

Configurazione di OEAP e RLAN su Catalyst 9800 WLC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[AP Join dietro NAT](#)

[Configurazione](#)

[Verifica](#)

[Accedere a OEAP e configurare il SSID personale](#)

[Configurazione di RLAN su 9800 WLC](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento spiega come configurare Cisco OfficeExtend access point (OEAP) e la RLAN (Remote Local Area Network) su 9800 WLC.

Un punto di accesso Cisco OfficeExtend (OEAP) fornisce comunicazioni sicure da un controller a un Cisco AP in una postazione remota, estendendo senza problemi la WLAN aziendale su Internet fino alla residenza di un dipendente. L'esperienza dell'utente nel suo ufficio di casa è esattamente la stessa che avrebbe nel suo ufficio aziendale. La crittografia Datagram Transport Layer Security (DTLS) tra un punto di accesso e il controller assicura che tutte le comunicazioni abbiano il massimo livello di sicurezza.

Una LAN remota (RLAN) viene utilizzata per autenticare i client cablati tramite il controller. Quando il client cablato si unisce correttamente al controller, le porte LAN commutano il traffico tra la modalità di commutazione centrale e locale. Il traffico proveniente dai client cablati viene considerato traffico client wireless. L'access point RLAN invia la richiesta di autenticazione per autenticare il client cablato. L'autenticazione dei client cablati nella RLAN è simile a quella del client wireless centrale autenticato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 9800 WLC
- Accesso CLI (Command-Line Interface) ai controller e ai punti di accesso wireless

Componenti usati

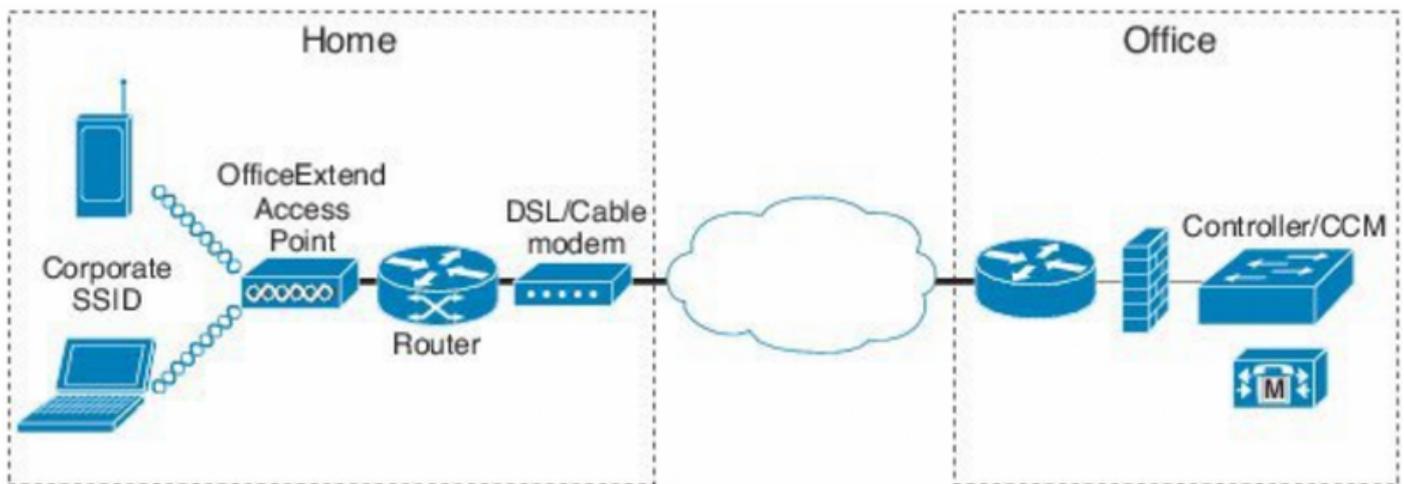
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 9800 WLC versione 17.02.01
- Serie 1815/1810 AP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



