

Configurar OEAP e RLAN no Catalyst 9800 WLC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[AP Join por trás do NAT](#)

[Configuração](#)

[Verificar](#)

[Efetue login no OEAP e configure o SSID pessoal](#)

[Configurar RLAN na WLC 9800](#)

[Troubleshoot](#)

Introduction

Este documento explica como configurar o Cisco OfficeExtend Access Point (OEAP) e a Remote Local Area Network (RLAN) na WLC 9800.

Um ponto de acesso Cisco OfficeExtend (OEAP) fornece comunicações seguras de um controlador para um AP Cisco em um local remoto, estendendo perfeitamente a WLAN corporativa pela Internet para a residência de um funcionário. A experiência de um usuário no escritório doméstico é exatamente a mesma que seria no escritório corporativo. A criptografia DTLS (Datagram Transport Layer Security) entre um ponto de acesso e o controlador garante que todas as comunicações tenham o mais alto nível de segurança.

Uma LAN remota (RLAN) é usada para autenticar clientes com fio usando o controlador. Depois que o cliente com fio ingressa com êxito no controlador, as portas LAN comutam o tráfego entre os modos de comutação central ou local. O tráfego dos clientes com fio é tratado como tráfego de cliente sem fio. O RLAN no ponto de acesso (AP) envia a solicitação de autenticação para autenticar o cliente com fio. A autenticação dos clientes com fio em RLAN é semelhante ao cliente sem fio autenticado central.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- WLC 9800
- Acesso à CLI (Command-Line Interface, interface de linha de comando) para os controladores e pontos de acesso sem fio

Componentes Utilizados

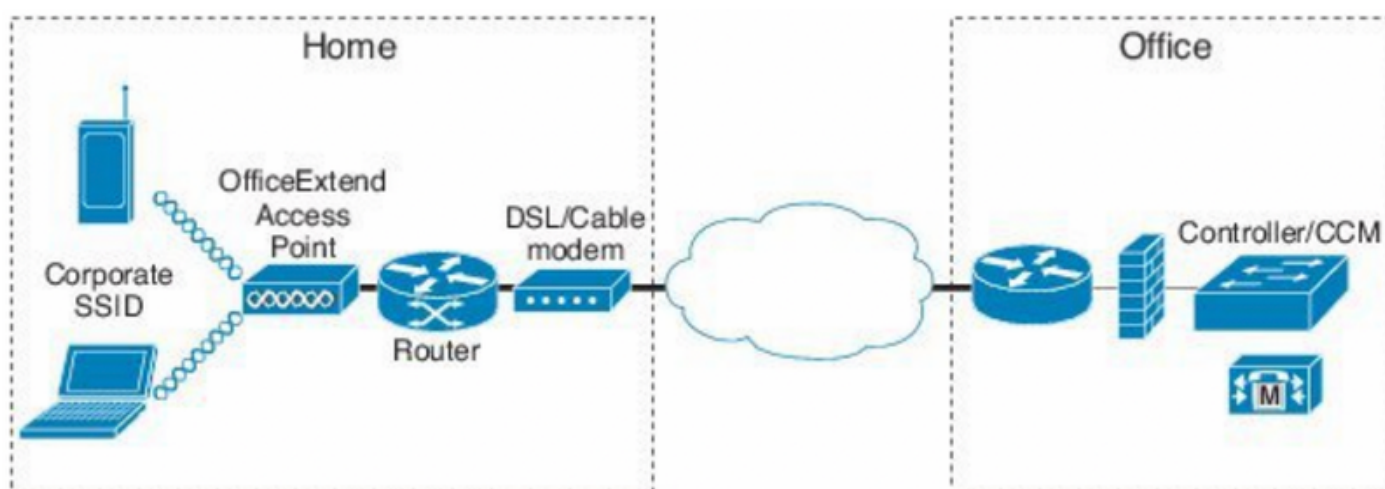
As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9800 WLC versão 17.02.01
- AP 1815/1810 Series

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.

