

# Catalyst 9800 WLCでのOEAPおよびRLANの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[NATの背後のAP加入](#)

[コンフィギュレーション](#)

[確認](#)

[OEAPにログインし、パーソナルSSIDを設定する](#)

[9800 WLCでのRLANの設定](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Cisco OfficeExtendアクセスポイント(OEAP)およびリモートローカルエリアネットワーク(RLAN)を9800 WLCで設定する方法について説明します。

Cisco OfficeExtendアクセスポイント(OEAP)は、コントローラからリモートロケーションのCisco APへのセキュアな通信を提供し、企業のWLANをインターネット経由で従業員の自宅にシームレスに拡張します。ホームオフィスでのユーザエクスペリエンスは、企業オフィスでのユーザエクスペリエンスとまったく同じです。アクセスポイントとコントローラ間のDatagram Transport Layer Security(DTLS)暗号化により、すべての通信のセキュリティが最高レベルになります。

リモートLAN(RLAN)は、コントローラを使用して有線クライアントを認証するために使用されます。有線クライアントがコントローラに正常に加入すると、LANポートは中央スイッチングモードとローカルスイッチングモードの間でトラフィックをスイッチングします。有線クライアントからのトラフィックは、ワイヤレスクライアントトラフィックとして扱われます。アクセスポイント(AP)のRLANは、有線クライアントを認証するための認証要求を送信します。RLANでの有線クライアントの認証は、中央の認証済みワイヤレスクライアントに似ています。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- 9800 WLC
- ワイヤレスコントローラとアクセスポイントへのコマンドラインインターフェイス(CLI)アクセス

## 使用するコンポーネント

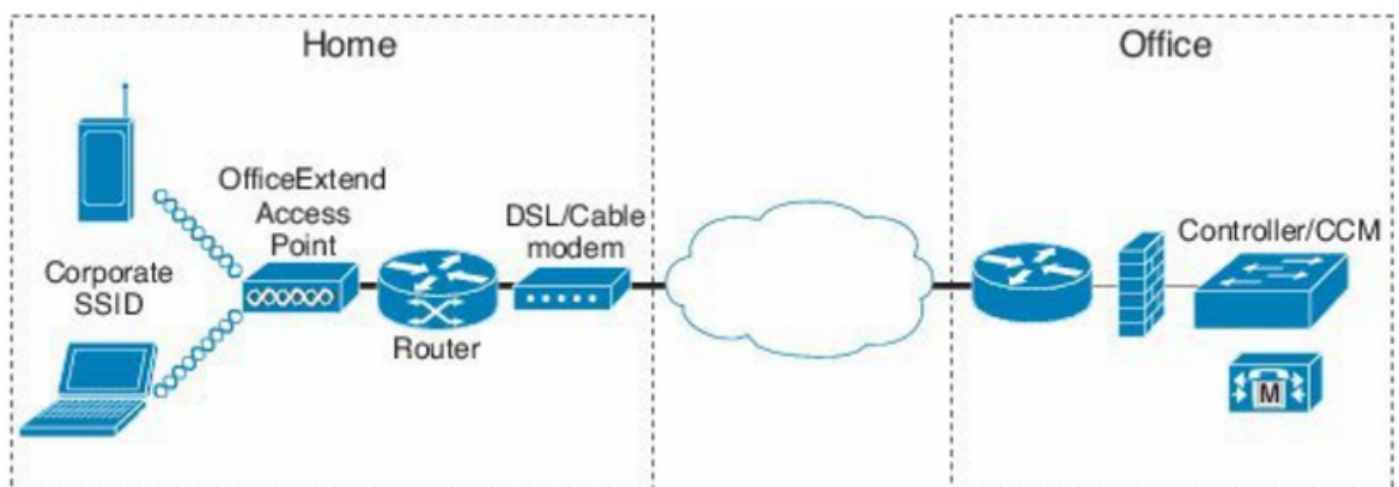
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9800 WLCバージョン17.02.01
- 1815/1810シリーズAP

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ネットワーク図



## NATの背後のAP加入

16.12.xコードでは、CLIからNAT IPアドレスを設定する必要があります。GUIオプションはありません。パブリックまたはプライベートIPを使用してCAPWAP検出を選択することもできます。

```
(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
```

17.xコードで、**[Configuration] > [Interface] > [Wireless]**に移動し、**[Wireless Management Interface]**をクリックして、GUIからNAT IPおよびCAPWAP検出タイプを設定します。

