

Configurar o FlexConnect com autenticação no Catalyst 9800 WLC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

Introduction

Este documento descreve como configurar o FlexConnect com autenticação central ou local no Catalyst 9800 Wireless LAN Controller.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modelo de configuração Catalyst Wireless 9800
- FlexConnect
- 802.1x

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C9800-CL, Cisco IOS-XE® 17.3.4

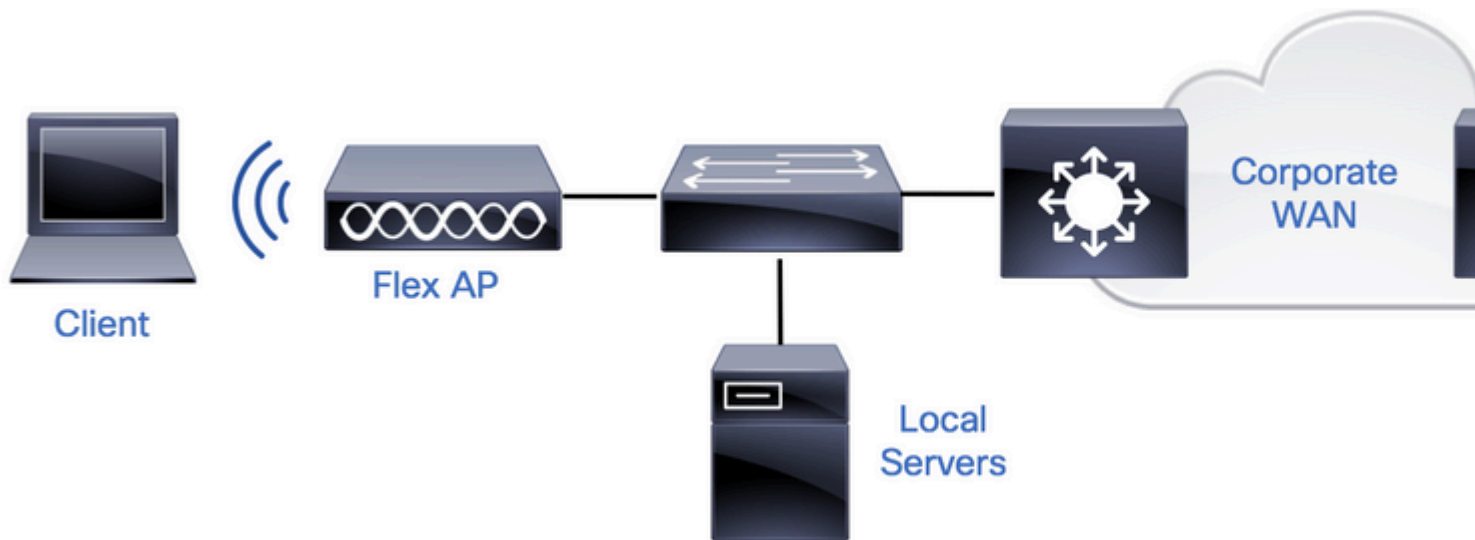
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O FlexConnect é uma solução sem fio para implantação em escritórios remotos. Ele permite configurar pontos de acesso (APs) em locais remotos a partir do escritório corporativo por meio de um link de rede de longa distância (WAN) sem a necessidade de implantar um controlador em cada local. Os APs FlexConnect podem comutar o tráfego de dados do cliente localmente e executar a autenticação do cliente localmente quando a conexão com o controlador é perdida. No modo conectado, os APs FlexConnect também podem executar autenticação local.

Configurar

Diagrama de Rede



Configurações


Configuração de AAA em 9800 WLCs


Etapa 1. Declare o servidor RADIUS. **Na GUI:** Navegue até Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add and enter the RADIUS server information.