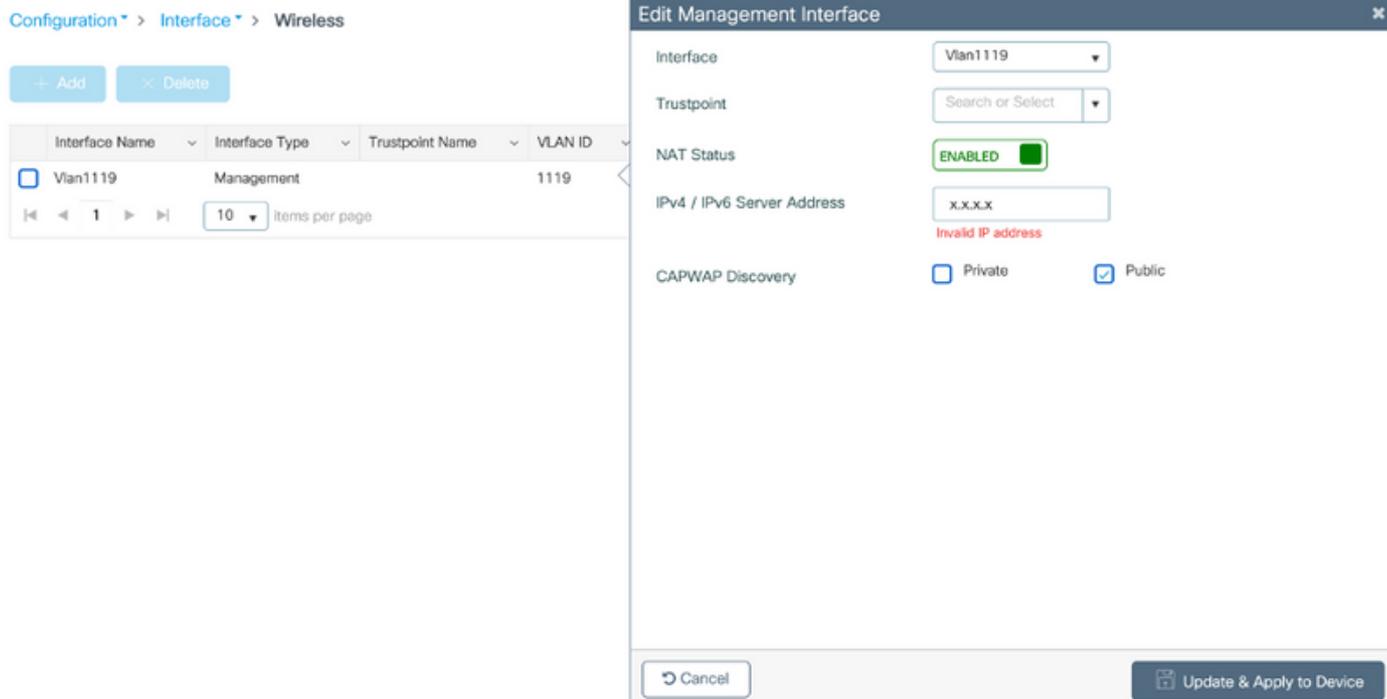
AP Join dietro NAT

Nei codici 16.12.x, è necessario configurare l'indirizzo IP NAT dalla CLI. Nessuna opzione GUI disponibile. È inoltre possibile selezionare il rilevamento CAPWAP tramite IP pubblico o privato.

```
(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
```

Nei codici 17.x, selezionare **Configurazione > Interfaccia > Wireless** e fare clic su **Wireless Management Interface** (Interfaccia di gestione wireless) per configurare il tipo di rilevamento NAT IP e CAPWAP dalla GUI.



Configurazione

1. Per creare un profilo Flex, abilitare **Office Extend AP** e passare a **Configurazione > Tag e profili > 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. Per creare un tag del sito e un profilo Flex mappa, passare a **Configurazione > Tag e profili > Tag**.

