

# FlexConnect auf Catalyst 9800 Wireless Controller verstehen

## Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[WLAN-Profil erstellen/ändern](#)

[Erstellen/Ändern eines Richtlinienprofils](#)

[Erstellen/Ändern eines Policy Tags](#)

[Erstellen/Ändern eines Flex-Profiles](#)

[Site-Tag erstellen/ändern](#)

[Richtlinien-Tag-Zuweisung zu AP](#)

[Zuweisen von Richtlinien-Tags pro AP](#)

[Richtlinien-Tag-Zuweisung für mehrere APs](#)

[Flexconnect-ACLs](#)

[Zentrales WLAN](#)

[Lokal geschaltetes WLAN](#)

[Überprüfen Sie, ob die ACL angewendet wurde.](#)

[Verifizierung](#)

[Konfiguration von VLANs/Schnittstellen](#)

[WLAN-Konfiguration](#)

[AP-Konfiguration](#)

[Tag-Konfiguration](#)

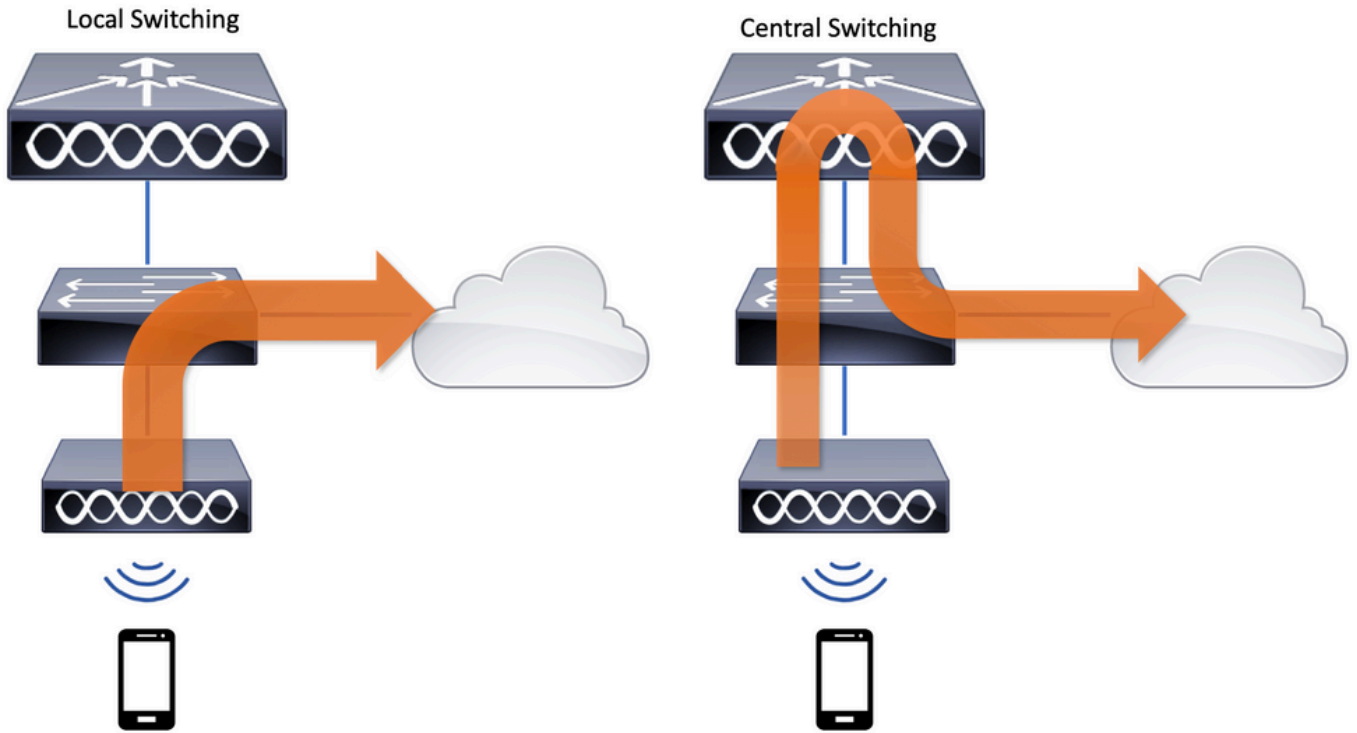
[Profilkonfiguration](#)

## Einleitung

In diesem Dokument werden die FlexConnect-Funktion und ihre allgemeine Konfiguration auf Wireless-Controllern der Serie 9800 beschrieben.

## Hintergrundinformationen

FlexConnect bezieht sich auf die Fähigkeit eines Access Points (AP), zu bestimmen, ob der Datenverkehr von den Wireless-Clients auf AP-Ebene direkt in das Netzwerk geleitet wird (lokales Switching) oder ob der Datenverkehr auf den 9800-Controller (zentrales Switching) zentralisiert wird.



## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

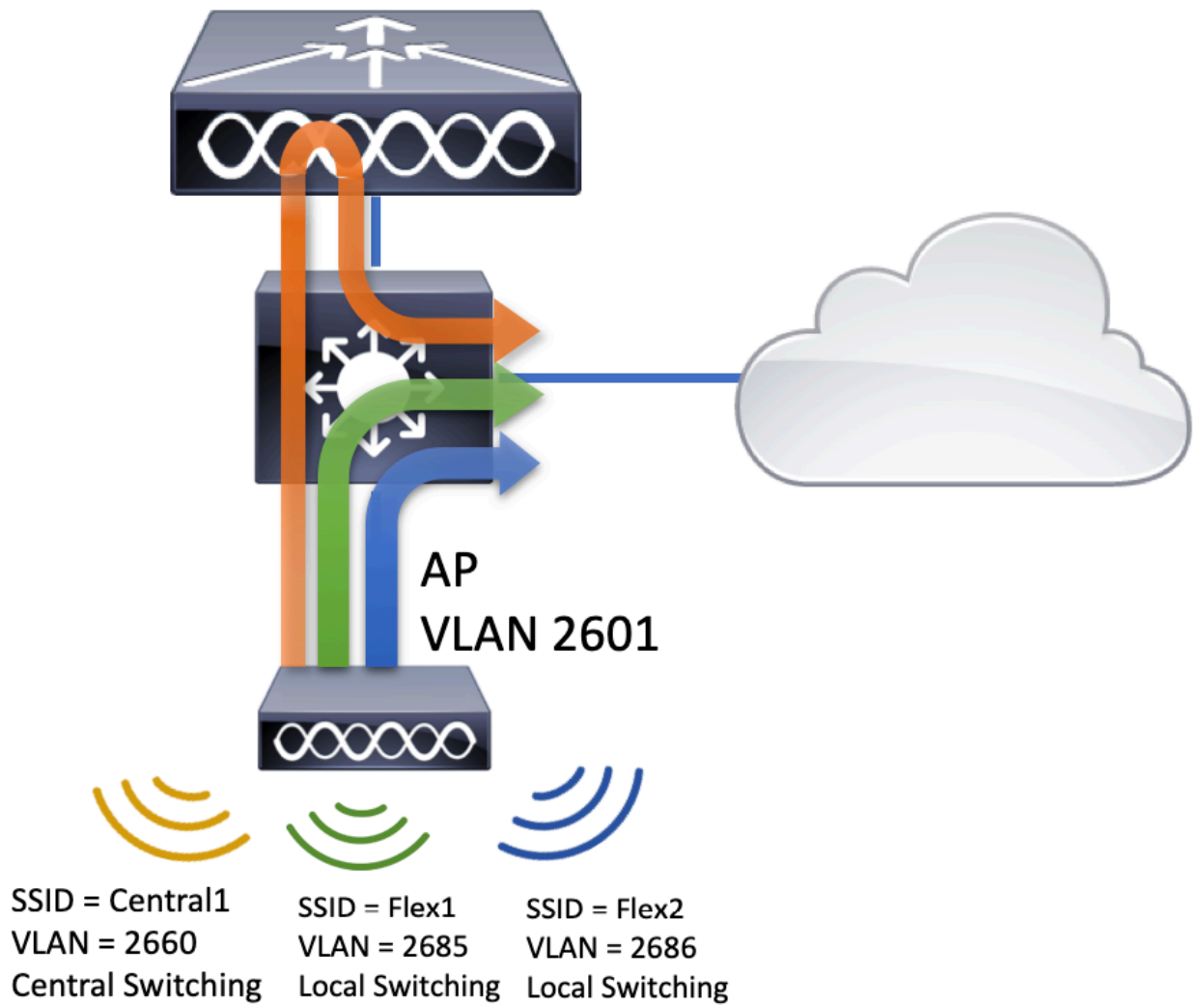
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Wireless Controller der Serie 9800 mit Cisco IOS®-XE Gibraltar v17.3.x

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 verstehen.