The screenshot shows the Cisco GUI configuration interface. The breadcrumb trail is Configuration > Security > AAA. The 'Servers / Groups' tab is selected. Under this tab, there are buttons for '+ Add' and 'Delete'. The 'RADIUS' sub-tab is selected, and the 'Servers' sub-tab is also selected. Below the sub-tabs, there is a table with columns for Name, Address, and Auth Port. The table is currently empty.

Certifique-se de que o Suporte para CoA esteja habilitado se você planeja usar qualquer tipo de segurança que exija CoA no futuro.

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

Observação: Observação: Radius CoA não é suportado na implantação de autenticação local do Flex connect. .

Etapa 2. Adicione o servidor RADIUS a um grupo RADIUS. **Na GUI:** Navegue até 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

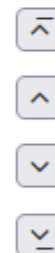
^
↓



Assigned Servers

AmmlSE

^
↑
↓
⌵



Cancel

Update & Apply to

Etapa 3. Crie uma lista de métodos de autenticação. **Na GUI:** Navegue até 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

Do 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

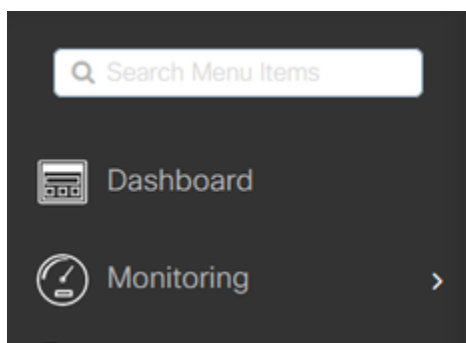
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

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

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

Configuração de WLAN

Etapa 1. **Na GUI:** Navegue até Configuration > Wireless > WLANs e clique em +Add para criar uma nova WLAN e insira as informações da WLAN. Em seguida, clique em Apply to Device (Aplicar ao dispositivo).



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

Etapa 2. Na GUI: navegue até a guia Security para configurar o modo de segurança de Camada 2/Camada 3, contanto que o método de criptografia e a Authentication List, caso 802.1x esteja em uso. Em seguida, clique em 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

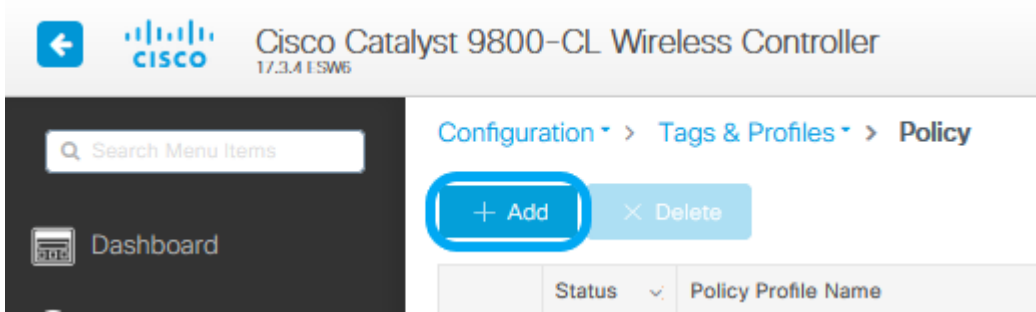
...