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. Passare alla voce 1815 AP con il tag del sito creato da **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

Verifica

Una volta che l'access point 1815 si è nuovamente unito al WLC, verificare questo output:

```
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: È possibile abilitare o disabilitare la crittografia dei dati DTLS per un punto di accesso specifico o per tutti i punti di accesso utilizzando il comando `ap link-encryption`

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

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

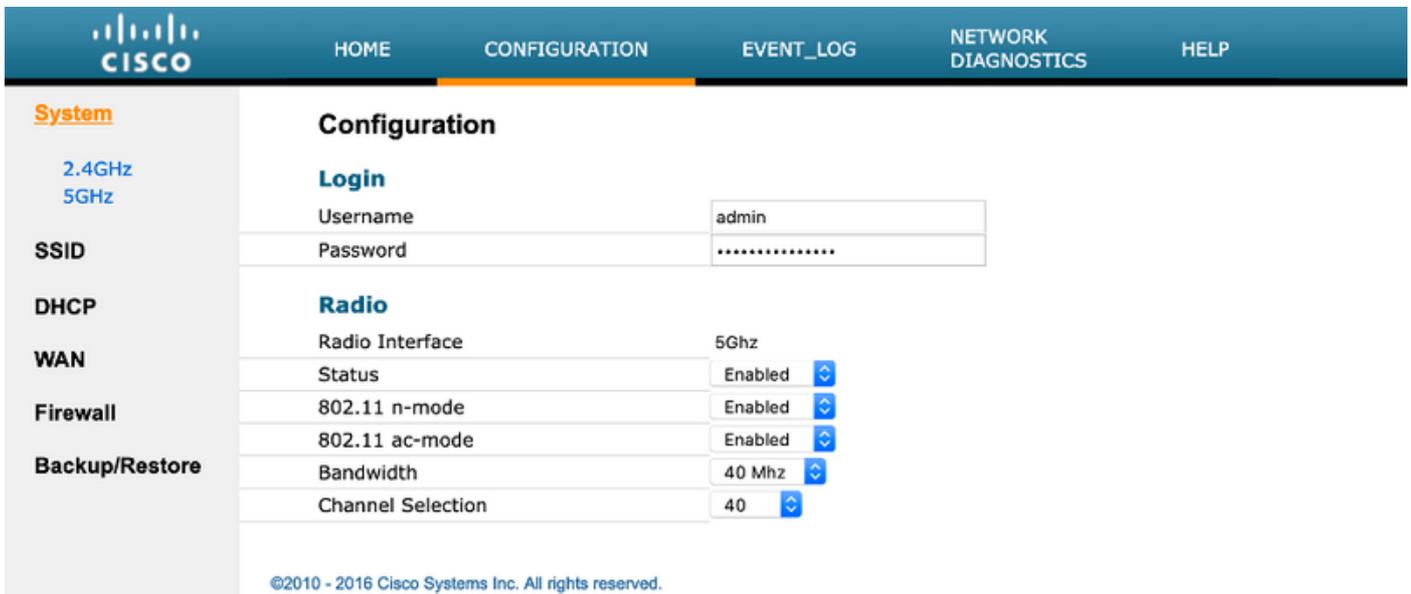
Disabling link-encryption globally will reboot the APs with link-encryption.

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

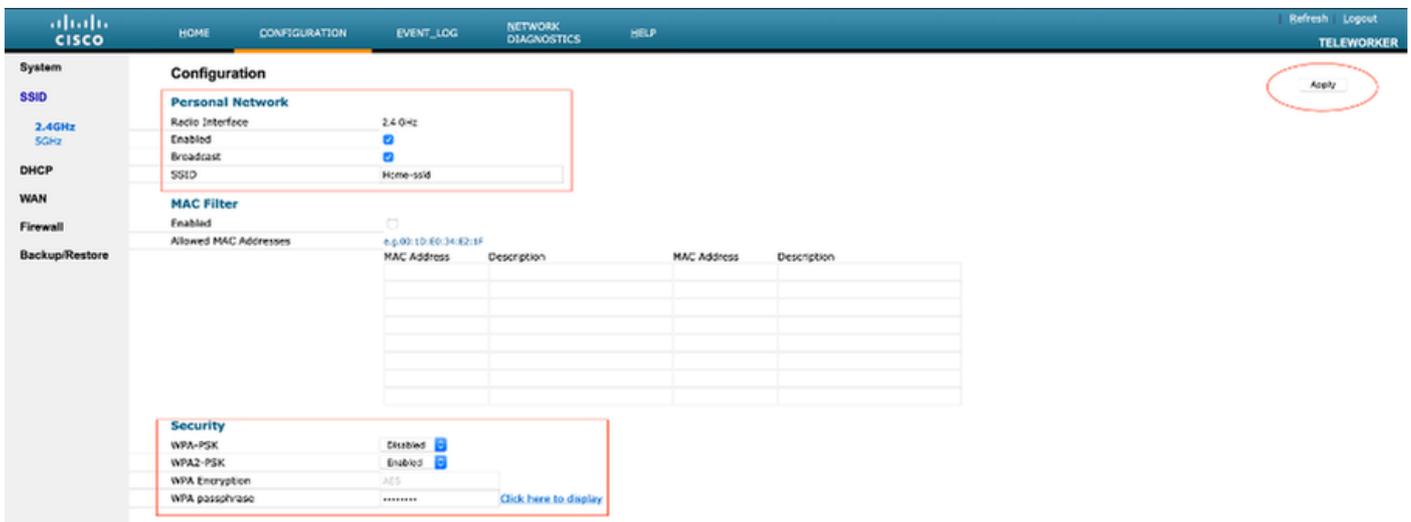
Accedere a OEAP e configurare il SSID personale

1. È possibile accedere all'interfaccia Web dell'OEAP con il relativo indirizzo IP. Le credenziali predefinite per l'accesso sono **admin** e **admin**.

2. Si consiglia di modificare le credenziali predefinite per motivi di sicurezza.



3. Passare a **Configuration> SSID> 2.4GHz/5GHz** per configurare il SSID personale.



4. Abilitare l'interfaccia radio.

5. Inserire il SSID e abilitare la trasmissione

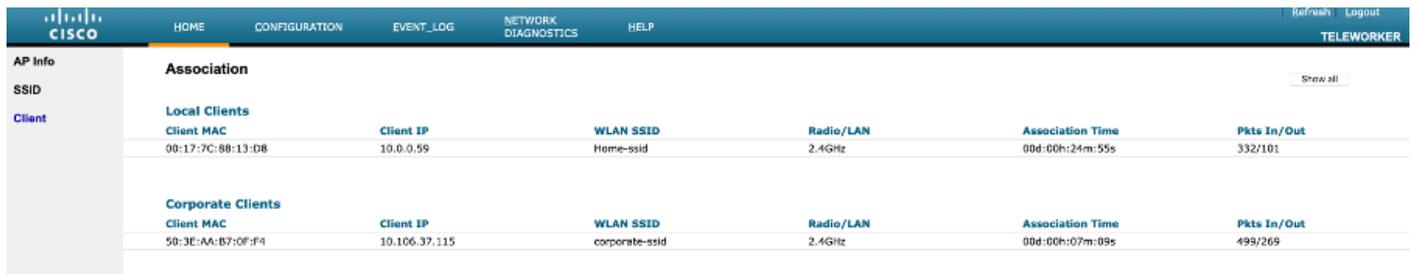
6. Per la cifratura, scegliere **WPA-PSK** o **WPA2-PSK** e inserire la passphrase per il tipo di sicurezza corrispondente.

7. Fare clic su **Applica** per rendere effettive le impostazioni.

8. Per impostazione predefinita, i clienti che si connettono al SSID personale ottengono l'indirizzo IP dalla rete 10.0.0.1/24.

9. Gli utenti privati possono usare lo stesso access point per connettersi e per comunicare che il traffico non viene trasmesso tramite il tunnel DTLS.

10. Per controllare le associazioni client su OEAP, selezionare **Home > Client**. È possibile visualizzare i client locali e aziendali associati a OEAP.



