

Konfigurieren von FlexConnect mit Authentifizierung auf dem Catalyst 9800 WLC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

Einleitung

In diesem Dokument wird die Konfiguration von FlexConnect mit zentraler oder lokaler Authentifizierung auf dem Catalyst 9800 Wireless LAN-Controller beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Catalyst Wireless 9800-Konfigurationsmodell
- FlexConnect
- 802.1x

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C980-CL, Cisco IOS-XE® 17.3.4

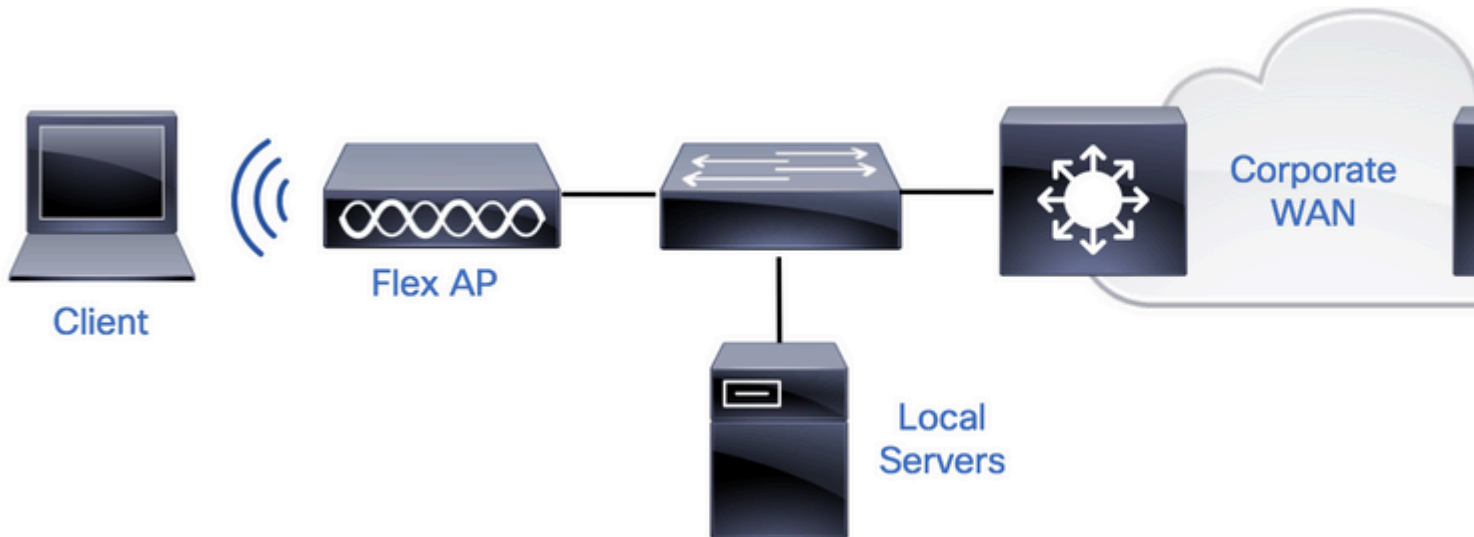
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

FlexConnect ist eine Wireless-Lösung für Bereitstellungen in Zweigstellen. Sie ermöglicht die Konfiguration von Access Points (APs) an Remote-Standorten vom Büro aus über eine Wide Area Network (WAN)-Verbindung, ohne dass an jedem Standort ein Controller bereitgestellt werden muss. Die FlexConnect-APs können den Client-Datenverkehr lokal schalten und die Client-Authentifizierung lokal durchführen, wenn die Verbindung zum Controller unterbrochen wird. Im verbundenen Modus können die FlexConnect-APs auch eine lokale Authentifizierung durchführen.

