

Configurar a Autenticação da Web Local com Autenticação Externa

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Mapa de Parâmetros](#)

[Banco de Dados para Autenticação](#)

[Configurar](#)

[Autenticação da Web local com autenticação local na CLI](#)

[MethodLists para Autenticação Local](#)

[Mapas de Parâmetros](#)

[Parâmetros de segurança da WLAN](#)

[Criar um perfil de política](#)

[Criar uma Marca de Diretiva](#)

[Atribuir uma etiqueta de política a um AP](#)

[Criar nome de usuário convidado](#)

[Autenticação da Web Local com Autenticação Local via WebUI](#)

[Verificar](#)

[Autenticação da Web local no switching local do FlexConnect](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar a Autenticação da Web Local com Autenticação Local em uma controladora Wireless LAN (WLC) 9800.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento do modelo de configuração da WLC 9800.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco WLC série 9800.
- Conhecimento abrangente de autenticação da Web.

Componentes Utilizados

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

- 9800-CL WLC Cisco IOS® XE versão 17.12.5
- Access point Cisco C917AXI.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A Autenticação da Web Local (LWA) é um método de autenticação da rede local sem fio (WLAN) que pode ser configurado na WLC. Quando um usuário seleciona a WLAN na lista de redes disponíveis, ele é redirecionado para um portal da Web. Neste portal, dependendo da configuração, o usuário pode ser solicitado a inserir um nome de usuário e uma senha, aceitar uma Política de Uso Aceitável (AUP) ou uma combinação de ambas as ações para finalizar sua conexão.

Para obter informações sobre os quatro tipos de páginas de autenticação da Web apresentados durante o processo de login, consulte o guia [Configurar autenticação da Web local](#) e revise as opções disponíveis para o tipo de autenticação da Web. Você também pode consultar o guia [Configure Local Web Authentication with External Authentication](#) na seção Types of Authentication.

Mapa de Parâmetros

O Mapa de Parâmetros é um elemento de configuração essencial em uma WLC que permite a Autenticação da Web. Ele consiste em um conjunto de configurações que controlam várias facetas do processo de autenticação da Web, incluindo o tipo de autenticação, URLs de redirecionamento, parâmetros anexados, tempos limite e páginas da Web personalizadas. Para ativar e gerenciar a autenticação baseada na Web para um SSID específico, esse mapa deve estar vinculado ao perfil da WLAN.

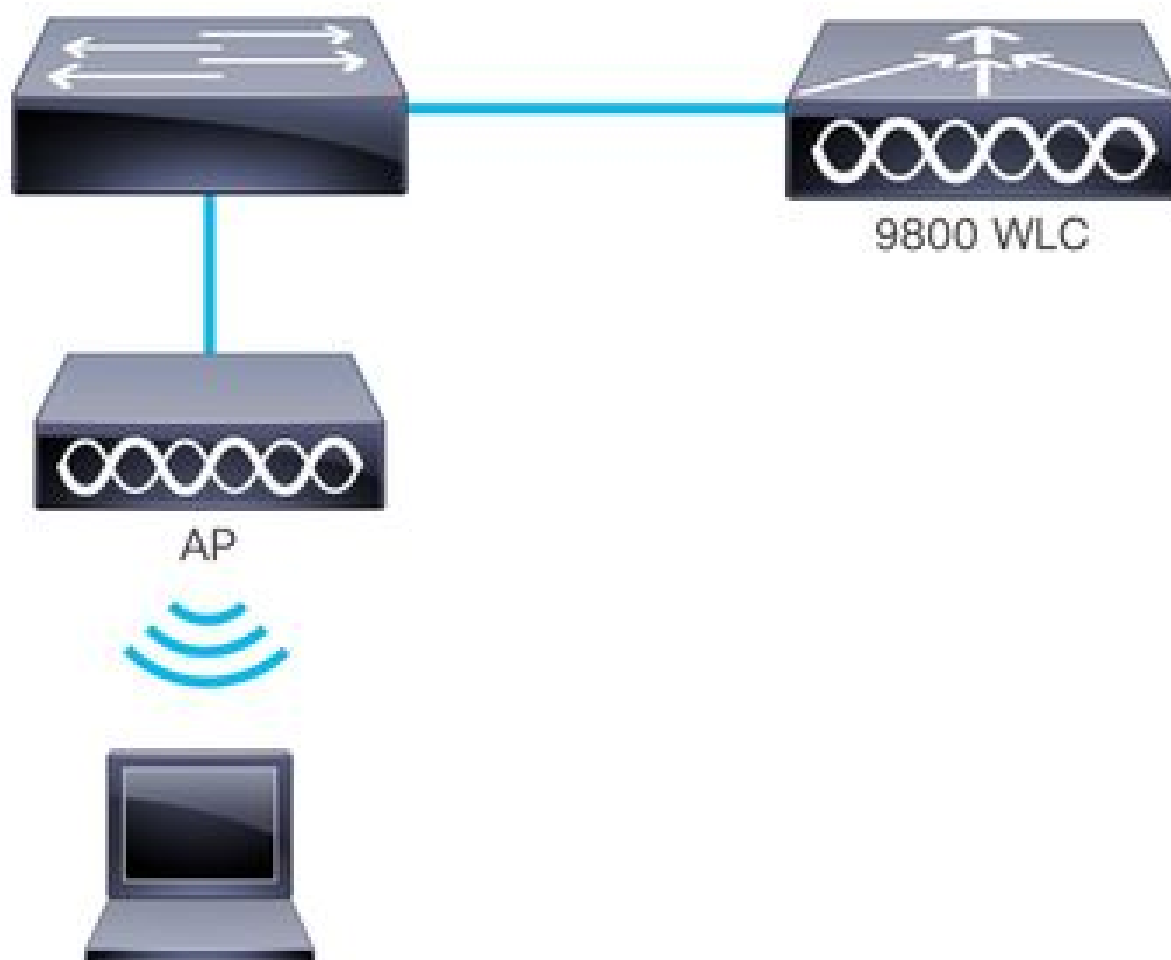
A controladora Wireless LAN vem com um mapa de parâmetros global padrão, mas os administradores têm a opção de criar mapas de parâmetros personalizados para personalizar o comportamento da Autenticação da Web de acordo com necessidades específicas.