Cancel

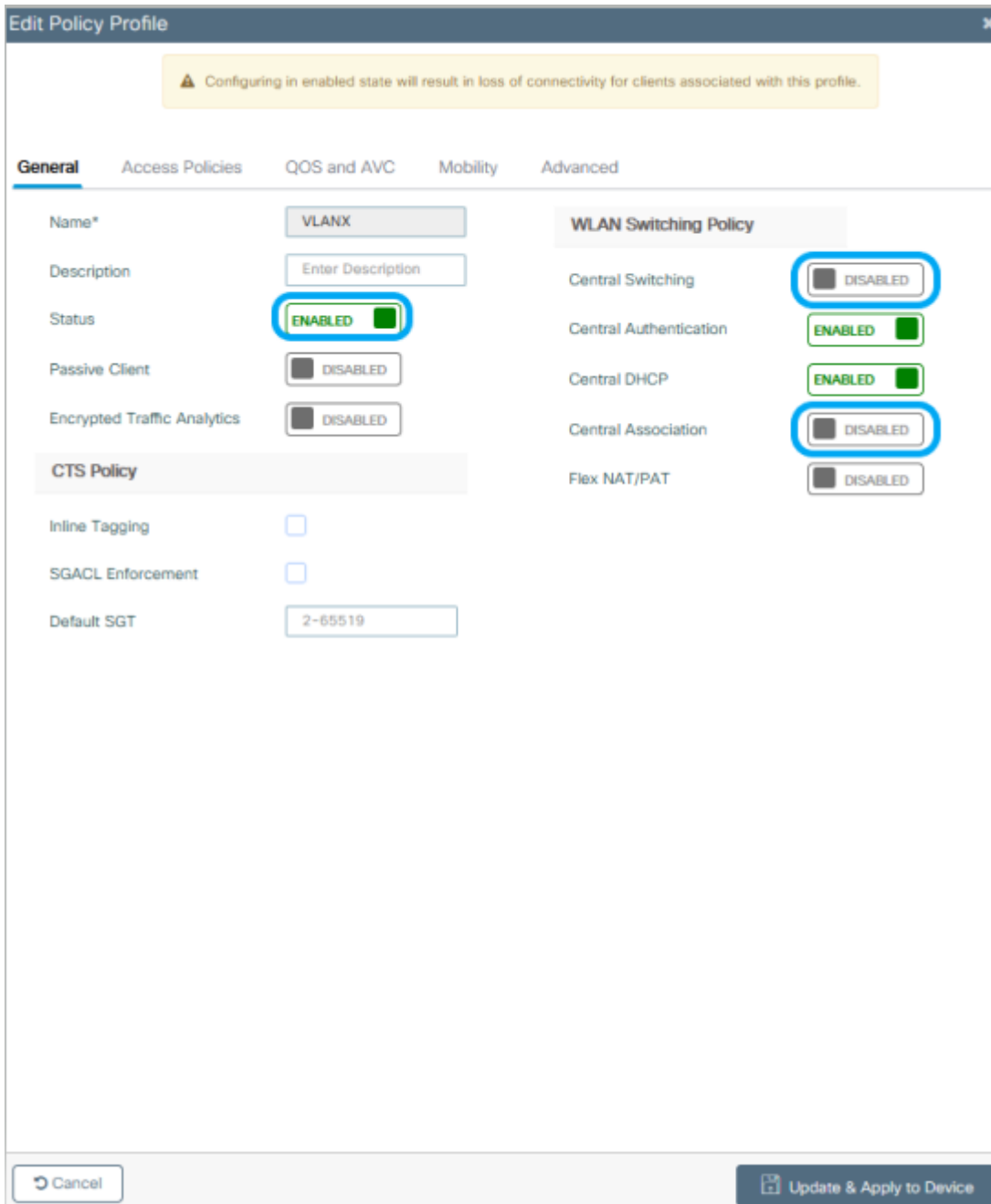
Update & Apply to Device

Configuração de perfil de política

Etapa 1. **Na GUI:** Navegue até Configuration > Tags & Profiles > Policy e clique em +Add para criar um **Policy Profile**.



Etapa 2. Adicione o nome e desmarque a caixa Central Switching. Com essa configuração, o controlador processa a autenticação do cliente e o ponto de acesso FlexConnect comuta os pacotes de dados do cliente localmente.




Observação: a associação e a comutação devem estar sempre emparelhadas; se a comutação central estiver desativada, a associação central também deverá ser desativada em todos os perfis de política quando os APs Flexconnect forem usados.

Etapa 3. **Na GUI:** navegue até a guia Access Policies (Políticas de acesso) para atribuir a VLAN à qual os clientes sem fio podem

ser atribuídos quando se conectam a essa WLAN por padrão.