Configurar

Diagrama de Rede



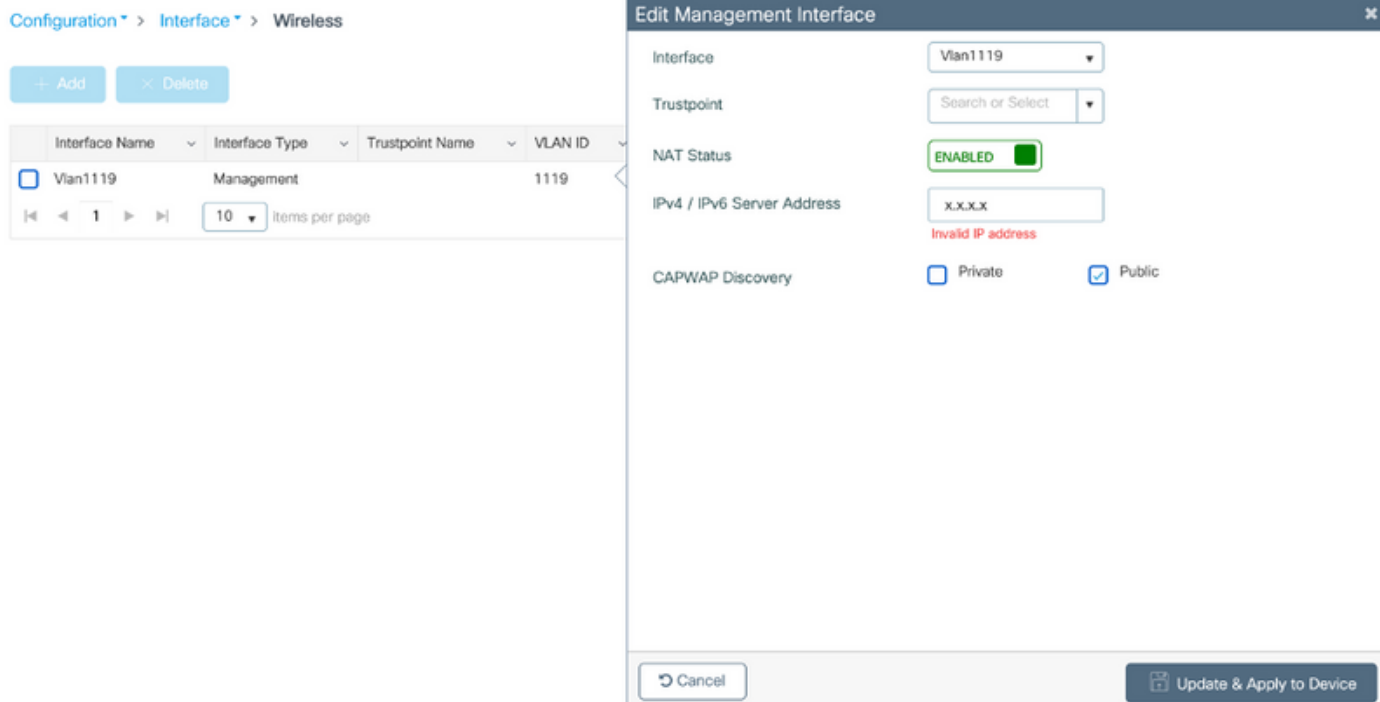
AP Join por trás do NAT

Nos códigos 16.12.x, você precisa configurar o endereço IP NAT da CLI. Não há nenhuma opção de GUI disponível. Você também pode selecionar a descoberta de CAPWAP através de IP público ou privado.

```
(config)#wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface)#capwap-discovery ?
  private  Include private IP in CAPWAP Discovery Response

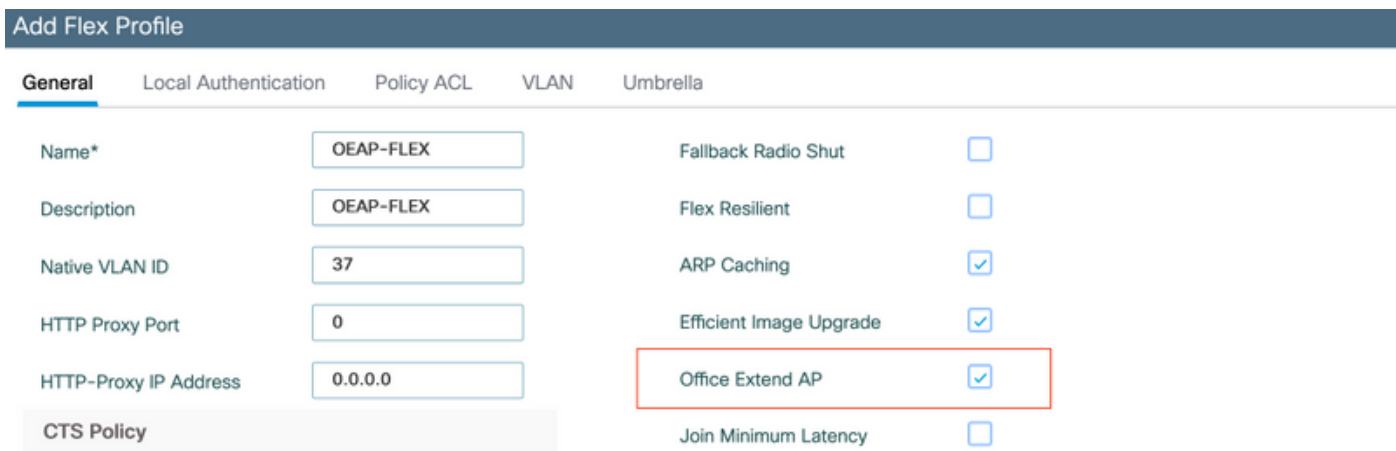
  public   Include public IP in CAPWAP Discovery Response
```

Nos códigos 17.x, navegue para **Configuration > Interface > Wireless** e clique em **Wireless Management Interface**, para configurar o tipo de descoberta de NAT IP e CAPWAP na GUI.



Configuração

1. Para criar um perfil Flex, ative o **Office Extend AP** e navegue para **Configuration > Tags & Profiles > Flex**.



2. Para criar uma etiqueta de site e mapear o Flex Profile, navegue para **Configuration > Tags & Profiles > Tags**.

Add Site Tag

Name*

Home-Office

Description

Enter Description

AP Join Profile

default-ap-profile ▼

Flex Profile

OEAP-FLEX| ▼

Control Plane Name

▼

Enable Local Site

Cancel

3. Navegue para marcar o AP 1815 com a tag Site criada por **Configuration > Wireless Setup >Advanced > Tag APs**.

Tag APs



Tags

Policy