Konfigurieren

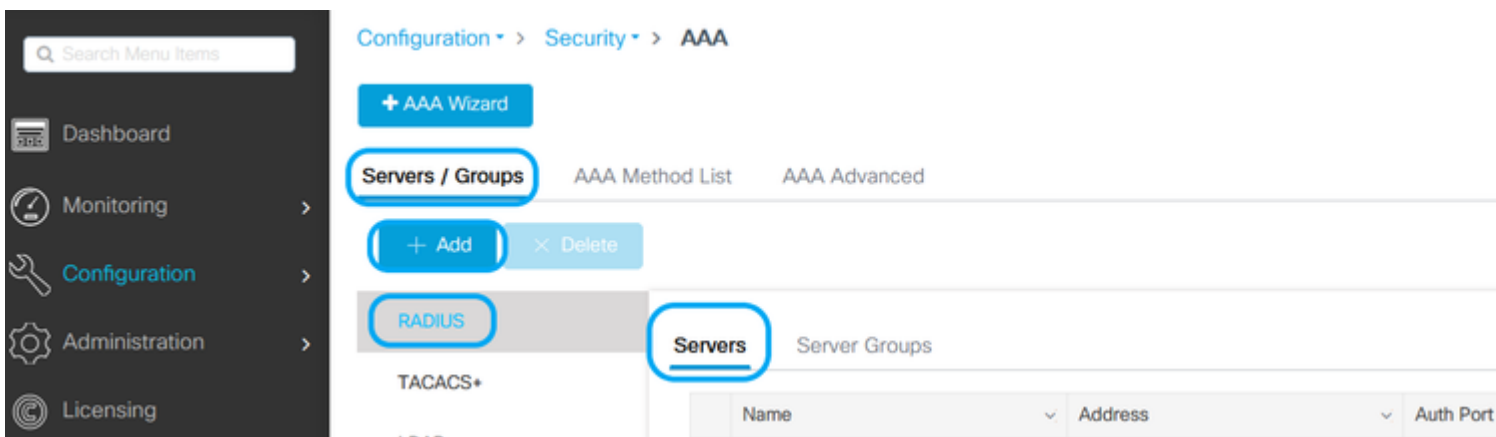
Netzwerkdiagramm



Konfigurationen


AAA-Konfiguration auf 9800 WLCs


Schritt 1: Deklarieren des RADIUS-Servers **Von GUI:** Navigieren Sie zu Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add (Konfiguration > Sicherheit > AAA > Server / Gruppen > RADIUS > Server > + Hinzufügen), und geben Sie die RADIUS-Serverinformationen ein.



Stellen Sie sicher, dass Support für CoA aktiviert ist, wenn Sie beabsichtigen, Sicherheitsfunktionen zu verwenden, die CoA in Zukunft erfordern.

Edit AAA Radius Server

Name*	<input type="text" value="AmmlSE"/>
Server Address*	<input type="text" value="10.48.76.30"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Hidden"/>
Key* 	<input type="text" value="●●●●●●●●●●●●●●●●●●●●"/>
Confirm Key*	<input type="text" value="●●●●●●●●●●●●●●●●●●●●"/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

 Cancel

Hinweis: Radius CoA wird in der FlexConnect-Bereitstellung für lokale Authentifizierung nicht unterstützt. .

Schritt 2: Hinzufügen des RADIUS-Servers zu einer RADIUS-Gruppe **Von GUI:** Navigieren Sie zu Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Licensing

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

Servers **Server Groups**

Name	Server 1	Server 2
------	----------	----------

Edit AAA Radius Server Group

Name*	AmmlSE
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	2
Source Interface VLAN ID	76

Available Servers



Assigned Servers

AmmlSE



Cancel

Update & Apply to

Schritt 3: Erstellen einer Liste von Authentifizierungsmethoden **Von GUI:** Navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authentication > + Add.

Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA /

Authentication

+ Add

Authorization

Name

Quick Setup: AAA Authentication

Method List Name*

AmmISE

Type*

dot1x

Group Type

group

Fallback to local

Available Server Groups

radius
ldap
tacacs+



Assigned Server Groups

AmmISE

Cancel

Up

Aus CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
```

```
# timeout 300
# retransmit 3
# key <shared-key>
# exit

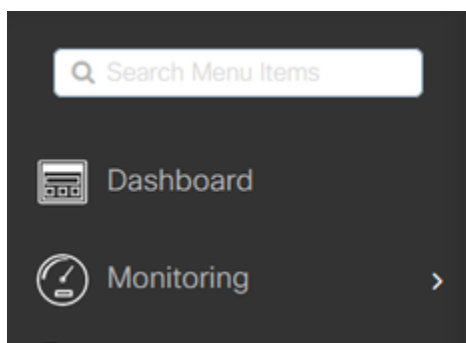
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

WLAN-Konfiguration

Schritt 1: **Aus GUI:** Navigieren Sie zu Configuration > Wireless > WLANs, und klicken Sie auf +Add, um ein neues WLAN zu erstellen, und geben Sie die WLAN-Informationen ein. Klicken Sie dann auf Auf Gerät anwenden.



