

在Catalyst 9800无线控制器系列上配置802.1X身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[WLC 配置](#)

[9800 WLC上的AAA配置](#)

[WLAN配置文件配置](#)

[策略配置文件配置](#)

[策略标签配置](#)

[策略标记分配](#)

[ISE 配置](#)

[声明WLC on ISE](#)

[在ISE上创建新用户](#)

[创建授权配置文件](#)

[创建策略集](#)

[创建身份验证策略](#)

[创建授权策略](#)

[验证](#)

[故障排除](#)

[排除WLC故障](#)

[对ISE进行故障排除](#)

简介

本文档介绍如何在Cisco Catalyst 9800系列无线控制器上设置具有802.1X安全性的WLAN。

先决条件

要求

Cisco 建议您了解以下主题：

- 802.1X

使用的组件

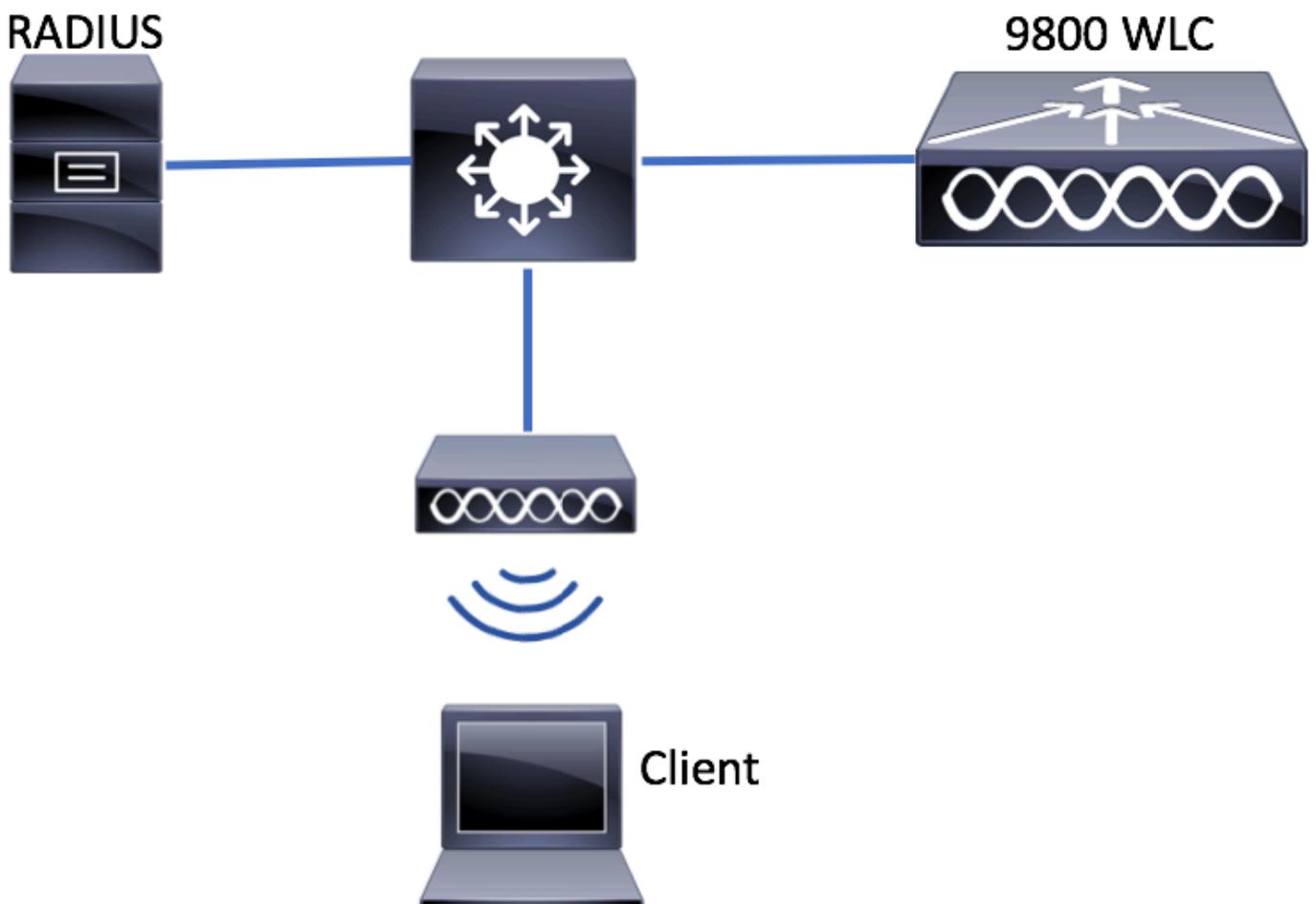
本文档中的信息基于以下软件和硬件版本：

- Catalyst 9800无线控制器系列(Catalyst 9800-CL)
- 思科IOS® XE直布罗陀17.3.x
- 思科ISE 3.0

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。

配置

网络图

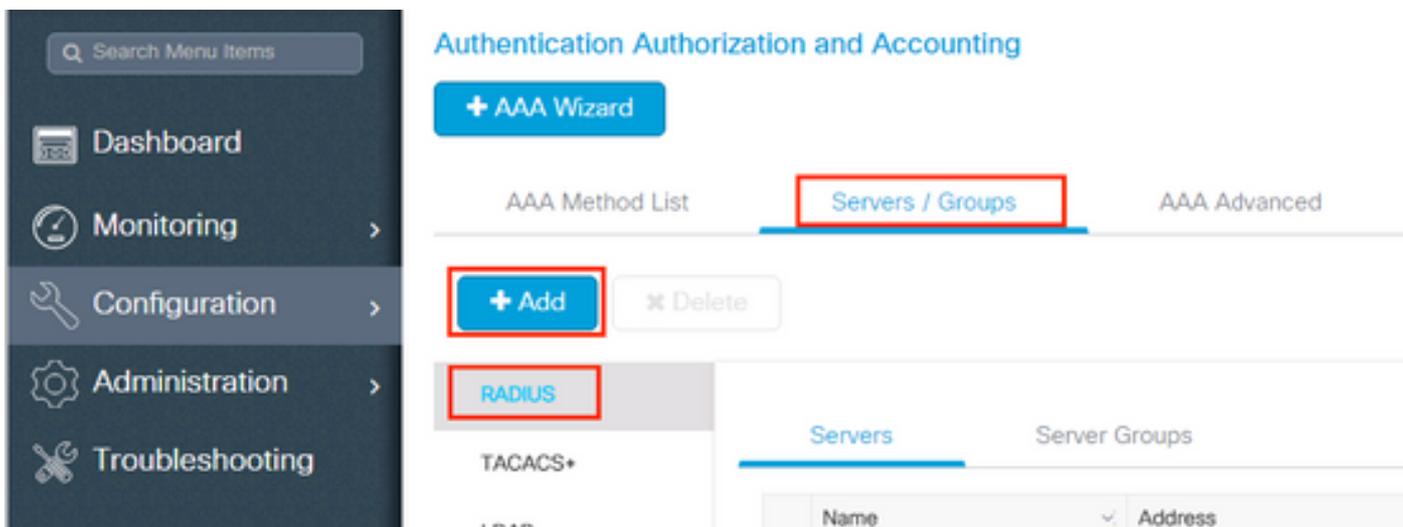


WLC 配置

9800 WLC上的AAA配置

GUI:

步骤1:声明RADIUS服务器。导航到 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** 并输入RADIUS服务器信息。



如果计划将来使用集中式Web身份验证（或任何需要授权更改[CoA]的安全类型），请确保启用支持CoA。

Create AAA Radius Server ✕

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

第二步：将RADIUS服务器添加到RADIUS组。导航至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**。为您的组指定名称并移动您之前在列表中创建的服务器 Assigned Servers。

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

第三步：创建身份验证方法列表。导航至 **Configuration > Security > AAA > AAA Method List > Authentication > + Add**。

The screenshot shows the 'Authentication Authorization and Accounting' configuration page. On the left is a dark sidebar with menu items: 'Dashboard', 'Monitoring', 'Configuration' (highlighted with a red box), and 'Administration'. The main content area has a search bar and a '+ AAA Wizard' button. Below that, 'AAA Method List' is highlighted with a red box. Underneath, the 'Authentication' tab is selected and highlighted with a red box. To the right of the 'Authentication' tab, a '+ Add' button is highlighted with a red box. A table with a 'Name' column is partially visible at the bottom.

