

Configure FlexConnect with Authentication on Catalyst 9800 WLC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

Introduction

This document describes how to configure FlexConnect with central or local authentication on Catalyst 9800 Wireless LAN controller.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Catalyst Wireless 9800 configuration model
- FlexConnect
- 802.1x

Components Used

The information in this document is based on these software and hardware versions:

- C9800-CL, Cisco IOS-XE® 17.3.4

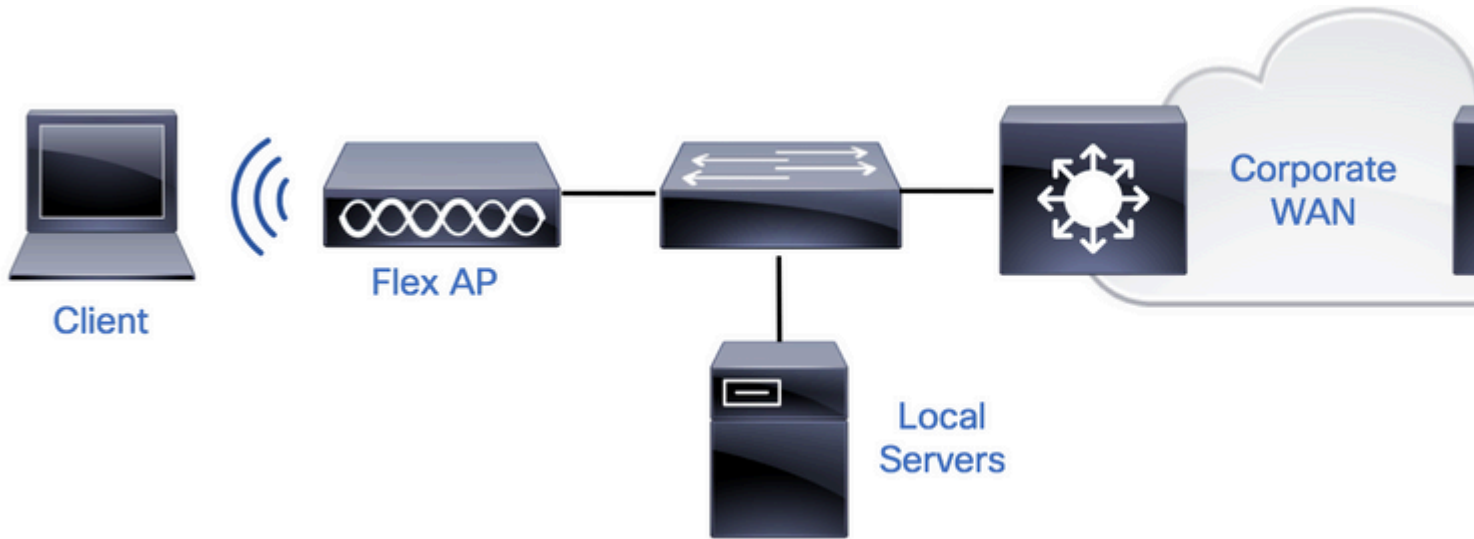
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

FlexConnect is a wireless solution for remote office deployment. It allows you to configure Access Points (APs) in remote locations from the corporate office through a Wide Area Network (WAN) link without the need to deploy a controller in each location. The FlexConnect APs can switch the client data traffic locally and perform client authentication locally when the connection to the controller is lost. In connected mode, the FlexConnect APs can also perform local authentication.

Configure

Network Diagram



Configurations

AAA Configuration on 9800 WLCs


Step 1. Declare RADIUS server. **From GUI:** Navigate to Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add and enter the RADIUS server information.


The screenshot shows the Cisco GUI configuration page for AAA. The breadcrumb trail is Configuration > Security > AAA. The 'Servers / Groups' tab is selected, and the 'RADIUS' sub-tab is active. The 'Servers' sub-tab is also highlighted. A table with columns for Name, Address, and Auth Port is visible at the bottom.

Name	Address	Auth Port
...

Ensure that Support for CoA is enabled if you plan to use any kind of security that requires CoA in the future.