Configuration > Tags & Profiles > WLANs



Number of WLANs selected : 0

<input type="checkbox"/>	Status ▾	Name	ID
--------------------------	----------	------	----

Add WLAN

General

Security

Advanced

Profile Name*

802.1x-WLAN

Radio Policy

All

SSID*

802.1x

Broadcast SSID

ENABLED

WLAN ID*

1

Status

ENABLED



 Cancel

Schritt 2: **Von GUI:** Navigieren Sie zur Registerkarte Security (Sicherheit), um den Sicherheitsmodus für Layer 2/Layer 3 so lange wie die Verschlüsselungsmethode zu konfigurieren, und zur Authentication List (Authentifizierungsliste), falls 802.1x verwendet wird. Klicken Sie dann auf Aktualisieren und auf Gerät anwenden.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 ...

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

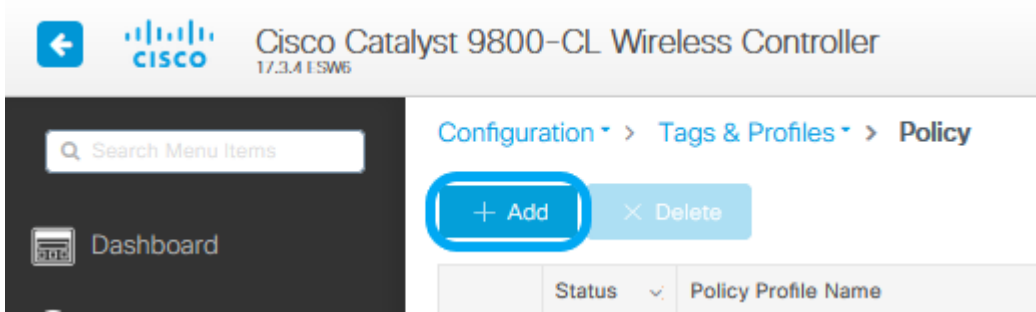
MPSK

Cancel

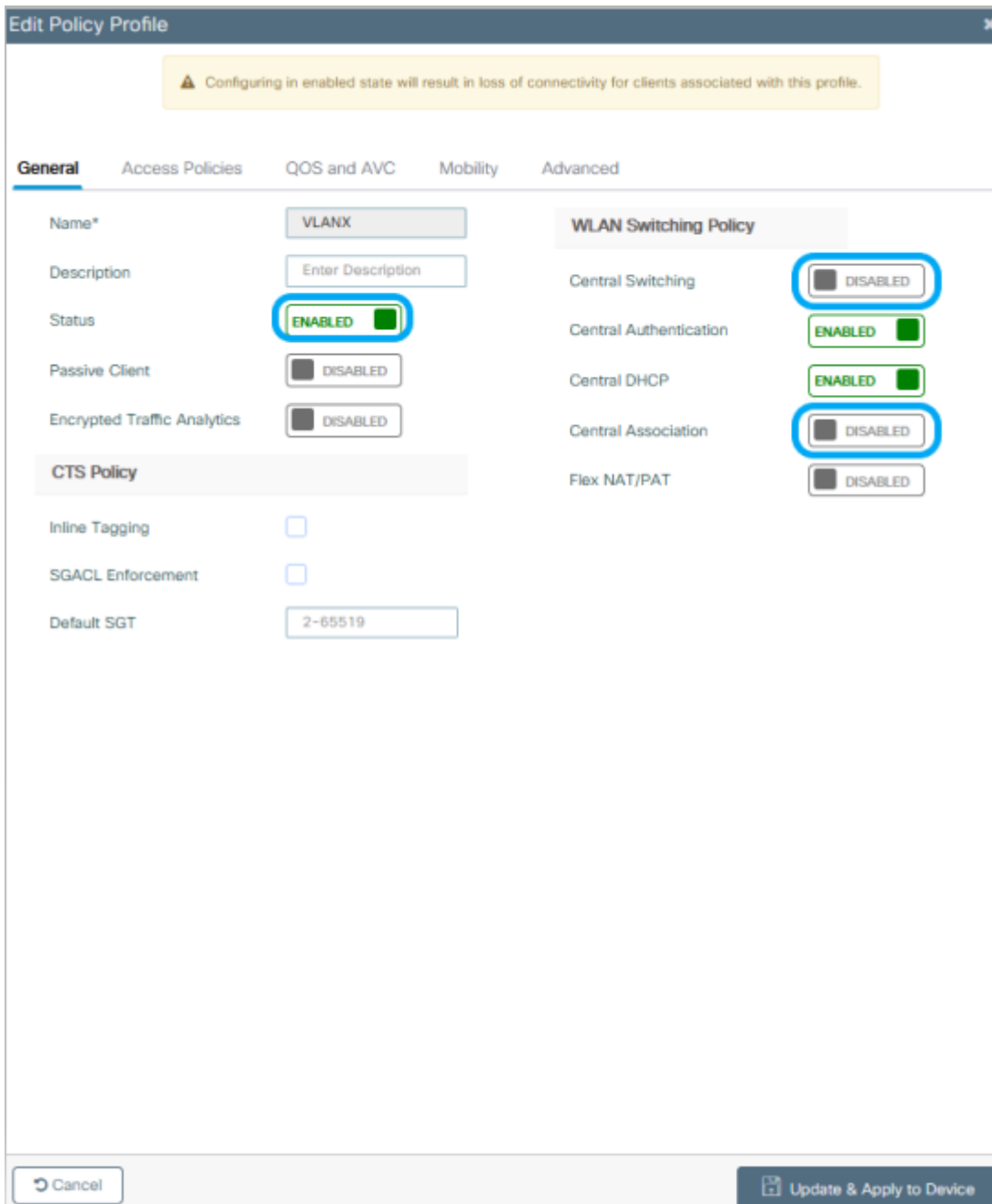
Update & Apply to Device

Richtlinienprofilkonfiguration

Schritt 1: **Von GUI:** Navigieren Sie zu Configuration > Tags & Profiles > Policy, und klicken Sie auf +Add, um ein Richtlinienprofil zu erstellen.



Schritt 2: Fügen Sie den Namen hinzu, und deaktivieren Sie das Kontrollkästchen Central Switching. Bei dieser Konfiguration verarbeitet der Controller die Client-Authentifizierung, und der FlexConnect Access Point schaltet die Client-Datenpakete lokal um.



Hinweis: Zuordnung und Switching müssen immer gekoppelt sein. Wenn die zentrale Switching-Funktion deaktiviert ist, muss die zentrale Zuordnung bei Verwendung von Flexconnect APs auch in allen Richtlinienprofilen deaktiviert sein.

