

Konfigurieren von OEAP und RLAN auf Catalyst 9800 WLC

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Zugangspunkt hinter der NAT](#)

[Konfiguration](#)

[Überprüfen](#)

[Melden Sie sich bei OEAP an, und konfigurieren Sie die persönliche SSID.](#)

[RLAN auf 9800 WLC konfigurieren](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird erläutert, wie der Cisco OfficeExtend Access Point (OEAP) und das Remote Local Area Network (RLAN) auf dem 9800 WLC konfiguriert werden.

Ein Cisco OfficeExtend Access Point (OEAP) ermöglicht die sichere Kommunikation von einem Controller zu einem Cisco AP an einem Remote-Standort und erweitert nahtlos das Unternehmens-WLAN über das Internet auf den Wohnsitz eines Mitarbeiters. Das Anwendererlebnis im Heimbüro ist genauso wie im Büro. Die DTLS-Verschlüsselung (Datagram Transport Layer Security) zwischen Access Point und Controller stellt sicher, dass alle Kommunikationen ein Höchstmaß an Sicherheit bieten.

Ein Remote LAN (RLAN) wird zur Authentifizierung von kabelgebundenen Clients über den Controller verwendet. Sobald der kabelgebundene Client erfolgreich zum Controller gehört, schalten die LAN-Ports den Datenverkehr zwischen zentralen oder lokalen Switching-Modi um. Der Datenverkehr von den kabelgebundenen Clients wird als Wireless-Client-Datenverkehr behandelt. Das RLAN im Access Point (AP) sendet die Authentifizierungsanfrage, um den kabelgebundenen Client zu authentifizieren. Die Authentifizierung der kabelgebundenen Clients im RLAN ähnelt dem zentralen authentifizierten Wireless-Client.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- 9800 WLC
- CLI-Zugriff (Command Line Interface) auf die Wireless-Controller und Access Points

Verwendete Komponenten

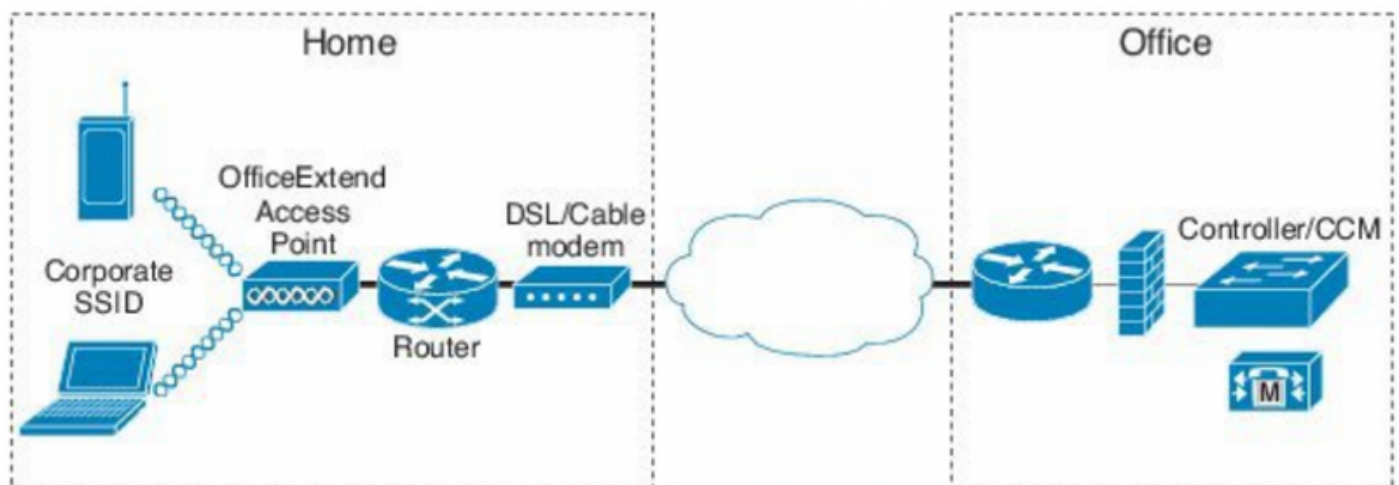
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst 9800 WLC Version 17.02.01
- AP der Serien 1815/1810

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Zugangspunkt hinter der NAT

Bei 16.12.x-Codes müssen Sie die NAT-IP-Adresse über die CLI konfigurieren. Es ist keine GUI-Option verfügbar. Sie können die CAPWAP-Erkennung auch über eine öffentliche oder private IP auswählen.

```
(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
```

Navigieren Sie unter 17.x-Codes zu **Configuration > Interface > Wireless (Konfiguration > Schnittstelle > Wireless)**, und klicken Sie dann auf **Wireless Management Interface (Wireless-Verwaltungsschnittstelle)**, um den Erkennungstyp NAT IP und CAPWAP über die GUI zu konfigurieren.

+ 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

Konfiguration

1. Um ein Flex-Profil zu erstellen, aktivieren Sie **Office Extend AP** und navigieren Sie zu **Configuration > Tags & Profiles > Flex**.