Banco de Dados para Autenticação

Se o mapa de parâmetros estiver configurado para usar um nome de usuário e uma senha, você deverá definir as credenciais de autenticação, que são armazenadas localmente na WLC. Ao criar uma conta de usuário convidado por meio da GUI, você pode definir o número máximo de logins simultâneos permitidos por conta de convidado. Os valores válidos variam de 0 a 64, onde 0 indica que logins simultâneos ilimitados são permitidos para esse usuário convidado.

O LWA destina-se principalmente a pequenas implantações. Ele suporta a integração com outros métodos de autenticação, você pode verificar a [Combinação de Autenticações Suportada para um Cliente](#) para obter mais informações.

A imagem representa uma topologia genérica de LWA:



Topologia Genérica de LWA com Autenticação Local

Dispositivos na topologia de rede do LWA:

- Cliente/solicitante: inicia a solicitação de conexão com a WLAN, depois com os servidores DHCP e DNS, e responde às comunicações da WLC.
- Ponto de acesso: conectado a um switch, ele transmite a WLAN convidada e fornece conectividade sem fio para dispositivos convidados. Permite o tráfego DHCP e DNS antes que o usuário convidado conclua a autenticação inserindo credenciais válidas, aceitando uma AUP ou uma combinação de ambas as ações.
- WLC/Autenticador: Gerencia os APs e os dispositivos clientes. A WLC hospeda a URL de redirecionamento e aplica a ACL (Access Control List, lista de controle de acesso) que

controla o tráfego e sua criação por padrão ao configurar o mapa de parâmetros. Ele intercepta solicitações HTTP de usuários convidados e as redireciona para um portal da Web (página de logon) onde os usuários devem se autenticar. A WLC captura credenciais de usuário, autentica convidados e verifica o banco de dados local para verificar a validade da credencial.

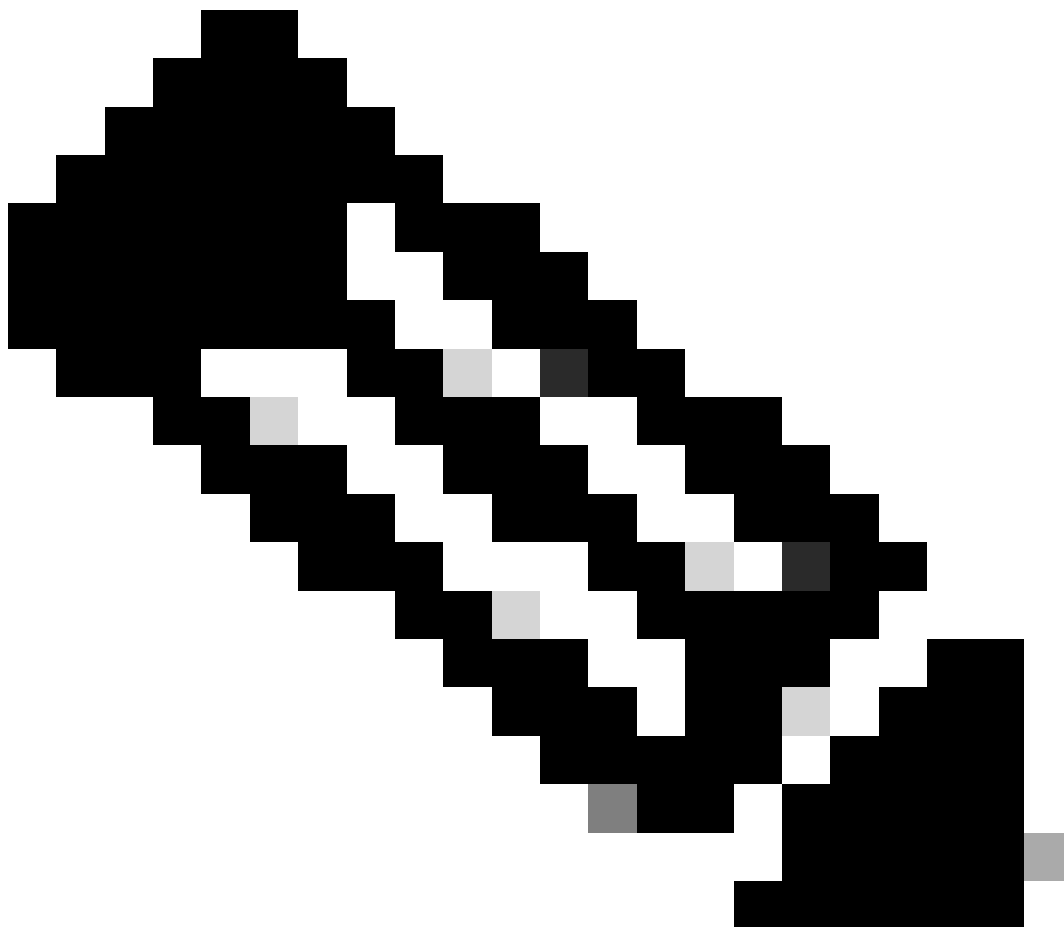
- Servidor de autenticação: neste cenário, a WLC funciona como o servidor de autenticação. Ele valida as credenciais do usuário convidado e concede ou nega o acesso à rede de acordo.

