

Configuración de OEAP y RLAN en el WLC Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Unión de AP detrás de NAT](#)

[Configuración](#)

[Verificación](#)

[Inicie sesión en OEAP y configure el SSID personal](#)

[Configuración de RLAN en WLC 9800](#)

[Troubleshoot](#)

Introducción

Este documento explica cómo configurar el punto de acceso Cisco OfficeExtend (OEAP) y la red de área local remota (RLAN) en el WLC 9800.

Un punto de acceso Cisco OfficeExtend (OEAP) proporciona comunicaciones seguras desde un controlador a un punto de acceso Cisco en una ubicación remota, ampliando sin problemas la WLAN corporativa a través de Internet a la residencia de un empleado. La experiencia del usuario en la oficina doméstica es exactamente la misma que en la oficina corporativa. El cifrado de seguridad de la capa de transporte del datagrama (DTLS) entre un punto de acceso y el controlador garantiza que todas las comunicaciones tengan el mayor nivel de seguridad.

Se utiliza una LAN remota (RLAN) para autenticar clientes con cables mediante el controlador. Una vez que el cliente cableado se une correctamente al controlador, los puertos LAN conmutan el tráfico entre los modos de conmutación central o local. El tráfico de los clientes por cable se trata como tráfico de cliente inalámbrico. El RLAN en punto de acceso (AP) envía la solicitud de autenticación para autenticar el cliente con cables. La autenticación de los clientes cableados en RLAN es similar al cliente inalámbrico central autenticado.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- WLC 9800
- Acceso de la interfaz de línea de comandos (CLI) a los controladores inalámbricos y los

puntos de acceso

Componentes Utilizados

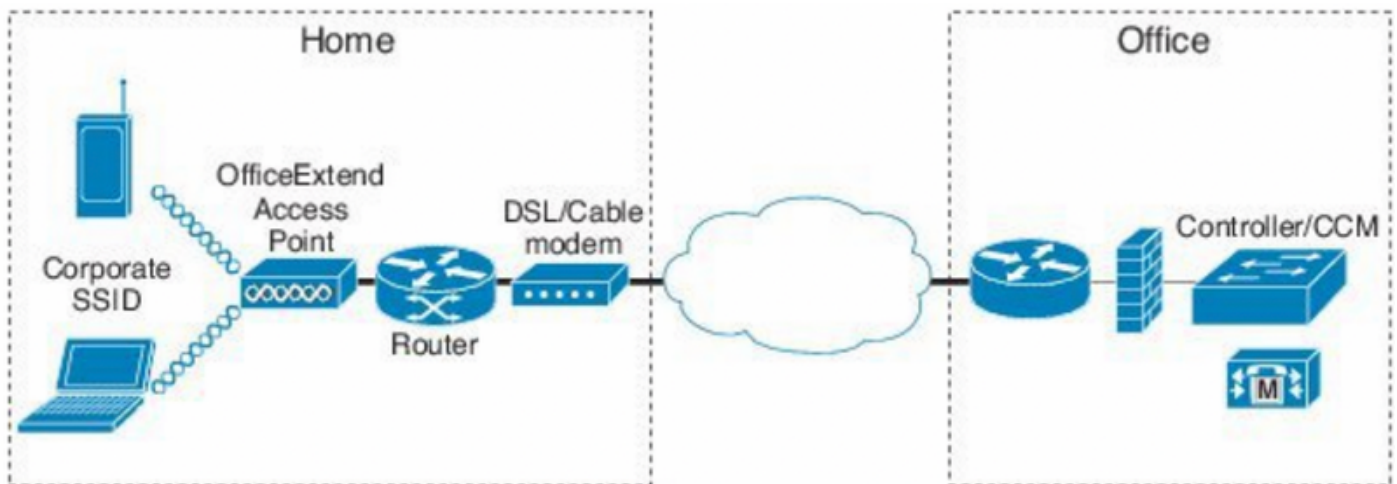
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9800 WLC versión 17.02.01
- AP serie 1815/1810