Edit AAA Radius Server

Name*	<input type="text" value="AmmlSE"/>
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="text" value="●●●●●●●●●●●●●●●●●●●●"/>
Confirm Key*	<input type="text" 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

 Cancel

Note: Note: Radius CoA is not supported in Flex connect local auth deployment. .

Step 2. Add the RADIUS server to a RADIUS group. **From GUI:** Navigate to Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Licensing

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

Servers **Server Groups**

Name	Server 1	Server 2
------	----------	----------

Edit AAA Radius Server Group

Name*	AmmlSE
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	2
Source Interface VLAN ID	76

Available Servers

^
↓




Assigned Servers

AmmlSE

^
↑
↓
⌵



 Cancel

 Update & Apply to

Step 3. Create an Authentication Method List. **From GUI:** Navigate to Configuration > Security > AAA > AAA Method List > Authentication > + Add

Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA /

Authentication

+ Add

Authorization

Name

Quick Setup: AAA Authentication

Method List Name*

AmmISE

Type*

dot1x

Group Type

group

Fallback to local

Available Server Groups

radius
ldap
tacacs+



Assigned Server Groups

AmmISE

Cancel

Up

From 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

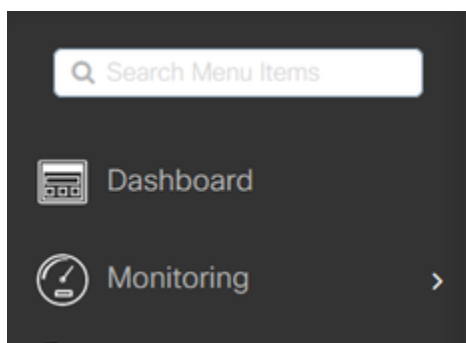
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

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

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

WLAN Configuration

Step 1. **From GUI:** Navigate to Configuration > Wireless > WLANs and click +Add to create a new WLAN, and enter the WLAN information. Then click Apply to Device.



Configuration > Tags & Profiles > WLANs



Number of WLANs selected : 0

<input type="checkbox"/>	Status ▾	Name	ID
--------------------------	----------	------	----

Add WLAN

General

Security

Advanced

Profile Name*

802.1x-WLAN

Radio Policy

All

SSID*

802.1x

Broadcast SSID

ENABLED

WLAN ID*

1

Status

ENABLED



 Cancel

Step 2. **From GUI:** Navigate to the Security tab to configure the Layer2/Layer3 security mode as long as the encryption method, and Authentication List in case 802.1x is in use. Then click Update & Apply to Device.