Configurar

Autenticação da Web local com autenticação local na CLI

Listas de métodos para autenticação local

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



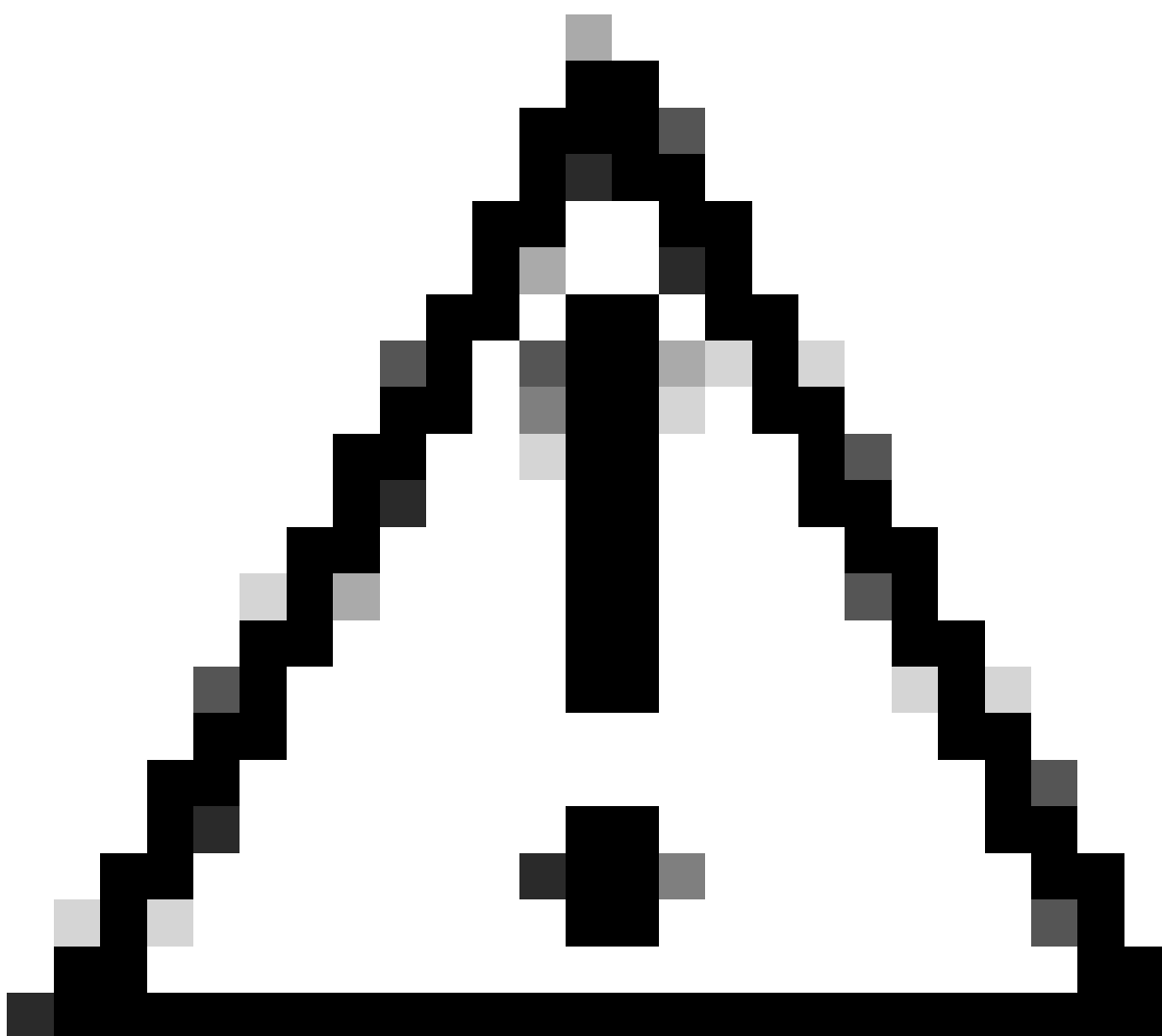
Note: Para que a lista de métodos de login local funcione, certifique-se de que a configuração de rede de autorização aaa local padrão exista na WLC. Isso é necessário quando a WLC autoriza o usuário a entrar na rede.

Mapas de Parâmetros

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#webauth-http-enable
```

```
9800WLC(config-params-parameter-map)#end
```



Caution: O IP virtual deve ser um endereço não roteável proposto no RFC 5737. Por padrão, o IP 192.0.2.1 está definido. Consulte mais informações sobre o endereço IP virtual em [Cisco Catalyst 9800 Series Configuration Best Practices](#). No AireOs, na maior parte do tempo, o IP usado era 1.1.1.1. Isso não é mais recomendado, pois se tornou um IP público.

A capacidade de criar vários mapas de parâmetros permite fluxos personalizados: páginas da Web personalizadas e parâmetros de apresentação específicos para cada WLAN. O mapa de parâmetros globais determina o ponto de confiança e, portanto, o certificado que a WLC apresenta ao cliente no portal de redirecionamento. Além disso, ele controla os tipos de tráfego

de cliente interceptados, como HTTP/HTTPS para o portal de redirecionamento, domínio ou resolução de nome de host para o endereço IP virtual. Essa separação permite que o mapa global manipule configurações abrangentes, como apresentação de certificado e interceptação de tráfego, enquanto os mapas de parâmetros definidos pelo usuário fornecem experiência granular por WLAN.

Parâmetros de segurança da WLAN

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Criar um perfil de política

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

Criar uma Marca de Diretiva