default-policy-tag ▼

Site

Home-Office ▼

RF

default-rf-tag ▼

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel



Apply to Device

Verificar

Depois que o AP 1815 reingressar na WLC, verifique esta saída:

```
vk-9800-1#show ap name AP1815 config general
```

```
Cisco AP Name      : AP1815
```

```
=====
```

```
Cisco AP Identifier      : 002c.c8de.3460
```

```
Country Code            : Multiple Countries : IN,US
```

```
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-ABDN
```

```
AP Country Code        : US - United States
```

```
Site Tag Name         : Home-Office
```

```
RF Tag Name            : default-rf-tag
```

```
Policy Tag Name        : default-policy-tag
```

```
AP join Profile        : default-ap-profile
```

```
Flex Profile         : OEAP-FLEX
```

```
Administrative State    : Enabled
```

```
Operation State        : Registered
```

```
AP Mode                : FlexConnect
```

```
AP VLAN tagging state   : Disabled
```

```
AP VLAN tag            : 0
```

```
CAPWAP Preferred mode   : IPv4
```

```
CAPWAP UDP-Lite        : Not Configured
```

```
AP Submode             : Not Configured
```

```
Office Extend Mode   : Enabled
```

```
Dhcp Server            : Disabled
```

```
Remote AP Debug        : Disabled
```

```
vk-9800-1#show ap link-encryption
```