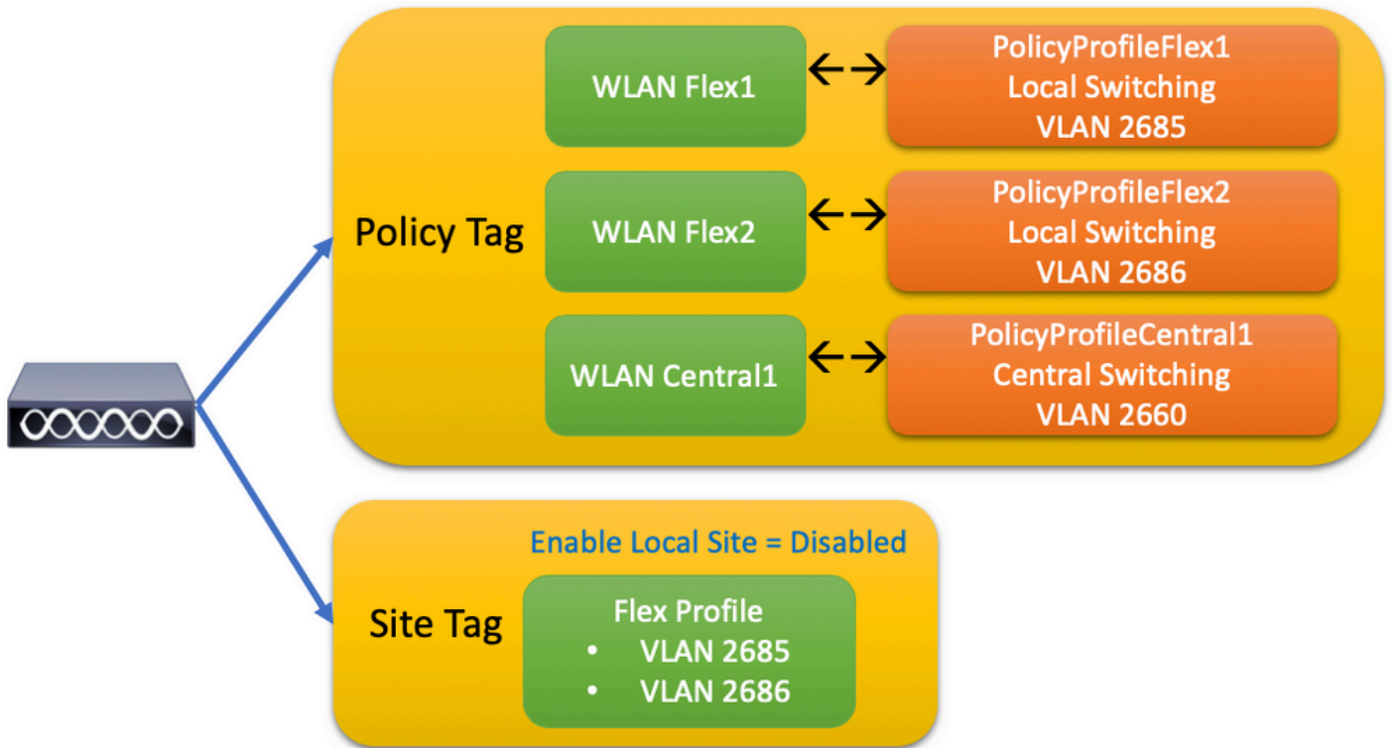
### Netzwerkdiagramm

Dieses Dokument basiert auf folgender Topologie:



## Konfigurationen

Dies ist das visuelle Schema der Konfiguration, die für das Szenario dieses Dokuments erforderlich ist:



Um einen FlexConnect Local Switching Service Set Identifier (SSID) zu konfigurieren, gehen Sie wie folgt vor:

1. Erstellen/Ändern eines WLAN-Profiles
2. Erstellen/Ändern eines Richtlinienprofils
3. Erstellen/Ändern eines Policy Tags
4. Erstellen/Ändern eines Flex-Profiles
5. Site-Tag erstellen/ändern
6. Richtlinien-Tag-Zuweisung zu AP

In diesen Abschnitten wird Schritt für Schritt erläutert, wie Sie diese konfigurieren.

## WLAN-Profil erstellen/ändern

Mit diesem Leitfaden können Sie die drei SSIDs erstellen:

[SSID erstellen](#)

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >

## WIRELESS NETWORKS

Number of WLANs selected : 0

<input type="checkbox"/>	Name	ID	SSID
<input type="checkbox"/>	Flex1	2	Flex1
<input type="checkbox"/>	Flex2	3	Flex2
<input type="checkbox"/>	Central1	4	Central1

## Erstellen/Ändern eines Richtlinienprofils

Schritt 1: Navigieren Sie zu Configuration > Tags & Profiles > Policy. Wählen Sie entweder den Namen einer bereits vorhandenen aus, oder klicken Sie auf **+ Hinzufügen**, um eine neue hinzuzufügen.

Add Policy Profile
✕

General

Access Policies

QOS and AVC

Mobility

Advanced

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

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 ENABLED

Central DHCP  DISABLED

Central Association  DISABLED

Flex NAT/PAT  DISABLED

↶ Cancel

Wenn Sie Central Switching wird diese Warnmeldung angezeigt. Klicken Sie auf Yes und fahren Sie mit der Konfiguration fort.

Disabling Central Switching will cause Export Anchor to be disabled

No Yes

Schritt 2: Wechseln Sie zum Access Policies und geben Sie das VLAN ein (es wird in der Dropdown-Liste nicht angezeigt, da dieses VLAN auf dem 9800 WLC nicht vorhanden ist). Klicken Sie anschließend auf Save & Apply to Device.

Add Policy Profile

General Access Policies QOS and AVC Mobility Advanced

**WLAN Local Profiling**

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name Search or Select

**VLAN**

VLAN/VLAN Group 2685

Multicast VLAN Enter Multicast VLAN

**WLAN ACL**

IPv4 ACL Search or Select

IPv6 ACL Search or Select

**URL Filters**

Pre Auth Search or Select

Post Auth Search or Select

Cancel Save & Apply to Device

Schritt 3: Wiederholen Sie den Vorgang für PolicyProfileFlex2.