Schritt 3: **Von GUI:** Navigieren Sie zur Registerkarte Access Policies (Zugriffsrichtlinien), um das VLAN zuzuweisen, dem die Wireless-Clients zugewiesen werden können, wenn sie standardmäßig eine Verbindung zu diesem WLAN herstellen. Sie können entweder einen VLAN-Namen aus dem Dropdown-Menü auswählen oder als Best Practice manuell eine VLAN-ID eingeben.

Edit Policy Profile ✕

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

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling	<input type="checkbox"/>	
HTTP TLV Caching	<input type="checkbox"/>	
DHCP TLV Caching	<input type="checkbox"/>	

WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Schritt 4: **Von GUI:** Navigieren Sie zur Registerkarte Advanced (Erweitert), um die WLAN-Timeouts, DHCP, die WLAN Flex Policy und die AAA-Richtlinie zu konfigurieren, falls diese verwendet werden. Klicken Sie dann auf Aktualisieren und auf Gerät anwenden.

✕
Edit Policy Profile

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

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name ✕ ▼

Accounting List ▼ ⓘ

Fabric Profile ▼

mDNS Service Policy ▼ [Clear](#)

Hotspot Server ▼

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map ▼ [Clear](#)

Flex DHCP Option for DNS ENABLED

DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL ▼

Air Time Fairness Policies

2.4 GHz Policy ▼

5 GHz Policy ▼

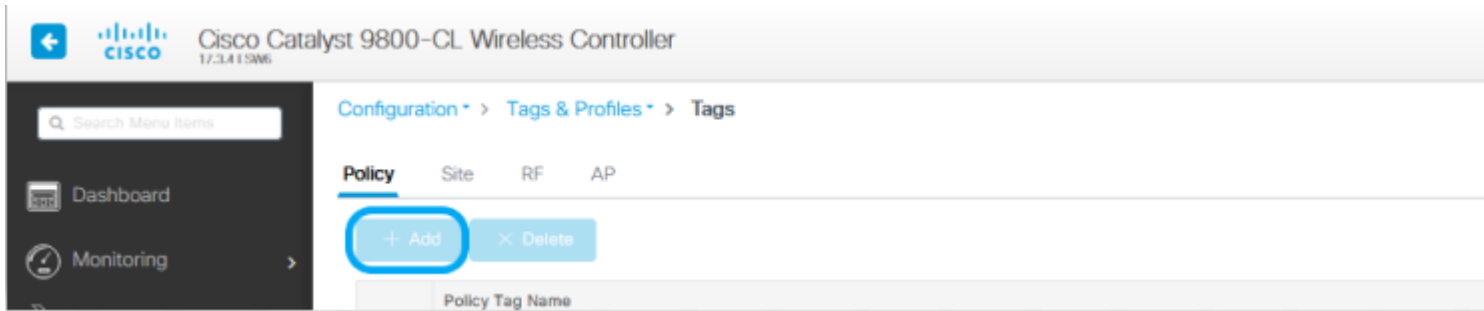
EoGRE Tunnel Profiles

↶ Cancel

➦ Update & Apply to Device

Richtlinien-Tag-Konfiguration

Schritt 1: **Von GUI:** Navigieren Sie zu Konfiguration > Tags & Profile > Tags > Policy > +Hinzufügen.