	Encryption	Dnstream	Upstream	Last
AP Name	State	Count	Count	Update

N2	Disabled	0	0	06/08/20 00:47:33

when you enable the OfficeExtend mode for an access point DTLS data encryption is enabled automatically.

```
AP1815#show capwap client config
```

```
AdminState           : ADMIN_ENABLED(1)
Name                 : AP1815
Location             : default location
Primary controller name : vk-9800-1
ssh status           : Enabled
ApMode               : FlexConnect
ApSubMode            : Not Configured
Link-Encryption      : Enabled
OfficeExtend AP      : Enabled
Discovery Timer      : 10
Heartbeat Timer      : 30
Syslog server        : 255.255.255.255
Syslog Facility      : 0
Syslog level         : informational
```

Note: Você pode habilitar ou desabilitar a criptografia de dados DTLS para um ponto de acesso específico ou para todos os pontos de acesso usando o comando `ap link-encryption`

```
vk-9800-1(config)#ap profile default-ap-profile
```

```
vk-9800-1(config-ap-profile)#no link-encryption
```

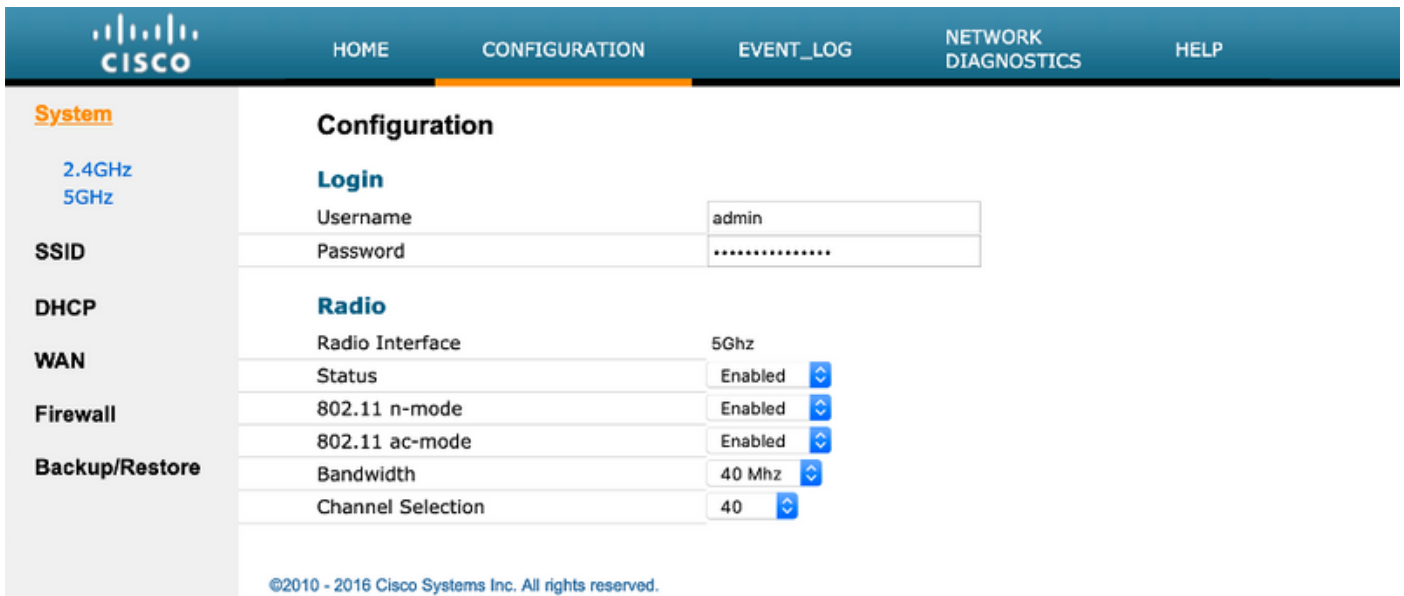
Disabling link-encryption globally will reboot the APs with link-encryption.

```
Are you sure you want to continue? (y/n) [y]:y
```