### Add Policy Profile

General Access Policies QOS and AVC Mobility Advanced

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

**Name\*** PolicyProfileFlex2

Description Enter Description

Status **ENABLED**

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

**CTS Policy**

Inline Tagging

SGACL Enforcement

Default SGT 2-65519

**WLAN Switching Policy**

Central Switching  DISABLED

Central Authentication **ENABLED**

Central DHCP  DISABLED

Central Association  DISABLED

Flex NAT/PAT  DISABLED

Cancel Apply to Device

### Add Policy Profile

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

**WLAN Local Profiling**

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name Search or Select

**VLAN**

VLAN/VLAN Group 2686

Multicast VLAN Enter Multicast VLAN

**WLAN ACL**

IPv4 ACL Search or Select

IPv6 ACL Search or Select

**URL Filters**

Pre Auth Search or Select

Post Auth Search or Select

Cancel Save & Apply to Device

Schritt 4: Vergewissern Sie sich für den zentral gewitchten SSID, dass das erforderliche VLAN auf dem 9800 WLC vorhanden ist, und erstellen Sie es, falls dies nicht der Fall ist.

**Hinweis:** Bei FlexConnect-APs mit lokal geschalteten WLANs wird der Datenverkehr am WAP vermittelt, und die DHCP-Anfragen vom Client gehen direkt über die WAP-Schnittstelle in das kabelgebundene Netzwerk. Der WAP hat keine SVI im Client-Subnetz und kann daher keinen DHCP-Proxy ausführen. Daher hat die DHCP-Relay-Konfiguration (DHCP-Server-IP-Adresse) auf der Registerkarte "Policy Profile" (Richtlinienprofil) > "Advanced" (Erweitert) keine Bedeutung für lokal geschaltete WLANs. In diesen Szenarien muss der Switch-Port das Client-VLAN zulassen und dann, wenn sich der DHCP-Server in einem anderen VLAN befindet, die IP-Hilfsadresse im SVI/Standard-Client-Gateway konfigurieren, damit dieser weiß, wohin die DHCP-Anfrage vom Client gesendet werden soll.

### [Client-VLANs deklarieren](#)

Schritt 5: Erstellen Sie ein Richtlinienprofil für die zentrale SSID.

Navigieren Sie zu Configuration > Tags & Profiles > Policy. Wählen Sie entweder den Namen eines bereits vorhandenen aus, oder klicken Sie auf + Add um eine neue hinzuzufügen.

#### Add Policy Profile ✕

General    Access Policies    QOS and AVC    Mobility    Advanced

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

Name*	<input type="text" value="PolicyProfileCentral1"/>	<b>WLAN Switching Policy</b>
Description	<input type="text" value="Enter Description"/>	<input checked="" type="checkbox"/> Central Switching
Status	<input checked="" type="checkbox"/> ENABLED	<input checked="" type="checkbox"/> Central Authentication
Passive Client	<input type="checkbox"/> DISABLED	<input checked="" type="checkbox"/> Central DHCP
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	<input checked="" type="checkbox"/> Central Association
<b>CTS Policy</b>		<input type="checkbox"/> Flex NAT/PAT
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	<input type="text" value="2-65519"/>	



Add Policy Profile

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

**WLAN Local Profiling**

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

**VLAN**

VLAN/VLAN Group

Multicast VLAN

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**URL Filters**

Pre Auth

Post Auth

Daher gibt es drei Richtlinienprofile.

	Policy Profile Name	Description
<input type="checkbox"/>	PolicyProfileFlex1	
<input type="checkbox"/>	PolicyProfileFlex2	
<input type="checkbox"/>	PolicyProfileCentral1	

1 10 items per page

CLI:

```
# config t
# vlan 2660
# exit # wireless profile policy PolicyProfileFlex1 # no central switching # vlan 2685 # no
shutdown # exit # wireless profile policy PolicyProfileFlex2 # no central switching # vlan 2686
# no shutdown # exit # wireless profile policy PolicyProfileCentral1 # vlan VLAN2660 # no
shutdown # end
```

## Erstellen/Ändern eines Policy Tags

Das Policy Tag (Richtlinien-Tag) ist das Element, mit dem Sie angeben können, welche SSID mit welchem Richtlinienprofil verknüpft ist.

Schritt 1: Navigieren Sie zu Configuration > Tags & Profiles > Tags > Policy. Wählen Sie entweder den Namen eines bereits vorhandenen aus, oder klicken Sie auf + Add um eine neue hinzuzufügen.

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

### Manage Tags

Policy	Site	RF	AP
<input type="checkbox"/> + Add			
<input type="checkbox"/> x Delete			
Policy Tag Name			
<input type="checkbox"/>	PT1		
<input type="checkbox"/>	PT2		
<input type="checkbox"/>	PT3		
<input type="checkbox"/>	PolTag1		
<input type="checkbox"/>	new-policy		

Schritt 2: Klicken Sie innerhalb des Richtlinien-Tags auf **+Add**, wählen Sie aus der Dropdown-Liste **WLAN Profile Name**, der dem Policy Tag hinzugefügt werden soll, und Policy Profile mit dem Sie es verknüpfen möchten. Klicken Sie anschließend auf das Kontrollkästchen.