输入相关信息:

Quick Setup: AAA Authentication

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

CLI :

```
# config t # aaa new-model # radius server <radius-server-name> # address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813 # timeout 300 # retransmit 3
# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

有关AAA失效服务器检测的注意事项

配置RADIUS服务器之后，可以检查它是否被视为“ALIVE”：

```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC (2) : current
```

可以在WLC上配置 **dead criteria**, 和 **deadtime** ，特别是在使用多个RADIUS服务器的情况下。

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

注意： **dead criteria** 是用于将RADIUS服务器标记为停机的条件。它包括：1.超时(秒)，表示从控制器上次从RADIUS服务器收到有效数据包到服务器标记为失效之间必须经过的时间。2.一个计数器，表示在RADIUS服务器标记为失效之前控制器上必须发生的连续超时次数。

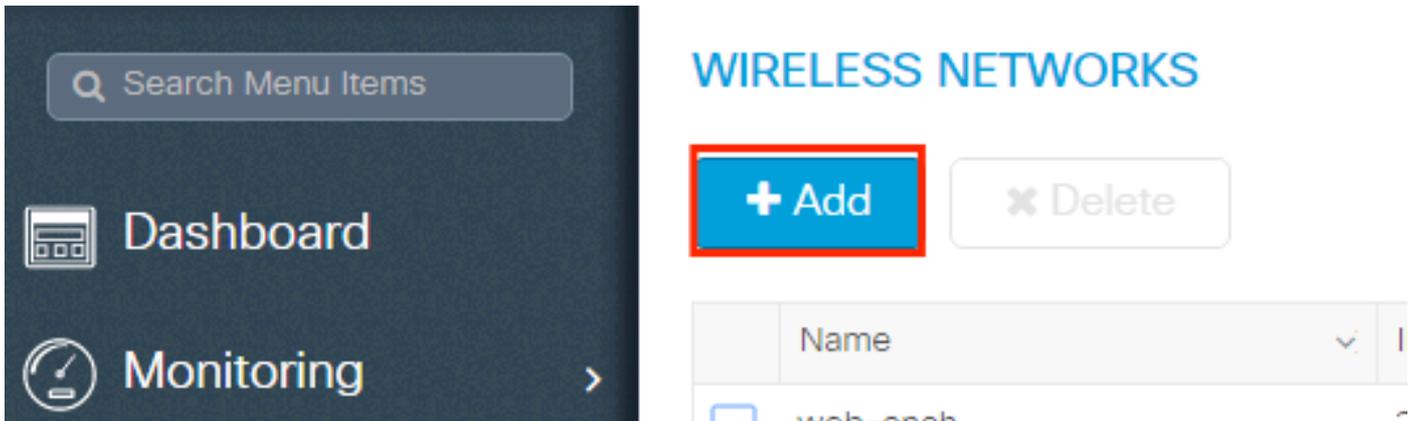
注： **deadtime**指定在失效条件将其标记为失效后，服务器保持失效状态的时间（以分钟为单位）。一旦死区时间过期，控制