```
9800WLC>enable
```

```
9800WLC#configure terminal
9800WLC(config)#wireless tag policy
```

```
9800WLC(config-policy-tag)#wlan LWA_LA policy
```

```
9800WLC(config-policy-tag)# end
```

Atribuir uma etiqueta de política a um AP

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap
```

```
>
```

```
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
```

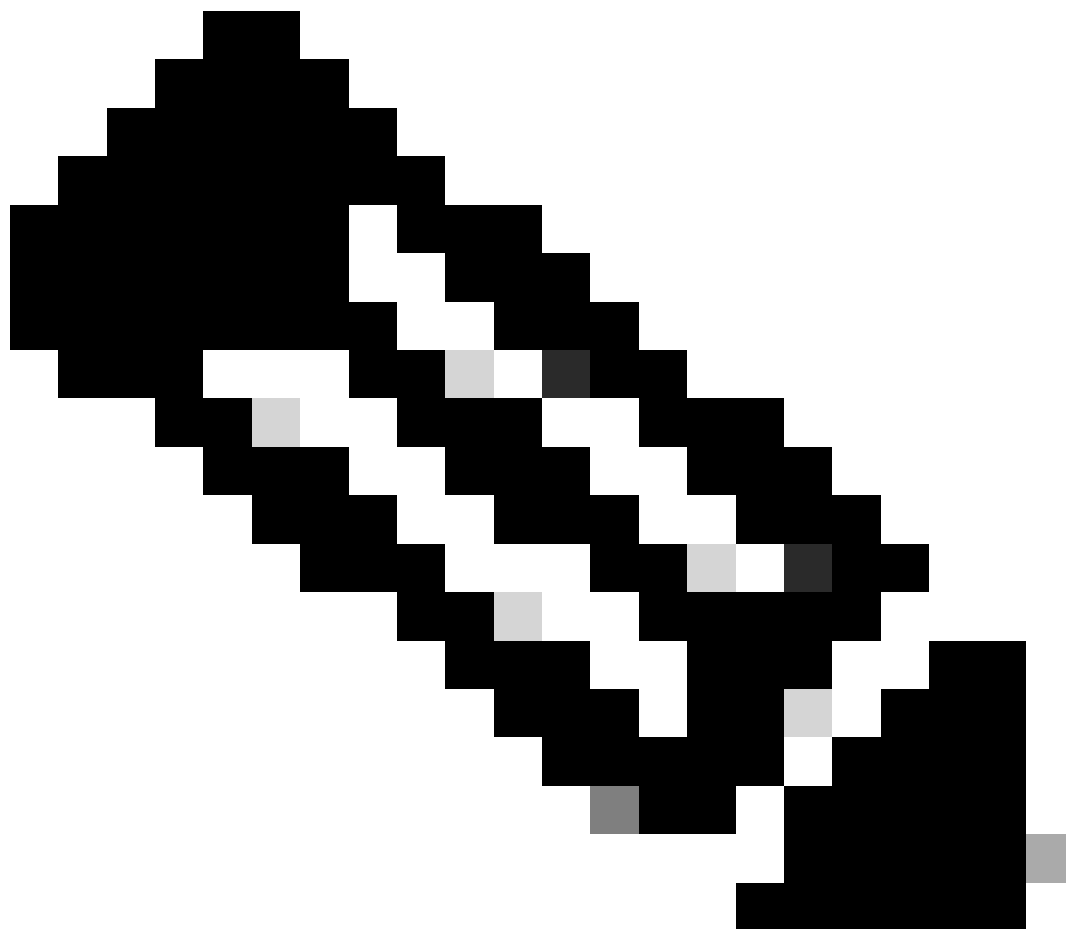
```
9800WLC(config-ap-tag)#end
```

Criar nome de usuário convidado

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description
```

```
guest-user lifetime year 0 month 11 day 30 hour 23
```

```
9800WLC(config-user-name)#end
```

Note: Ao definir o tempo de vida do usuário convidado, se o ano for definido como 1, você não poderá especificar os parâmetros subsequentes que são meses, dias, horas e minutos, já que o tempo de vida máximo é de 1 ano.

Autenticação da Web Local com Autenticação Local via WebUI

Listas de métodos para autenticação local

Navegue para Configuration > Security > AAA > AAA Method List > Authentication > Add para criar a lista de métodos a ser usada posteriormente na configuração da WLAN.

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

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

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	login	local	N/A	N/A

Quick Setup: AAA Authentication

Method List Name*

LWA-AUTHENTICATION

Type*

login

i

Group Type

local

i

Available Server Groups

radius
ldap
tacacs+
AAA-group

>
<
>>
<<

Assigned Server Groups

^
^
v
v

Cancel

Apply to Device

Depois de clicar em Apply to Device, confirme a criação da lista de métodos AAA:



Verifique se há uma lista de métodos de autorização local, isso é um requisito para que a lista de métodos de login local criada funcione.

Configuration > Security > AAA > AAA Method List > Authorization > Add

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

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

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	exec	local	N/A	N/A

Quick Setup: AAA Authorization

Method List Name*

Type* ⓘ

Group Type ⓘ

Authenticated ☐

Available Server Groups

- radius
- ldap
- tacacs+
- AAA-group

Assigned Server Groups

> < >> <<

[Cancel](#) [Apply to Device](#)

Depois de clicar em Apply to Device, confirme a criação da lista de métodos AAA:

Configuration > Security > AAA

[+ AAA Wizard](#)

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

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2	Group3	Group4
☐ default	exec	local	N/A	N/A	N/A	N/A
☐ default	network	local	N/A	N/A	N/A	N/A

1 - 2 of 2 items

Mapas de Parâmetros

Edite o Mapa de Parâmetros Globais em Configuration > Security > Web Auth

Configuration > Security > Web Auth

+ Add - Delete

Selected Rows: 0

Parameter Map Name
☐ global

1 10 items per page

General

Parameter-map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☐

Disable Cisco Logo: ☐

Sleeping Client Status: ☐

Sleeping Client Timeout (minutes): 720

Advanced

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::::

Web Auth intercept HTTPs: ☐

Enable HTTP server for Web Auth: ☒

