

FlexConnect met verificatie configureren op Catalyst 9800 WLC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

Inleiding

Dit document beschrijft hoe u FlexConnect met centrale of lokale verificatie kunt configureren op Catalyst 9800 draadloze LAN-controller.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst draadloze 9800 configuratiemodel
- FlexConnect
- 802.1x

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C980-CL, Cisco IOS-XE® 17.3.4

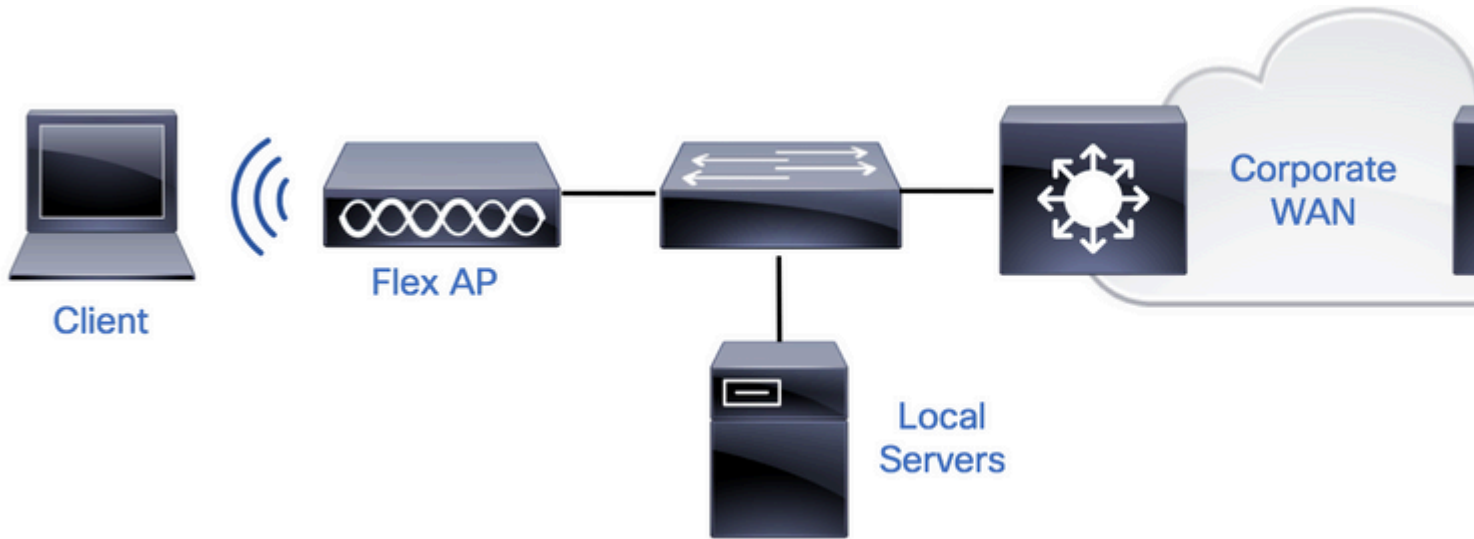
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

FlexConnect is een draadloze oplossing voor implementatie in externe vestigingen. Hiermee kunt u access points (AP's) configureren op externe locaties vanuit het kantoor van het bedrijf via een Wide Area Network (WAN)-link zonder dat u in elke locatie een controller hoeft te implementeren. De FlexConnect AP's kunnen het clientgegevensverkeer lokaal switches en de clientverificatie lokaal uitvoeren wanneer de verbinding met de controller verloren gaat. In de verbonden modus kunnen de FlexConnect AP's ook lokale verificatie uitvoeren.

Configureren

Netwerkdigram



Configuraties


AAA-configuratie op 9800 WLC's™


Stap 1. RADIUS-server declareren. **Van GUI:** Navigeer naar Configuratie > Beveiliging > AAA > Servers / Groepen > RADIUS > Servers > + Voeg de RADIUS-serverinformatie toe en voer deze in.

