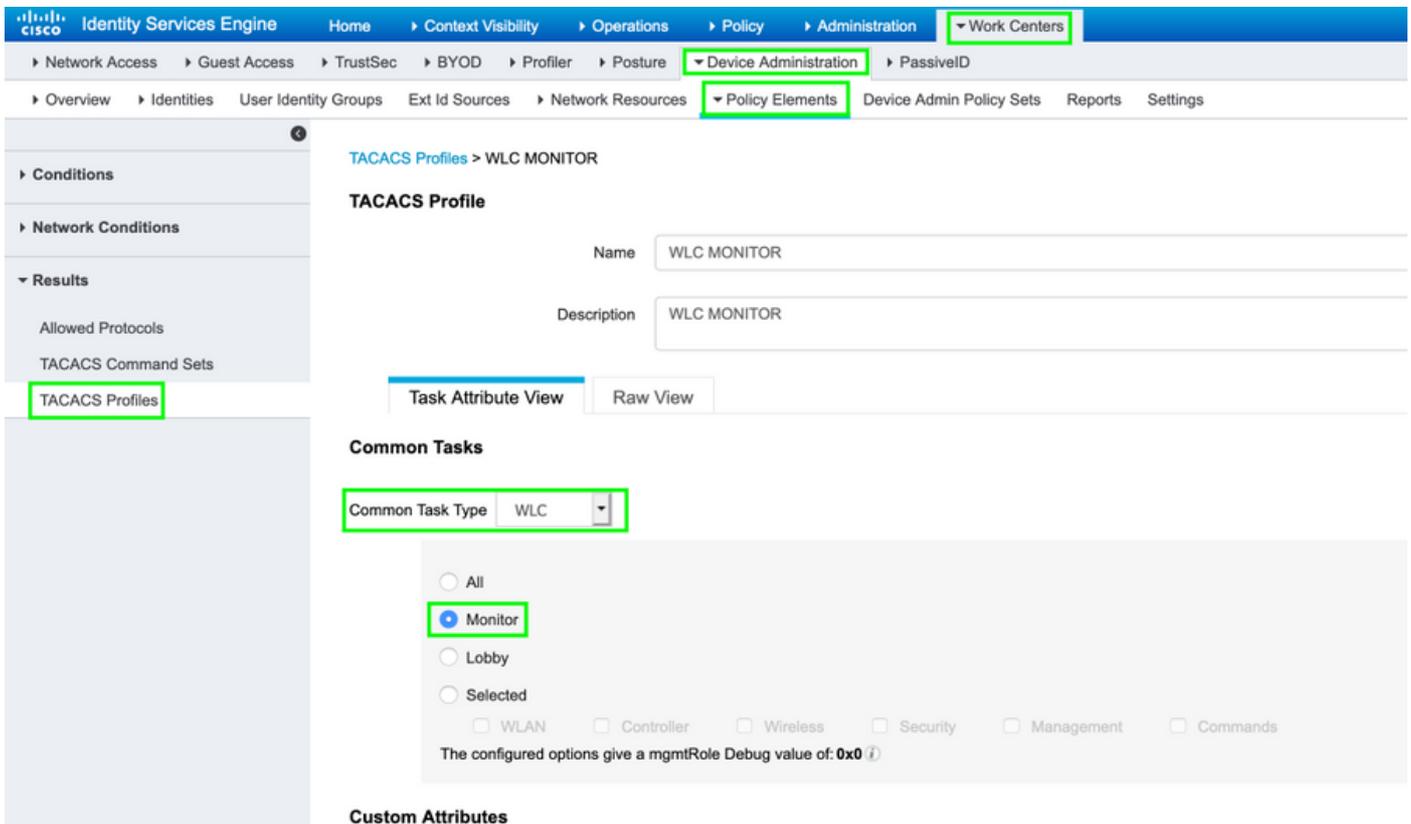
导航至工作中心(Work Centers)>设备管理(Device Administration)>网络资源(Network Resources)>网络设备(Network Devices)。单击Add，提供名称、IP地址并选择设备类型为WLC，选中TACACS+ Authentication Settings复选框并提供Shared Secret密钥，如图所示：

The screenshot displays the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Network Devices. The left sidebar shows 'Network Devices' selected. The main content area is titled 'Network Devices' and 'New Network Device'. The configuration fields are as follows:

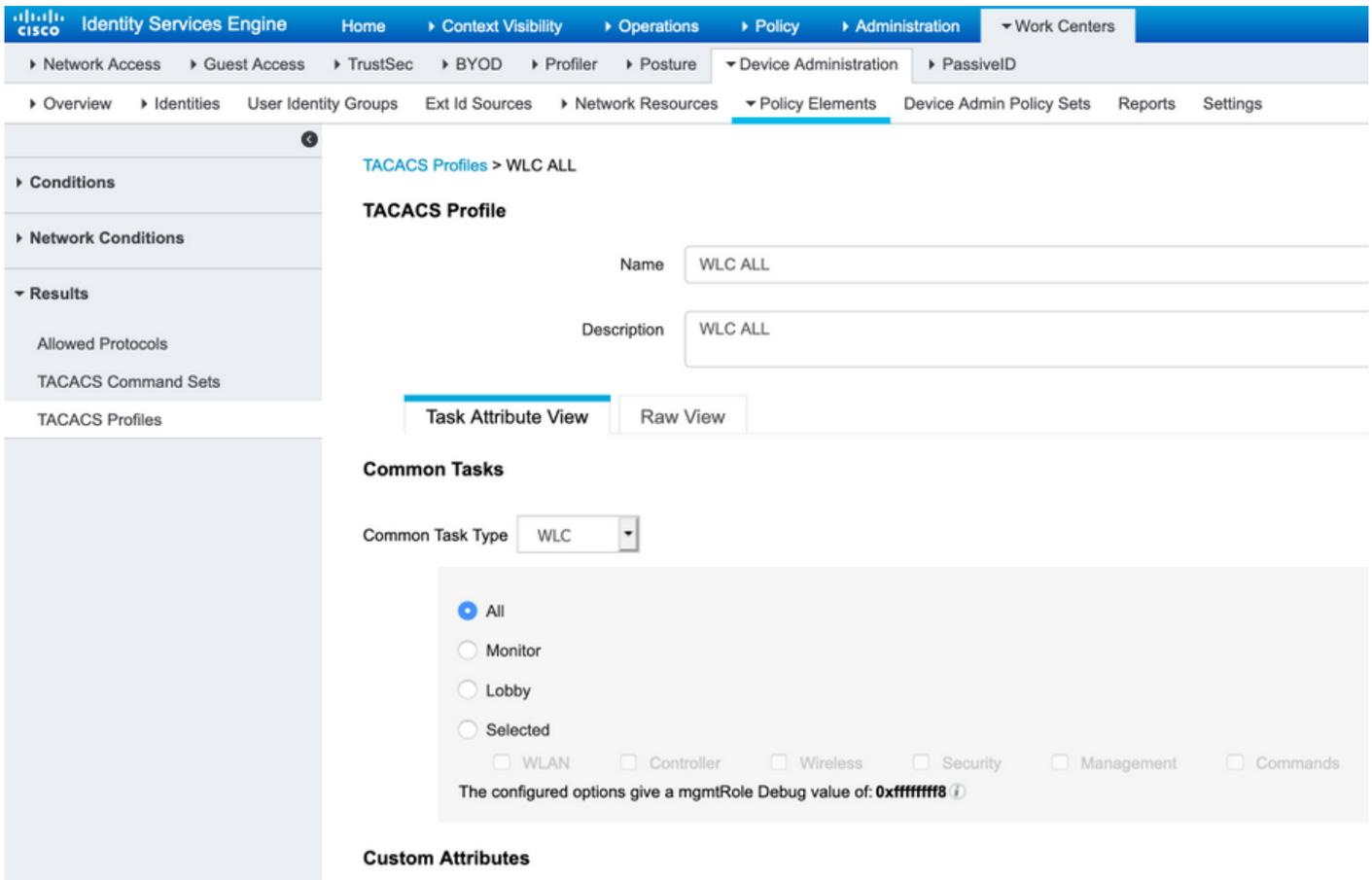
- Name:** FloorWLC
- Description:** (empty)
- IP Address:** 10.106.37.180 / 32
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
 - Location:** All Locations (Set To Default)
 - IPSEC:** Is IPSEC Device (Set To Default)
 - Device Type:** WLC (Set To Default)
- RADIUS Authentication Settings:** (unchecked)
- TACACS Authentication Settings:** (checked)
 - Shared Secret:** (masked with dots, Show button)
 - Enable Single Connect Mode:** (unchecked)
 - Legacy Cisco Device:** (selected)
 - TACACS Draft Compliance Single Connect Support:** (unchecked)
- SNMP Settings:** (unchecked)