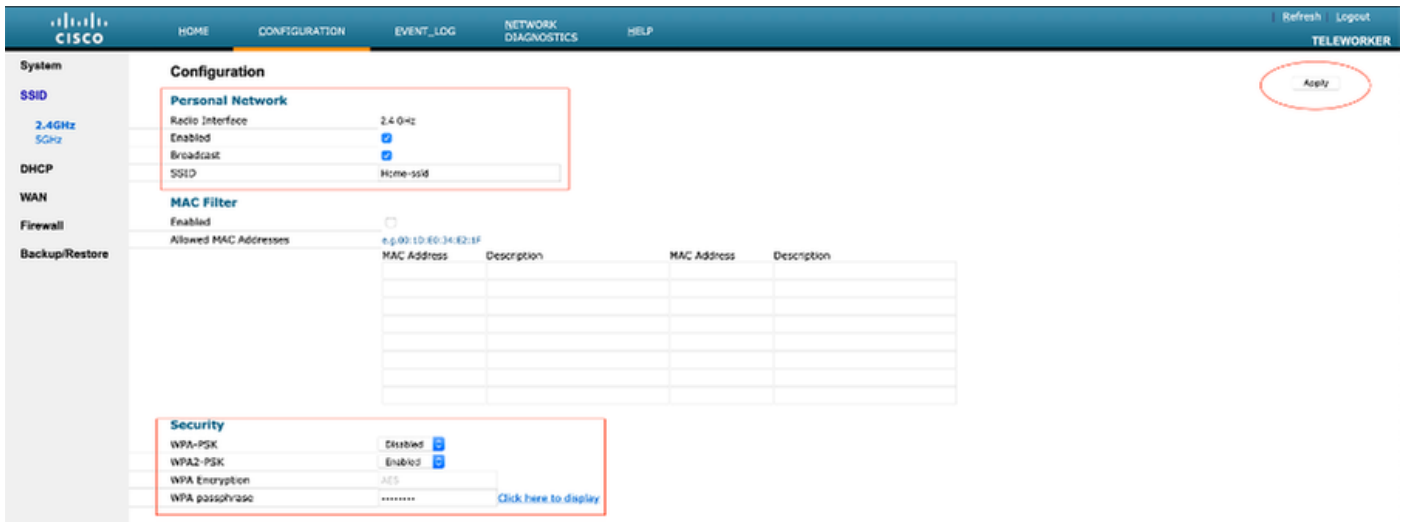
Efetue login no OEAP e configure o SSID pessoal

1. Você pode acessar a interface da Web do OEAP com seu endereço IP. As credenciais padrão para fazer login são **admin** e **admin**.

2. É recomendável alterar as credenciais padrão por motivos de segurança.



3. Navegue até **Configuration> SSID> 2.4GHz/5GHz** para configurar o SSID pessoal.



4. Ative a interface de rádio.

5. Insira o SSID e ative a transmissão

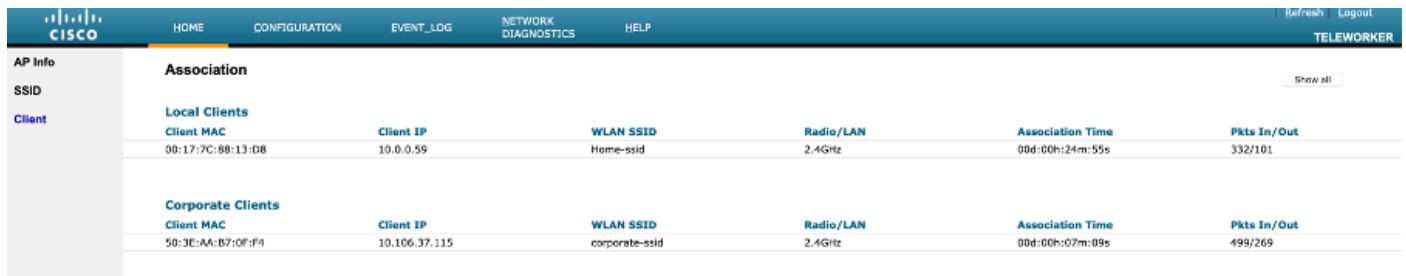
6. Para criptografia, escolha **WPA-PSK** ou **WPA2-PSK** e insira a senha para o tipo de segurança correspondente.