Disable HTTP secure server for Web Auth: ☐

Banner Configuration

Banner Title:

Banner Type: ☒ None ☐ Banner Text ☐ Read From File

Selecione o tipo de autenticação da Web a ser usado, IP virtual e o ponto de confiança que a WLC apresenta no portal da Web. Nesse caso, o certificado Autoassinado é selecionado e provavelmente causará uma isenção de responsabilidade do tipo "sua conexão não é uma rede privada::ERR_CERT_AUTHORITY_INVALID", pois é um LSC (Locally Significant Certificate) e não é assinado por uma CA reconhecível na Internet. Para corrigir isso, use um certificado assinado por terceiros. Os detalhes estão descritos em [Gerar e fazer download de certificados CSR em WLCs Catalyst 9800](#) ou há uma opção de vídeo que explica o upload e a criação do Truspoint [Renew Certificates for WebAuth & WebAdmin em WLC Cisco 9800 | Configuração do controlador seguro de LAN sem fio](#).

General

Advanced

Parameter-map Name

global

Maximum HTTP connections

100

Init-State Timeout(secs)

120

Type

webauth

Captive Bypass Portal

☐

Disable Success Window

☐

Disable Logout Window

☐

Disable Cisco Logo

☐

Sleeping Client Status

☐

Sleeping Client Timeout (minutes)

720

Virtual IPv4 Address

192.0.2.1

Trustpoint

TP-self-signed-... ▾

Virtual IPv4 Hostname

Virtual IPv6 Address

XXXXXX::X

Web Auth intercept HTTPs

☐

Enable HTTP server for Web Auth

☒

Disable HTTP secure server for Web Auth

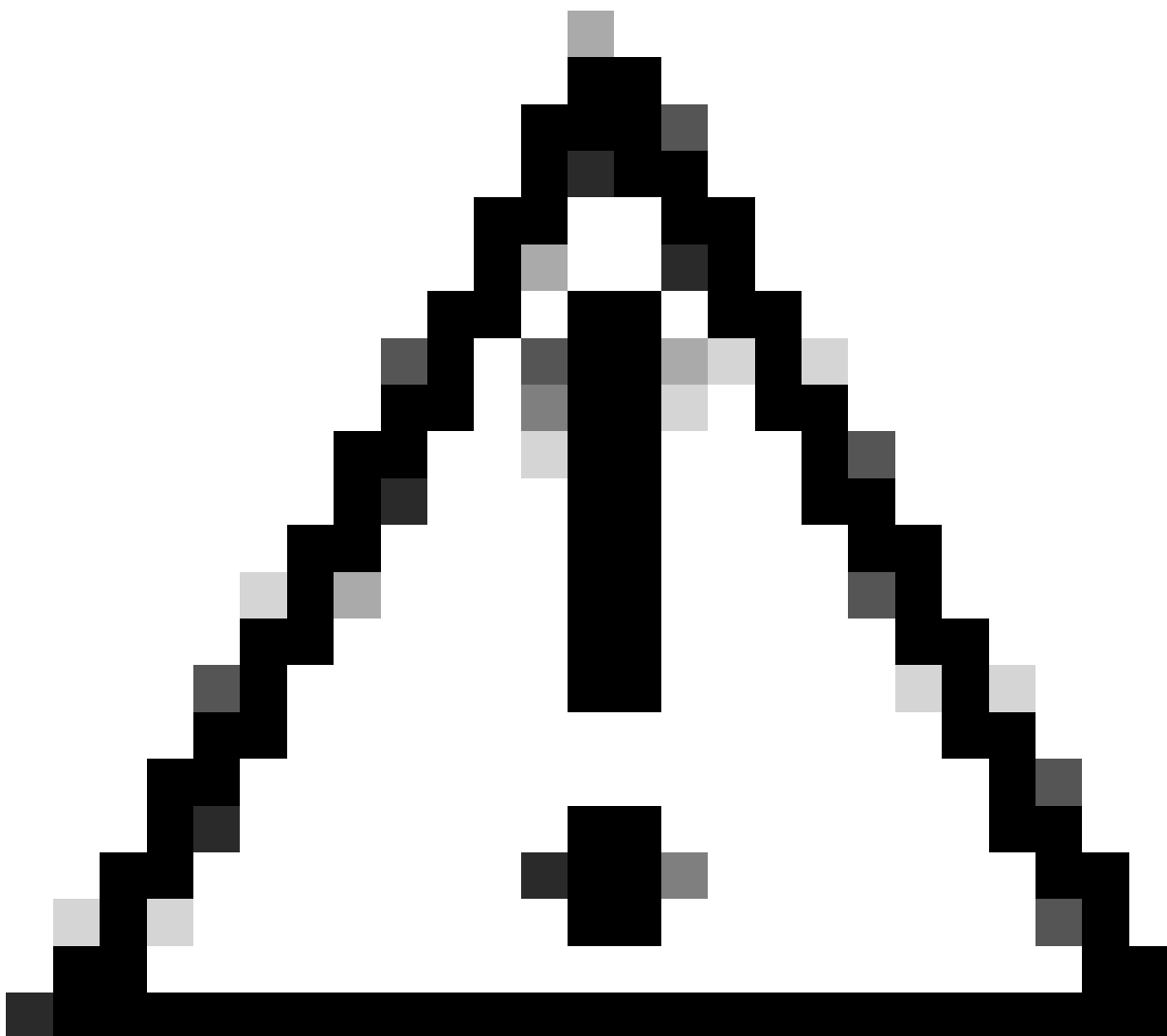
☐

Banner Configuration

Banner Title

Banner Type

☒ None ☐ Banner Text ☐ Read From File



Caution: Se o HTTP estiver desabilitado globalmente no 9800, verifique se a opção Habilitar servidor HTTP para Web Auth está marcada, pois a Cisco separou a dependência desses processos. Espera-se que Clientes ou Suplicantes iniciem um processo de conexão HTTP e que essa sessão seja interceptada pelo controlador para apresentar o portal da Web. Por esse motivo, não é recomendável habilitar o Web Auth Intercept HTTPS, a menos que seja absolutamente necessário, pois essa configuração é desnecessária para a maioria das implantações e pode aumentar a utilização da CPU do controlador, possivelmente afetando o desempenho.

Parâmetros de segurança da WLAN

Navegue até Configuration > Tags & Profiles > WLANs e clique em Add.

⚠ 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

Profile Name*

LWA_LA

SSID*

LWA LA

WLAN ID*

1

Status

ENABLED ☒

Broadcast SSID

ENABLED ☒

Radio Policy ⓘ

6 GHz

Status

ENABLED ☒☒ Slot 2/3

✖ WPA3 Enabled

✔ Dot11ax Enabled

5 GHz

Status

ENABLED ☒☒ Slot 0☒ Slot 1☒ Slot 2

2.4 GHz

Status

ENABLED ☒☒ Slot 0802.11b/g
Policy

802.11b/g ▼

Na guia Security, para Layer2, selecione None.

Edit WLAN

⚠ 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

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

☐ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☒ None

MAC Filtering

☐

OWE Transition Mode

☐

Lobby Admin Access

☐

Fast Transition

Status

Adaptive Ena...

Over the DS

☐

Reassociation Timeout *

20

Na guia Security, para Layer3, marque a caixa Web Policy, selecione o Parameter Map configurado anteriormente no menu suspenso e na Authentication List.