The screenshot shows the Cisco OEAP web interface. The top navigation bar includes 'HOME', 'CONFIGURATION', 'EVENT_LOG', 'NETWORK DIAGNOSTICS', and 'HELP'. The left sidebar has 'AP Info', 'SSID', and 'Client' (selected). The main content area is titled 'Association' and contains two tables: 'Local Clients' and 'Corporate Clients'. Both tables have 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	
90:17:7C:88:13: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

Configurazione di RLAN su 9800 WLC

Una LAN remota (RLAN) viene utilizzata per autenticare i client cablati tramite il controller. Quando il client cablato si unisce correttamente al controller, le porte LAN commutano il traffico tra la modalità di commutazione centrale e locale. Il traffico proveniente dai client cablati viene considerato traffico client wireless. L'access point RLAN invia la richiesta di autenticazione per autenticare il client cablato. OSPF (Open Shortest Path First)

L'autenticazione dei client cablati nella RLAN è simile a quella del client wireless centrale autenticato.

Nota: In questo esempio, per l'autenticazione dei client RLAN viene utilizzato il protocollo EAP locale. La configurazione EAP locale deve essere presente sul WLC per configurare i passaggi seguenti. Include metodi di autenticazione e autorizzazione aaa, profilo EAP locale e credenziali locali.

[Esempio di autenticazione EAP locale su Catalyst 9800 WLC](#)

1. Per creare il profilo RLAN, selezionare **Configurazione > Wireless > LAN remota** e immettere un nome e un ID RLAN per il profilo RLAN, come mostrato nell'immagine.

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. Selezionare **Security** > **Layer2** per abilitare 802.1x per una RLAN, impostare lo stato 802.1x su Enabled, come mostrato nell'immagine.

Edit RLAN Profile

General **Security**

Layer2 Layer3 AAA

802.1x **ENABLED**

MAC Filtering Not Configured ▼

Authentication List default ▼

3. Passare a **Sicurezza** > **AAA**, impostare Autenticazione EAP locale su Abilitata e scegliere il nome del profilo EAP richiesto dall'elenco a discesa, come mostrato nell'immagine.

Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP ▼

4. Per creare la policy RLAN, selezionare **Configurazione > Wireless > LAN remota** e nella pagina LAN remota fare clic sulla scheda **Policy RLAN**, come mostrato nell'immagine.

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 ▼	

Passare a Criteri di accesso, configurare la VLAN e la modalità host e applicare le impostazioni.

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. Per creare un tag di policy e mappare il profilo RLAN sulla policy RLAN, selezionare **Configurazione > Tag e profili > Tag**.

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. Abilitare la porta LAN e applicare il codice di matricola all'access point. Selezionare **Configurazione > Wireless > Access Point** e fare clic sull'access point.

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

Applicare l'impostazione e l'access point si unisce nuovamente al WLC. Fare clic su nell'**access point**, quindi selezionare **Interfacce** e abilitare la 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

Applicare le impostazioni e verificare lo stato.

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. Collegare un PC alla porta LAN3 dell'access point. Il PC verrà autenticato tramite 802.1x e riceverà un indirizzo IP dalla VLAN configurata.

Passare a **Monitoraggio > Wireless > Client** per controllare lo stato del client.

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
```

Risoluzione dei problemi

Problemi comuni:

- Funziona solo il SSID locale, il SSID configurato sul WLC non viene trasmesso: verificare che l'AP si sia unito correttamente al controller.
- Impossibile accedere alla GUI OEAP: Verificare se l'access point ha un indirizzo IP e verificare la raggiungibilità (firewall, ACL, ecc. nella rete)
- I client wireless o cablati con commutazione centrale non sono in grado di autenticarsi o ottenere l'indirizzo IP: Prendere tracce RA, sempre su tracce, ecc.

Esempio di tracce Always on per il client Wired 802.1x:

[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