### Add Policy Tag

Name\* PolicyTag1

Description Enter Description

+ Add  x Delete

WLAN Profile	Policy Profile
No items to display	

0 10 items per page

Cancel Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ 0 ▶	No items to display

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

✕
✓

↶ Cancel
📄 Save & Apply to Device

Wiederholen Sie den Vorgang für die drei SSIDs, und klicken Sie anschließend auf **Save & Apply to Device**.

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> Flex1	PolicyProfileFlex1
<input type="checkbox"/> Flex2	PolicyProfileFlex2
<input type="checkbox"/> Central1	PolicyProfileCentral1

◀ 1 ▶ 10 items per page 1 - 3 of 3 items

↶ Cancel
📄 Save & Apply to Device

CLI:

```
# config t
# wireless tag policy PolicyTag1
# wlan Flex1 policy PolicyProfileFlex1
# wlan Flex2 policy PolicyProfileFlex2
```

```
# wlan Centrall policy PolicyProfileCentrall
# end
```

## Erstellen/Ändern eines Flex-Profiles

Beachten Sie in der für dieses Dokument verwendeten Topologie, dass es in Local Switching zwei SSIDs mit zwei verschiedenen VLANs gibt. Innerhalb des Flex Profile geben Sie das VLAN der APs (natives VLAN) und jedes andere VLAN an, das der AP kennen muss, in diesem Fall die von den SSIDs verwendeten VLANs.

Schritt 1: Navigieren Sie zu Configuration > Tags & Profiles > Flex und entweder eine neue erstellen oder eine bereits vorhandene ändern.

The screenshot shows the 'Flex Profile' configuration page. On the left is a dark sidebar with navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area has a search bar and two buttons: '+ Add' (highlighted with a red box) and 'x Delete'. Below the buttons is a table with the following data:

	Flex Profile Name
<input type="checkbox"/>	new-flex-profile
<input type="checkbox"/>	default-flex-profile

At the bottom of the table, there are navigation controls showing '1' items per page and a dropdown menu set to '10 items per page'.

Schritt 2: Definieren Sie einen Namen für das Flex Profile, und geben Sie das APs-VLAN (Native VLAN ID) an.

The screenshot shows the 'Add Flex Profile' configuration form. The 'General' tab is selected. The form has the following fields and options:

- Name\*: FlexProfileLab (highlighted with a red box)
- Description: Enter Description
- Native VLAN ID: 2601 (highlighted with a red box)
- HTTP Proxy Port: 0
- HTTP-Proxy IP Address: 0.0.0.0
- CTS Policy: default-sxp-profile (dropdown menu)
- Inline Tagging:
- SGACL Enforcement:
- Multicast Overridden Interface:
- Fallback Radio Shut:
- Flex Resilient:
- ARP Caching:
- Efficient Image Upgrade:
- Office Extend AP:
- Join Minimum Latency:

At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons.

Schritt 3: Navigieren Sie zum VLAN und geben Sie das benötigte VLAN an.

In diesem Szenario befinden sich Clients in den VLANs 2685 und 2686. Diese VLANs sind auf dem 9800 WLC nicht vorhanden. Fügen Sie sie dem Flex Profile-System hinzu, sodass sie auf dem AP vorhanden sind.

General Local Authentication Policy ACL **VLAN**

**+ Add** ✕ Delete

VLAN Name	ID	ACL Name
No items to display		

◀ 0 ▶ 10 items per page

↶ Cancel ↷ Save & Apply to Device

VLAN Name\*

VLAN Id\*

ACL Name

**✓ Save** ↶ Cancel

**Hinweis:** Wenn Sie das Richtlinienprofil erstellt haben und einen VLAN-Namen anstelle einer VLAN-ID ausgewählt haben, stellen Sie sicher, dass der VLAN-Name hier im Flex Profile-Profil exakt derselbe ist.

Wiederholen Sie den Vorgang für die erforderlichen VLANs.

General Local Authentication Policy ACL **VLAN**

**+ Add** ✕ Delete

VLAN Name	ID	ACL Name
<input type="checkbox"/> VLAN2685	2685	
<input type="checkbox"/> VLAN2686	2686	

◀ 1 ▶ 10 items per page

1 - 2 of 2 items

↶ Cancel ↷ **Save & Apply to Device**

Beachten Sie, dass das für das zentrale Switching verwendete VLAN nicht hinzugefügt wurde, da

der Access Point davon nichts wissen muss.