Schritt 2: Weisen Sie einen Namen zu, und ordnen Sie das zuvor erstellte Richtlinienprofil und WLAN-Profil zu.

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Policy

Description

Enter Description

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> 802.1x-WLAN	VLANX

10 items per page 1 - 1 of 1 items

Map WLAN and Policy

WLAN Profile*

802.1x-WLAN

Policy Profile*

VLANX

×

✓

> RLAN-POLICY Maps: 0

Cancel

Update & Apply to Device

Flex Profile-Konfiguration

Schritt 1: **Von GUI:** Navigieren Sie zu Konfiguration > Tags & Profile > Flex, und klicken Sie auf +Hinzufügen, um ein neues zu erstellen.

Search Menu Items

Dashboard

Monitoring >

Configuration > Tags & Profiles > Flex

+ Add | X Delete

	Flex Profile Name
<input type="checkbox"/>	SaI_Flex

Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

Umbrella

Name*

Description

Native VLAN ID

HTTP Proxy Port

HTTP-Proxy IP Address

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name ▼

Fallback Radio Shut

Flex Resilient

ARP Caching

Efficient Image Upgrade

OfficeExtend AP

Join Minimum Latency

IP Overlap

mDNS Flex Profile ▼

Hinweis: Die native VLAN-ID bezieht sich auf das VLAN, das von den APs verwendet wird, denen dieses Flex Profile zugewiesen werden kann. Sie muss dieselbe VLAN-ID aufweisen, die auf dem Switch-Port, an dem die APs angeschlossen sind, als nativ konfiguriert wurde.

Schritt 2: Fügen Sie auf der Registerkarte VLAN die erforderlichen VLANs hinzu, d. h. die VLANs, die dem WLAN standardmäßig über ein Richtlinienprofil zugewiesen sind oder die VLANs, die über einen RADIUS-Server übertragen werden.

Klicken Sie dann auf Aktualisieren und auf Gerät anwenden.

Edit Flex Profile

General Local Authentication Policy ACL **VLAN** Umbrella

VLAN Name	ID	ACL Name
No items to display		

◀ ▶ 0 ▶▶ 10 items per page

VLAN Name*

VLAN Id*

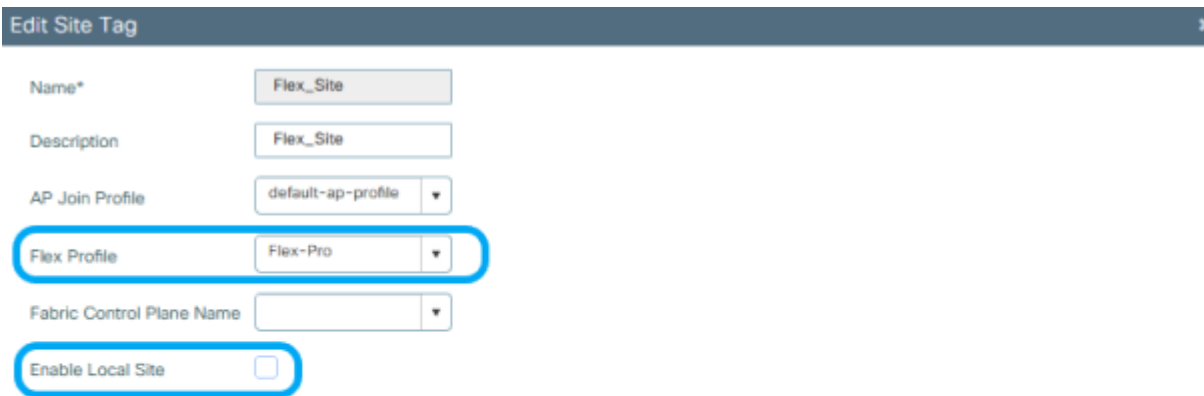
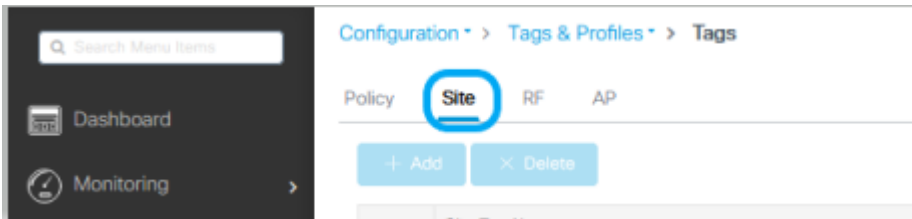
ACL Name

Hinweis: Bei Richtlinienprofil, wenn Sie das Standard-VLAN auswählen, das der SSID zugewiesen ist. Wenn Sie in diesem Schritt einen VLAN-Namen verwenden, stellen Sie sicher, dass Sie in der Flex Profile-Konfiguration denselben VLAN-Namen verwenden. Andernfalls können Clients keine Verbindung mit dem WLAN herstellen.