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



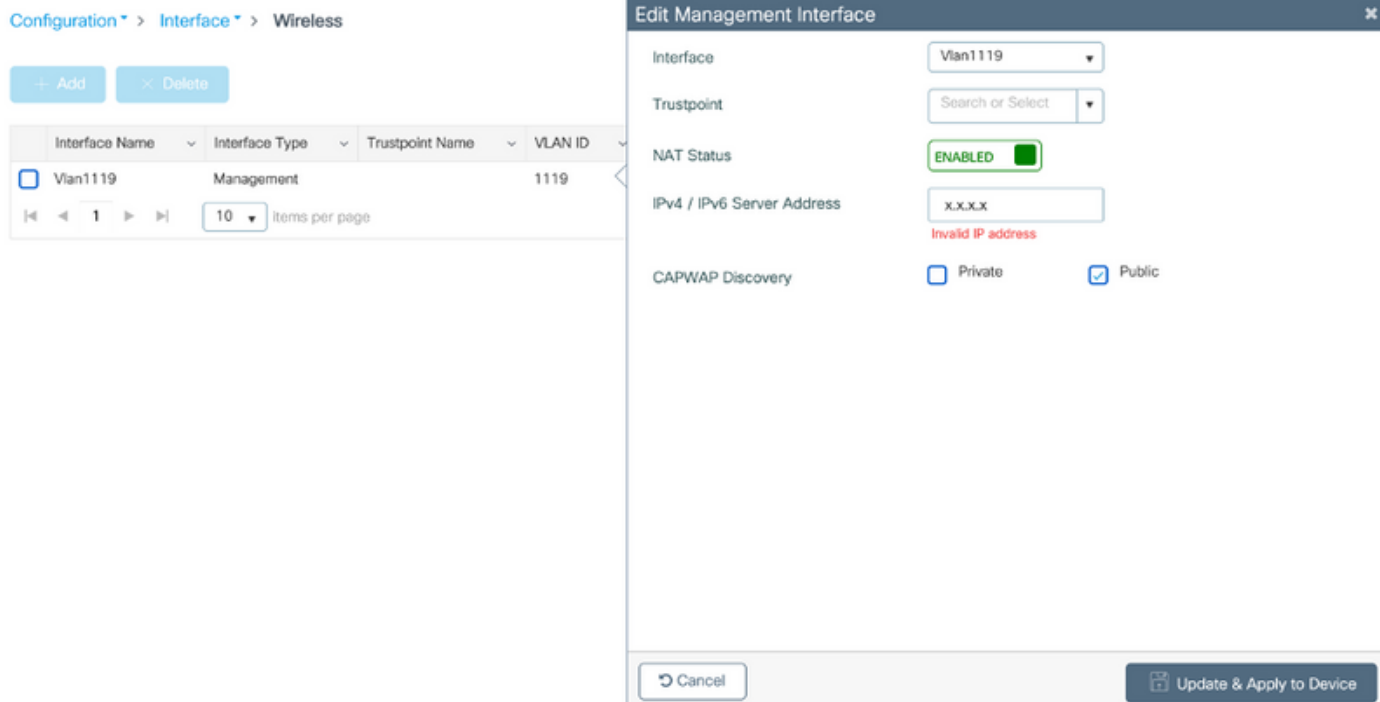
Unión de AP detrás de NAT

En los códigos 16.12.x, debe configurar la dirección IP NAT desde la CLI. No hay ninguna opción de GUI disponible. También puede seleccionar CAPWAP discovery a través de IP pública o privada.

```
(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
```

En los códigos 17.x, navegue hasta **Configuration > Interface > Wireless** y luego haga clic en **Wireless Management Interface**, para configurar NAT IP y el tipo de detección CAPWAP desde la GUI.



Configuración

1. Para crear un perfil Flex, habilite **Office Extend AP** y navegue hasta **Configuration > Tags & Profiles > Flex**.

Add Flex Profile

General	Local Authentication	Policy ACL	VLAN	Umbrella
Name*	OEAP-FLEX			Fallback Radio Shut <input type="checkbox"/>
Description	OEAP-FLEX			Flex Resilient <input type="checkbox"/>
Native VLAN ID	37			ARP Caching <input checked="" type="checkbox"/>
HTTP Proxy Port	0			Efficient Image Upgrade <input checked="" type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0			Office Extend AP <input checked="" type="checkbox"/>
CTS Policy				Join Minimum Latency <input type="checkbox"/>

2. Para crear una etiqueta de sitio y asignar un perfil flexible, navegue hasta **Configuración > Etiquetas y perfiles > Etiquetas**.

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 etiquetar el AP 1815 con la etiqueta del sitio creada por **Configuration > Wireless Setup > Advanced > Tag AP**.