The screenshot shows the Cisco GUI configuration interface. The breadcrumb trail is 'Configuration > Security > AAA'. Under 'AAA', there are tabs for '+ AAA Wizard', 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. The 'Servers / Groups' tab is selected. Below it are '+ Add' and 'Delete' buttons. Under the '+ Add' button, there are tabs for 'RADIUS' and 'Servers'. The 'Servers' tab is selected. Below the 'Servers' tab, there is a table with columns for 'Name', 'Address', and 'Auth Port'. The table is currently empty.

Zorg ervoor dat ondersteuning voor CoA is ingeschakeld als u van plan bent om in de toekomst elke vorm van beveiliging te gebruiken die CoA vereist.

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

Opmerking: Radius CoA wordt niet ondersteund in Flex Connect-implementatie van lokale audits. .

Stap 2. Voeg de RADIUS-server toe aan een RADIUS-groep. **Van GUI:** Navigeer naar Configuratie > Beveiliging > AAA > Servers / Groepen > RADIUS > Servergroepen > + 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

^

v



Assigned Servers


AmmlSE

^

v



 Cancel

 Update & Apply to

Stap 3. Maak een lijst met verificatiemethoden. **Van GUI:** Navigeer naar Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie > + Toevoegen

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

Van 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

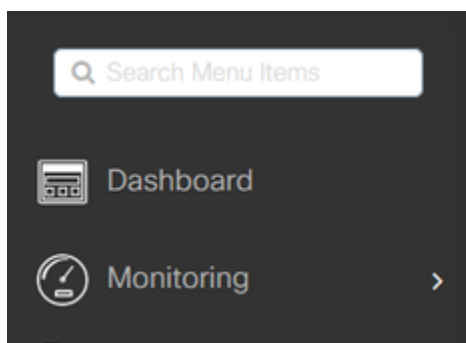
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

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

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

WLAN-configuratie

Stap 1. **Van GUI:** Navigeer naar Configuration > Wireless > WLANs en klik op +Add om een nieuw WLAN te maken en voer de WLAN-informatie in. Klik vervolgens op Toepassen op apparaat.



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

Stap 2. **Van GUI:** Navigeer aan het tabblad Security om de Layer 2/Layer 3-beveiligingsmodus te configureren zolang de coderingsmethode en de verificatielijst in het geval 802.1x in gebruik is. Klik vervolgens op Bijwerken en toepassen op apparaat.