 器会将服务器标记为UP (ALIVE)，并通知注册的客户端状态更改。如果在状态标记为UP后服务器仍然无法访问，并且满足dead条件，则在死区间隔内服务器将再次标记为已死。

WLAN配置文件配置

GUI:

步骤1:创建WLAN。导航到**Configuration > Wireless > WLANs > + Add**，然后根据需要配置网络。



第二步：输入无线局域网信息

Add WLAN

General Security Advanced

Profile Name*	<input type="text" value="prof-name"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="1"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

第三步：导航到安全选项卡并选择所需的安全方法。在本示例中，WPA2 + 802.1x。

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Protected Management Frame

Fast Transition Adaptive Enab... ▼

Over the DS

Reassociation Timeout 20

PMF Disabled ▼

WPA Parameters

WPA Policy

Add WLAN ✕

PMF Disabled ▼

WPA Parameters

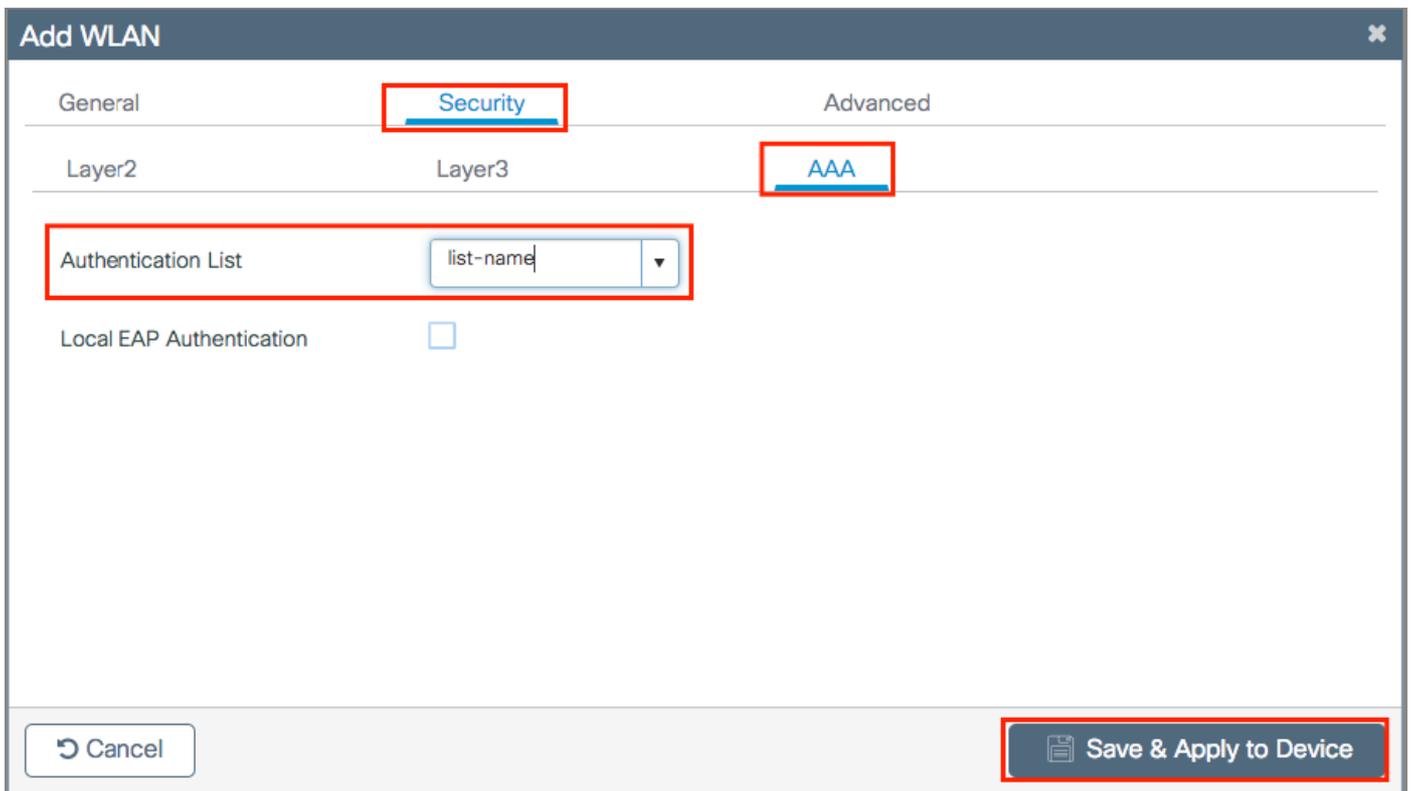
WPA Policy

WPA2 Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x ▼

第四步：从 Security > AAA 选项卡中，从9800 WLC上的AAA配置部分选择第3步中创建的身份验证方法。



CLI :