+ Add    × Delete

Interface Name	Interface Type	Trustpoint Name	VLAN ID
<input type="checkbox"/> Vlan1119	Management		1119

10 Items per page

### Edit Management Interface

Interface	Vlan1119
Trustpoint	Search or Select
NAT Status	ENABLED <input checked="" type="checkbox"/>
IPv4 / IPv6 Server Address	x.x.x.x <small>Invalid IP address</small>
CAPWAP Discovery	<input type="checkbox"/> Private <input checked="" type="checkbox"/> Public

## コンフィギュレーション

1. Flexプロファイルを作成するには、Office Extend APを有効にして、[Configuration] > [Tags & Profiles] > [Flex]に移動します。

### 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. サイトタグを作成し、Flex Profileをマップするには、[Configuration] > [Tags & Profiles] > [Tags]に移動します。

## 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. 1815 APにタグを付けます。[Configuration] > [Wireless Setup] > [Advanced] > [Tag APs]を選択します。

## 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

# 確認

1815 APがWLCに再接続したら、次の出力を確認します。

```
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
```

	<b>Encryption</b>	Dnstream	Upstream	Last
AP Name	<b>State</b>	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
```

**注** : ap link-encryptionコマンドを使用して、特定のアクセスポイントまたはすべてのアクセスポイントのDTLSデータ暗号化を有効または無効にできます

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

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

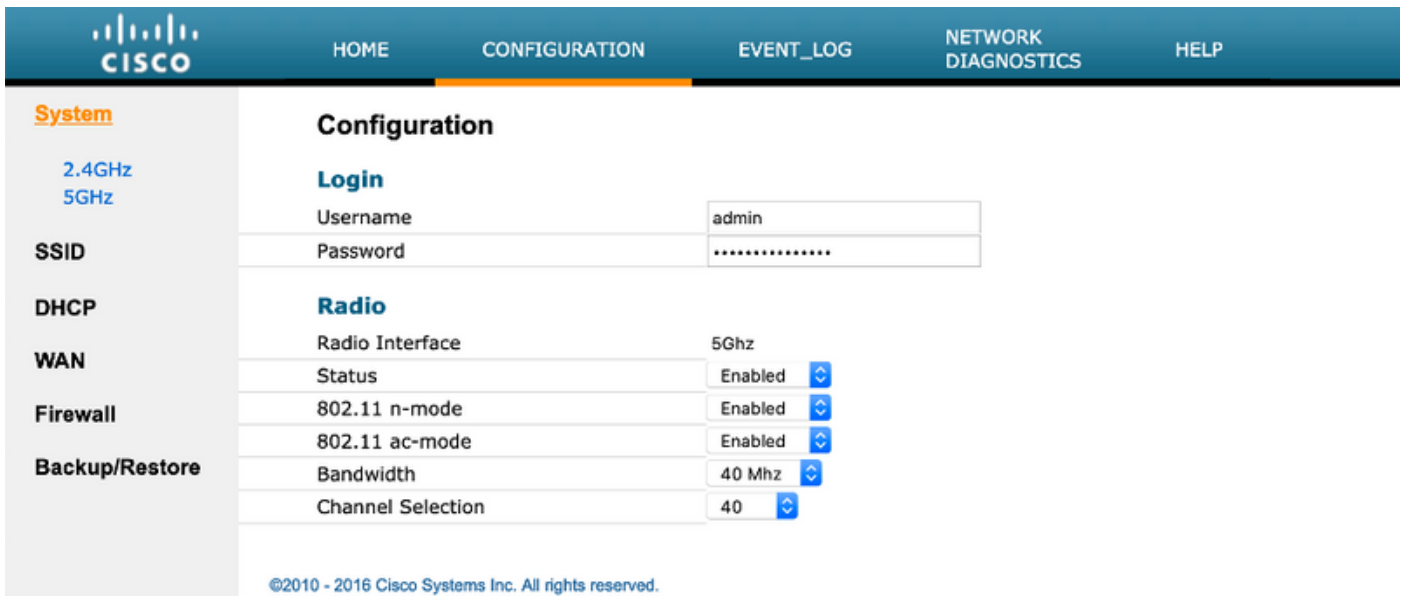
Disabling link-encryption globally will reboot the APs with link-encryption.

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

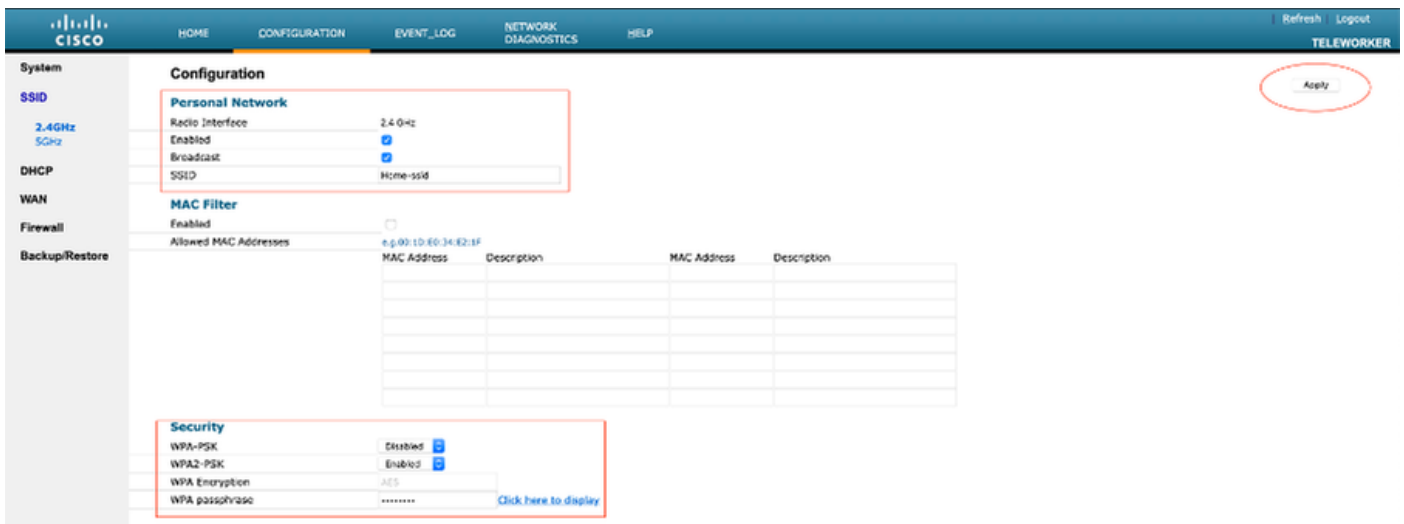
## OEAPにログインし、パーソナルSSIDを設定する

1. OEAPのWebインターフェイスにIPアドレスでアクセスできます。ログインするデフォルトの認証情報はadminとadminです。

2. セキュリティ上の理由から、デフォルトのクレデンシャルを変更することを推奨します。



3. [Configuration] > [SSID] > [2.4GHz/5GHz] に移動し、パーソナルSSIDを設定します。



4. 無線インターフェイスを有効にします。

5. SSIDを入力し、ブロードキャストを有効にします

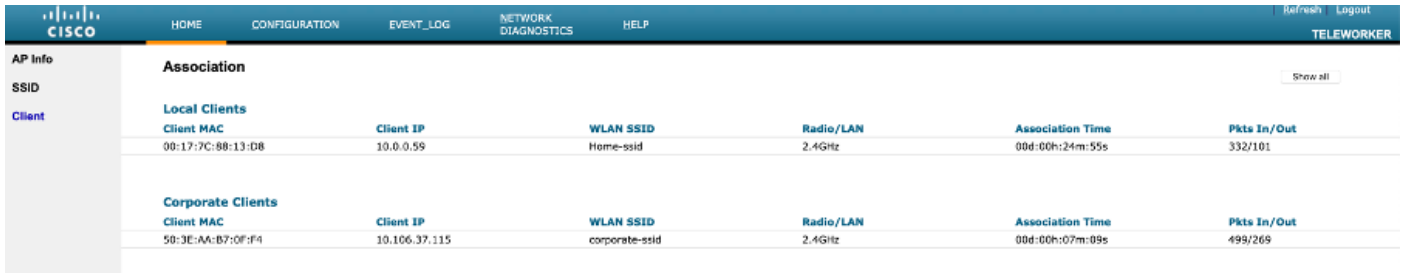
6. 暗号化の場合は、[WPA-PSK]または[WPA2-PSK]を選択し、対応するセキュリティタイプのパスワードを入力します。