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. Um eine Site-Tag zu erstellen und ein Flex-Profil zuzuordnen, navigieren Sie zu **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. Navigieren Sie zum Tag 1815 AP mit der Site-Tag-Nummer, die durch **Configuration > Wireless Setup > Advanced > Tag APs** erstellt wurde.

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

Überprüfen

Wenn der 1815 AP wieder dem WLC beitrifft, überprüfen Sie diese Ausgabe:

```
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
```

Hinweis: Sie können die DTLS-Datenverschlüsselung für einen bestimmten Access Point oder für alle Access Points mithilfe des Befehls AP link Encryption aktivieren oder deaktivieren.

```
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
```

Melden Sie sich bei OEAP an, und konfigurieren Sie die persönliche SSID.

1. Sie können über die IP-Adresse auf die Webschnittstelle des OEAP zugreifen. Die Standardanmeldeinformationen sind **admin** und **admin**.

2. Aus Sicherheitsgründen wird empfohlen, die Standardanmeldeinformationen zu ändern.

The screenshot shows the Cisco configuration interface. The top navigation bar includes HOME, CONFIGURATION, EVENT_LOG, NETWORK DIAGNOSTICS, and HELP. The left sidebar lists System, SSID, DHCP, WAN, Firewall, and Backup/Restore. The main content area is titled 'Configuration' and is divided into 'Login' and 'Radio' sections. In the 'Login' section, the Username is 'admin' and the Password is masked with dots. In the 'Radio' section, the Radio Interface is '5Ghz', Status is 'Enabled', 802.11 n-mode is 'Enabled', 802.11 ac-mode is 'Enabled', Bandwidth is '40 Mhz', and Channel Selection is '40'. A copyright notice at the bottom reads: ©2010 - 2016 Cisco Systems Inc. All rights reserved.

3. Navigieren Sie zu **Configuration > SSID > 2,4 GHz/5 GHz**, um die persönliche SSID zu konfigurieren.

The screenshot shows the Cisco configuration interface for the 'Personal Network' section. The top navigation bar includes HOME, CONFIGURATION, EVENT_LOG, NETWORK DIAGNOSTICS, and HELP. The left sidebar lists System, SSID, DHCP, WAN, Firewall, and Backup/Restore. The main content area is titled 'Configuration' and is divided into 'Personal Network', 'MAC Filter', and 'Security' sections. In the 'Personal Network' section, the Radio Interface is '2.4 GHz', Enabled is checked, Broadcast is checked, and the SSID is 'Home-ssid'. In the 'Security' section, WPA-PSK is 'Disabled', WPA2-PSK is 'Enabled', WPA Encryption is 'AES', and the WPA passphrase is masked with dots. A table for 'Allowed MAC Addresses' is also visible. An 'Apply' button is circled in red in the top right corner.

4. Aktivieren der Funkschnittstelle.

5. Geben Sie die SSID ein, und aktivieren Sie Broadcast.

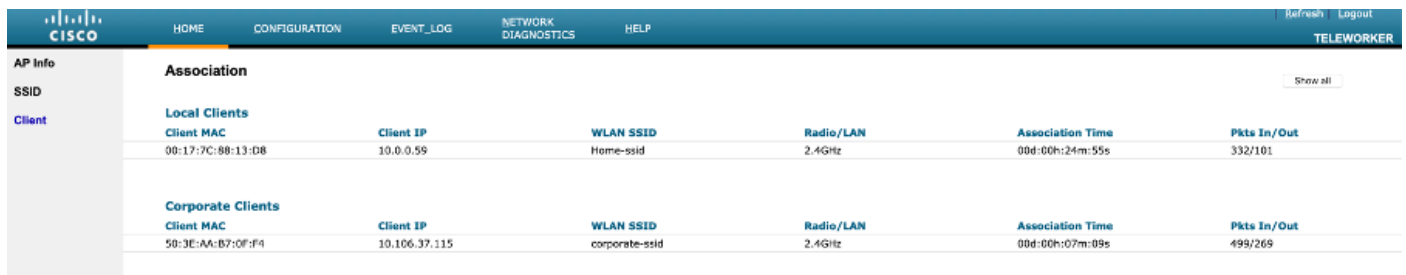
6. Wählen Sie für die Verschlüsselung **WPA-PSK** oder **WPA2-PSK** aus, und geben Sie die Passphrase für den entsprechenden Sicherheitstyp ein.

7. Klicken Sie auf Apply, um die Einstellungen zu übernehmen.

8. Clients, die eine Verbindung zum persönlichen SSID herstellen, erhalten standardmäßig die IP-Adresse vom Netzwerk 10.0.0.1/24.

9. Privatanutzer können den gleichen AP für die Verbindung zu Hause verwenden, und der Datenverkehr wird nicht über den DTLS-Tunnel geleitet.

10. Um die Clientzuordnungen im OEAP zu überprüfen, navigieren Sie zu **Home > Client**. Sie können die lokalen Clients und Corporate Clients sehen, die dem OEAP zugeordnet sind.