Edit WLAN

⚠ 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

Web Policy

☒

Web Auth Parameter Map

global

Authentication List

LWA_AUTHENTI...

On MAC Filter Failure

☐

Splash Web Redirect

DISABLED

Preauthentication ACL

IPv4

None

IPv6

None

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Criar um perfil de política

Para criar o perfil de política a ser vinculado ao perfil de WLAN, navegue para Configuration > Tags & Profiles > Policy.

Edit Policy Profile

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

LWA_CentralSW

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

☐

SGACL Enforcement

☐

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Na guia Access Policies, selecione a VLAN de onde os Clientes/Solicitantes devem solicitar um IP.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

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

RADIUS Profiling

☐

HTTP TLV Caching

☐

DHCP TLV Caching

☐

WLAN Local Profiling

Global State of Device Classification

Enabled ⓘ

Local Subscriber Policy Name

Search or Select ▼ ⓘ

VLAN

VLAN/VLAN Group

2622 ▼ ⓘ

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 ▼ ⓘ

Criar uma Marca de Diretiva

Para este guia de configuração, criamos uma marca de política personalizada chamada LWA.

Edit Policy Tag

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

Name*

LWA

Description

LWA_LA

✓ WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
☐ LWA_LA	LWA_CentralSW
1 - 1 of 1 items	

Associar a WLAN e o Perfil de Diretiva

Para vincular as políticas de comutação do Policy Profile e da WLAN, navegue para Configuration

> Tags & Profiles > WLANs, selecione o Perfil da WLAN e clique em Add to Policy Tags.

The screenshot shows the 'Edit WLAN' window with a warning message at the top: 'Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.' Below this, there are four tabs: 'General', 'Security', 'Advanced', and 'Add To Policy Tags'. The 'Add To Policy Tags' tab is active. It contains two buttons: '+ Add' and '× Delete'. Below the buttons is a table with two columns: 'Policy Tag' and 'Policy Profile'. The table has one row with the values 'LWA' and 'LWA_CentralSW'. At the bottom of the table, there are pagination controls showing '1' of '10' items, and a status bar indicating '1 - 1 of 1 items'.

Policy Tag	Policy Profile
LWA	LWA_CentralSW

Atribuir uma etiqueta de política a um AP

Para marcar o AP com a tag Policy criada, navegue para Configuration > Wireless > Access Points, selecione o AP e, na guia General, à direita, há as tags usadas pelo AP.

Edit AP

General

Interfaces

High Availability

Inventory

Geolocation

Advanced

Support Bundle

General

AP Name*

9117

Location*

default location

Base Radio MAC

cc0

Ethernet MAC

c00

Admin Status

ENABLED

AP Mode

Local

Operation Status

Registered

Fabric Status

Disabled

LED Settings

LED State

ENABLED

Brightness Level

8

Flash Settings

Flash State

DISABLED

Apply

Time Statistics

Up Time

8 days 15 hrs 26 mins 48 secs

Controller Association Latency

1 sec

Tags