```
# config t # wlan <profile-name> <wlan-id> <ssid-name> # security dot1x authentication-list <dot1x-list-name> # no shutdown
```

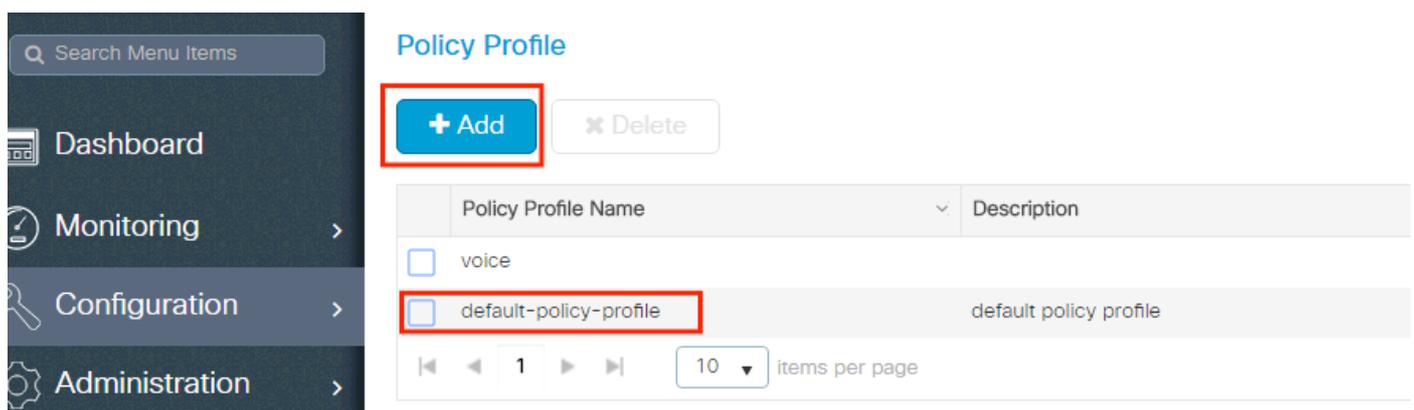
策略配置文件配置

在策略配置文件中，您可以决定将客户端分配到哪个VLAN，以及其他设置（如访问控制列表[ACL]、服务质量[QoS]、移动锚点、计时器等）。

您可以使用默认策略配置文件，也可以创建新配置文件。

GUI:

导航到配置> 标签和配置文件> 策略配置文件，然后配置默认策略配置文件或创建新配置文件。



确保已启用配置文件。

此外，如果您的接入点(AP)处于本地模式，请确保策略配置文件已启用集中交换和集中身份验证。

Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	default-policy-profile	WLAN Switching Policy Central Switching <input checked="" type="checkbox"/> Central Authentication <input checked="" type="checkbox"/> Central DHCP <input checked="" type="checkbox"/> Central Association Enable <input checked="" type="checkbox"/> Flex NAT/PAT <input type="checkbox"/>
Description	default policy profile	
Status	ENABLED <input checked="" type="checkbox"/>	
Passive Client	<input type="checkbox"/> DISABLED	
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	
CTS Policy		
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	2-65519	

在访问策略选项卡中选择需要将客户端分配到的VLAN。

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2602



Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select



IPv6 ACL

Search or Select



URL Filters

Pre Auth

Search or Select



Post Auth

Search or Select



如果计划让ISE返回属性在Access-Accept like VLAN Assignment中，请在 **Advanced** 选项卡中启用AAA覆盖：

Edit Policy Profile
✕

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy [Clear](#)

WLAN Flex Policy

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

AAA Policy

Allow AAA Override

NAC State

Policy Name

2.4 GHz Policy

5 GHz Policy

↶ Cancel

↶ Update & Apply to Device

CLI :

