

在Catalyst 9800 WLC上配置带有身份验证的FlexConnect

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

简介

本文档介绍如何在Catalyst 9800无线LAN控制器上配置带有中央或本地身份验证的FlexConnect。

先决条件

要求

Cisco 建议您了解以下主题：

- Catalyst无线9800配置型号
- FlexConnect
- 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：

- C9800-CL、Cisco IOS-XE® 17.3.4

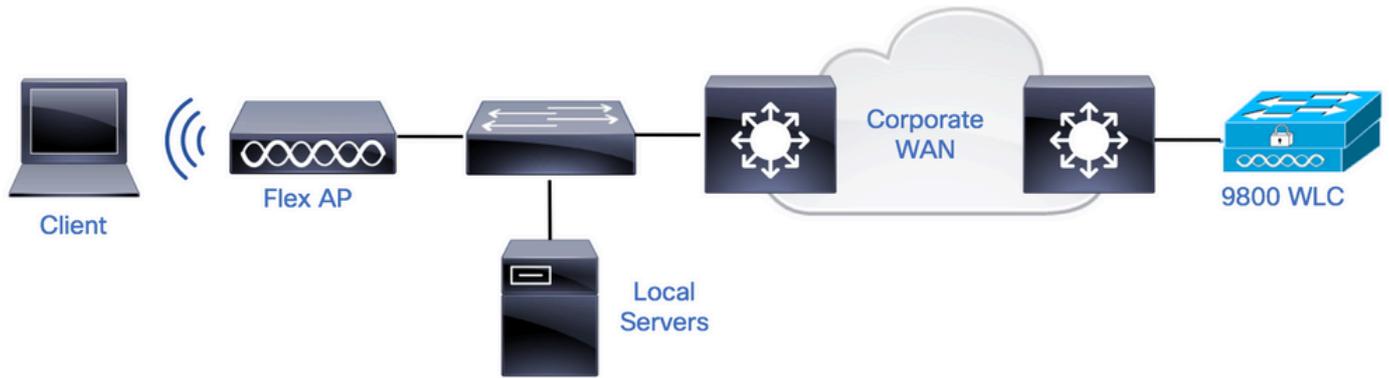
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FlexConnect是用于远程办公室部署的无线解决方案。它允许您通过广域网(WAN)链路从公司办公室远程配置接入点(AP)，而无需在每个位置部署控制器。FlexConnect AP可以在本地交换客户端数据流量，并在与控制器的连接断开时执行本地客户端身份验证。在连接模式下，FlexConnect AP还可以执行本地身份验证。