⚠ 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

Lobby Admin Access

MAC Filtering

Fast Transition

Protected Management Frame

Over the DS

PMF

Reassociation Timeout

WPA Parameters

MPSK Configuration

MPSK

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

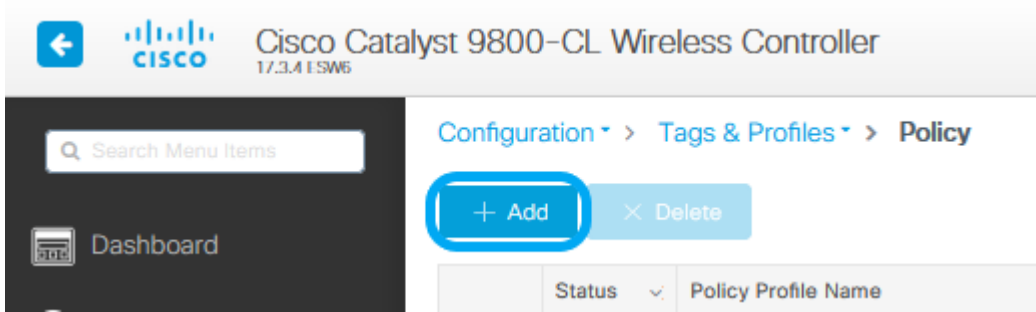
FT + PSK

Cancel

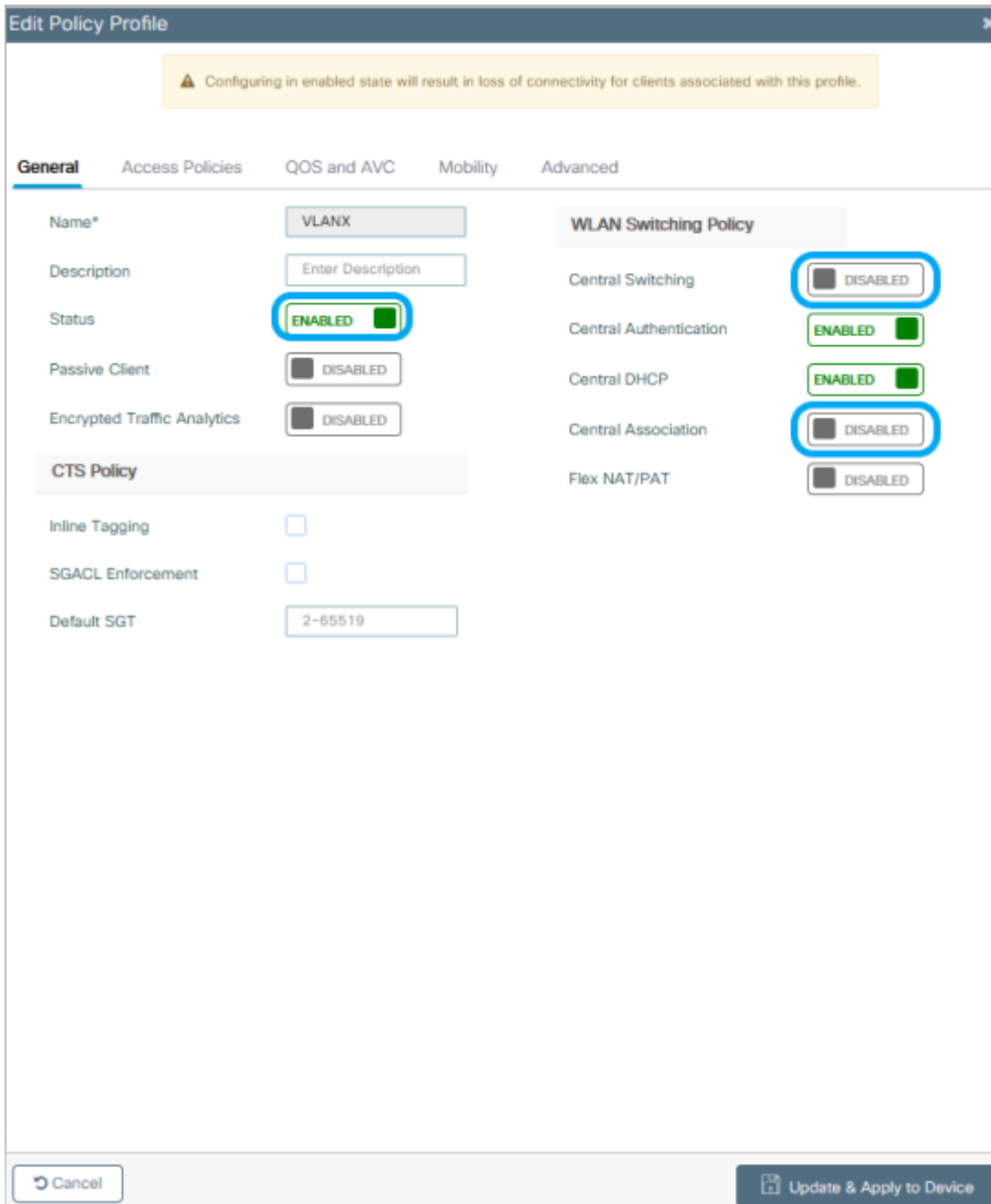
Update & Apply to Device

Policy Profile Configuration

Step 1. **From GUI:** Navigate to Configuration > Tags & Profiles > Policy and click +Add to create a Policy Profile.



Step 2. Add the name and uncheck the Central Switching box. With this setup, the controller handles client authentication, and the FlexConnect Access Point switches client data packets locally.



Note: Association and switching must be always paired, if central switching is disabled central association must disable as well on all policy profiles when Flexconnect APs are used.

Step 3. **From GUI:** Navigate to the Access Policies tab to assign the VLAN to which the wireless clients can be assigned when they connect to this WLAN by default.