```
# config # wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> # no shutdown
```

策略标签配置

策略标记用于将SSID与策略配置文件关联起来。您可以新建策略标签，也可以使用 default-policy 标签。

注意： default-policy-tag会自动将WLAN ID介于1和16之间的所有SSID映射到default-policy-profile。不能修改或删除。如果您拥有的WLAN的ID为17或更高，则不能使用default-policy-tag。

GUI:

如果需要，请导航到 **Configuration > Tags & Profiles > Tags > Policy** 并添加新设备。

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

Manage Tags

Policy Site RF AP

+ Add **✕ Delete**

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

将 WLAN 配置文件关联到所需的策略配置文件。

Add Policy Tag

Name*

Description

+ Add **✕ Delete**

WLAN Profile Policy Profile

0 10 items per page No items to display

Cancel **Save & Apply to Device**

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile*

Policy Profile*

✕
✓

↶ Cancel
Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile

◀ ◁ 1 ▷ ▶ 10 items per page 1 - 1 of 1 items

↶ Cancel
Save & Apply to Device

CLI :

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

策略标记分配

将策略标签分配给所需的 AP。

GUI:

要将标签分配给一个AP，请导航至 **Configuration > Wireless > Access Points > AP Name > General Tags**, 分配相关策略标签，然后点击 **Update & Apply to Device**。

Edit AP

General | Interfaces | High Availability | Inventory | Advanced

General		Version	
AP Name*	AP3802-02-WS	Primary Software Version	10.0.200.50
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	00:42:68:c6:41:20	Predownloaded Version	N/A
Ethernet MAC	00:42:68:a0:d0:22	Next Retry Time	N/A
Admin Status	Enabled	Boot Version	1.0.0
AP Mode	Local	IOS Version	10.0.200.52
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled		

Tags

Policy	default-policy-tag
Site	default-site-tag
RF	default-rf-tag

IP Config

IP Address	172.16.0.207
Static IP	<input type="checkbox"/>

Time Statistics

Up Time	9 days 1 hrs 17 mins 24 secs
Controller Associated Time	0 days 3 hrs 26 mins 41 secs
Controller Association Latency	8 days 21 hrs 50 mins 33 secs

Cancel | **Update & Apply to Device**

注意： 请注意，当AP上的策略标记更改时，它将断开与9800 WLC的关联，并在稍后重新加入。

要将相同的策略标签分配给多个AP，请导航至 **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Start Now →



Flex Profile



Site Tag



RF Profile



RF Tag



Apply



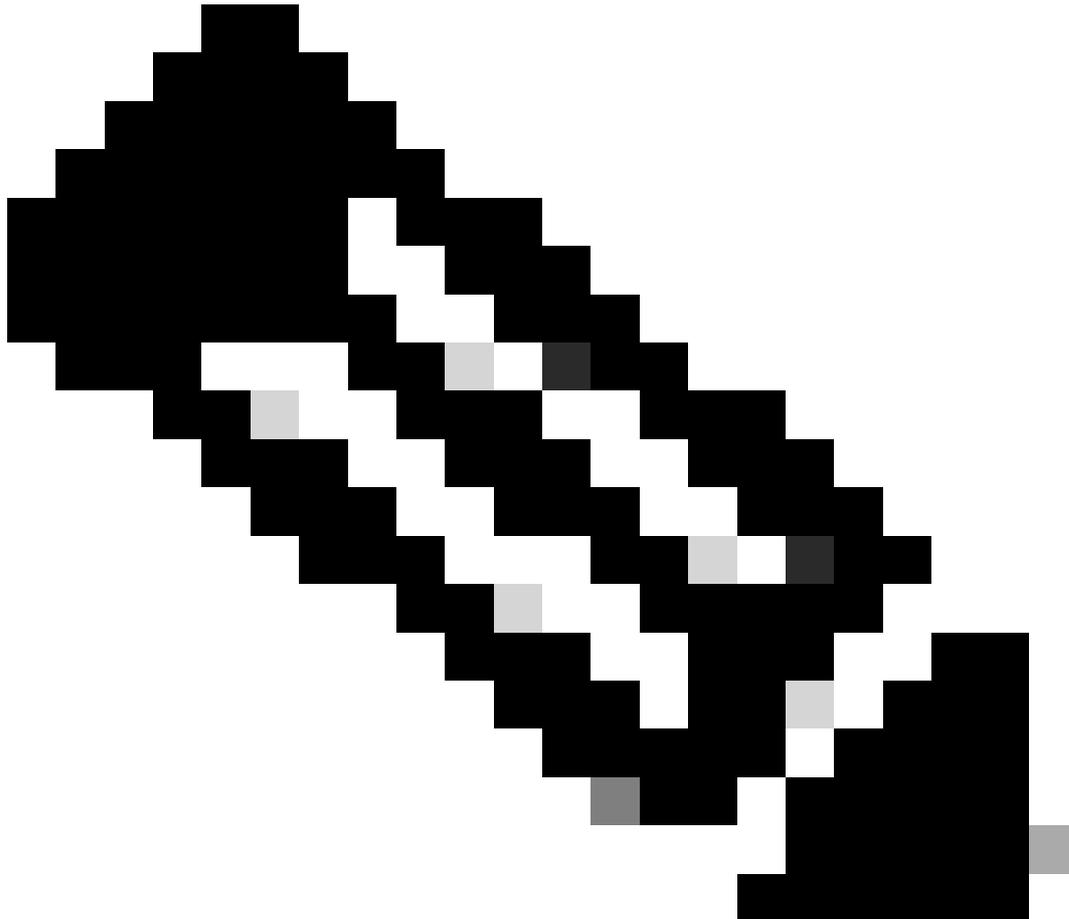
Tag APs



Done