配置

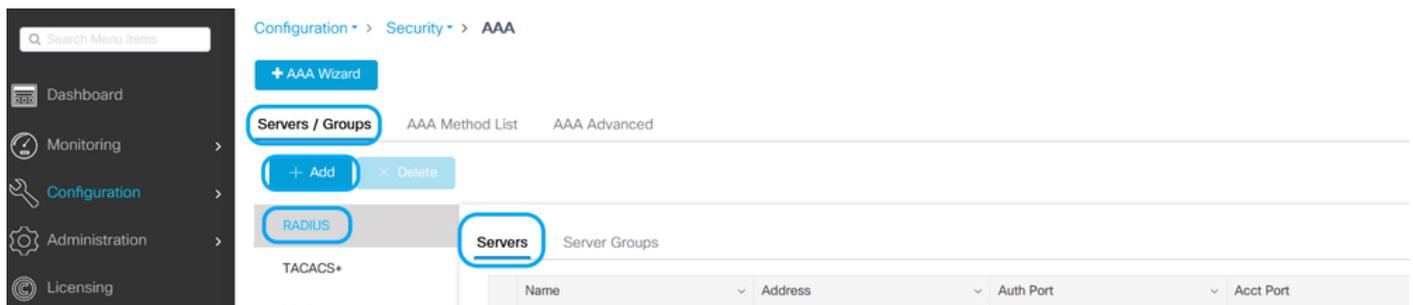
网络图



配置

9800 WLC上的AAA配置

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



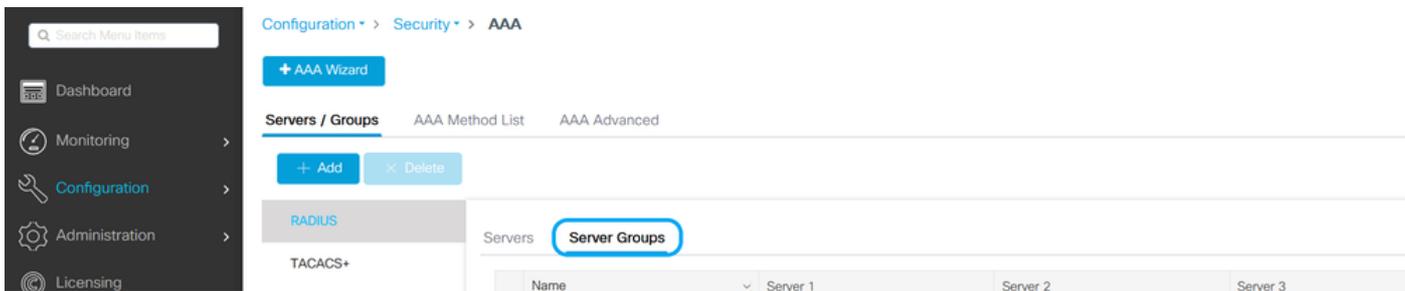
如果您计划在未来使用任何需要CoA的安全类型，请确保启用CoA支持。

Edit AAA Radius Server ✕

Name*	<input type="text" value="AmmISE"/>
Server Address*	<input type="text" value="10.48.76.30"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Hidden"/>
Key* ⓘ	<input type="password" value="●●●●●●●●●●"/>
Confirm Key*	<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="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

 **注意：** Flex connect本地身份验证部署不支持Radius CoA。 .

第二步：将RADIUS服务器添加到RADIUS组。从**GUI**：导航到Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add。



Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

Servers **Server Groups**

Name	Server 1	Server 2	Server 3

Edit AAA Radius Server Group ✕

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Source Interface VLAN ID

Available Servers

- >
- <
- >>
- <<

Assigned Servers

- ⬆
- ⬆
- ⬇
- ⬇

↶ Cancel

💾 Update & Apply to Device

第三步：创建身份验证方法列表。从**GUI**：导航到配置>安全> AAA > AAA方法列表>身份验证> + Add

- 📊 Dashboard
- 🕒 Monitoring >
- 🔧 Configuration >
- ⚙️ Administration >

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

+ Add ✕ Delete

Name	Type
------	------

Quick Setup: AAA Authentication



Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AmmISE

Cancel

从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
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

WLAN 配置

步骤1:从**GUI** : 导航到配置>无线> WLAN , 然后单击+添加以创建新的**WLAN** , 然后输入**WLAN**信息。然后单击应用到设备。

The screenshot displays the WLAN configuration interface. On the left is a navigation menu with 'Dashboard' and 'Monitoring'. The main area shows the breadcrumb 'Configuration > Tags & Profiles > WLANs' and buttons for '+ Add', 'Delete', 'Enable WLAN', and 'Disable WLAN'. Below these is a table with columns for 'Status', 'Name', 'ID', and 'SSID', and a 'Number of WLANs selected : 0' indicator. A modal window titled 'Add WLAN' is open, showing the 'General' tab with the following fields: Profile Name* (802.1x-WLAN), SSID* (802.1x), WLAN ID* (1), Status (ENABLED), Radio Policy (All), and Broadcast SSID (ENABLED). At the bottom of the modal are 'Cancel' and 'Apply to Device' buttons.

第二步 : 从**GUI**:导航到Security选项卡 , 配置第2层/第3层安全模式 , 只要加密方法还在使用 , 身份验证列表在802.1x的情况下也在使用。然后单击更新并应用到设备。

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

PSK

CCKM

FT + 802.1x

FT + PSK

FT + PSK + ...

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Cancel

Update & Apply to Device

策略配置文件配置

步骤1:从GUI中：导航至Configuration > Tags & Profiles > Policy，然后点击+Add以创建策略配置文件。



Search Menu Items



Dashboard

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Status



Policy Profile Name

第二步：添加名称并取消选中Central Switching框。通过此设置，控制器处理客户端身份验证，FlexConnect接入点在本地交换客户端数据包。

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

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching DISABLED

Central Authentication ENABLED

Central DHCP ENABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

Cancel

Update & Apply to Device

 注意：关联和交换必须始终成对，如果禁用了中心交换，则使用Flexconnect AP时，在所有策略配置文件上，关联也必须禁用。

第三步：从**GUI**：导航到访问策略选项卡，以分配无线客户端在默认情况下连接到此**WLAN**时可以分配到的**VLAN**。您可以从下拉列表中选择一個VLAN名称，也可以手动键入VLAN ID。

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

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local ProfilingGlobal State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

76 ▼

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 ▼

Cancel

Update & Apply to Device

第四步：从GUI：导航到Advanced选项卡，以配置WLAN超时、DHCP、WLAN Flex Policy和AAA策略，以防它们正在使用中。然后单击Update & Apply to Device。