Você pode selecionar um nome de VLAN no menu suspenso ou, como prática recomendada, digitar manualmente uma ID de VLAN.

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"/>	
HTTP TLV Caching	<input type="checkbox"/>	
DHCP TLV Caching	<input type="checkbox"/>	

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Etapa 4. **Na GUI:** navegue até a guia Advanced **para configurar os timeouts de WLAN, DHCP, WLAN Flex Policy e a política AAA caso estejam em uso.** Em seguida, clique em Update & Apply to Device (Atualizar e aplicar ao dispositivo).

✕
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 ▼

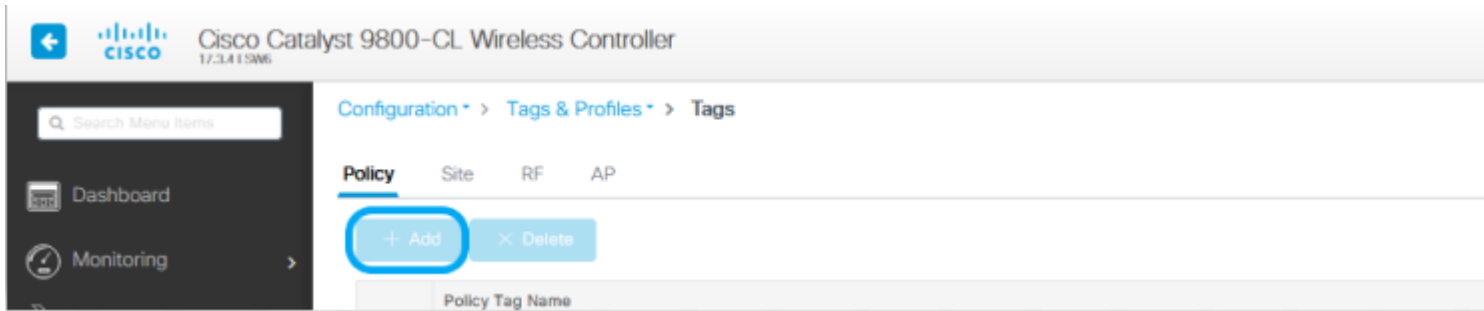
EoGRE Tunnel Profiles

↶ Cancel

↶
Update & Apply to Device

Configuração de marca de política

Etapa 1. Na GUI: Navegue até Configuração > Marcas e perfis > Marcas > Política > +Adicionar.



Etapa 2. Atribua um nome e mapeie o perfil de política e o perfil de WLAN criados antes.

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

Configuração do Perfil Flex

Etapa 1. **Na GUI:** Navegue até Configuration > Tags & Profiles > Flex e clique em +Add para criar uma nova.

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 ▼

Observação: o ID da VLAN nativa se refere à VLAN usada pelos APs que podem ter esse perfil Flex atribuído e deve ser o mesmo ID de VLAN configurado como nativo na porta do switch onde os APs estão conectados.

Etapa 2. Na guia VLAN, adicione as VLANs necessárias, aquelas atribuídas por padrão à WLAN através de um Policy Profile ou aquelas enviadas por um servidor RADIUS. Em seguida, clique em Update & Apply to Device (Atualizar e aplicar ao

dispositivo).

Edit Flex Profile

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

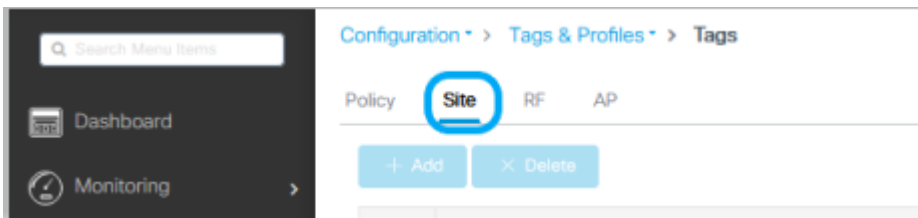
↻ Upd

Observação: para Policy Profile, quando você seleciona a VLAN padrão atribuída ao SSID. Se você usar um nome de VLAN nessa etapa, certifique-se de usar o mesmo nome de VLAN na configuração do perfil Flex, caso contrário, os clientes não poderão se conectar à WLAN.