⚠ 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

Lobby Admin Access

MAC Filtering

Fast Transition

Protected Management Frame

Over the DS

PMF

Reassociation Timeout

WPA Parameters

MPSK Configuration

MPSK

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

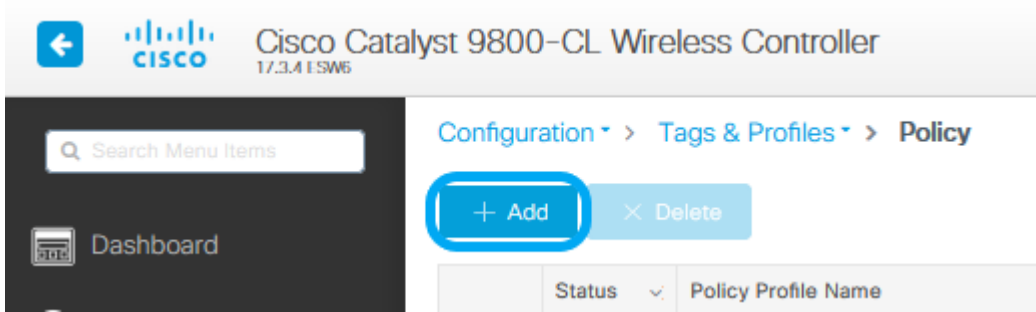
FT + PSK

Cancel

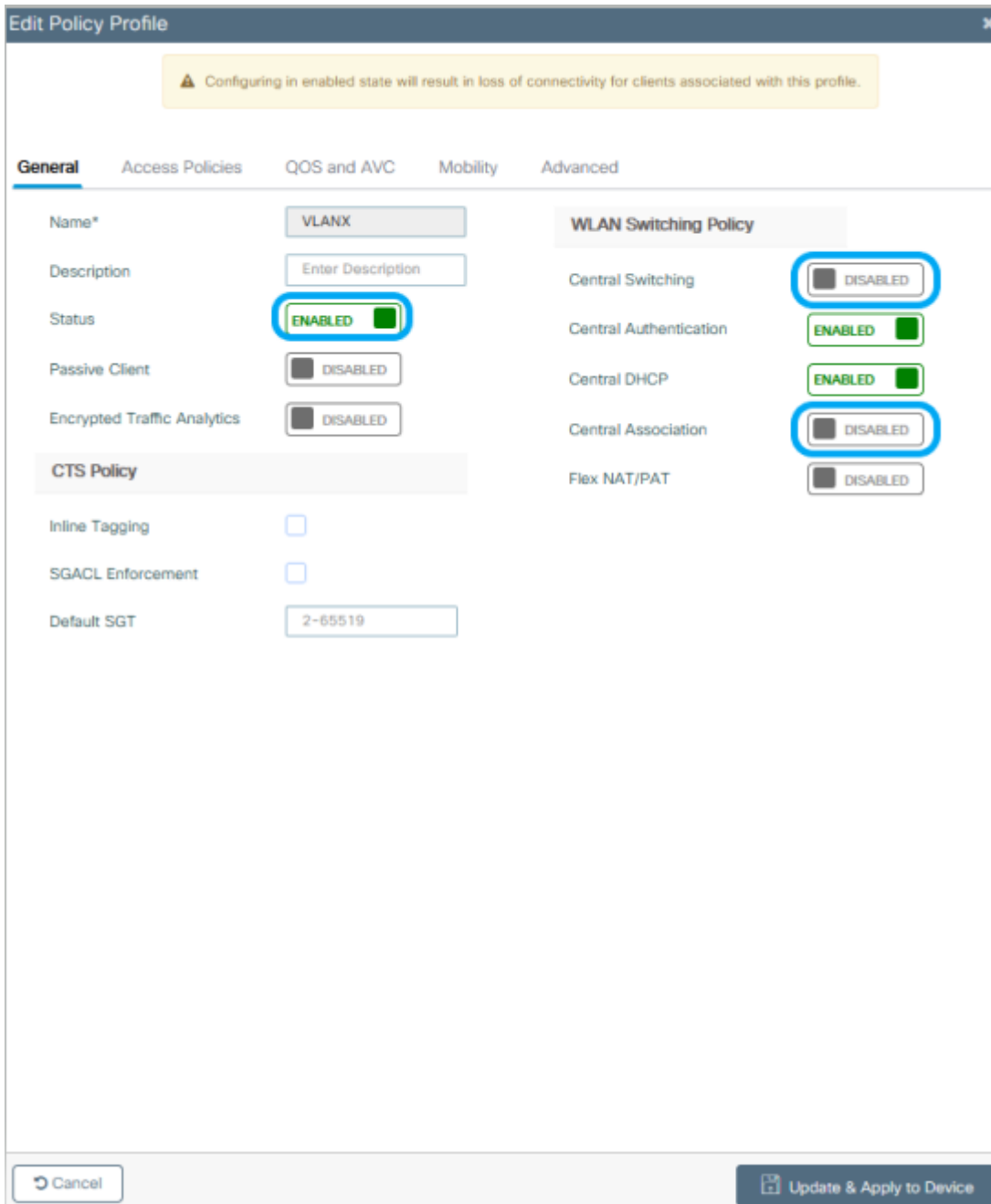
Update & Apply to Device

Configuratie van beleidsprofiel

Stap 1. **Van GUI:** Navigeer aan Configuratie > Markeringen & Profielen > Beleid en klik +Add om een Beleidsprofiel te creëren.



Stap 2. Voeg de naam toe en vink het vakje Central Switching uit. Bij deze installatie wordt de clientverificatie door de controller verwerkt en worden de clientgegevenspakketten van FlexConnect Access Point switches lokaal verwerkt.



Opmerking: associatie en switching moeten altijd gekoppeld zijn, als centrale switching uitgeschakeld is moet centrale associatie ook uitgeschakeld worden op alle beleidsprofielen wanneer Flexconnect AP's worden gebruikt.