Edit Policy Profile
✕

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

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

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List ⓘ

Fabric Profile

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

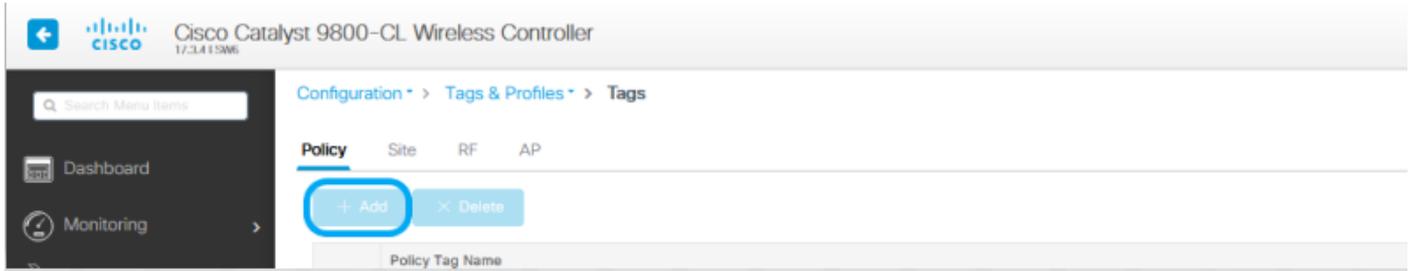
EoGRE Tunnel Profiles

↶ Cancel

↶ Update & Apply to Device

策略标签配置

步骤1:从**GUI** : 导航至配置>标记和配置文件>标记>策略> +添加。



第二步：分配名称，并映射之前创建的策略配置文件和WLAN配置文件。

Edit Policy Tag



⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Policy

Description

Enter Description

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
802.1x-WLAN	VLANX

10 items per page 1 - 1 of 1 items

Map WLAN and Policy

WLAN Profile*

802.1x-WLAN

Policy Profile*

VLANX



RAN-POLICY Maps: 0

Cancel

Update & Apply to Device

第1步：从GUI中：导航到配置>标记和配置文件> Flex，然后单击+添加以创建一个新配置。

The image shows two parts of a network configuration interface. The top part is a navigation breadcrumb: Configuration > Tags & Profiles > Flex. Below this, there are two buttons: '+ Add' (highlighted with a blue circle) and '× Delete'. A table below shows a single entry with a checkbox and the name 'Sa_Flex' under the header 'Flex Profile Name'.

The bottom part is a dialog titled 'Edit Flex Profile'. It has tabs for 'General', 'Local Authentication', 'Policy ACL', 'VLAN', and 'Umbrella'. The 'General' tab is active and contains the following fields:

Field	Value	Field	Value
Name*	Flex-Pro	Fallback Radio Shut	<input type="checkbox"/>
Description	Enter Description	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	71	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	0	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP	<input type="checkbox"/>
CTS Policy		Join Minimum Latency	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>	mDNS Flex Profile	Search or Select ▼
CTS Profile Name	default-sxp-profile ▼		

At the bottom of the dialog, there are two buttons: 'Cancel' and 'Update & Apply to Device'.

 注：本地VLAN ID是指可分配此Flex配置文件的AP使用的VLAN，并且必须在连接AP的交换机端口上配置与本地相同的VLAN ID。

第二步：在VLAN选项卡下，添加所需的VLAN、通过策略配置文件默认分配给WLAN的VLAN或RADIUS服务器推送的VLAN。然后单击Update & Apply to Device。

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add - Delete

VLAN Name	ID	ACL Name
No items to display		

VLAN Name* VLAN76

VLAN Id* 76

ACL Name Select ACL

Save Cancel

Cancel Update & Apply to Device

注意：对于Policy Profile，当您选择分配给SSID的默认VLAN时。如果在该步骤中使用VLAN名称，请确保在Flex Profile配置中使用相同的VLAN名称，否则，客户端无法连接到WLAN。

注意：要为flexConnect配置AAA覆盖的ACL，请仅在“policy ACL”上配置它，如果ACL已分配给特定VLAN，请在添加VLAN时添加ACL，然后在“policy ACL”上添加ACL。

站点标签配置

步骤1:从GUI：导航至配置>标记和配置文件>标记>站点，然后单击+Add以创建新的站点标记。取消选中Enable Local Site框以允许AP在本地交换客户端数据流量，并添加之前创建的Flex配置文件。