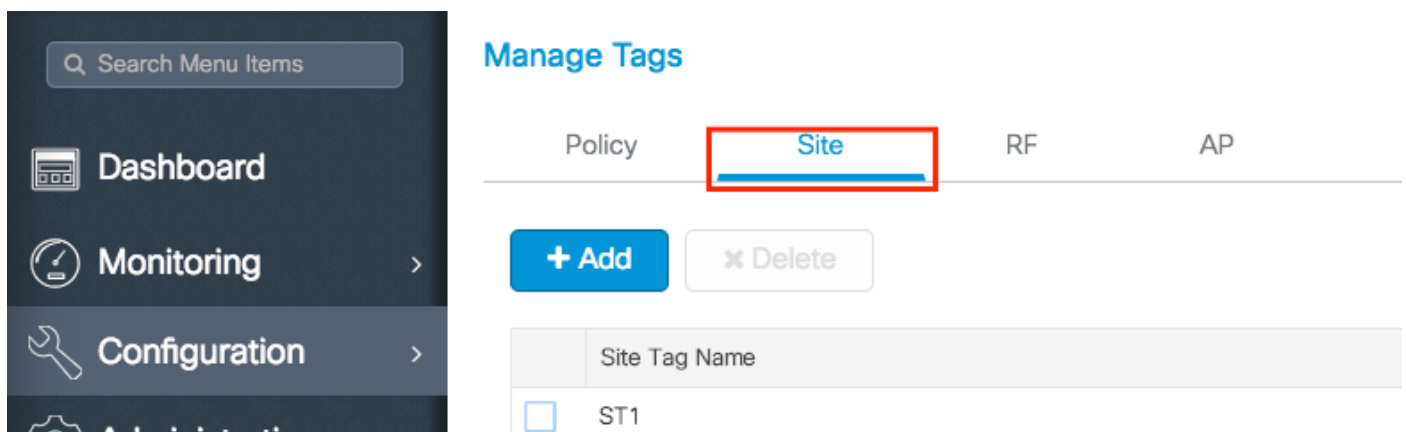
CLI:

```
# config t
# wireless profile flex FlexProfileLab # native-vlan-id 2601 # vlan-name VLAN2685 # vlan-id 2685
# vlan-name VLAN2686 # vlan-id 2686 # end
```

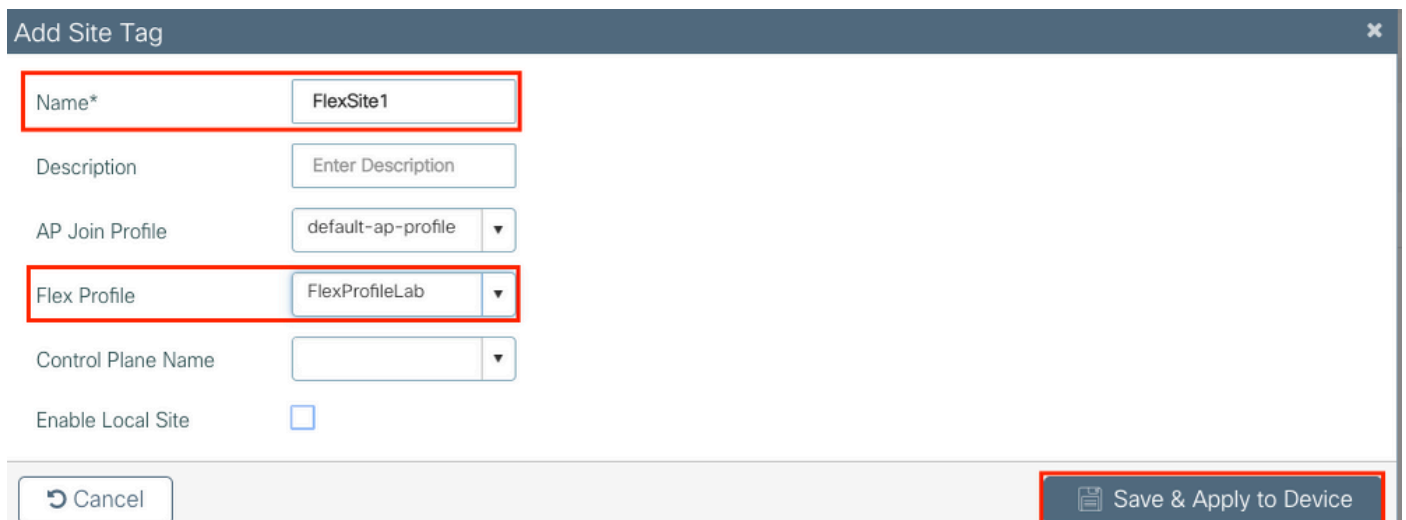
## Site-Tag erstellen/ändern

Das Site-Tag ist das Element, mit dem Sie angeben können, welcher Access Point-Teilnehmer und/oder welches Flex-Profil den Access Points zugewiesen wird.

Schritt 1: Navigieren Sie zu **Configuration > Tags & Profiles > Tags > Site**. Wählen Sie entweder den Namen eines bereits vorhandenen aus, oder klicken Sie auf **+ Add** um eine neue hinzuzufügen.



Schritt 2: Deaktivieren Sie im Site-Tag die **Enable Local Site** (Jeder AP, der eine Site-Tag-Nummer mit der **Enable Local Site** Option disabled in den FlexConnect-Modus konvertiert). Sobald die Option deaktiviert ist, können Sie auch die **Flex Profile**. Nach diesem Klick **Save & Apply to Device**.



CLI:

```
# config t
# wireless tag site FlexSite1
# flex-profile FlexProfileLab
# no local-site
```

## Richtlinien-Tag-Zuweisung zu AP

Sie können einem Access Point direkt eine Policy Tag-Nummer zuweisen oder einer Gruppe von Access Points gleichzeitig dieselbe Policy Tag-Nummer zuweisen. Wählen Sie die passende Lösung aus.