```
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name> // Detailed information on given policy profile
```

故障排除



注意：外部负载均衡器的使用正常。但是，使用calling-station-id RADIUS属性确保您的负载均衡器按客户端运行。依赖UDP源端口不是平衡来自9800的RADIUS请求的受支持机制。

排除WLC故障

WLC 9800提供无间断跟踪功能。这样可以确保始终记录所有客户端连接相关的错误、警告和通知级别消息，并且可以在发生事故或故障情况后查看日志。

这取决于生成的日志量，但通常情况下，您可以返回几小时到几天。

要查看9800 WLC在默认情况下收集的跟踪，可以通过SSH/Telnet连接到9800 WLC并执行以下步骤：（确保将会话记录到文本文件）。

步骤1:检查WLC当前时间，以便您可以在问题发生之前跟踪登录时间。

```
# show clock
```

第二步：根据系统配置的指示，从WLC缓冲区或外部系统日志收集系统日志。这样可以快速查看系统运行状况和错误（如有）。

```
# show logging
```

第三步：验证是否启用了任何调试条件。

```
# show debugging IOSXE Conditional Debug Configs: Conditional Debug Global State: Stop IOSXE Packet Tracing Configs: Packet Infra debugs: Ip Ad
```

 **注意：**如果看到列出了任何条件，则意味着遇到已启用条件（mac地址、ip地址等）的所有进程的跟踪都会记录到调试级别。这会增加日志量。因此，建议在非主动调试时清除所有条件。

第四步：假设测试中的mac地址未列为步骤3中的条件，收集特定mac地址的“永远在线”通知级别跟踪：

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

您可以显示会话中的内容，也可以将文件复制到外部TFTP服务器：

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

条件调试和无线电主动跟踪

如果永远在线跟踪不能为您提供足够的信息来确定所调查问题的触发因素，您可以启用条件调试并捕获无线活动(RA)跟踪，从而为与指定条件（本例中为客户端MAC地址）交互的所有进程提供调试级别跟踪。您可以通过GUI或CLI执行此操作。

CLI：

要启用条件调试，请执行以下步骤：

第五步：确保没有启用调试条件。

```
# clear platform condition all
```

第六步：启用要监控的无线客户端mac地址的调试条件。

此命令开始监控提供的mac地址达30分钟（1800秒）。您可以选择将此时间增加到2085978494秒。

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```



注意：要同时监控多个客户端，请对每个mac地址运行debug wireless mac <aaaa.bbbb.cccc>命令。



注意：您不会在终端会话中看到客户端活动的输出，因为所有内容都在内部缓冲以备日后查看。

步骤 7.重现要监控的问题或行为。

步骤 8如果在默认或配置的监控时间之前重现问题，请停止调试。

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

监控时间结束或无线网络调试停止后，9800 WLC 会生成一个本地文件，其名称为：

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤 9 收集 MAC 地址活动的文件。 可以将ra trace.log复制到外部服务器，也可以直接在屏幕上显示输出。

检查RA跟踪文件的名称：

```
# dir bootflash: | inc ra_trace
```

将文件复制到外部服务器：

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

显示内容：

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤 10如果根本原因仍不明显，请收集内部日志，这些日志是调试级别日志的更详细视图。您无需再次调试客户端，因为我们详细查看已收集和内部存储的调试日志。

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

 **注意：**此命令输出返回所有进程的所有日志级别的跟踪，而且非常大。在解析跟踪信息时如需帮助，请联系 Cisco TAC。

您可以将 ra-internal-FILENAME.txt 复制到外部服务器，也可以直接在屏幕上显示输出。

将文件复制到外部服务器：

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

显示内容：