The screenshot shows the Cisco Teleworker 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 has a 'Show all' button. It is divided into two sections: 'Local Clients' and 'Corporate Clients'. Each section has 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: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

RLAN auf 9800 WLC konfigurieren

Ein Remote LAN (RLAN) wird zur Authentifizierung von kabelgebundenen Clients über den Controller verwendet. Sobald der kabelgebundene Client erfolgreich zum Controller gehört, schalten die LAN-Ports den Datenverkehr zwischen zentralen oder lokalen Switching-Modi um. Der Datenverkehr von den kabelgebundenen Clients wird als Wireless-Client-Datenverkehr behandelt. Das RLAN im Access Point (AP) sendet die Authentifizierungsanfrage, um den kabelgebundenen Client zu authentifizieren. Die

Die Authentifizierung der kabelgebundenen Clients im RLAN ähnelt dem zentralen authentifizierten Wireless-Client.

Hinweis: In diesem Beispiel wird lokales EAP für die RLAN-Client-Authentifizierung verwendet. Für die Konfiguration der nachfolgenden Schritte muss auf dem WLC eine lokale EAP-Konfiguration vorhanden sein. Sie umfasst Authentifizierungs- und Autorisierungsmethoden, lokales EAP-Profil und lokale Anmeldeinformationen.

[Lokale EAP-Authentifizierung für Catalyst 9800 WLC-Konfigurationsbeispiel](#)

1. Um ein RLAN-Profil zu erstellen, navigieren Sie zu **Configuration > Wireless > Remote LAN** und geben Sie einen Namen und eine RLAN-ID für das RLAN-Profil ein, wie in diesem Bild gezeigt.

Add RLAN Profile

General Security

Profile Name*

RLAN ID*

Status **ENABLED**

Client Association Limit

mDNS Mode

2. Navigieren Sie zu **Security > Layer2**, um 802.1x für ein RLAN zu aktivieren, legen Sie den 802.1x-Status auf Enabled (Aktiviert) fest, wie in diesem Bild gezeigt.

Edit RLAN Profile

General **Security**

Layer2 Layer3 AAA

802.1x **ENABLED**

MAC Filtering

Authentication List

3. Navigieren Sie zu **Security > AAA**, legen Sie die lokale EAP-Authentifizierung auf enabled fest, und wählen Sie den erforderlichen EAP-Profilnamen aus der Dropdown-Liste aus, wie in diesem Bild gezeigt.

Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP

4. Um eine RLAN-Richtlinie zu erstellen, navigieren Sie zu **Configuration > Wireless > Remote LAN** und klicken Sie auf der Seite Remote LAN (Remote-LAN) auf die Registerkarte **RLAN Policy (RLAN-Richtlinie)**, wie in diesem Bild gezeigt.

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	

Navigieren Sie zu Zugriffsrichtlinien, konfigurieren Sie das VLAN und den Hostmodus, und wenden Sie die Einstellungen an.

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. Um Richtlinien-Tag zu erstellen und RLAN-Profil der RLAN-Richtlinie zuzuordnen, navigieren

Sie zu Konfiguration > Tags & Profile > Tags.

Add Policy Tag ✕

Name*

Description

> WLAN-POLICY Maps: 0

✓ RLAN-POLICY Maps: 0

Port ID	RLAN Profile	RLAN Policy Profile
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. Aktivieren Sie den LAN-Port, und wenden Sie die Richtlinie-TAG auf den AP an. Navigieren Sie zu **Konfiguration > Wireless > Access Points**, und klicken Sie auf den **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

Wenden Sie die Einstellung an, und der Access Point schließt sich dem WLC erneut an. Klicken Sie auf den **AP**, wählen Sie **Schnittstellen aus** und aktivieren Sie den LAN-Port.

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

Übernehmen Sie die Einstellungen, und überprüfen Sie den 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. Schließen Sie einen PC am LAN3-Port des AP an. Der PC wird über 802.1x authentifiziert und erhält eine IP-Adresse aus dem konfigurierten VLAN.

Navigieren Sie zu **Monitoring > Wireless > Clients**, um den Client-Status zu überprüfen.

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
```

Fehlerbehebung

Häufige Fragen:

- Nur die Arbeit der lokalen SSID, SSIDs auf dem WLC konfiguriert nicht gesendet werden: Überprüfen Sie, ob der Access Point dem Controller ordnungsgemäß angeschlossen ist.
- Zugriff auf die OEAP-GUI nicht möglich: Überprüfen Sie, ob ap über IP-Adresse verfügt und ob die Erreichbarkeit (Firewall, ACL usw. im Netzwerk) überprüft wird.
- Zentrale Switched Wireless- oder kabelgebundene Clients können sich nicht authentifizieren oder die IP-Adresse nicht erhalten: Nehmen Sie RA Traces, immer auf Traces, etc.

Beispiel für Always-On-Traces für kabelgebundenen 802.1x-Client:

[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