Stap 3. **Van GUI:** Navigeer naar het tabblad Toegangsbeleid om het VLAN toe te wijzen waaraan de draadloze clients kunnen

worden toegewezen wanneer zij standaard verbinding maken met dit WLAN.
U kunt één VLAN-naam in de vervolgkeuzelijst selecteren of als beste praktijk handmatig een VLAN-id typen.

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

Stap 4. **Van GUI:** Navigeer naar het tabblad Advanced om de WLAN-timeouts, DHCP, WLAN Flex Policy en AAA-beleid te configureren voor het geval ze in gebruik zijn. Klik vervolgens op Bijwerken en toepassen op apparaat.

✕
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 ▼

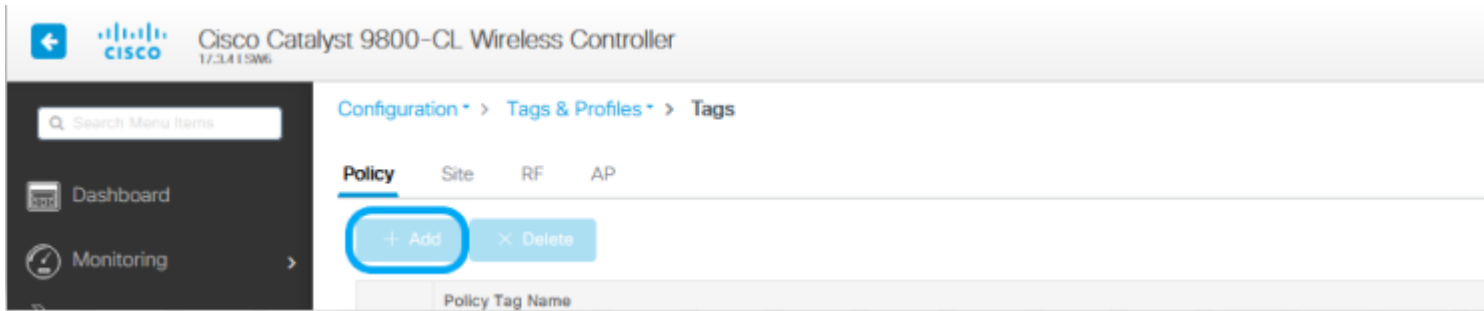
EoGRE Tunnel Profiles

↶ Cancel

↶ Update & Apply to Device

Configuratie van beleidstag

Stap 1. **Van GUI:** Navigeer aan Configuratie > Markeringen & Profielen > Markeringen > Beleid > +Add.



Stap 2. Wijs een naam toe en geef het beleidsprofiel en het WLAN-profiel dat u eerder hebt gemaakt, in kaart.

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-profielconfiguratie

Stap 1. **Van GUI:** Navigeer aan Configuratie > Markeringen & Profielen > Flex en klik +Add om nieuwe te creëren.

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 ▼

Opmerking: Native VLAN-id verwijst naar het VLAN dat wordt gebruikt door de AP's die dit Flex Profile kunnen toewijzen, en het moet dezelfde VLAN-id zijn die is geconfigureerd als native op de switch-poort waarop de AP's zijn aangesloten.

Stap 2. Voeg onder het tabblad VLAN de benodigde VLAN's toe, de VLAN's die standaard aan het WLAN zijn toegewezen via een beleidsprofiel of de VLAN's die door een RADIUS-server worden gedrukt. Klik vervolgens op Bijwerken

en toepassen op apparaat.