7. Clique em Apply para que as configurações entrem em vigor.

8. Por padrão, os clientes que se conectam ao SSID pessoal obtêm o endereço IP da rede 10.0.0.1/24.

9. Os usuários domésticos podem usar o mesmo AP para se conectar para uso doméstico e o tráfego não é transmitido pelo túnel DTLS.

10. Para verificar associações de clientes no OEAP, navegue para **Home > Client**. Você pode ver os clientes locais e corporativos associados ao OEAP.



The screenshot shows the Cisco OEAP interface with a navigation bar at the top containing 'HOME', 'CONFIGURATION', 'EVENT_LOG', 'NETWORK DIAGNOSTICS', and 'HELP'. On the right side of the navigation bar are 'Refresh' and 'Logout' buttons. The main content area is titled 'Association' and includes a 'Show all' button. It is divided into two sections: 'Local Clients' and 'Corporate Clients'. Each section contains a table with columns for 'Client MAC', 'Client IP', 'WLAN SSID', 'Radio/LAN', 'Association Time', and 'Pkts In/Out'.

Local Clients						
Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out	
00:17:7C:8B:13:D8	10.0.0.59	Home-ssid	2.4Ghz	00d:00h:24m:55s	332/101	

Corporate Clients						
Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out	
50:3E:AA:B7:0F:F4	10.106.37.115	corporate-ssid	2.4Ghz	00d:00h:07m:09s	499/269	

To clear personal ssid from office-extend ap

```
ewlc#ap name cisco-ap clear-personalssid-config
```

clear-personalssid-config Clears the Personal SSID config on an OfficeExtend AP

Configurar RLAN na WLC 9800

Uma LAN remota (RLAN) é usada para autenticar clientes com fio usando o controlador. Depois que o cliente com fio ingressa com êxito no controlador, as portas LAN comutam o tráfego entre os modos de comutação central ou local. O tráfego dos clientes com fio é tratado como tráfego de cliente sem fio. O RLAN no ponto de acesso (AP) envia a solicitação de autenticação para autenticar o cliente com fio. O

A autenticação dos clientes com fio em RLAN é semelhante ao cliente sem fio autenticado central.

Note: O EAP local está sendo usado para autenticação de cliente RLAN neste exemplo. A configuração EAP local deve estar presente na WLC para configurar as etapas abaixo. Ele inclui métodos de autenticação e autorização de aaa, perfil EAP local e credenciais locais.

[Autenticação EAP local no exemplo de configuração do Catalyst 9800 WLC](#)

1. Para criar um perfil de RLAN, navegue para **Configuration > Wireless > Remote LAN** e insira um nome e uma ID de RLAN para o perfil de RLAN, como mostrado nesta imagem.

Add RLAN Profile

General Security

Profile Name*

RLAN ID*

Status **ENABLED**

Client Association Limit

mDNS Mode

2. Navegue até **Security > Layer2**, para habilitar 802.1x para uma RLAN, defina o status 802.1x como Enabled (Habilitado), como mostrado nesta imagem.

Edit RLAN Profile

General **Security**

Layer2 Layer3 AAA

802.1x **ENABLED**

MAC Filtering

Authentication List

3. Navegue até **Security > AAA**, defina Local EAP Authentication como enabled e escolha o EAP Profile Name necessário na lista suspensa, como mostrado nesta imagem.

Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP ▼

4. Para criar uma política de RLAN, navegue para **Configuration > Wireless > Remote LAN** e, na página Remote LAN, clique na guia **RLAN Policy**, como mostrado nesta imagem.