Search Menu Items

Dashboard

Monitoring

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+ Add - Delete

Edit Site Tag

Name* Flex_Site

Description Flex_Site

AP Join Profile default-ap-profile

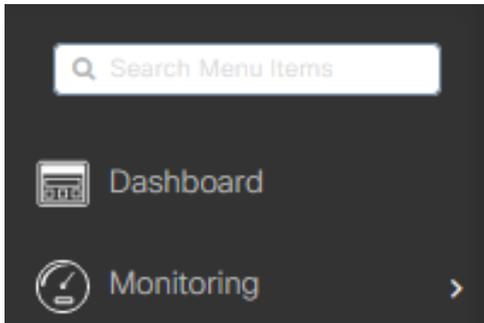
Flex Profile Flex-Pro

Fabric Control Plane Name

Enable Local Site

 注意：当禁用启用本地站点时，获取此站点标记分配的AP可配置为FlexConnect模式。

第二步：从**GUI**：导航到Configuration > Wireless > Access Points > AP name，将Site Tag和Policy Tag添加到关联的**AP**。这会导致AP重新启动其CAPWAP隧道并返回到9800 WLC。



Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

General

AP Name*	<input type="text" value="talomar1"/>
Location*	<input type="text" value="default location"/>
Base Radio MAC	b4de.31d7.b920
Ethernet MAC	005d.7319.bb2a
Admin Status	<input checked="" type="checkbox"/> ENABLED
AP Mode	<input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Local"/>
Operation Status	Registered
Fabric Status	Disabled
LED State	<input checked="" type="checkbox"/> ENABLED
LED Brightness Level	<input type="text" value="8"/>

Version

Primary Software Version	17.3.4.154
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	17.3.4.154
Mini IOS Version	0.0.0.0

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy	<input type="text" value="Policy"/>
Site	<input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Flex_Site"/>
RF	<input type="text" value="default-rf-tag"/>
Write Tag Config to AP	<input type="checkbox"/>

IP Config

CAPWAP Preferred Mode	IPv4
DHCP IPv4 Address	10.48.70.77
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Time Statistics

Up Time	0 days 0 hrs 3 mins 28 secs
Controller Association Latency	2 mins 40 secs

AP重新加入后，请注意AP现在处于FlexConnect模式。

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location	Country
taloman1	AR-AP2802I-E-K9	2	●	10.48.70.77	b4de.31d7.8920	Flex	Registered	Healthy	Policy	Flex_Site	default-rt-tag	Static	default location	BE

使用外部RADIUS服务器的本地身份验证

步骤1:将AP作为网络设备添加到RADIUS服务器。有关示例，请参阅[如何使用身份服务引擎\(ISE\)作为RADIUS服务器](#)

第二步：创建WLAN。

配置可以与之前配置的配置相同。

Add WLAN ✕

General

Security

Advanced

Profile Name*

SSID*

WLAN ID*

Status ENABLED

Radio Policy

Broadcast SSID ENABLED

Cancel

📄
Apply to Device

第三步：策略配置文件配置。

您可以创建新配置或使用之前配置的。此时，取消选中Central Switching、Central Authentication、Central DHCP和Central Association Enable框。

Add Policy Profile



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

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Local

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

DISABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

第四步：策略标签配置。

关联已配置的WLAN和已创建的策略配置文件。

第五步：Flex配置文件配置。

创建Flex配置文件，导航到本地身份验证选项卡，配置Radius服务器组并选中RADIUS框。

Radius Server Group: AmmISE LEAP

Local Accounting Radius Server Group: Select Accounting S... PEAP

Local Client Roaming: TLS

EAP Fast Profile: Select Profile RADIUS

Users

Select CSV File

Username	
No items to display	

第六步：站点标记配置。
配置在步骤5中配置的Flex配置文件，并取消选中Enable Local Site框。

Add Site Tag ✕

Name*	<input type="text" value="Local Auth"/>
Description	<input type="text" value="Enter Description"/>
AP Join Profile	<input type="text" value="default-ap-profile"/> ▼
Flex Profile	<input type="text" value="Local"/> ▼
Fabric Control Plane Name	<input type="text"/> ▼
Enable Local Site	<input type="checkbox"/>

验证

从GUI：导航到Monitoring > Wireless > Clients 并确认Policy Manager State和FlexConnect参数。

集中身份验证：

[General](#)[QoS Statistics](#)[ATF Statistics](#)[Mobility History](#)[Call Statistics](#)[Client Properties](#)[AP Properties](#)[Security Information](#)[Client Statistics](#)[QoS Properties](#)