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

Verificación

Una vez que el AP 1815 se reúne al WLC, verifique este resultado:

```
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
```

Nota: Puede activar o desactivar el cifrado de datos DTLS para un punto de acceso específico o para todos los puntos de acceso mediante el comando `ap link-encryption`

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

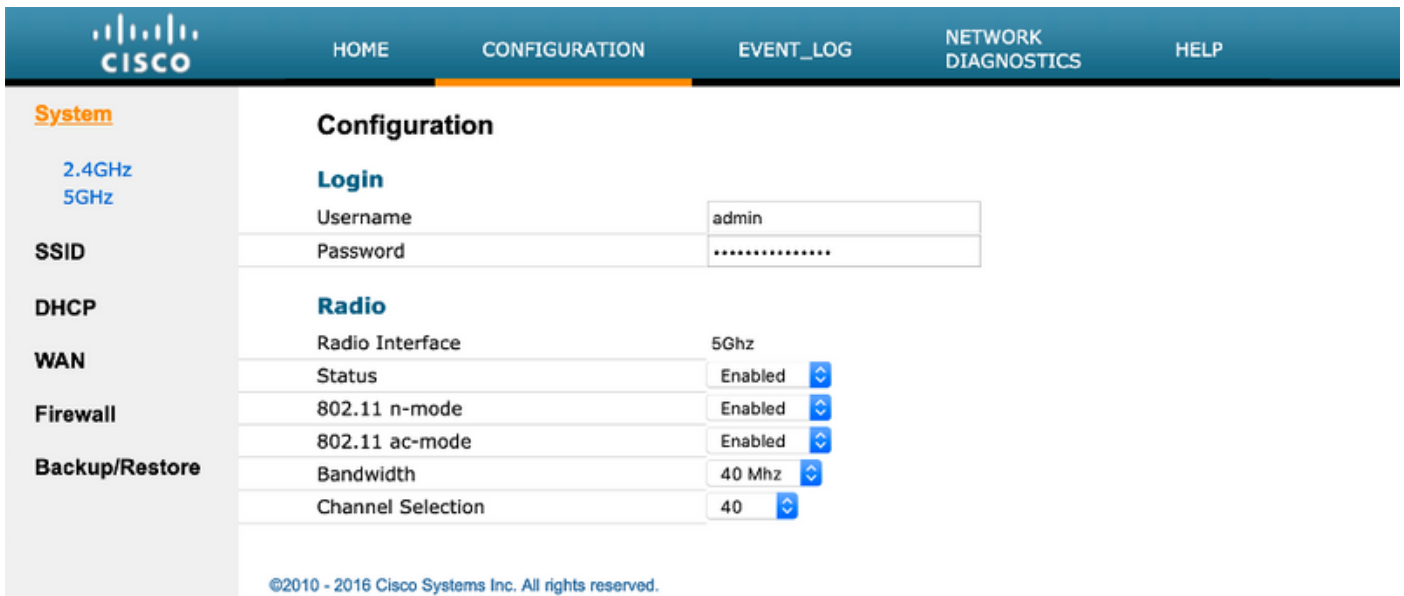
```
vk-9800-1(config-ap-profile)#no link-encryption
```