7. [Apply]をクリックして設定を有効にします。

8. パーソナルSSIDに接続するクライアントは、デフォルトで10.0.0.1/24ネットワークからIPアドレスを取得します。

9. ホームユーザは同じAPを使用して自宅に接続でき、トラフィックがDTLSトンネルを通過しません。

10. OEAPでクライアントの関連付けを確認するには、[Home] > [Client]に移動します。OEAPに  
関連付けられたローカルクライアントと社内クライアントを確認できます。



The screenshot shows the Cisco Teleworker interface. The top navigation bar includes HOME, CONFIGURATION, EVENT\_LOG, NETWORK DIAGNOSTICS, and HELP. The main content area is titled 'Association' and has 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

## 9800 WLCでのRLANの設定

リモートLAN(RLAN)は、コントローラを使用して有線クライアントを認証するために使用されます。有線クライアントがコントローラに正常に加入すると、LANポートは中央スイッチングモードとローカルスイッチングモードの間でトラフィックをスイッチングします。有線クライアントからのトラフィックは、ワイヤレスクライアントトラフィックとして扱われます。アクセスポイント(AP)のRLANは、有線クライアントを認証するための認証要求を送信します。「

RLANでの有線クライアントの認証は、中央の認証済みワイヤレスクライアントに似ています。

注：この例では、ローカルEAPをRLANクライアント認証に使用しています。次の手順を設定するには、WLCにローカルEAP設定が存在する必要があります。これには、aaa認証および許可方式、ローカルEAPプロファイル、およびローカルクレデンシャルが含まれます。

### [Catalyst 9800 WLCでのローカルEAP認証の設定例](#)

1. RLANプロファイルを作成するには、次の図に示すように、[Configuration] > [Wireless] > [Remote LAN]に移動し、RLANプロファイルの名前とRLAN IDを入力します。



### Add RLAN Profile

General Security

Profile Name\*

RLAN ID\*

Status **ENABLED**

Client Association Limit

mDNS Mode

2. [Security] > [Layer2] に移動し、RLANで802.1xを有効にするには、次の図に示すように、802.1xのステータスを[Enabled]に設定します。

### Edit RLAN Profile

General **Security**

**Layer2** Layer3 AAA

802.1x **ENABLED**

MAC Filtering

Authentication List

3. 次の図に示すように、[Security] > [AAA] に移動し、[Local EAP Authentication]を[enabled]に設定し、ドロップダウンリストから必要なEAPプロファイル名を選択します。

## Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP ▼

4. RLANポリシーを作成するには、[Configuration] > [Wireless] > [Remote LAN]に移動し、[Remote LAN]ページで[RLAN Policy]タブをクリックします（次の図を参照）。

### 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 ▼	

[Access Policies]に移動し、VLANとホストモードを設定して、設定を適用します。