Edit Flex Profile

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add

× Delete

VLAN Name	ID	ACL Name
No items to display		

10 items per page

VLAN Name*

VLAN76

VLAN Id*

76

ACL Name

Select ACL

✓ Save

↶ Cancel

↶ Cancel

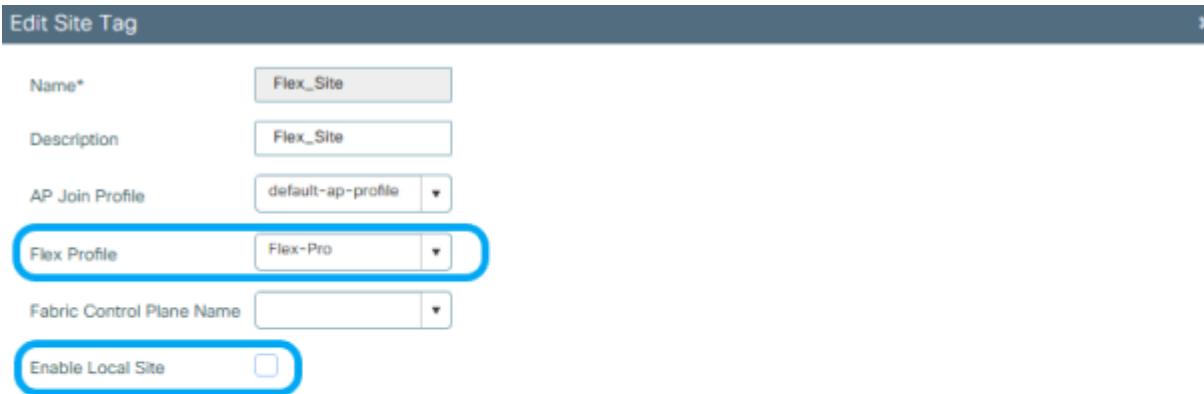
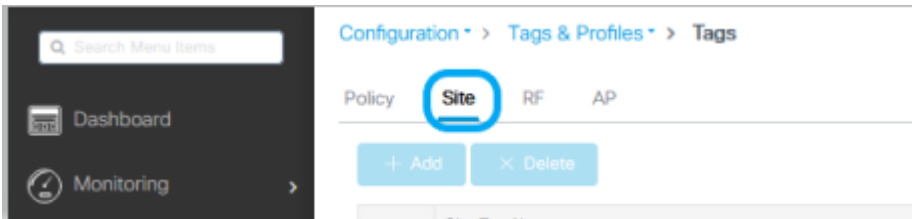
↶ Upd

Opmerking: voor beleidsprofiel, wanneer u het standaard VLAN selecteert dat aan de SSID is toegewezen. Als u een VLAN-naam in die stap gebruikt, zorg er dan voor dat u dezelfde VLAN-naam gebruikt in de Flex Profile Configuration, anders kunnen clients geen verbinding maken met het WLAN.

Opmerking: om een ACL voor flexConnect met AAA-opheffing te configureren, moet u deze alleen configureren op "beleids-ACL". Als ACL is toegewezen aan een specifiek VLAN, moet u ACL toevoegen wanneer u VLAN toevoegt en vervolgens ACL toevoegen op "beleid-ACL".

Configuratie van sitetag

Stap 1. **Van GUI:** Navigeren naar Configuratie > Tags & profielen > Tags > Site en klik op +Add om een nieuwe Site tag te maken. Schakel het vakje Local Site inschakelen uit om AP's toe te staan lokaal switch te maken van het clientgegevensverkeer en het eerder gemaakte Flex Profile toe te voegen.

A screenshot of the 'Edit Site Tag' configuration form. The form has a dark blue header with the title 'Edit Site Tag' and a close button. The fields are: 'Name*' with the value 'Flex_Site'; 'Description' with the value 'Flex_Site'; 'AP Join Profile' with a dropdown menu showing 'default-ap-profile'; 'Flex Profile' with a dropdown menu showing 'Flex-Pro' (this field is circled in blue); 'Fabric Control Plane Name' with a dropdown menu; and 'Enable Local Site' with an unchecked checkbox (this checkbox is also circled in blue).

Opmerking: aangezien de optie Local Site inschakelen is uitgeschakeld, kunnen de toegangspunten die deze sitetag toegewezen krijgen, worden geconfigureerd als FlexConnect-modus.

Stap 2. **Van GUI:** Navigeer naar Configuration > Wireless > Access points > AP-naam om de Site Tag en Policy Tag aan een gekoppeld AP toe te voegen. Dit kan de AP ertoe bewegen zijn CAPWAP-tunnel opnieuw te starten en terug te keren naar de 9800 WLC.