Observação: para configurar uma ACL para flexConnect com substituição de AAA, configure-a apenas em "ACL de política", se a ACL estiver atribuída a uma VLAN específica, adicione a ACL ao adicionar a VLAN e adicione a ACL à "ACL de política".

Configuração da Marca do Site

Etapa 1. **Na GUI:** Navegue até Configuration > Tags & Profiles > Tags > Site e clique em +Add para criar uma nova tag Site. Desmarque a caixa Enable Local Site para permitir que os APs troquem o tráfego de dados do cliente localmente e adicione o Flex Profile criado anteriormente.



Edit Site Tag

Name*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

Cancel

Update & Apply to Device

Observação: como Habilitar site local está desabilitado, os APs que recebem essa marca de site podem ser configurados como modo FlexConnect.

Etapa 2. **Na GUI:** Navegue até Configuration > Wireless > Access Points > AP name para adicionar a tag de site e a tag de política a um AP associado. Isso pode fazer com que o AP reinicie seu túnel CAPWAP e junte-se novamente à WLC 9800.

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

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

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

Quando o AP entrar novamente, observe que o AP está agora no modo FlexConnect.

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

Autenticação local com servidor RADIUS externo

Etapa 1. Adicione o AP como um dispositivo de rede no servidor RADIUS. Para obter um exemplo, consulte [Como usar o Identity Service Engine \(ISE\) como o servidor RADIUS](#)

Etapa 2. Crie uma WLAN.

A configuração pode ser a mesma que a configurada anteriormente.

Add WLAN

General Security Advanced

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

Etapa 3. Configuração de perfil de política.

Você pode criar um novo ou usar o configurado anteriormente. Desta vez, desmarque as caixas Central Switching, Central Authentication, Central DHCP e Central Association Enable.

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

Etapa 4. Configuração de marca de política.

Associe a WLAN configurada e o perfil de política criado.

Etapa 5. Configuração do Perfil Flex.

Crie um perfil Flex, navegue até a guia Autenticação local, configure o Grupo de servidores Radius e marque a caixa RADIUS.

Edit Flex Profile

General **Local Authentication** Policy ACL VLAN Umbrella

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

+ Add

× Delete

Select File



Upload

Select CSV File

Username
0

10 items per page

No items to display

Cancel

Update

Etapa 6. Configuração de marca de site.
Configure o perfil Flex configurado na etapa 5 e desmarque a caixa Habilitar site local.

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

Verificar

Na GUI: Navegue até **Monitoring > Wireless > Clients** e confirme o **Policy Manager State** e os parâmetros do FlexConnect.

Autenticação Central:

Client	
General	
Client Properties	
MAC Address	484b.aa52.5937
IPv4 Address	172.16.76.41
User Name	andressi
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

Autenticação Local:

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		

Você pode usar estes comandos para verificar a configuração atual:

Do 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

A WLC 9800 fornece recursos de rastreamento SEMPRE ATIVOS. Isso garante que todos os erros, avisos e mensagens de nível de aviso relacionados à conectividade do cliente sejam constantemente registrados e que você possa exibir registros de uma condição de incidente ou falha após sua ocorrência.

Observação: com base no volume de logs gerados, você pode voltar de algumas horas a vários dias.

Para visualizar os rastreamentos que a WLC 9800 coletou por padrão, você pode se conectar via SSH/Telnet à WLC 9800 e passar por essas etapas (certifique-se de registrar a sessão em um arquivo de texto).

Etapa 1. Verifique a hora atual do controlador para que você possa acompanhar os registros no tempo de volta até quando o problema ocorreu.