Policy

LWA

Site

default-site-tag

RF

default-rf-tag

Write Tag Config to AP

Version

Primary Software Version

17.12.5.41

Predownloaded Status

N/A

Predownloaded Version

N/A

Next Retry Time

N/A

Boot Version

1.1.2.4

IOS Version

17.12.5.41

Mini IOS Version

0.0.0.0

IP Config

CAPWAP Preferred Mode

IPv4

DHCP IPv4 Address

172.16.60.40

Static IP (IPv4/IPv6)

Cancel

Update & Apply to Device

Criar nome de usuário convidado

Se você selecionou o tipo de webauth no Mapa de Parâmetros, um Nome de Usuário Convidado será necessário para criá-lo, navegue até Configuração > Segurança > Usuário Convidado.

O tempo de vida máximo do usuário é de 1 ano. Você pode especificar o contrário com as opções disponíveis.

[+ Add](#) [- Delete](#)

Selected Rows: 0

☐ User Name
☐ johndoe

1 10 items per page

Edit Guest User

General

Enter User Name* johndoe

Password* [🔑](#)

☐ Generate password

Confirm Password

Description* Guest-User

AAA Attribute list [+](#)

No. of Simultaneous User Logins*
Enter 0 for unlimited users

Start Time 15:21:19 UTC Aug 26 2025

Expiry Time 15:21:19 UTC Aug 21 2026

Remaining Time 0 years 11 months 29 days 23 hours 34 mins 24 secs

Lifetime

Years*

Months*

Days*

Hours*

Mins*

Verificar

Via GUI

Cisco Catalyst 9800-CL Wireless Controller 17.12.5

Welcome admin

Monitoring > Wireless > Clients

Monitoring Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

☐	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐	9ef2.4b16.a507	172.16.74.83	fe80-9cf2-4b16-fe16:a507	9117	0	LWA LA	1	WLAN	Run	11ax(2.4)	johndoe	N/A	Local	No

1 - 1 of 1 clients

Monitoring > Wireless > Clients

Clients
Sleeping Clients
Excluded Clients

Delete
Refresh

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID
☐	507	172.16.74.83	fe80::9cf2:4bff:fe16:a507	-9117	0	LWA LA

1
10

Client
360 View
General
QoS Statistics
ATF Statistics
Mobility History
Call Statistics

Client Properties
AP Properties
Security Information
Client Statistics
QoS Properties
EoGRE

MAC Address
Client MAC Type
Client DUID
IPv4 Address
IPv6 Address
User Name
Policy Profile
Flex Profile
Wireless LAN Id
WLAN Profile Name
Wireless LAN Network Name (SSID)
BSSID
Uptime(sec)
Idle state timeout
Session Timeout
Session Warning Time
Client Active State
Power Save mode
Current TxRateSet
Supported Rates
QoS Average Data Rate Upstream
QoS Realtime Average Data Rate Upstream
QoS Burst Data Rate Upstream
QoS Realtime Burst Data Rate Upstream
QoS Average Data Rate Downstream
QoS Realtime Average Data Rate Downstream
QoS Burst Data Rate Downstream
QoS Realtime Burst Data Rate Downstream
Join Time Of Client
Policy Manager State
Last Policy Manager State
Transition Disable Bitmap
User Defined (Private) Network
User Defined (Private) Network Drop
Unicast

y507
Locally Administered Address
NA
172.16.74.83
fe80::9cf2:4bff:fe16:a507
johndoe
LWA_CentralSW
N/A
1
LWA_LA
LWA LA
0cd0.f897.acc0
151 seconds
N/A
28800 sec (Remaining time: 28678 sec)
Timer not running
Active
ON
1.0
1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
09/10/2025 21:26:11 UTC
Run
Webauth Pending
0x00
Disabled
Disabled

OK

Usando a CLI