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

Edit AP

General Interfaces High Availability Inventory ICap Advanced Support Bundle

General

AP Name* talomari1

Location* default location

Base Radio MAC b4de.31d7.b920

Ethernet MAC 005d.7319.bb2a

Admin Status **ENABLED**

AP Mode **Local** ▼

Operation Status Registered

Fabric Status Disabled

LED State **ENABLED**

LED Brightness Level 8 ▼

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy Policy ▼

Site **Flex_Site** ▼

RF default-rf-tag ▼

Write Tag Config to AP

Version

Primary Software Version 17.3.4.154

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.1.2.4

IOS Version 17.3.4.154

Mini IOS Version 0.0.0.0

IP Config

CAPWAP Preferred Mode IPv4

DHCP IPv4 Address 10.48.70.77

Static IP (IPv4/IPv6)

Time Statistics

Up Time 0 days 0 hrs 3 mins 28 secs

Controller Association Latency 2 mins 40 secs

Cancel Update & Apply to Device

Wanneer het toegangspunt weer is aangesloten, ziet u dat het toegangspunt zich nu in de FlexConnect-modus bevindt.

▼ 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 verificatie met externe RADIUS-server

Stap 1. Voeg het toegangspunt als netwerkapparaat toe aan de RADIUS-server. Raadpleeg bijvoorbeeld [Hoe u Identity Service Engine \(ISE\) gebruikt als RADIUS-server](#)

Stap 2. Maak een WLAN.

De configuratie kan hetzelfde zijn als de configuratie die eerder is geconfigureerd.

Add WLAN ✕

General

Security

Advanced

Profile Name*

SSID*

WLAN ID*

Status ENABLED

Radio Policy

Broadcast SSID ENABLED

↶ Cancel

▶ Apply to Device

Stap 3. Configuratie beleidsprofiel.

U kunt een nieuwe maken of de eerder geconfigureerde software gebruiken. Schakel deze keer de selectievakjes Central Switching, Central Verification, Central DHCP en Central Association Enable uit.

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

Stap 4. Configuratie van beleidstags.

Associeer het geconfigureerde WLAN en het gemaakte beleidsprofiel.

Stap 5. Configuratie Flex-profiel.

Maak een Flex Profile, navigeer naar het tabblad Local Authentication, configureer de Radius Server Group en controleer het vakje RADIUS.

Edit Flex Profile

General **Local Authentication** Policy ACL VLAN Umbrella

Radius Server Group

AmmISE

Local Accounting Radius Server Group

Select Accounting S

Local Client Roaming

EAP Fast Profile

Select Profile

LEAP

PEAP

TLS

RADIUS

Users

+ Add

× Delete

Select File



Upload

Select CSV File

Username
0

10 items per page

No items to display

Cancel

Update

Stap 6. Configuratie van sitetag.

Configureer het Flex Profile dat in stap 5 is geconfigureerd en schakel het vakje Local Site inschakelen uit.

Add Site Tag

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

Cancel

Apply to D

Verifiëren

Van GUI: Navigeer naar **Monitoring > Wireless > Clients** en bevestig de **Policy Manager-status** en de FlexConnect-parameters.

Centrale verificatie:

Client	
General	
Client Properties	
MAC Address	484b.aa52.5937
IPv4 Address	172.16.76.41
User Name	address1
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 verificatie:

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		addressi		
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		

U kunt deze opdrachten gebruiken om de huidige configuratie te verifiëren:

Van 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>
```

Problemen oplossen

WLC 9800 biedt ALTIJD-ON traceermogelijkheden. Dit zorgt ervoor dat alle aan de client gerelateerde fouten, waarschuwingen en meldingen op het niveau constant worden vastgelegd en u kunt logbestanden bekijken voor een incident of storing nadat het is opgetreden.

Opmerking: op basis van het volume van de gegenereerde logbestanden kunt u enkele uren teruggaan naar meerdere dagen.

Om de sporen te bekijken die 9800 WLC standaard heeft verzameld, kunt u via SSH/Telnet verbinding maken met de 9800 WLC en deze stappen doorlopen (zorg ervoor dat u de sessie aan een tekstbestand registreert).

Stap 1. Controleer de huidige controllertijd zodat u de logbestanden kunt volgen in de tijd terug naar toen het probleem zich voordeed.

Van CLI:

```
# show clock
```

Stap 2. Verzamel syslogs van de controllerbuffer of externe syslog zoals die door de systeemconfiguratie wordt gedictieerd. Dit geeft een snel overzicht van de systeemstatus en eventuele fouten.

Van CLI:

```
# show logging
```

Stap 3. Controleer of de debug-voorwaarden zijn ingeschakeld.

Van CLI:

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

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

Opmerking: Als u een voorwaarde vermeld vindt, betekent het dat de sporen zijn ingelogd om het debug-niveau voor alle processen die de ingeschakelde voorwaarden (mac-adres, ip-adres enzovoort) tegenkomen. Dit zou het volume van de boomstammen doen toenemen. Daarom wordt aanbevolen alle voorwaarden te wissen wanneer niet actief debuggen

Stap 4. Als u aanneemt dat het mac-adres dat wordt getest niet als voorwaarde in Stap 3 is vermeld, verzamelt u de altijd beschikbare meldingen op het niveau voor het specifieke mac-adres.

Van CLI:

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

U kunt de inhoud op de sessie weergeven of u kunt het bestand kopiëren naar een externe TFTP-server.

Van CLI:

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

Voorwaardelijke debug en radio actief spoor

Als de altijd-on sporen u niet genoeg informatie geven om de trigger voor het probleem dat wordt onderzocht te bepalen, kunt u voorwaardelijke debugging inschakelen en Radio Active (RA)-spoor opnemen, dat debug level traces kan bieden voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval). Om het voorwaardelijke zuiveren toe te laten, ga door deze stappen.

Stap 5. Zorg ervoor dat de debug-voorwaarden niet zijn ingeschakeld.

Van CLI:

```
# clear platform condition all
```

Stap 6. Schakel de debug-voorwaarde in voor het draadloze client-MAC-adres dat u wilt controleren.

Met deze opdracht wordt het opgegeven MAC-adres gedurende 30 minuten (1800 seconden) bewaakt. U kunt deze tijd optioneel tot 2085978494 seconden verlengen.

Van CLI:

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

Opmerking: als u meer dan één client tegelijk wilt bewaken, voert u de opdracht debug wireless mac <aaaa.bbbb.ccc> per mac-adres uit.

Opmerking: U ziet de output van de client activiteit niet op de terminal sessie, omdat alles intern wordt gebufferd om later bekeken te worden.

Stap 7. Reproduceer het probleem of gedrag dat u wilt controleren.

Stap 8. Stop de debugs als het probleem wordt gereproduceerd voordat de standaard of de ingestelde monitortijd is ingesteld.

Van CLI:

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

Zodra de monitor-tijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam:

```
ra_trace_MAC_aabbcccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 9. Verzamel het bestand van de mac-adresactiviteit. U kunt het spoor .log naar een externe server kopiëren of de uitvoer direct op het scherm weergeven.

Controleer de naam van het RA traces bestand

Van CLI:

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

Kopieert het bestand naar een externe server:

Van CLI:

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

Geef de inhoud weer:

Van CLI:

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

Stap 10. Als de worteloorzaak nog niet duidelijk is, verzamel de interne logboeken die een meer breedspakige mening van debug niveau-logboeken zijn. U hoeft de client niet opnieuw te debuggen omdat u een gedetailleerde kijk hebt genomen op debug-logbestanden die al zijn verzameld en intern zijn opgeslagen.

Van CLI:

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

Opmerking: deze opdrachtoutput geeft sporen voor alle registratieniveaus voor alle processen en is vrij omvangrijk. Neem contact op met Cisco TAC om te helpen bij het doorlopen van deze sporen.

U kunt de Ra-internal-FILENAME.txt kopiëren naar een externe server of de uitvoer rechtstreeks op het

scherm weergeven.

Kopieert het bestand naar een externe server:

Van CLI:

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

Geef de inhoud weer:

Van CLI:

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

Stap 11. Verwijder de debug-voorwaarden.

Van CLI:

```
# clear platform condition all
```

Opmerking: Zorg ervoor dat u altijd de debug-voorwaarden verwijdert na een probleemoplossing sessie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.