## Zuweisen von Richtlinien-Tags pro AP

Navigieren Sie zu Configuration > Wireless > Access Points > AP name > General > Tags. Über die **site** die gewünschten Tags aus, und klicken Sie auf Update & Apply to Device.

Edit AP ✕

---

General
Interfaces
High Availability
Inventory
Advanced

**General**

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status

AP Mode

Operation Status Registered

Fabric Status Disabled

**Tags**

**⚠** Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

**Version**

Primary Software Version 16.10.1.0

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 15.3.0.0

IOS Version 15.3(3)JPG1S

Mini IOS Version 0.0.0.0

**IP Config**

CAPWAP Preferred Mode Not Configured

DHCP IPv4 Address 172.16.1.110

Static IP (IPv4/IPv6)

**Time Statistics**

Up Time 6 days 20 hrs 27 mins 53 secs

Controller Association Latency 5 days 18 hrs 0 mins 30 secs

↶ Cancel

↻ Update & Apply to Device

**Hinweis:** Beachten Sie, dass nach der Änderung die Richtlinien-Tag-Nummer auf einem AP ihre Verknüpfung mit den 9800-WLCs verliert und innerhalb von etwa einer Minute wieder hinzugefügt wird.




**Hinweis:** Wenn der Access Point im lokalen Modus (oder einem anderen Modus) konfiguriert ist und dann eine Site-Tag-Nummer mit `Enable Local Site` deaktiviert ist, startet der Access Point neu und kehrt im FlexConnect-Modus zurück.

CLI:

```
# config t
# ap <ethernet-mac-addr>
# site-tag <site-tag-name>
# end
```

## Richtlinien-Tag-Zuweisung für mehrere APs

Navigieren Sie zu **Configuration > Wireless Setup > Advanced > Start Now**.

Klicken Sie auf **Tag APs** -Symbol, wählen Sie anschließend die Liste der APs aus, denen Sie die Tags zuweisen möchten (Sie können auf den Pfeil nach unten neben **AP name** [oder ein anderes Feld], um die Liste der Access Points zu filtern).

Number of APs: 2

Selected Number of APs: 2

<input type="checkbox"/>	AP Name	AP
<input checked="" type="checkbox"/>	AP3802-karlcisn	
<input checked="" type="checkbox"/>	AP2802-01	

Show items with value that:

Is equal to

Nachdem Sie die gewünschten APs ausgewählt haben, klicken Sie auf **+ Tag APs**.

Number of APs: 2  
Selected Number of APs: 2

AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
<input checked="" type="checkbox"/> AP3802-karlcsn	AIR-AP3802I-A-K9	0042.68c6.4120	Local	Disabled	Registered	Location-typical-density	Location-typical-density	Location-typical-density	default location	MX	Local
<input checked="" type="checkbox"/> AP2802-01	AIR-AP2802I-B-K9	2c5a.0f40.6900	Local	Enabled	Registered	PT1	default-site-tag	default-rf-tag	CALO	US	Local

10 items per page 1 - 2 of 2 items

Wählen Sie die Tags aus, die Sie den APs zuweisen möchten, und klicken Sie auf **Save & Apply to Device**.

## Tag APs

Tags

Policy: PT1 ▼

Site: ST1 ▼

RF: default-rf-tag ▼

*Changing AP Tag(s) will cause associated AP(s) to reconnect*

Cancel **Save & Apply to Device**

**Hinweis:** Beachten Sie, dass nach der Änderung des Richtlinien-Tags an einem AP die Verknüpfung mit den 9800-WLCs unterbrochen wird und die Anmeldung innerhalb von etwa einer Minute erfolgt.

**Hinweis:** Wenn der Access Point im lokalen Modus (oder einem anderen Modus) konfiguriert ist und dann eine Site-Tag-Nummer mit `Enable Local Site` deaktiviert ist, startet der Access Point neu und kehrt im FlexConnect-Modus zurück.

CLI:

Es gibt keine CLI-Option zum Zuweisen desselben Tags zu mehreren APs.

## Flexconnect-ACLs

Wenn Sie ein lokal geschaltetes WLAN verwenden, sollten Sie zunächst prüfen, wie eine ACL auf die Clients angewendet werden kann.

Bei einem zentral geschalteten WLAN wird der gesamte Datenverkehr am WLC freigegeben, sodass die ACL nicht an den WAP weitergeleitet werden muss. Wenn der Datenverkehr jedoch lokal vermittelt wird (Flex Connect - Lokales Switching), muss die ACL (definiert auf dem Controller) zum AP verschoben werden, da der Datenverkehr am AP freigegeben wird. Dies geschieht, wenn Sie die ACL dem Flex-Profil hinzufügen.

## Zentrales WLAN

So wenden Sie eine ACL auf Clients an, die an ein zentral geschaltetes WLAN angeschlossen sind:

**Schritt 1** - Wenden Sie die ACL auf das Richtlinienprofil an. Gehen Sie zu **Configuration > Tags & Profiles > Policy**, und wählen Sie das Richtlinienprofil aus, das mit dem zentral geschalteten WLAN verknüpft ist. Wählen Sie im Abschnitt **"Access Policies" (Zugriffsrichtlinien) > "WLAN ACL"** (WLAN-Zugriffskontrollliste) die Zugriffskontrollliste aus, die Sie auf die Clients anwenden möchten.