The screenshot shows the 'Edit RLAN Policy' configuration page with the 'General' tab selected. A warning message at the top states: 'Configuring in enabled state will result in loss of connectivity for clients associated with this policy.' The configuration fields are as follows:

Field	Value
Policy Name*	RLAN-Policy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
PoE	<input type="checkbox"/>
Power Level	4 ▼
RLAN Switching Policy	Central Switching: ENABLED <input checked="" type="checkbox"/> Central DHCP: ENABLED <input checked="" type="checkbox"/>

Navegue até Access Policies (Políticas de acesso) e configure a VLAN e o Host Mode (Modo de host) e aplique as configurações.

The screenshot shows the 'Edit RLAN Policy' configuration page with the 'Access Policies' tab selected. The configuration fields are as follows:

Field	Value
Pre-Authentication	<input type="checkbox"/>
VLAN	VLAN0039 ▼
Host Mode	singlehost ▼
Remote LAN ACL	IPv4 ACL: Not Configured ▼ IPv6 ACL: Not Configured ▼

5. Para criar a tag Policy e o perfil Map RLAN para a política RLAN, navegue até **Configuration > Tags & Profiles > Tags**.

Add Policy Tag



Name*

RLAN-TAG

Description

Enter Description

WLAN-POLICY Maps: 0

RLAN-POLICY Maps: 0

+ Add

× Delete

Port ID	RLAN Profile	RLAN Policy Profile
No items to display		

Map RLAN and Policy

Port ID*

3

RLAN Profile*

RLAN-TEST

RLAN Policy Profile*

RLAN-Policy



Cancel



Apply to Device

Add Policy Tag ✕

Name*

Description

➤ WLAN-POLICY Maps: 0

▼ RLAN-POLICY Maps: 1

	Port ID	RLAN Profile	RLAN Policy Profile
<input type="checkbox"/>	3	RLAN-TEST	RLAN-Policy

⏪ ◀ 1 ▶ ⏩ items per page 1 - 1 of 1 items

6. Ative a porta LAN e aplique a TAG de política no AP. Navegue até **Configuration > Wireless > Access Points** e clique no **AP**.

Edit AP

Location*	default location	Predownloaded Status	N/A
Base Radio MAC	0042.5ab7.8f60	Predownloaded Version	N/A
Ethernet MAC	0042.5ab6.4ab0	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Local ▼	IOS Version	17.2.1.11
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	<input type="checkbox"/> DISABLED	CAPWAP Preferred Mode	Not Configured
LED Brightness Level	8 ▼	DHCP IPv4 Address	10.106.39.198
Tags		Static IP (IPv4/IPv6)	<input type="checkbox"/>
<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.</p>			
Policy	RLAN-TAG ▼	Time Statistics	
Site	default-site-tag ▼	Up Time	0 days 13 hrs 33 mins 40 secs
RF	default-rf-tag ▼	Controller Association Latency	20 secs

Aplique a configuração e o AP reingressa na WLC. Clique no **AP**, selecione **Interfaces** e ative a porta LAN.

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11n - 2.4 GHz	All	Enabled		Disabled		-A
1	802.11ac	All	Enabled		Disabled		-D

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

PoE Pre-Standard Switch: Disabled

PoE Power Injector MAC Address: Disabled

LAN Port Settings

Port ID	Status	VLAN ID	PoE	Power Level	RLAN
LAN1	<input type="checkbox"/>	0	<input type="checkbox"/>	NA	
LAN2	<input type="checkbox"/>	0	NA	NA	
LAN3	<input checked="" type="checkbox"/>	39	NA	NA	

10 items per page 1 - 3 of 3 items

Aplique as configurações e verifique o status.

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11n - 2.4 GHz	All	Enabled		Disabled		-A
1	802.11ac	All	Enabled		Disabled		-D

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

PoE Pre-Standard Switch: Disabled

PoE Power Injector MAC Address: Disabled

LAN Port Settings

Port ID	Status	VLAN ID	PoE	Power Level	RLAN
LAN1	<input type="checkbox"/>	0	<input type="checkbox"/>	NA	
LAN2	<input type="checkbox"/>	0	NA	NA	
LAN3	<input checked="" type="checkbox"/>	39	NA	NA	

10 items per page 1 - 3 of 3 items

7. Conecte um PC na porta LAN3 do AP. O PC será autenticado via 802.1x e receberá um endereço IP da VLAN configurada.

Navegue até **Monitoring > Wireless > Clients** para verificar o status do cliente.