MAC Address	484b.aa52.5937
IPv4 Address	172.16.76.41
User Name	address1
Policy Profile	VLAN2669
Flex Profile	RemoteSite1
Wireless LAN Id	1
Wireless LAN Name	eWLC_do1x
BSSID	38ed.18c6.902f
Uptime(sec)	9 seconds
CCX version	No CCX support
Power Save mode	OFF
Supported Rates	9.0,18.0,36.0,48.0,54.0
Policy Manager State	Run
Last Policy Manager State	IP Learn Complete
Encrypted Traffic Analytics	No
Multicast VLAN	0
Access VLAN	2669
Anchor VLAN	0
Server IP	10.88.173.94
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None
IPv6 DNS Capable	No
FlexConnect Data Switching	Local
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central
FlexConnect Central Association	Yes

本地 认证:

General	QoS Statistics	ATF Statistics	Mobility History	Call Statistics
Client Properties	AP Properties	Security Information	Client Statistics	QoS Properties
MAC Address		484b.aa52.5937		
IPv4 Address		172.16.76.41		
IPv6 Address		fe80::80c6e782:7c78:68f9		
User Name		address1		
Policy Profile		VLAN2669		
Flex Profile		RemoteSite1		
Wireless LAN Id		1		
Wireless LAN Name		eWLC_do1x		
BSSID		38ed.18c6.932f		
Uptime(sec)		11 seconds		
CCX version		No CCX support		
Power Save mode		OFF		
Policy Manager State		Run		
Last Policy Manager State		IP Learn Complete		
Encrypted Traffic Analytics		No		
Multicast VLAN		0		
Access VLAN		2669		
Anchor VLAN		0		
DNS Snooped IPv4 Addresses		None		
DNS Snooped IPv6 Addresses		None		
11v DMS Capable		No		
FlexConnect Data Switching		Local		
FlexConnect DHCP Status		Local		
FlexConnect Authentication		Local		
FlexConnect Central Association		No		

您可以使用以下命令验证当前配置：

从CLI:

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

故障排除

WLC 9800提供无间断跟踪功能。这可确保持续记录所有客户端连接相关的错误、警告和通知级别消息，并且您可以在发生事故或故障情况后查看其日志。

 注：根据生成的日志量，您可以将时间从几个小时缩短到几天。

为了查看9800 WLC在默认情况下收集的跟踪，您可以通过SSH/Telnet连接到9800 WLC并完成以下步骤（确保您将会话记录到文本文件）。

步骤1:检查控制器当前时间，以便您可以在问题发生之前的时间跟踪日志。

从CLI:

```
# show clock
```

第二步：根据系统配置的指示，从控制器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（如果有）。

从CLI:

```
# show logging
```

第三步：验证是否启用了任何调试条件。

从CLI:

```
# show debugging
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address                               Port
-----|-----
```

 注：如果找到列出的任何条件，则意味着遇到启用条件（mac地址、ip地址等）的所有进程的



跟踪将记录到调试级别。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：如果您假设在步骤3中未将所测试的mac地址列为条件，请收集特定mac地址的始终在线通知级别跟踪。

从CLI:

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

您可以显示会话内容，也可以将文件复制到外部 TFTP 服务器。

从CLI:

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

条件调试和无线电活动跟踪

如果永远在线(always-on)跟踪不能为您提供足够的信息来确定所调查问题的触发器，则可以启用条件调试并捕获无线活动(RA)跟踪，该跟踪可以为与指定条件（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。要启用条件调试，请完成以下步骤。

第五步：确保未启用调试条件。

从CLI:

```
# clear platform condition all
```

第六步：为要监控的无线客户端MAC地址启用调试条件。

此命令开始监控提供的mac地址达30分钟（1800秒）。您可以选择延长监控时间，最多监控2085978494秒。

从CLI:

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

 注:要一次监控多个客户端，请对每个mac地址运行debug wireless mac <aaaa.bbbb.cccc>命令。

 注意:您不会在终端会话上看到客户端活动的输出，因为所有内容都在内部缓冲，供以后查看。

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器时间开启之前重现问题，则停止调试。

从CLI:

```
# 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_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤 9 收集 MAC 地址活动的文件。 您可以将 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

从CLI:

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

将文件复制到外部服务器：

从CLI:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

显示内容：

从CLI:

```
# 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，因为您详细查看了已收集并内部存储的调试日志。

从CLI:

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

 **注意：**此命令输出返回所有进程的所有日志记录级别的跟踪，而且数量相当大。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：

从CLI:

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

显示内容：

从CLI:

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

步骤 11 删除调试条件。

从CLI:

```
# clear platform condition all
```

 **注意：**请确保在故障排除会话后始终删除调试条件。

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）。