

Catalyst 9800 WLC에서 OEAP 및 RLAN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[NAT 뒤에 AP 조인](#)

[구성](#)

[다음을 확인합니다.](#)

[OEAP에 로그인하여 개인 SSID 구성](#)

[9800 WLC에서 RLAN 구성](#)

[문제 해결](#)

소개

이 문서에서는 9800 WLC에서 Cisco OfficeExtend 액세스 포인트(OEAP) 및 RLAN(Remote Local Area Network)을 구성하는 방법에 대해 설명합니다.

Cisco OfficeExtend 액세스 포인트(OEAP)는 컨트롤러로부터 원격 위치의 Cisco AP로의 안전한 통신을 제공하며 인터넷을 통해 기업 WLAN을 직원의 거주지로 원활하게 확장합니다. 홈 오피스에서 사용하는 사용자의 경험은 기업 사무실에서와 정확히 동일합니다. 액세스 포인트와 컨트롤러 간의 DTLS(Datagram Transport Layer Security) 암호화를 통해 모든 통신에서 최고 수준의 보안을 유지할 수 있습니다.

RLAN(Remote LAN)은 컨트롤러를 사용하여 유선 클라이언트를 인증하는 데 사용됩니다. 유선 클라이언트가 컨트롤러에 성공적으로 연결되면 LAN 포트는 중앙 또는 로컬 스위칭 모드 간에 트래픽을 전환합니다. 유선 클라이언트의 트래픽은 무선 클라이언트 트래픽으로 처리됩니다. AP(Access Point)의 RLAN은 인증 요청을 전송하여 유선 클라이언트를 인증합니다. RLAN에서 유선 클라이언트의 인증은 중앙 인증 무선 클라이언트와 유사합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC
- 무선 컨트롤러 및 액세스 포인트에 대한 CLI(Command-Line Interface) 액세스

사용되는 구성 요소

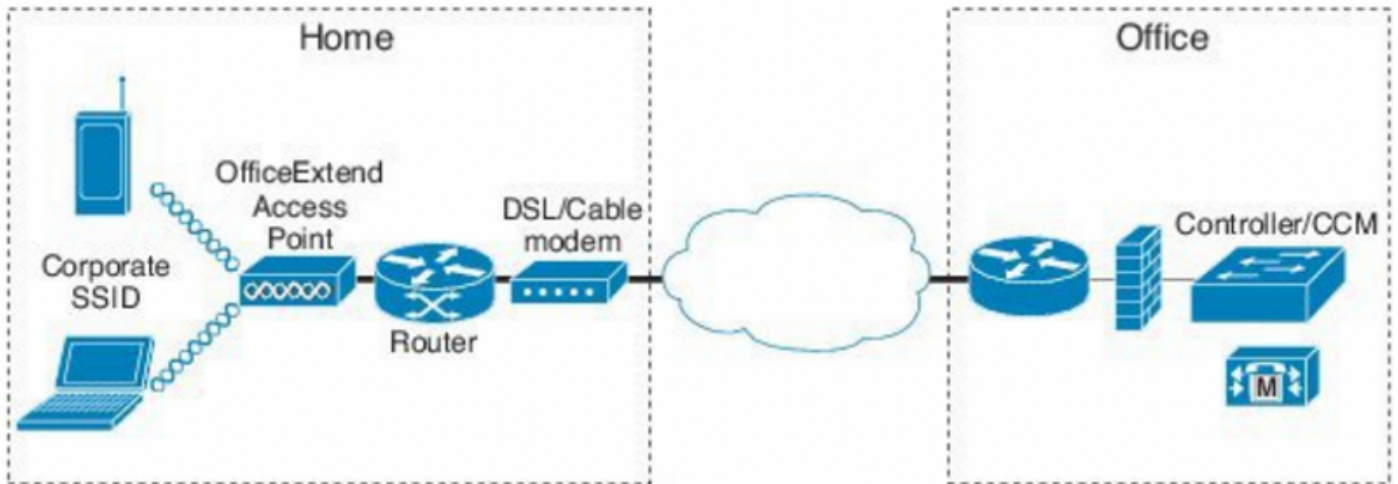
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