Hinweis: Um eine ACL für FlexConnect mit AAA-Übersteuerung zu konfigurieren, konfigurieren Sie sie nur in der Richtlinie "ACL". Wenn die ACL einem bestimmten VLAN zugewiesen ist, fügen Sie beim Hinzufügen des VLAN ACL hinzu, und fügen Sie dann die ACL in der Richtlinie "ACL" hinzu.

Site-Tag-Konfiguration

Schritt 1: **Von GUI:** Navigieren Sie zu Konfiguration > Tags & Profile > Tags > Site, und klicken Sie auf +Hinzufügen, um einen neuen Site-Tag zu erstellen. Deaktivieren Sie das Kontrollkästchen Enable Local Site (Lokalen Standort aktivieren), damit APs den Client-Datenverkehr lokal schalten können, und fügen Sie das zuvor erstellte Flex Profile hinzu.



The screenshot shows the 'Edit Site Tag' form. The fields are as follows:

- Name*: Flex_Site
- Description: Flex_Site
- AP Join Profile: default-ap-profile
- Flex Profile: Flex-Pro (highlighted with a blue circle)
- Fabric Control Plane Name: (empty)
- Enable Local Site: (highlighted with a blue circle)

Hinweis: Wenn "Lokalen Standort aktivieren" deaktiviert ist, können die APs, denen dieser Standort-Tag zugewiesen wird, als FlexConnect-Modus konfiguriert werden.

Schritt 2: **Von GUI:** Navigieren Sie zu Configuration > Wireless > Access Points > AP name, um die Site-Tag-Nummer und die Policy-Tag-Nummer einem verknüpften AP hinzuzufügen. Dies kann dazu führen, dass der AP seinen CAPWAP-Tunnel neu startet und wieder am 9800 WLC angeschlossen wird.

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

Edit AP

General Interfaces High Availability Inventory ICap Advanced Support Bundle

General		Version	
AP Name*	talomari1	Primary Software Version	17.3.4.154
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	b4de.31d7.b920	Predownloaded Version	N/A
Ethernet MAC	005d.7319.bb2a	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Local ▼	IOS Version	17.3.4.154
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8 ▼	DHCP IPv4 Address	10.48.70.77
Tags		Static IP (IPv4/IPv6)	<input type="checkbox"/>
<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.</p>			
Policy	Policy ▼	Time Statistics	
Site	Flex_Site ▼	Up Time	0 days 0 hrs 3 mins 28 secs
RF	default-rf-tag ▼	Controller Association Latency	2 mins 40 secs
Write Tag Config to AP	<input type="checkbox"/>		

Cancel Update & Apply to Device

Sobald der Access Point wieder angeschlossen ist, befindet sich der Access Point im FlexConnect-Modus.

▼ All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag
talomari1	AR-AP2802I-E-K9	2	✔	10.48.70.77	b4de.31d7.b920	Flex	Registered	Healthy	Policy	Flex_Site

Items per page: 10

Lokale Authentifizierung mit externem RADIUS-Server

Schritt 1: Fügen Sie den Access Point als Netzwerkgerät zum RADIUS-Server hinzu. Ein Beispiel finden Sie unter [Verwendung der Identity Service Engine \(ISE\) als RADIUS-Server](#).

Schritt 2: Erstellen Sie ein WLAN.

Die Konfiguration kann mit der zuvor konfigurierten übereinstimmen.

Add WLAN ✕

General

Security

Advanced

Profile Name*

SSID*

WLAN ID*

Status ENABLED

Radio Policy

Broadcast SSID ENABLED

↶ Cancel

▶ Apply to Device

Schritt 3: Richtlinienprofilkonfiguration.

Sie können entweder eine neue erstellen oder die zuvor konfigurierte verwenden. Deaktivieren Sie diesmal die Kästchen Central Switching, Central Authentication, Central DHCP und Central Association Enable.

Add Policy Profile



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

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching DISABLED

Central Authentication DISABLED

Central DHCP DISABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

Cancel

Apply to Device

Schritt 4: Richtlinien-Tag-Konfiguration.