Do CLI:

```
# show clock
```

Etapa 2. Colete syslogs do buffer do controlador ou do syslog externo, conforme ditado pela configuração do sistema. Isso fornece uma visão rápida da integridade do sistema e dos erros, se houver.

Do CLI:

```
# show logging
```

Etapa 3. Verifique se as condições de depuração estão ativadas.

Do CLI:

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

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

Observação: se você encontrar alguma condição listada, isso significa que os rastreamentos são registrados no nível de depuração para todos os processos que encontram as condições ativadas (endereço mac, endereço ip e assim por diante). Isso aumentaria o volume de registros. Portanto, recomenda-se limpar todas as condições quando não estiver depurando ativamente

Etapa 4. Se você presumir que o endereço mac em teste não foi listado como uma condição na Etapa 3, colete os rastreamentos de nível de aviso sempre ativo para o endereço mac específico.

Do CLI:

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

Você pode exibir o conteúdo da sessão ou copiar o arquivo para um servidor TFTP externo.

Do CLI:

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

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

Depuração condicional e rastreamento ativo de rádio

Se os rastreamentos sempre ativos não fornecerem informações suficientes para determinar o disparador do problema sob investigação, você poderá habilitar a depuração condicional e capturar o rastreamento de Radio Ativo (RA), que pode fornecer rastreamentos no nível de depuração para todos os processos que interagem com a condição especificada (endereço mac do cliente, neste caso). Para habilitar a depuração condicional, siga estas etapas.

Etapa 5. Verifique se não há condições de depuração ativadas.

Do CLI:

```
# clear platform condition all
```

Etapa 6. Ative a condição de depuração para o endereço MAC do cliente sem fio que você deseja monitorar.

Esse comando começa a monitorar o endereço mac fornecido por 30 minutos (1800 segundos). Como alternativa, você pode aumentar esse tempo para até 2.085.978.494 segundos.

Do CLI:

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

Observação: para monitorar mais de um cliente de cada vez, execute o comando `debug wireless mac<aaaa.bbbb.cccc>` por endereço MAC.

Observação: você não vê a saída da atividade do cliente na sessão do terminal, pois tudo é armazenado em buffer internamente para ser visualizado posteriormente.

Passo 7. Reproduza o problema ou comportamento que você deseja monitorar.

Etapa 8. Interrompa as depurações se o problema for reproduzido antes que o tempo de monitoramento padrão ou configurado acabe.

Do CLI:

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

Depois que o monitor-time tiver passado ou a conexão sem fio de depuração for interrompida, o 9800 WLC gerará um arquivo local com o nome:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Etapa 9. Colete o arquivo da atividade do endereço MAC. Você pode copiar o registro de rastreamento de RA para um servidor externo ou exibir a saída diretamente na tela.

Verifique o nome do arquivo de rastreamentos de RA

Do CLI:

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

Copie o arquivo para um servidor externo:

Do CLI:

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

Mostre o conteúdo:

Do CLI:

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

Etapa 10. Se a causa do problema ainda não for evidente, colete os registros internos, que são uma visualização mais detalhada dos registros de nível de depuração. Não é necessário depurar o cliente novamente, pois você examinou detalhadamente os logs de depuração já coletados e armazenados internamente.

Do CLI:

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

Observação: a saída desse comando retorna rastros para todos os níveis de registro de todos os processos e é bastante volumosa. Entre em contato com o Cisco TAC para ajudar a analisar esses rastreamentos.

Você pode copiar o ra-internal-FILENAME.txt para um servidor externo ou exibir a saída diretamente na tela.

Copie o arquivo para um servidor externo:

Do CLI:

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

Mostre o conteúdo:

Do CLI:

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

Etapa 11. Remova as condições de depuração.

Do CLI:

```
# clear platform condition all
```

Observação: certifique-se de sempre remover as condições de depuração após uma sessão de Troubleshooting.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.