네트워크 다이어그램



NAT 뒤에 AP 조인

16.12.x 코드에서 CLI에서 NAT IP 주소를 구성해야 합니다. 사용 가능한 GUI 옵션이 없습니다. 퍼블릭 또는 프라이빗 IP를 통해 CAPWAP 검색을 선택할 수도 있습니다.

```
(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 코드에서 **Configuration > Interface > Wireless**로 이동한 다음 **Wireless Management Interface**를 클릭하여 GUI에서 NAT IP 및 CAPWAP 검색 유형을 구성합니다.

+ Add × Delete

Interface Name	Interface Type	Trustpoint Name	VLAN ID
Vlan1119	Management		1119

10 Items per page

Edit Management Interface

Interface:

Trustpoint:

NAT Status: ENABLED

IPv4 / IPv6 Server Address:
Invalid IP address

CAPWAP Discovery: Private Public

구성

1. Flex 프로필을 만들려면 **Office 확장 AP**를 사용하도록 설정하고 구성 > 태그 및 프로파일 > Flex로 이동합니다.

Add Flex Profile

General Local Authentication Policy ACL VLAN Umbrella

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

2. 사이트 태그를 생성하고 플렉스 프로파일을 매핑하려면 구성 > 태그 및 프로파일 > 태그로 이동합니다.

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 AP에 Configuration(컨피그레이션) > Wireless Setup(무선 설정) > Advanced(고급) > Tag APs(태그 AP)를 사용하여 태그를 지정합니다.

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

다음을 확인합니다.

1815 AP가 WLC에 다시 연결되면 다음 출력을 확인합니다.