Verknüpfen Sie das konfigurierte WLAN und das erstellte Richtlinienprofil.

Schritt 5: Flex Profile-Konfiguration

Erstellen Sie ein Flex Profile, navigieren Sie zur Registerkarte Local Authentication (Lokale Authentifizierung), konfigurieren Sie die Radius Server Group (Server-Gruppe mit Radius), und aktivieren Sie das Kontrollkästchen RADIUS.

Edit Flex Profile

General **Local Authentication** Policy ACL VLAN Umbrella

Radius Server Group

AmmISE

LEAP

Local Accounting Radius Server Group

Select Accounting S

PEAP

Local Client Roaming

TLS

EAP Fast Profile

Select Profile

RADIUS

Users

+ Add

× Delete

Select File



Upload

Select CSV File

Username
0

10 items per page

No items to display

Cancel

Update

Schritt 6: Konfiguration von Site-Tags.

Konfigurieren Sie das in Schritt 5 konfigurierte Flex Profile, und deaktivieren Sie das Kontrollkästchen Enable Local Site (Lokalen Standort aktivieren).

Add Site Tag

Name*	Local Auth
Description	Enter Description
AP Join Profile	default-ap-profile ▼
Flex Profile	Local ▼
Fabric Control Plane Name	▼
Enable Local Site	<input type="checkbox"/>

Cancel



Apply to All

Überprüfung

Von GUI: Navigieren Sie zu **Monitoring > Wireless > Clients**, und bestätigen Sie den **Policy Manager-Status** sowie die **FlexConnect-Parameter**.

Zentrale Authentifizierung:

Client	
General	
QoS Statistics	
ATF Statistics	
Mobility History	
Call Statistics	
Client Properties	
AP Properties	
Security Information	
Client Statistics	
QoS Properties	
MAC Address	484b.aa52.5937
IPv4 Address	172.16.76.41
User Name	andressi
Policy Profile	VLAN2669
Flex Profile	RemoteSite1
Wireless LAN Id	1
Wireless LAN Name	eWLC_do1x
BSSID	38ed.18c6.932f
Uptime(sec)	9 seconds
CCX version	No CCX support
Power Save mode	OFF
Supported Rates	9.0,18.0,36.0,48.0,54.0
Policy Manager State	Run
Last Policy Manager State	IP Learn Complete
Encrypted Traffic Analytics	No
Multicast VLAN	0
Access VLAN	2669
Anchor VLAN	0
Server IP	10.88.173.94
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None
11v DMS Capable	No
FlexConnect Data Switching	Local
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central
FlexConnect Central Association	Yes

Lokale Authentifizierung:

Client				
General	QOS Statistics	ATF Statistics	Mobility History	Call Statistics
Client Properties	AP Properties	Security Information	Client Statistics	QOS Properties
MAC Address		484b.aa52.5937		
IPv4 Address		172.16.76.41		
IPv6 Address		fe80::80be782:7c78:68f9		
User Name		andressi		
Policy Profile		VLAN2669		
Flex Profile		RemoteSite1		
Wireless LAN Id		1		
Wireless LAN Name		eWLC_do1x		
BSSID		38ed.18c6.932f		
Uptime(sec)		11 seconds		
CCX version		No CCX support		
Power Save mode		OFF		
Policy Manager State		Run		
Last Policy Manager State		IP Learn Complete		
Encrypted Traffic Analytics		No		
Multicast VLAN		0		
Access VLAN		2669		
Anchor VLAN		0		
DNS Snooped IPv4 Addresses		None		
DNS Snooped IPv6 Addresses		None		
11v DMS Capable		No		
FlexConnect Data Switching		Local		
FlexConnect DHCP Status		Local		
FlexConnect Authentication		Local		
FlexConnect Central Association		No		

Sie können diese Befehle verwenden, um die aktuelle Konfiguration zu überprüfen:

Aus CLI:

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Fehlerbehebung

Der WLC 9800 bietet IMMER-EIN-Ablaufverfolgungsfunktionen. So wird sichergestellt, dass alle Fehler, Warnungen und Benachrichtigungen im Zusammenhang mit der Client-Verbindung ständig protokolliert werden und dass Sie nach einem Vorfall oder Ausfall Protokolle anzeigen können.

Hinweis: Je nach Umfang der generierten Protokolle können Sie einige Stunden bis mehrere Tage zurückgehen.

Um die Traces anzuzeigen, die 9800 WLC standardmäßig gesammelt hat, können Sie sich über SSH/Telnet mit dem 9800 WLC verbinden und diese Schritte durchlaufen (stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

Schritt 1: Überprüfen Sie die aktuelle Uhrzeit des Controllers, damit Sie die Protokolle bis zum Auftreten des Problems nachverfolgen können.