```

9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name          Type ID State Protocol Method  Role
-----
9ef2.4b16.a507   xxxxx-9117 WLAN 1 Run  11ax(2.4) Web Auth Local
9800WLC#show wireless client mac-address

```

detail

Client MAC Address : 9ef2.4b16.a507

Client MAC Type : Locally Administered Address

Client DUID: NA

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

Signal to Noise Ratio : 4 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

Autenticação da Web local no switching local do FlexConnect

Para este cenário, supõe-se que o AP esteja no modo FlexConnect. Para que um AP esteja no Modo FlexConnect, você precisa de um Perfil Flex associado no SiteTag, onde a caixa de seleção Ativar site local está desativada. Esta tag de site usa o nome de perfil Flex_LWA e o nome de perfil ap-join padrão:

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+

 Add

-

 Delete

+

 Clone

Reset APs

Site Tag Name

☐ FlexConnect

☐ default-site-tag

1

10

Edit Site Tag

Name*

FlexConnect

Description

Enter Description

AP Join Profile

default-ap-profile

Flex Profile

Flex_LWA

Fabric Control Plane Name

Enable Local Site

☐

Load*

0

Atribuir uma etiqueta de política a um AP

Navegue até Configuration > Wireless > Access Points, selecione o AP e, na guia General, à direita, há as tags usadas pelo AP.

Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- Geolocation
- Advanced
- Support Bundle

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED ☒

AP Mode

Operation Status Registered

Fabric Status Disabled

LED Settings

LED State ☐ DISABLED

Flash Settings

Flash State ☐ DISABLED

Tags

Policy

Site

RF

Write Tag Config to AP

Version

Primary Software Version	17.12.5.41
Predownload Status	N/A
Predownload Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
iOS Version	17.12.5.41
Mini iOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	Not Configured
DHCP IPv4 Address	172.16.60.40
Static IP (IPv4/IPv6)	☐

Time Statistics

Up Time	8 days 15 hrs 51 mins 4 secs
Controller Association Latency	1 sec



aviso: Alterar as marcas faz com que o AP se desjunte da WLC.

Configuration > Wireless > Access Points

▼ All Access Points

Total APs: 1

Misconfigured APs
Tag : 0 Country Code : 0 LSC Fallback : 0 Select an Action ▼

Multiple APs can be configured at once from [Bulk AP Provisioning](#) feature

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Configuration Status	Country Code Misconfigured	LSC Fallback Misconfigure
9117	C9117AXI-A	2	✓	8 days 15 hrs 54 mins 53 secs	172.16.60.40	cc0	c00	Flex	No	Registered	Healthy	No	No

O Perfil de Política associado à WLAN é Comutação Local

Edit WLAN

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

+ Add

× Delete

Policy Tag

Policy Profile

LWA

LWA_LocalSW

1

10

1 - 1 of 1 items

Configuration > Tags & Profiles > Policy

+ Add

× Delete

🔄 Clone

Policy Profile Name "is equal to" LWA_LocalSW

Admin Status

Associated Policy Tags

Policy Profile Name

LWA_LocalSW

1

10

Edit Policy Profile

Disabling a Policy or configuring it in "Enabled" state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QoS and AVC

Mobility

Advanced

Name*

LWA_LocalSW

WLAN Switching Policy

Description

Enter Description

Central Switching

DISABLED

Status

ENABLED

Central Authentication

ENABLED

Passive Client

DISABLED

Central DHCP

ENABLED

IP MAC Binding

ENABLED

Flex NAT/PAT

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

Verificar

9800WLC>enable

9800WLC#show wireless client summary

Number of Clients: 1

MAC Address	AP Name	Type	ID	State	Protocol	Method	Role
-------------	---------	------	----	-------	----------	--------	------

9ef2.4b16.a507	xxxxx-9117	WLAN	1	Run	11ax(2.4)	Web Auth	Local
----------------	------------	------	---	-----	-----------	----------	-------

9800WLC#show wireless client mac-address

detail

Client MAC Address :

Client MAC Type : Locally Administered Address

Client DUID: NA

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

The screenshot displays the Cisco WLC interface. On the left, the 'Clients' tab is active, showing a list of clients. The selected client has the following details:

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID
507	172.16.74.83	fe80::9cf2:4bff:fe16:a507	9117	0	LWA LA

On the right, the 'Client Properties' window is open, showing the 'General' tab. The 'Policy Profile' and 'Flex Profile' are highlighted with a red box. The 'Flex Profile' is set to 'Flex_LWA'.

Property	Value
MAC Address	9ef2.4b16.a507
Client MAC Type	Locally Administered Address
Client DUID	NA
IPv4 Address	172.16.74.83
IPv6 Address	fe80::9cf2:4bff:fe16:a507
User Name	john doe
Policy Profile	LWA_LocalSW
Flex Profile	Flex_LWA
Wireless LAN Id	1
WLAN Profile Name	LWA_LA
Wireless LAN Network Name (SSID)	LWA LA
BSSID	cc0
Uptime(sec)	103 seconds
Idle state timeout	N/A
Session Timeout	28800 sec (Remaining time: 28737 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	OFF
Current TxRateSet	m11 ss2
Supported Rates	1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
QoS Average Data Rate Upstream	0 (kbps)
QoS Realtime Average Data Rate Upstream	0 (kbps)
QoS Burst Data Rate Upstream	0 (kbps)
QoS Realtime Burst Data Rate Upstream	0 (kbps)
QoS Average Data Rate Downstream	0 (kbps)
QoS Realtime Average Data Rate Downstream	0 (kbps)
QoS Burst Data Rate Downstream	0 (kbps)
QoS Realtime Burst Data Rate Downstream	0 (kbps)
Join Time Of Client	09/11/2025 17:38:26 UTC
Policy Manager State	Run
Last Policy Manager State	Webauth Pending
Transition Disable Bitmap	0x00
User Defined (Private) Network	Disabled
User Defined (Private) Network Drop Unicast	Disabled

Troubleshooting

O status "Autenticação da Web pendente" indica que o cliente foi associado ao ponto de acesso, mas ainda não concluiu o processo de autenticação da Web. Durante esse estado, o controlador intercepta o tráfego HTTP do cliente e o redireciona para um portal de autenticação da Web para login do usuário ou aceitação dos termos. O cliente permanece nesse estado até que a autenticação da Web bem-sucedida seja concluída, após o que o estado do gerenciador de políticas do cliente muda para "Executar" e o acesso total à rede é concedido.

para ver o fluxo da conexão do cliente visualmente, verifique o Fluxo de LWA em [Configurar Autenticação da Web Local com Autenticação Externa](#).

Os estágios pelos quais o cliente passa da perspectiva do cliente são descritos em [Troubleshooting de Problemas Comuns com LWA em 9800 WLCs](#).

- [Suporte Técnico e Documentação - Cisco Systems](#)

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.