You can either select one VLAN name from the drop-down or as a best practice, manually type a VLAN ID.

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

RADIUS Profiling	<input type="checkbox"/>	WLAN ACL
HTTP TLV Caching	<input type="checkbox"/>	IPv4 ACL <input type="text" value="Search or Select"/> ▼
DHCP TLV Caching	<input type="checkbox"/>	IPv6 ACL <input type="text" value="Search or Select"/> ▼
WLAN Local Profiling		URL Filters
Global State of Device Classification	Disabled ⓘ	Pre Auth <input type="text" value="Search or Select"/> ▼
Local Subscriber Policy Name	<input type="text" value="Search or Select"/> ▼	Post Auth <input type="text" value="Search or Select"/> ▼
VLAN		
VLAN/VLAN Group	<input type="text" value="76"/> ▼	
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>	

Step 4. **From GUI:** Navigate to the Advanced tab to configure the WLAN timeouts, DHCP, WLAN Flex Policy, and AAA policy in case they are in use. Then click 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

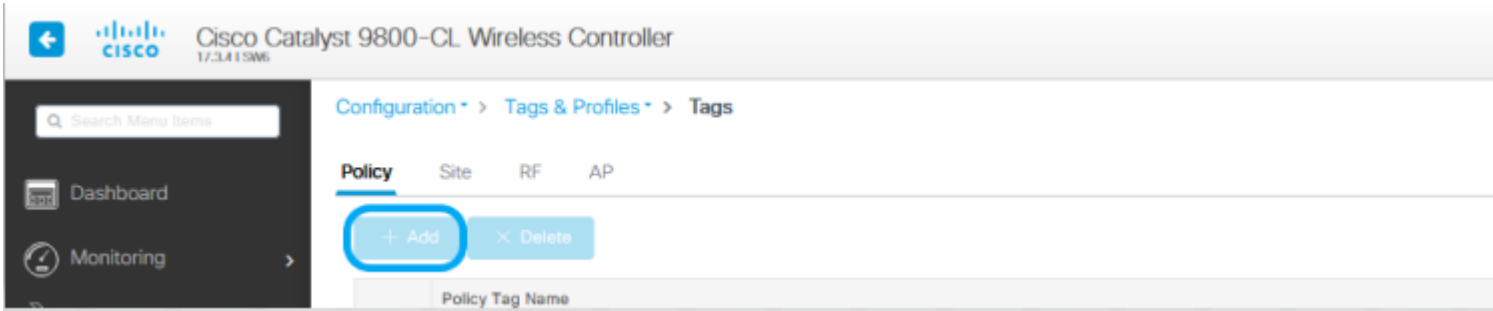
EoGRE Tunnel Profiles

↶ Cancel

🔄 Update & Apply to Device

Policy Tag Configuration

Step 1. **From GUI:** Navigate to Configuration > Tags & Profiles > Tags > Policy > +Add.



Step 2. Assign a name, and map the Policy Profile and WLAN Profile create before.

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
<input type="checkbox"/> 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



> RLAN-POLICY Maps: 0

Cancel

Update & Apply to Device

Flex Profile Configuration

Step 1. **From GUI:** Navigate to Configuration > Tags & Profiles > Flex and click +Add to create a new one.

Search Menu Items

Dashboard

Monitoring >

Configuration > Tags & Profiles > Flex

+ Add | X Delete

	Flex Profile Name
<input type="checkbox"/>	SaI_Flex

Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

Umbrella

Name*

Description

Native VLAN ID

HTTP Proxy Port

HTTP-Proxy IP Address

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name ▼

Fallback Radio Shut

Flex Resilient

ARP Caching

Efficient Image Upgrade

OfficeExtend AP

Join Minimum Latency

IP Overlap

mDNS Flex Profile ▼

Note: Native VLAN ID refers to the VLAN used by the APs that can get this Flex Profile assigned, and it must be the same VLAN ID configured as native on the switch port where the APs are connected.

Step 2. Under the VLAN tab, add the needed VLANs, those assigned by default to the WLAN through a Policy Profile, or the ones pushed by a RADIUS server. Then click Update & Apply to Device.

Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

Umbrella

+ Add

× Delete

VLAN Name	ID	ACL Name
No items to display		

10 items per page

VLAN Name*

VLAN76

VLAN Id*

76

ACL Name

Select ACL

✓ Save

↻ Cancel

↻ Cancel

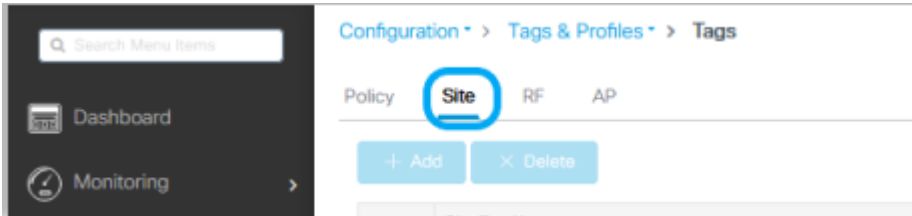
⏪ Upd

Note: For Policy Profile, when you select the default VLAN assigned to the SSID. If you use a VLAN name on that step, ensure that you use the same VLAN name on the Flex Profile configuration, otherwise, clients are not be able to connect to the WLAN.

Note: To configure an ACL for flexConnect with AAA override, only configure it on "policy ACL", if ACL is assigned to a specific VLAN, add ACL on when you add the VLAN and then add the ACL on the "policy ACL".

Site Tag Configuration

Step 1. **From GUI:** Navigate to Configuration > Tags & Profiles > Tags > Site and click +Add to create a new Site tag. Uncheck the Enable Local Site box to allow APs to switch the client data traffic locally, and add the Flex Profile created previously.



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	<input type="checkbox"/>

Note: As Enable Local Site is disabled, the APs that get this Site tag assigned can be configured as FlexConnect mode.

Step 2. **From GUI:** Navigate to Configuration > Wireless > Access Points > AP name to add the Site Tag and Policy Tag to an associated AP. This can cause the AP to restart its CAPWAP tunnel and join back to the 9800 WLC.

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

Edit AP

General Interfaces High Availability Inventory ICap Advanced Support Bundle

General

AP Name* talomari1

Location* default location

Base Radio MAC b4de.31d7.b920

Ethernet MAC 005d.7319.bb2a

Admin Status **ENABLED**

AP Mode Local

Operation Status Registered

Fabric Status Disabled

LED State **ENABLED**

LED Brightness Level 8

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 Policy

Site Flex_Site

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version 17.3.4.154

Predownload Status N/A

Predownload 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

IP Config

CAPWAP Preferred Mode IPv4

DHCP IPv4 Address 10.48.70.77

Static IP (IPv4/IPv6)

Time Statistics

Up Time 0 days 0 hrs 3 mins 28 secs

Controller Association Latency 2 mins 40 secs

Cancel Update & Apply to Device

Once the AP joins back, notice the AP is now in FlexConnect mode.

▼ 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
talomari1	AR-AP2802I-E-K9	2	✔	10.48.70.77	b4de.31d7.b920	Flex	Registered	Healthy	Policy	Flex_Site

Local Authentication with external RADIUS Server

Step 1. Add the AP as a network device into the RADIUS server. For an example refer to [How to use Identity Service Engine \(ISE\) as the RADIUS server](#)

Step 2. Create a WLAN.

The configuration can be the same as the one previously configured.

Add WLAN

General Security Advanced

Profile Name*	<input type="text" value="Local auth"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="Local auth"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="9"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Step 3. Policy Profile Configuration.

You can either create a new one or use the previously configured. This time, uncheck the Central Switching, Central Authentication, Central DHCP, and Central Association Enable boxes.

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*

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 DISABLED

Central DHCP DISABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

Cancel

Apply to Device

Step 4. Policy tag configuration.

Associate the WLAN configured and the Policy Profile created.

Step 5. Flex Profile Configuration.

Create a Flex Profile, navigate to the Local Authentication tab, configure the Radius Server Group and check the RADIUS box.