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。

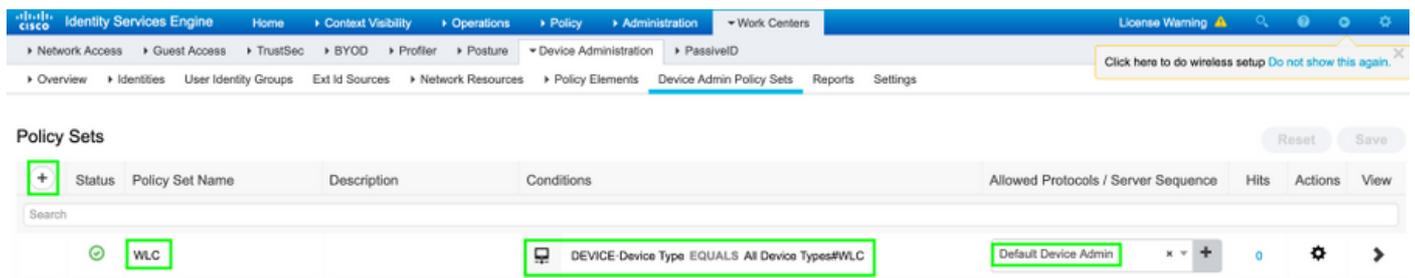


另有一个默认配置文件All，允许对用户进行完全访问，如图所示。



步骤6.创建策略集。

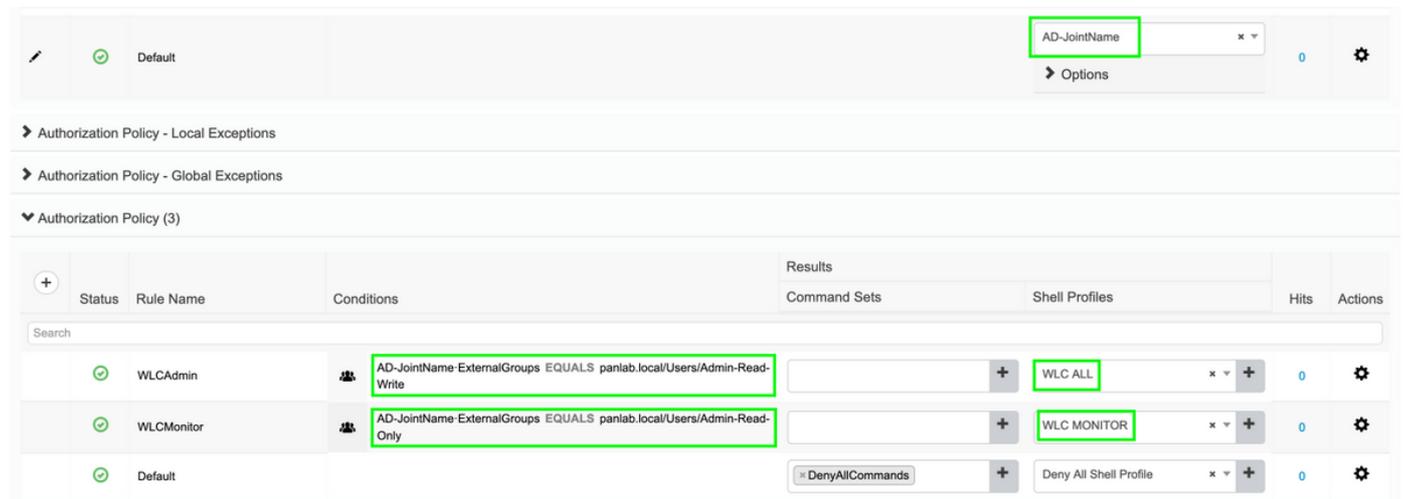
导航至**工作中心>设备管理>设备管理策略集**。单击(+)并为策略集指定名称。在策略条件中，选择**Device Type as WLC**，Allowed protocols可以是**Default Device Admin**，如图所示。



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。

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMM

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - Authentication**
 - Accounting
 - Authorization
 - Fallback
 - DNS

TACACS+ Authentication Servers > New

Server Index (Priority)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server Timeout seconds

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - Authentication
 - Accounting**
 - Authorization
 - Fallback
 - DNS

TACACS+ Accounting Servers > New

Server Index (Priority)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server Timeout seconds

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：

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT CO

Security

- AAA
- Local EAP
- Advanced EAP
- Priority Order**
 - Management User**
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth

Priority Order > Management User

Authentication

Not Used		Order Used for Authentication	
<input type="text" value="RADIUS"/>	>	<input type="text" value="TACACS+ LOCAL"/>	Up
	<		Down

If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.

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

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Network Device ...
Oct 03, 2019 03:15:55.969 PM	✓		admin2	Authorization	WLC >> WLCAdmin		FloorWLC
Oct 03, 2019 03:15:55.938 PM	✓		admin2	Authentication	WLC >> Default		FloorWLC
Oct 03, 2019 03:15:39.298 PM	✓		admin1	Authorization	WLC >> WLCMonitor		FloorWLC
Oct 03, 2019 03:15:39.268 PM	✓		admin1	Authentication	WLC >> Default		FloorWLC

Last Updated: Thu Oct 03 2019 15:16:26 GMT+0530 (India Standard Time)

故障排除

目前没有针对此配置的故障排除信息。