Aus CLI:

```
# show clock
```

Schritt 2: Erfassen Sie die Syslogs aus dem Controller-Puffer oder dem externen Syslog gemäß der Systemkonfiguration. Dadurch erhalten Sie eine Kurzübersicht über den Systemzustand und etwaige Fehler.

Aus CLI:

```
# show logging
```

Schritt 3: Überprüfen Sie, ob Debug-Bedingungen aktiviert sind.

Aus CLI:

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address                               Port
-----|-----
```

Hinweis: Wenn eine Bedingung aufgelistet ist, bedeutet dies, dass die Traces für alle Prozesse, die auf die aktivierten Bedingungen stoßen (MAC-Adresse, IP-Adresse usw.), auf Debugging-Ebene protokolliert werden. Dies würde das Protokollvolumen erhöhen. Daher wird empfohlen, alle Bedingungen zu löschen, wenn gerade kein Debugging aktiv ist

Schritt 4: Wenn Sie davon ausgehen, dass die zu testende MAC-Adresse in Schritt 3 nicht als Bedingung aufgeführt wurde, sammeln Sie die stets verfügbaren Traces auf Benachrichtigungsebene für die jeweilige MAC-Adresse.

Aus CLI:

```
# show logging profile wireless filter { mac | ip } { <aaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

Sie können entweder den Inhalt der Sitzung anzeigen oder die Datei auf einen externen TFTP-Server kopieren.

Aus CLI:

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Bedingtes Debuggen und Radio Active Trace

Wenn die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen liefern, um den Auslöser für das zu untersuchende Problem zu ermitteln, können Sie bedingtes Debugging aktivieren und die Radio Active (RA)-Ablaufverfolgung erfassen, die Ablaufverfolgungen auf Debugebene für alle Prozesse bereitstellen kann, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse). Führen Sie diese Schritte aus, um das bedingte Debuggen zu aktivieren.

Schritt 5: Stellen Sie sicher, dass keine Debug-Bedingungen aktiviert sind.

Aus CLI:

```
# clear platform condition all
```

Schritt 6: Aktivieren Sie die Debug-Bedingung für die MAC-Adresse des Wireless-Clients, die Sie überwachen möchten.

Mit diesem Befehl wird die angegebene MAC-Adresse 30 Minuten (1800 Sekunden) lang überwacht. Sie können diese Zeit optional auf bis zu 2085978494 Sekunden erhöhen.

Aus CLI:

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Hinweis: Um mehr als einen Client gleichzeitig zu überwachen, führen Sie den Befehl `debug wireless mac <aaaa.bbbb.cccc>` für jede MAC-Adresse aus.

Hinweis: Die Ausgabe der Client-Aktivität wird in der Terminal-Sitzung nicht angezeigt, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 7. Reproduzieren Sie das Problem oder Verhalten, das Sie überwachen möchten.

Schritt 8: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

Aus CLI:

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Sobald die Monitoring-Zeit abgelaufen ist oder das Wireless-Debugging beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 9. Rufen Sie die Datei mit der MAC-Adressaktivität ab. Sie können entweder die Datei `ra_trace.log` auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Überprüfen Sie den Namen der RA-Tracing-Datei

Aus CLI:

```
# dir bootflash: | inc ra_trace
```

Datei auf externen Server kopieren:

Aus CLI:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d
```

Inhalt anzeigen:

Aus CLI:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 10. Wenn die Ursache immer noch nicht offensichtlich ist, rufen Sie die internen Protokolle ab, die eine ausführlichere Ansicht der Protokolle auf Debug-Ebene darstellen. Sie müssen den Client nicht erneut debuggen, da Sie sich die Debugprotokolle, die bereits gesammelt und intern gespeichert wurden, genau angeschaut haben.

Aus CLI:

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra
```

Hinweis: Diese Befehlsausgabe gibt Traces für alle Protokollierungsebenen für alle Prozesse zurück und ist sehr umfangreich. Wenden Sie sich an das Cisco TAC, um diese Nachverfolgungen zu analysieren.

Sie können entweder die Datei `ra-internal-FILENAME.txt` auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Datei auf externen Server kopieren:

Aus CLI:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Inhalt anzeigen:

Aus CLI:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Schritt 11. Entfernen Sie die Debug-Bedingungen.

Aus CLI:

```
# clear platform condition all
```

Hinweis: Stellen Sie sicher, dass Sie die Debug-Bedingungen immer nach einer Fehlerbehebungssitzung entfernen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.