### 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. ポリスタグを作成し、RLANプロファイルをRLANポリシーにマップするには、[Configuration] > [Tags & Profiles] > [Tags]に移動します。

## 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
0		

10 items per page 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

+ Add

✕ Delete

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

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

↶ Cancel

📄 Apply to Device

6. LANポートを有効にし、APにポリシータグを適用します。[Configuration] > [Wireless] > [Access Points]に移動し、APをクリックします。

## 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	<b>IP Config</b>	
LED State	<input type="checkbox"/> DISABLED	CAPWAP Preferred Mode	Not Configured
LED Brightness Level	8 ▼	DHCP IPv4 Address	10.106.39.198
<b>Tags</b>		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  ▼	<b>Time Statistics</b>	
Site	default-site-tag ▼	Up Time	0 days 13 hrs 33 mins 40 secs
RF	default-rf-tag ▼	Controller Association Latency	20 secs

設定を適用し、APがWLCに再接続します。APをクリックして、[Interfaces]を選択し、LANポートを有効にします。

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

設定を適用し、ステータスを確認します。

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. APのLAN3ポートにPCを接続します。PCは802.1x経由で認証され、設定されたVLANからIPアドレスを取得します。

[Monitoring] > [Wireless] > [Clients]に移動し、クライアントのステータスを確認します。

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

10 items per page

1 - 2 of 2 clients

## Client

360 View General QOS Statistics ATF Statistics Mobility History Call StatisticsClient 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

## トラブルシューティング

## 一般的な問題:

- ローカルSSIDだけが機能し、WLCで設定されているSSIDがブロードキャストされない : APがコントローラに正しく加入しているかどうかを確認します。
- OEAP GUIにアクセスできない : apにIPアドレスがあるかどうかを確認し、到達可能性 (ファイアウォール、ACLなど、ネットワーク内)を確認します
- 中央でスイッチングされた無線または有線クライアントがIPアドレスを認証または取得できない : RAトレースを取得し、常にトレースを使用するなど

有線802.1xクライアントのAlways onトレースの例 :

[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, 11r = False, 11w = 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