```
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
```

참고:ap link-encryption 명령을 사용하여 특정 액세스 포인트 또는 모든 액세스 포인트에 대해 DTLS 데이터 암호화를 활성화하거나 비활성화할 수 있습니다

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

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

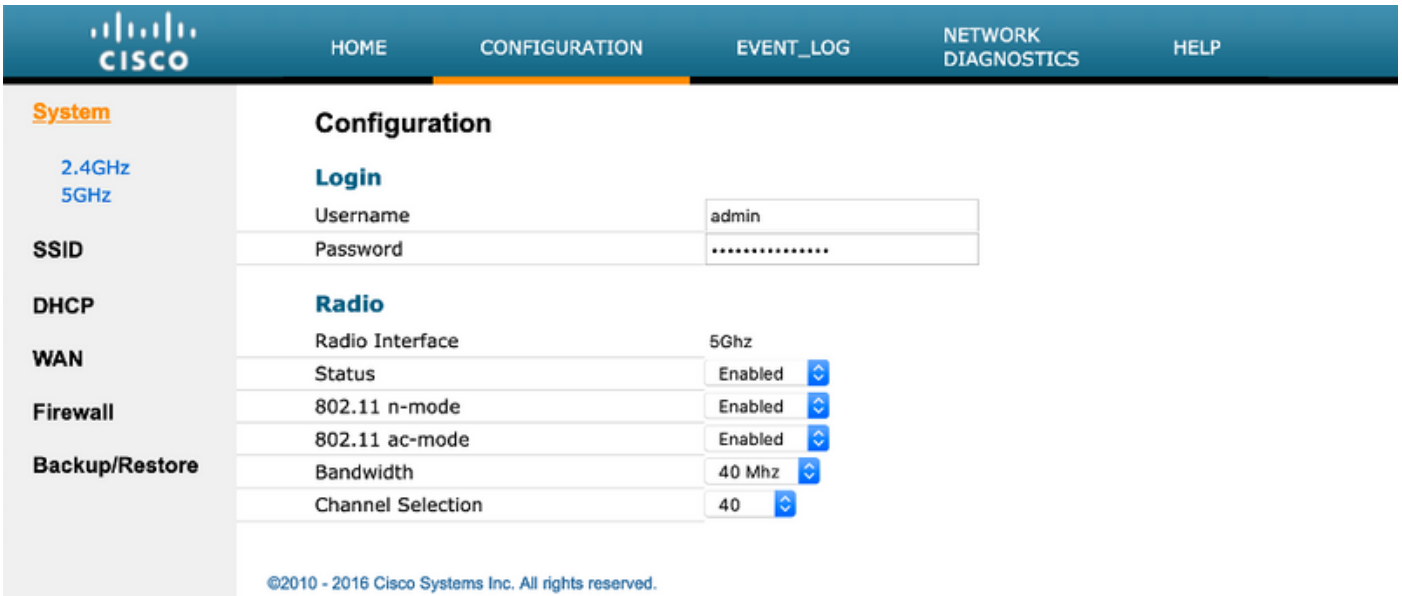
Disabling link-encryption globally will reboot the APs with link-encryption.

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

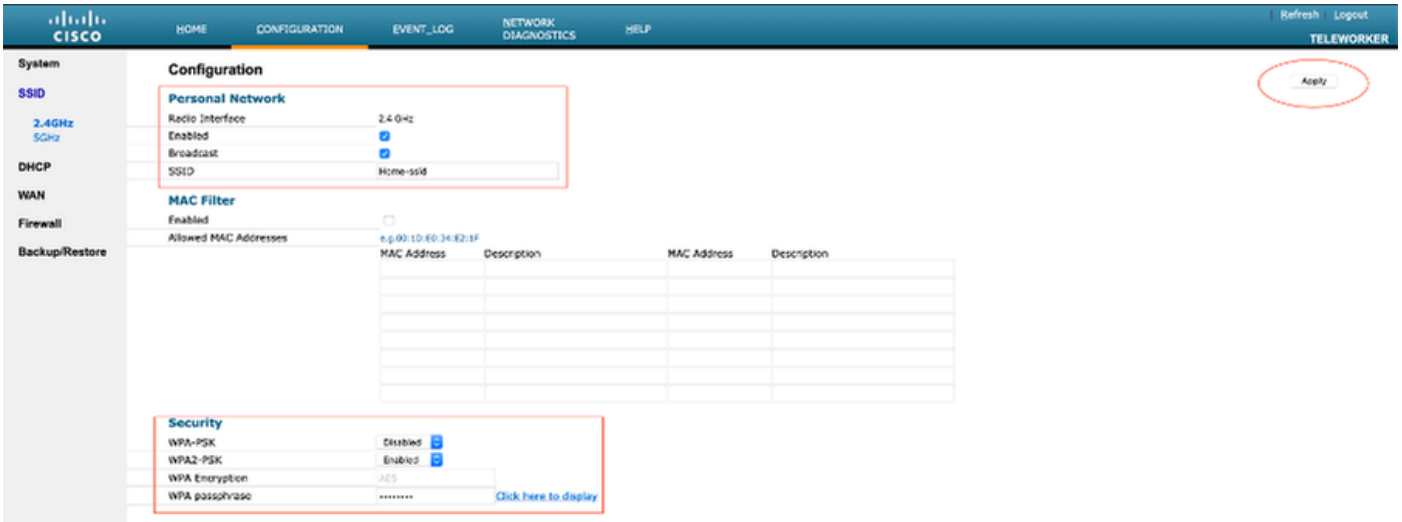
OEAP에 로그인하여 개인 SSID 구성

1. IP 주소로 OEAP의 웹 인터페이스에 액세스할 수 있습니다.로그인할 기본 자격 증명은 **admin** 및 **admin**입니다.

2. 보안상의 이유로 기본 접속 정보를 변경하는 것이 좋습니다.



3. Configuration(컨피그레이션) > SSID> 2.4GHz/5GHz로 이동하여 개인 SSID를 구성합니다.



4. 라디오 인터페이스를 활성화합니다.

5. SSID를 입력하고 브로드캐스트를 활성화합니다.

6. 암호화의 경우 WPA-PSK 또는 WPA2-PSK를 선택하고 해당 보안 유형의 암호를 입력합니다.

7. 설정을 적용하려면 적용을 클릭합니다.

8. 개인 SSID에 연결하는 클라이언트는 기본적으로 10.0.0.1/24 네트워크에서 IP 주소를 가져옵니다.

9. 가정 사용자는 동일한 AP를 사용하여 가정 용도로 연결할 수 있으며, DTLS 터널을 통해 트래픽이 전달되지 않습니다.

10. OEAP에서 클라이언트 연결을 확인하려면 홈 > 클라이언트로 이동합니다.OEAP와 연결된 로컬 클라이언트 및 기업 클라이언트를 볼 수 있습니다.

Association						
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 WLC에서 RLAN 구성

RLAN(Remote LAN)은 컨트롤러를 사용하여 유선 클라이언트를 인증하는 데 사용됩니다.유선 클라이언트가 컨트롤러에 성공적으로 연결되면 LAN 포트는 중앙 또는 로컬 스위칭 모드 간에 트래픽을 전환합니다.유선 클라이언트의 트래픽은 무선 클라이언트 트래픽으로 처리됩니다.AP(Access Point)의 RLAN은 인증 요청을 전송하여 유선 클라이언트를 인증합니다.더

RLAN에서 유선 클라이언트의 인증은 중앙 인증 무선 클라이언트와 유사합니다.

참고:이 예에서는 로컬 EAP가 RLAN 클라이언트 인증에 사용되고 있습니다.아래 단계를 구성하려면 WLC에 로컬 EAP 컨피그레이션이 있어야 합니다.aaa 인증 및 권한 부여 방법, 로컬 EAP 프로파일 및 로컬 자격 증명을 포함합니다.

[Catalyst 9800 WLC 컨피그레이션의 로컬 EAP 인증 예](#)

1. RLAN 프로필을 생성하려면 Configuration(컨피그레이션) > Wireless(무선) > Remote LAN(원격 LAN)으로 이동하고 이 이미지에 표시된 대로 RLAN 프로파일에 대한 이름 및 RLAN ID를 입력합니다.

Add RLAN Profile

General Security

Profile Name*

RLAN ID*

Status **ENABLED**

Client Association Limit

mDNS Mode

2. 보안 > 레이어2로 이동하여 RLAN에 802.1x를 활성화하려면 이 이미지에 표시된 대로 802.1x 상태를 사용으로 설정합니다.

Edit RLAN Profile

General **Security**

Layer2 Layer3 AAA

802.1x **ENABLED**

MAC Filtering

Authentication List

3. Security(보안) > AAA로 이동하고 Local EAP Authentication(로컬 EAP 인증)을 enabled(활성화됨)로 설정하고 이 이미지에 표시된 대로 드롭다운 목록에서 필요한 EAP 프로파일 이름을 선택합니다.

Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP ▼

4. RLAN 정책을 생성하려면 Configuration(구성) > Wireless(무선) > Remote LAN(원격 LAN)으로 이동하고 Remote LAN(원격 LAN) 페이지에서 이 이미지에 표시된 대로 RLAN Policy(RLAN 정책) 탭을 클릭합니다.

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

Description

Enter Description

Status

ENABLED

PoE

Power Level

4 ▼

RLAN Switching Policy

Central Switching

ENABLED

Central DHCP

ENABLED

Access Policies(액세스 정책)로 이동하고 VLAN 및 Host Mode(호스트 모드)를 구성하고 설정을 적용합니다.

Edit RLAN Policy

General **Access Policies** Advanced

Pre-Authentication

Host Mode

singlehost ▼

VLAN

VLAN0039 ▼

Remote LAN ACL

IPv4 ACL

Not Configured ▼

IPv6 ACL

Not Configured ▼

5. 정책 태그를 생성하고 RLAN 프로파일을 RLAN 정책에 매핑하려면 Configuration > Tags &

Profiles > Tags로 이동합니다.

Add Policy Tag ✕

Name*

Description

➤ WLAN-POLICY Maps: 0

✔ RLAN-POLICY Maps: 0

Port ID	RLAN Profile	RLAN Policy Profile
◀ 0 ▶ 10 items per page No items to display		

Map RLAN and Policy

Port ID*

RLAN Profile* RLAN Policy Profile*

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. LAN 포트를 활성화하고 AP에 정책 태그를 적용합니다. Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동하고 AP를 클릭합니다.

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 checked="" 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

설정을 적용하고 AP가 WLC에 다시 조인합니다. AP를 클릭한 다음 Interfaces(인터페이스)를 선택하고 LAN 포트를 활성화합니다.

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

설정을 적용하고 상태를 확인합니다.

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. AP의 LAN3 포트에 PC를 연결합니다. PC는 802.1x를 통해 인증되고 구성된 VLAN에서 IP 주소를 가져옵니다.

Monitoring(모니터링) > Wireless(무선) > Clients(클라이언트)로 이동하여 클라이언트 상태를 확인

합니다.

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

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::d8cae582:2703: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
```

문제 해결

일반적인 문제:

- 로컬 SSID의 작업만, WLC에 구성된 SSID가 브로드캐스트되지 않음: AP가 컨트롤러에 제대로 연결되었는지 확인합니다.
- OEAP GUI에 액세스할 수 없음: ap에 IP 주소가 있는지 확인하고 연결 가능성 확인(방화벽, ACL 등 in-network)
- 중앙 스위치드 무선 또는 유선 클라이언트가 IP 주소를 인증하거나 가져올 수 없음: RA 추적, 항

상 추적 등

유선 802.1x 클라이언트의 Always on 추적 샘플:

[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