```
# more bootflash:ra-internal-<FILENAME>.txt
```

步骤 11删除调试条件。

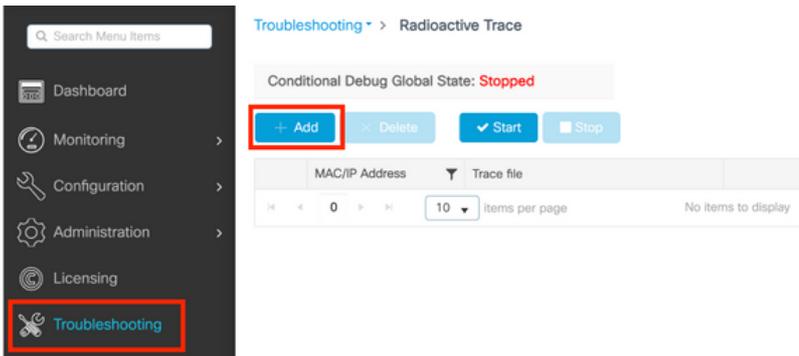
clear platform condition all



注意：请确保在故障排除会话之后始终删除调试条件。

GUI:

步骤1: 转到 **Troubleshooting > Radioactive Trace > + Add** 并指定要排除故障的客户端的MAC/IP地址。

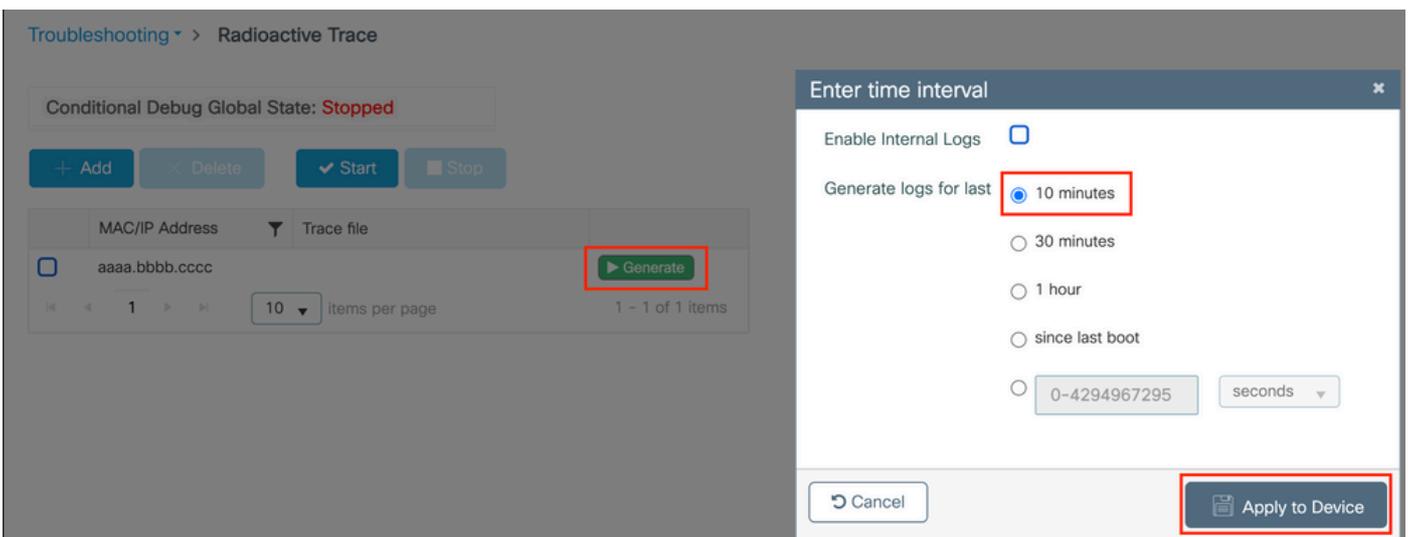


第二步：单击开始。

第三步：重现问题。

第四步：单击“停止”。

第五步：单击 **Generate** 按钮，选择要获取日志的时间间隔，然后单击 **Apply to Device**。In this example, the logs for the last 10 minutes are requested.



第六步：在计算机上下载放射性踪迹，然后单击“download (下载)”按钮并进行检查。

Conditional Debug Global State: **Stopped**

+ Add × Delete ✓ Start ■ Stop

MAC/IP Address	Trace file	
aaaa.bbbb.cccc	debugTrace_aaaa.bbbb.cccc.txt	 

10 items per page 1 - 1 of 1 items

Last Run Result

- ✓ State: Successful [See Details](#)
- MAC/IP Address: aaaa.bbbb.cccc
- Start Time: 08/24/2022 08:46:49
- End Time: 08/24/2022 08:47:00
- Trace file: debugTrace_aaaa.bbbb.cccc.txt 

对ISE进行故障排除

如果遇到客户端身份验证问题，您可以验证ISE服务器上的日志。转到 **Operations > RADIUS > Live Logs** 后，您将看到身份验证请求列表，以及匹配的策略集、每个请求的结果等。单击每行 **Details** 选项卡下的放大镜，可获取更多详细信息，如图所示：

Cisco ISE Operations · RADIUS Evaluation Mode 85 Days

Live Logs Live Sessions

Misconfigured Suppliants: 0 Misconfigured Network Devices: 0 RADIUS Drops: 0 Client Stopped Responding: 2 Repeat Counter: 0

Refresh: Never Show: Latest 20 records Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Netwo
Aug 23, 2022 06:18:42.5...			0	user1	08:BE:AC:27:85:...	Unknown	Policy_Set...	Policy_Set...	PermitAcc...	10.14.16.112,...	
Aug 23, 2022 09:45:48.1...				user1	BC:D0:74:2B:6D:...						9800-W

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）。