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

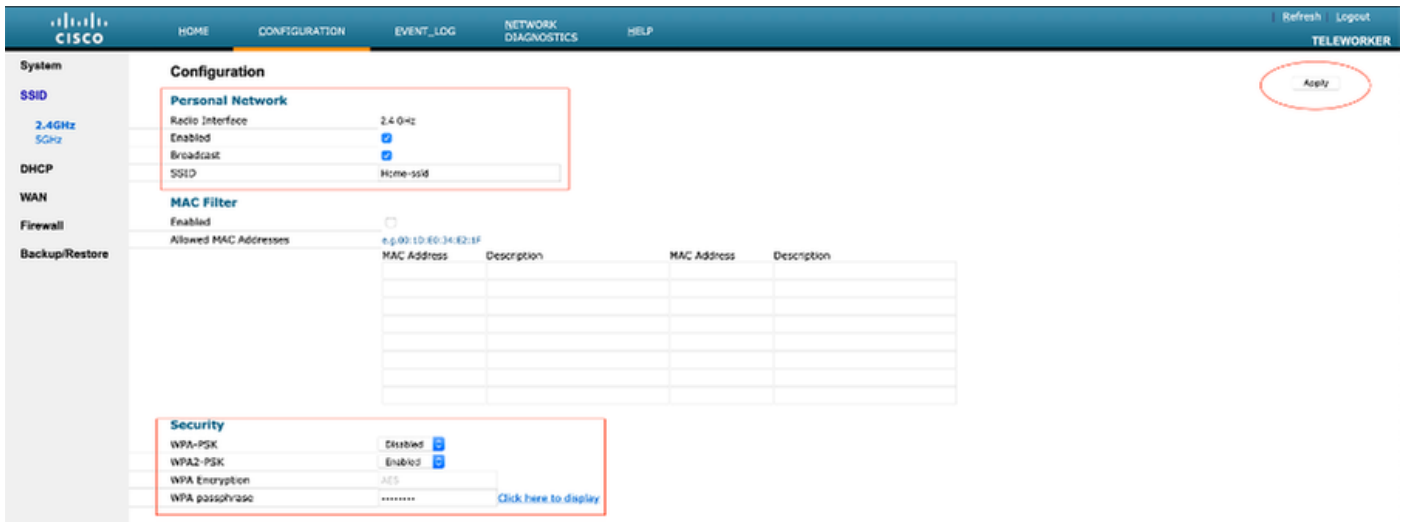
```
Are you sure you want to continue? (y/n) [y]:y
```

Inicie sesión en OEAP y configure el SSID personal

1. Puede acceder a la interfaz web de OEAP con su dirección IP. Las credenciales predeterminadas para iniciar sesión son **admin** y **admin**.
2. Se recomienda cambiar las credenciales predeterminadas por razones de seguridad.



3. Vaya a **Configuration > SSID > 2.4GHz/5GHz** para configurar el SSID personal.



4. Habilite la interfaz de radio.

5. Introduzca el SSID y active Broadcast (Difusión)

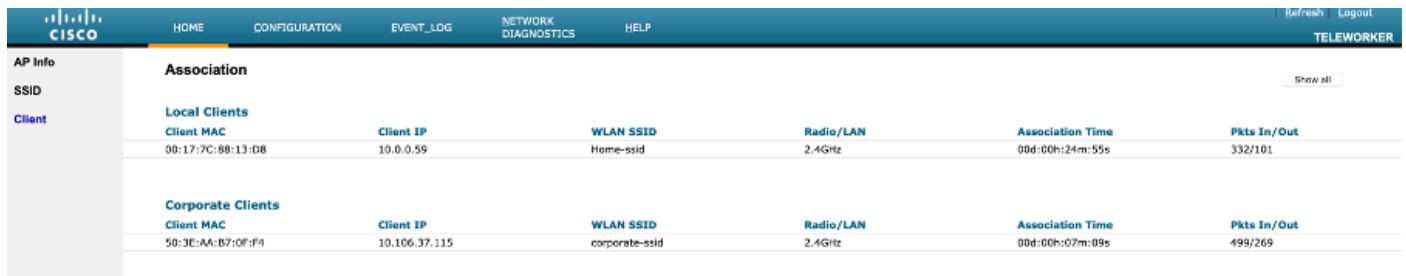
6. Para la encriptación, elija **WPA-PSK** o **WPA2-PSK** e introduzca la frase de paso para el tipo de seguridad correspondiente.

7. Haga clic en Aplicar para que los parámetros surtan efecto.

8. Los clientes que se conectan al SSID personal obtienen la dirección IP de la red 10.0.0.1/24 de forma predeterminada.

9. Los usuarios domésticos pueden utilizar el mismo AP para conectarse para su uso doméstico y que el tráfico no se pasa a través del túnel DTLS.

10. Para verificar las asociaciones de clientes en el OEAP, navegue hasta **Inicio > Cliente**. Puede ver los clientes locales y los clientes corporativos asociados con OEAP.



Association						
Local Clients						
Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out	
90:17:7C:86:13: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

Configuración de RLAN en WLC 9800

Se utiliza una LAN remota (RLAN) para autenticar clientes con cables mediante el controlador. Una vez que el cliente cableado se une correctamente al controlador, los puertos LAN conmutan el tráfico entre los modos de conmutación central o local. El tráfico de los clientes por cable se trata como tráfico de cliente inalámbrico. El RLAN en punto de acceso (AP) envía la solicitud de autenticación para autenticar el cliente con cables.

La autenticación de los clientes cableados en RLAN es similar al cliente inalámbrico central autenticado.