**Edit Policy Profile**

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

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

RADIUS Profiling	<input type="checkbox"/>	WLAN ACL
HTTP TLV Caching	<input type="checkbox"/>	IPv4 ACL <b>BLOCK-WLC</b>
DHCP TLV Caching	<input type="checkbox"/>	IPv6 ACL Search or Select

## Lokal geschaltetes WLAN

So wenden Sie eine ACL auf Clients an, die mit einem lokal geschalteten WLAN verbunden sind:

**Schritt 1** - Wenden Sie die ACL auf das Richtlinienprofil an. Gehen Sie zu **Configuration > Tags & Profiles > Policy**, und wählen Sie das Richtlinienprofil aus, das mit dem zentral geschalteten WLAN verknüpft ist. Wählen Sie im Abschnitt **"Access Policies" (Zugriffsrichtlinien) > "WLAN ACL"** (WLAN-Zugriffskontrollliste) die Zugriffskontrollliste aus, die Sie auf die Clients anwenden möchten.

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN ACL

IPv4 ACL BLOCK-WLC

IPv6 ACL Search or Select

**Schritt 2:** Wenden Sie die ACL auf das Flex-Profil an. Gehen Sie zu **Configuration > Tags & Profiles > Flex**, und wählen Sie das den Flex Connect-APs zugewiesene Flex-Profil aus. Fügen Sie im Abschnitt **"Policy ACL" (Richtlinien-ACL)** die ACL hinzu, und klicken Sie auf "Save" (Speichern).

General Local Authentication **Policy ACL** VLAN DNS Layer Security

+ Add - Delete

ACL Name	Central Web Auth	URL Filter
<input type="checkbox"/> ACL_WEBAUTH_REDIRECT	Enabled	

1 10 items per page 1 - 1 of 1 items

ACL Name\* BLOCK-WLC

Central Web Auth

URL Filter Search or Select

Save Cancel

**Überprüfen Sie, ob die ACL angewendet wurde.**

Sie können überprüfen, ob die ACL auf einen Client angewendet wird, wenn Sie zu **Überwachung > Wireless > Clients** wechseln. Wählen Sie den Client aus, den Sie überprüfen möchten.

Aktivieren Sie im Abschnitt **Allgemein > Sicherheitsinformationen** im Abschnitt **"Serverrichtlinien"** den Namen der Filter-ID: diese muss mit der angewendeten ACL übereinstimmen.

## Client

360 View

**General**

QOS Statistics

ATF Statistics

Mobility History

Call Statistics

Client Properties

AP Properties

**Security Information**

Client Statistics

QOS Properties

EoGRE

SM State

TERMINATE

### Local Policies

Service Template

wlan\_svc\_local-switched-policy-profile (priority 254)

VLAN

VLAN1416

Absolute Timer

1800

### Server Policies

Output SGT

0006-00

Filter-ID

BLOCK-WLC

### Resultant Policies

Output SGT

0006-00

Filter-ID

BLOCK-WLC

VLAN Name

VLAN1416

Bei Flex Connect-APs (lokale Switching-APs) können Sie überprüfen, ob die ACL an den AP angeschlossen ist, indem Sie den Befehl "#show ip access-lists" auf dem AP selbst eingeben.

## Verifizierung

Sie können diese Befehle verwenden, um die Konfiguration zu überprüfen.

## Konfiguration von VLANs/Schnittstellen

```
# show vlan brief
# show interfaces trunk
# show run interface <interface-id>
```

## WLAN-Konfiguration

```
# show wlan summary
# show run wlan [wlan-name] # show wlan { id <wlan-id> | name <wlan-name> | all }
```

## AP-Konfiguration

```
# show ap summary
# show ap tag summary
# show ap name <ap-name> tag { info | detail }
```

```
# show ap name <ap-name> tag detail
```

```
AP Name : AP2802-01 AP Mac : 0896.ad9d.143e Tag Type Tag Name -----
Policy Tag PT1 RF Tag default-rf-tag Site Tag default-site-tag Policy tag mapping -----
---- WLAN Profile Name Policy Name VLAN Central Switching IPv4 ACL IPv6 ACL -----
```

```
-----  
----- psk-pbl-ewlc  
ctrl-vl2602 VLAN0210 ENABLED Not Configured Not Configured Site tag mapping -----  
Flex Profile : default-flex-profile AP Profile : default-ap-profile Local-site : Yes RF tag  
mapping ----- 5ghz RF Policy : Global Config 2.4ghz RF Policy : Global Config
```

## Tag-Konfiguration

```
# show wireless tag { policy | rf | site } summary  
# show wireless tag { policy | rf | site } detailed <tag-name>
```

## Profilkonfiguration

```
# show wireless profile { flex | policy } summary  
# show wireless profile { flex | policy } detailed <profile-name> # show ap profile <AP-join-  
profile-name> detailed
```

## 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.