Edit Flex Profile

General **Local Authentication** Policy ACL VLAN Umbrella

Radius Server Group

AmmISE

Local Accounting Radius Server Group

Select Accounting S

Local Client Roaming

EAP Fast Profile

Select Profile

LEAP

PEAP

TLS

RADIUS

Users

+ Add

× Delete

Select File

Select CSV File



Upload

Username

0 10 items per page

No items to display

Cancel

Update

Step 6. Site tag configuration.

Configure the Flex Profile configured in step 5, and uncheck the Enable Local Site box.

Add Site Tag

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

Cancel

Apply to D

Verify

From GUI: Navigate to **Monitoring > Wireless > Clients** and confirm the **Policy Manager State** and the FlexConnect parameters.

Central Authentication:

Client	
General	
Client 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.18c6.932f
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
11v DMS Capable	No
FlexConnect Data Switching	Local
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central
FlexConnect Central Association	Yes

Local Authentication:

Client				
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::80be782:7c78:68f9		
User Name		addressi		
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		

You can use these commands to verify the current configuration:

From 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>
```

Troubleshoot

WLC 9800 provides ALWAYS-ON trace capabilities. This ensures all client connectivity related errors, warnings, and notice level messages are constantly logged and you can view logs for an incident or failure condition after it has occurred.

Note: Based on the volume of logs generated, you can go back few hours to several days.

In order to view the traces that 9800 WLC collected by default, you can connect via SSH/Telnet to the 9800 WLC and go through these steps (ensure you log the session to a text file).

Step 1. Check the controller current time so you can track the logs in the time back to when the issue happened.

From CLI:

```
# show clock
```

Step 2. Collect syslogs from the controller buffer or the external syslog as dictated by the system configuration. This provides a quick view into the system health and errors if any.

From CLI:

```
# show logging
```

Step 3. Verify if any debug conditions are enabled.

From CLI:

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

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

Note: If you find any condition listed, it means the traces are logged up to debug level for all the processes that encounter the enabled conditions (mac address, ip address and so on). This would increase the volume of logs. Therefore, it is recommended to clear all conditions when not actively debugging

Step 4. If you assume the mac address under test was not listed as a condition in Step 3, collect the always-on notice level traces for the specific mac address.

From CLI:

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

You can either display the content on the session or you can copy the file to an external TFTP server.

From CLI:

```
# more bootflash:always-on-<FILENAME.txt>
```

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

Conditional Debug and Radio Active Trace

If the always-on traces do not give you enough information to determine the trigger for the problem under investigation, you can enable conditional debugging and capture Radio Active (RA) trace, which can provide debug level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, go through these steps.

Step 5. Ensure there are no debug conditions are enabled.

From CLI:

```
# clear platform condition all
```

Step 6. Enable the debug condition for the wireless client mac address that you want to monitor.

This command starts to monitor the provided mac address for 30 minutes (1800 seconds). You can optionally increase this time to up to 2085978494 seconds.

From CLI:

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

Note: In order to monitor more than one client at a time, run debug wireless mac <aaaa.bbbb.cccc> command per mac address.

Note: You do not see the output of the client activity on the terminal session, as everything is buffered internally to be viewed later.

Step 7. Reproduce the issue or behavior that you want to monitor.

Step 8. Stop the debugs if the issue is reproduced before the default or configured monitor time is up.

From CLI:

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

Once the monitor-time has elapsed or the debug wireless has been stopped, the 9800 WLC generates a local file with the name:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Step 9. Collect the file of the mac address activity. You can either copy the ra trace .log to an external server or display the output directly on the screen.

Check the name of the RA traces file

From CLI:

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

Copy the file to an external server:

From CLI:

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

Display the content:

From CLI:

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

Step 10. If the root cause is still not obvious, collect the internal logs which are a more verbose view of debug level logs. You do not need to debug the client again because you took a detailed look at debug logs that have been already collected and internally stored.

From CLI:

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

Note: This command output returns traces for all logging levels for all processes and is quite voluminous. Please engage Cisco TAC to help parse through these traces.

You can either copy the ra-internal-FILENAME.txt to an external server or display the output directly on the screen.

Copy the file to an external server:

From CLI:

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

Display the content:

From CLI:

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

Step 11. Remove the debug conditions.

From CLI:

```
# clear platform condition all
```

Note: Ensure that you always remove the debug conditions after a troubleshooting session.