Nota: En este ejemplo se está utilizando EAP local para la autenticación de cliente RLAN. La configuración EAP local debe estar presente en el WLC para configurar los siguientes pasos. Incluye métodos de autenticación y autorización aaa, perfil EAP local y credenciales locales.

[Ejemplo de configuración de autenticación EAP local en el WLC de Catalyst 9800](#)

1. Para crear el perfil RLAN, navegue hasta **Configuration > Wireless > Remote LAN** e ingrese un Nombre y una ID RLAN para el perfil RLAN, como se muestra en esta imagen.

Add RLAN Profile

General Security

Profile Name* RLAN-TEST

RLAN ID* 1

Status **ENABLED**

Client Association Limit 0

mDNS Mode Bridging ▼

Cancel Apply to Device

2. Navegue hasta **Seguridad > Capa 2**, para habilitar 802.1x para una RLAN, configure el estado 802.1x como Habilitado, como se muestra en esta imagen.

Edit RLAN Profile

General **Security**

Layer2 Layer3 AAA

802.1x **ENABLED**

MAC Filtering Not Configured ▼

Authentication List default ▼

3. Navegue hasta **Seguridad > AAA**, establezca la Autenticación EAP local en habilitada y elija el Nombre de Perfil EAP requerido de la lista desplegable, como se muestra en esta imagen.

Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP ▼

4. Para crear la política RLAN, navegue hasta **Configuration > Wireless > Remote LAN** y en la página Remote LAN, haga clic en la pestaña **RLAN Policy**, como se muestra en esta imagen.

Edit RLAN Policy

General Access Policies Advanced

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

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

Navegue hasta Políticas de acceso y configure la VLAN y el modo de host y aplique los parámetros.

Edit RLAN Policy

General **Access Policies** Advanced

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

5. Para crear la etiqueta de política y asignar el perfil RLAN a la política RLAN, navegue hasta **Configuración > Etiquetas y perfiles > Etiquetas**.

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*

RLAN-TAG

Description

Enter Description

➤ WLAN-POLICY Maps: 0

▼ RLAN-POLICY Maps: 1

+ Add

✕ Delete

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

⏪ ⏩ 1 ⏪ ⏩ 10 items per page 1 - 1 of 1 items

↶ Cancel

📄 Apply to Device

6. Habilite el puerto LAN y aplique la TAG de política en el AP. Navegue hasta **Configuration > Wireless > Access Points** y haga clic en el AP.

Edit AP

Location*	default location
Base Radio MAC	0042.5ab7.8f60
Ethernet MAC	0042.5ab6.4ab0
Admin Status	ENABLED <input checked="" type="checkbox"/>
AP Mode	Local ▼
Operation Status	Registered
Fabric Status	Disabled
LED State	<input type="checkbox"/> DISABLED
LED Brightness Level	8 ▼

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy	RLAN-TAG ▼
Site	default-site-tag ▼
RF	default-rf-tag ▼

Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	17.2.1.11
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	Not Configured
DHCP IPv4 Address	10.106.39.198
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Time Statistics

Up Time	0 days 13 hrs 33 mins 40 secs
Controller Association Latency	20 secs

Aplice la configuración y el AP se reúne al WLC. Haga clic en el **AP**, luego seleccione **Interfaces** y habilite el puerto 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 los parámetros y verifique el estado.

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 un PC en el puerto LAN3 del AP. La PC se autenticará a través de 802.1x y obtendrá una dirección IP de la VLAN configurada.

Vaya a **Monitoring > Wireless > Clients** para comprobar el estado del cliente.

Delete



Total Client(s) in the Network: 2

Number of Client(s) selected: 0

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	State	Protocol	User Name	Device Type	Role
503e.aab7.0ff4	10.106.39.227	2001::c	AP1815	corporate-ssid	3	Run	11n(2.4)		N/A	Local
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 comunes:

- Sólo el trabajo del SSID local, el SSID configurado en el WLC no se transmite: Verifique si el AP se ha unido al controlador correctamente.
- No se puede acceder a la GUI de OEAP: Compruebe si AP tiene dirección IP y verifique el alcance (firewall, ACL, etc. en la red)
- Los clientes con cables o inalámbricos conmutados centralmente no pueden autenticar ni obtener la dirección IP: Tome seguimientos de RA, siempre en rastros, etc.

Ejemplo de rastros siempre activos para el cliente 802.1x con cables:

[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