Delete



Total Client(s) in the Network: 2

Number of Client(s) selected: 0

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	State	Protocol	User Name	Device Type	Role
<input type="checkbox"/>	503e.aab7.0ff4	10.106.39.227	2001::c	AP1815	corporate-ssid	3	Run	11n(2.4)		N/A	Local
<input type="checkbox"/>	b496.9126.dd6c	10.106.39.191	fe80:d8cax582:2703:f24e	AP1810	RLAN-TEST	1	Run	Ethernet	vinodh	N/A	Local

Client

360 View General QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QOS Properties EoGRE

Session Manager

IIF ID	0x9000000C
Authorized	TRUE
Common Session ID	00000000000000E79E8C7A9A
Acct Session ID	0x00000000
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE

```
vk-9800-1#show wireless client summary
```

```
Number of Clients: 2
```

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

```
-----
503e.aab7.0ff4 AP1815                WLAN 3   Run
11n(2.4) None          Local
b496.9126.dd6c AP1810                RLAN 1   Run
Ethernet Dot1x        Local
```

```
Number of Excluded Clients: 0
```

Troubleshoot

Problemas comuns:

- Somente o trabalho de SSID local, SSID configurado na WLC não está sendo transmitido: verifique se o AP ingressou corretamente no controlador.
- Não é possível acessar a GUI do OEAP: Verifique se o ap tem endereço IP e verifique a acessibilidade (firewall, ACL, etc na rede)
- Clientes sem fio ou com fio com switch central não podem autenticar ou obter o endereço IP: Tome rastros de RA, sempre sobre rastros, etc.

Exemplo de rastreamentos sempre ativos para o cliente 802.1x com fio:

[client-orch-sm] [18950]: (note): MAC: <client-mac> Association received. BSSID 00b0.e187.cfc0, old BSSID 0000.0000.0000, WLAN test_rlan, Slot 2 AP 00b0.e187.cfc0, Ap_1810

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [18950]: (ERR): MAC: <client-mac> Failed to dot11 determine ms physical radio type. Invalid radio type :0 of the client.

[dot11] [18950]: (ERR): MAC: <client-mac> Failed to dot11 send association response. Encoding of assoc response failed for client reason code: 14.

[dot11] [18950]: (note): MAC: <client-mac> Association success. AID 1, Roaming = False, WGB = False, llr = False, llw = False AID list: 0x1| 0x0| 0x0| 0x0

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-auth] [18950]: (note): MAC: <client-mac> L2 Authentication initiated. method DOT1X, Policy VLAN 1119,AAA override = 0 , NAC = 0

[ewlc-infra-evq] [18950]: (note): Authentication Success. Resolved Policy bitmap:11 for client <client-mac>

[client-orch-sm] [18950]: (note): MAC: <client-mac> Mobility discovery triggered. Client mode: Local

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS

[mm-client] [18950]: (note): MAC: <client-mac> Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Previous BSSID MAC: 0000.0000.0000 Client IFID: 0xa0000003, Client Role: Local PoA: 0x90000012 PoP: 0x0

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS

[dot11] [18950]: (note): MAC: <client-mac> Client datapath entry params - ssid:test_rlan,slot_id:2 bssid ifid: 0x0, radio_ifid: 0x90000006, wlan_ifid: 0xf0404001

[dpath_svc] [18950]: (note): MAC: <client-mac> Client datapath entry created for ifid 0xa0000003

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [18950]: (note): MAC: <client-mac> Client IP learn successful. Method: DHCP IP: <Client-IP>

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Get ATF policy name from WLAN profile:: Failed to get wlan profile. Searched wlan profile test_rlan

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name

[apmgr-bssid] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name from WLAN profile name: No such file or directory

[client-orch-sm] [18950]: (ERR): Failed to get client ATF policy name: No such file or directory

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition:
S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN