

Configurazione di FlexConnect con autenticazione su Catalyst 9800 WLC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

Introduzione

In questo documento viene descritto come configurare FlexConnect con l'autenticazione centrale o locale sul controller LAN wireless Catalyst 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst Wireless 9800 modello di configurazione
- FlexConnect
- 802.1x

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C9800-CL, Cisco IOS-XE® 17.3.4

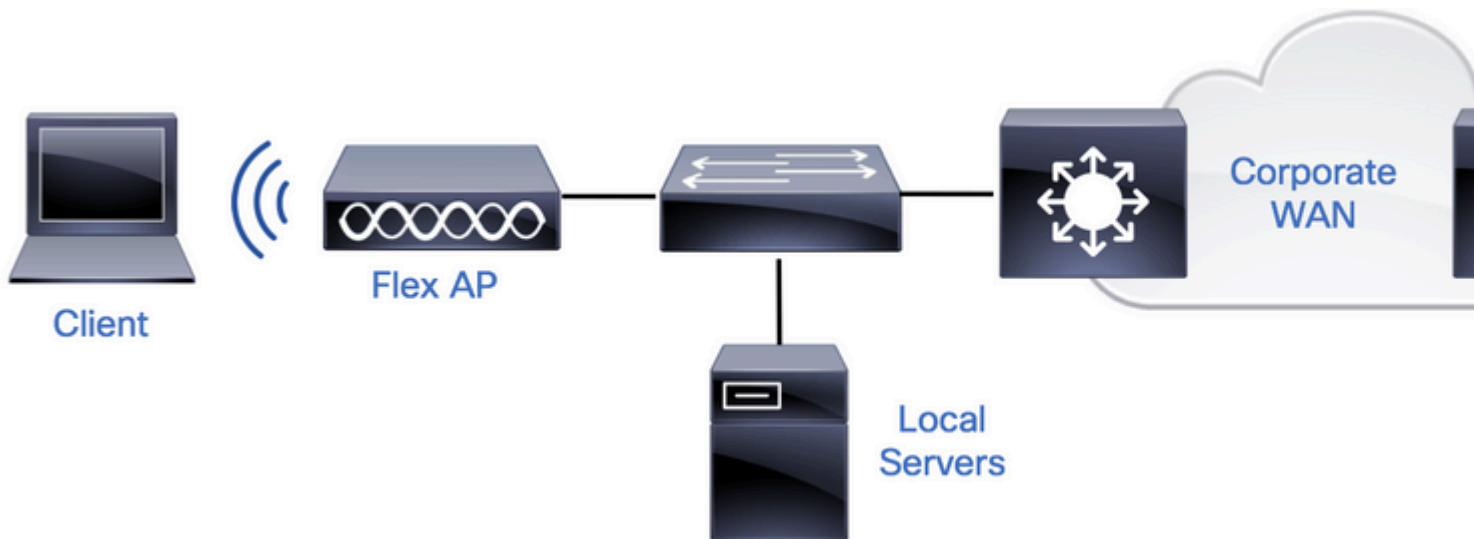
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

FlexConnect è una soluzione wireless per l'installazione negli uffici remoti. Consente di configurare i punti di accesso (AP) in postazioni remote dalla sede aziendale tramite un collegamento WAN (Wide Area Network) senza la necessità di installare un controller in ciascuna postazione. I punti di accesso FlexConnect possono commutare il traffico di dati client localmente ed eseguire l'autenticazione client localmente quando la connessione al controller viene persa. In modalità connessa, i punti di accesso FlexConnect possono anche eseguire l'autenticazione locale.

Configurazione

Esempio di rete



Configurazioni


Configurazione AAA su 9800 WLC


Passaggio 1. Dichiarare il server RADIUS. **Dalla GUI:** selezionare Configurazione > Sicurezza > AAA > Server / Gruppi > RADIUS > Server > + Aggiungi e immettere le informazioni sul server RADIUS.

The screenshot shows the Cisco GUI for AAA configuration. The breadcrumb trail is Configuration > Security > AAA. The 'Servers / Groups' tab is selected. The 'RADIUS' sub-tab is active, and the 'Servers' sub-tab is also selected. A table with columns 'Name', 'Address', and 'Auth Port' is visible at the bottom.

Verificare che il supporto per CoA sia abilitato se si prevede di utilizzare qualsiasi tipo di sicurezza che richieda CoA in futuro.

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

Nota: il CoA Radius non è supportato nella distribuzione dell'autenticazione locale di Flex Connect. .

Passaggio 2. Aggiungere il server RADIUS a un gruppo RADIUS. **Dalla GUI:** selezionare Configurazione > Sicurezza > AAA > Server / Gruppi > RADIUS > Gruppi di server > + Aggiungi.

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

Passaggio 3. Creare un elenco di metodi di autenticazione. **Dalla GUI:** selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > + Aggiungi

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

Dalla 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

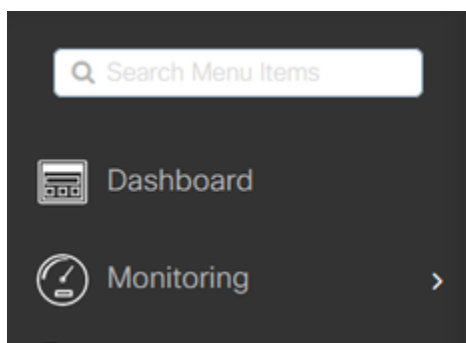
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

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

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

Configurazione della WLAN

Passaggio 1. **Dalla GUI:** selezionare Configurazione > Wireless > WLAN e fare clic su +Aggiungi per creare una nuova WLAN, quindi immettere le informazioni sulla WLAN. Quindi fare clic su Applica al dispositivo.



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

Passaggio 2. **Dalla GUI:** passare alla scheda Sicurezza per configurare la modalità di sicurezza Layer 2/Layer 3 finché il metodo di crittografia e l'elenco di autenticazione sono in uso. Quindi fare clic su Aggiorna e applica al dispositivo.

⚠ 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

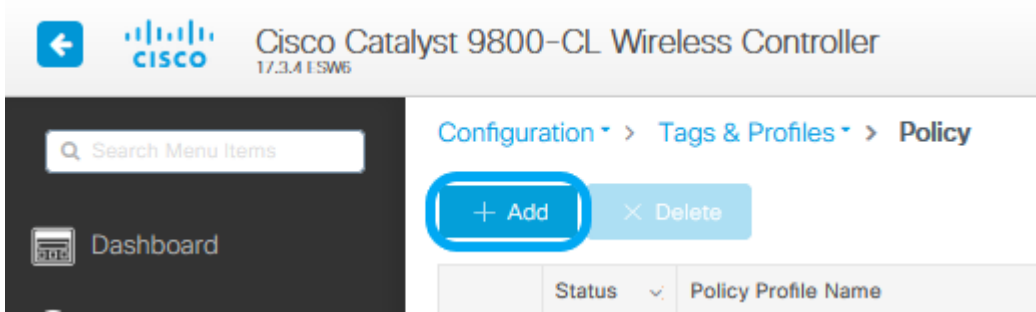
...

Cancel

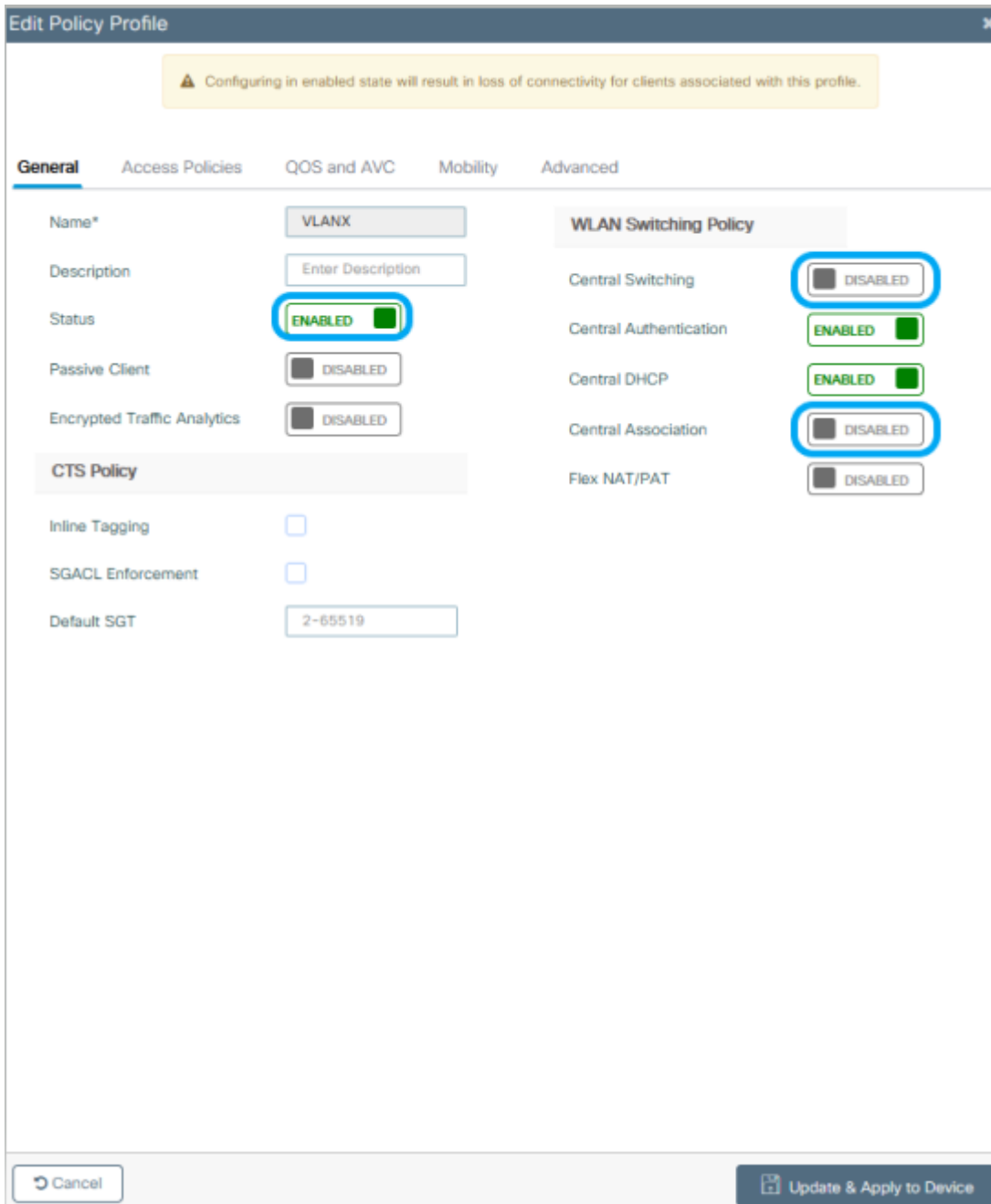
Update & Apply to Device

Configurazione del profilo di policy

Passaggio 1. **Dalla GUI:** selezionare Configurazione > Tag e profili > Criterio e fare clic su +Aggiungi per creare un profilo criterio.



Passaggio 2. Aggiungere il nome e deselezionare la casella Commutazione centrale. Con questa configurazione, il controller gestisce l'autenticazione client e il punto di accesso FlexConnect passa i pacchetti di dati client localmente.



Nota: l'associazione e la commutazione devono essere sempre associate. Se la commutazione centrale è disabilitata, anche l'associazione centrale deve essere disabilitata in tutti i profili di criteri quando si utilizzano gli access point Flexconnect.

Passaggio 3. **Dalla GUI:** passare alla scheda Criteri di accesso per assegnare la VLAN alla quale possono essere assegnati i client

wireless quando si connettono a questa WLAN per impostazione predefinita.

È possibile selezionare un nome di VLAN dall'elenco a discesa o, come procedura consigliata, digitare manualmente un ID VLAN.

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

Passaggio 4. **Dalla GUI:** passare alla scheda Advanced per configurare i timeout WLAN, il DHCP, il WLAN Flex Policy e il criterio AAA, nel caso siano in uso. Quindi fare clic su Aggiorna e applica al dispositivo.

✕
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

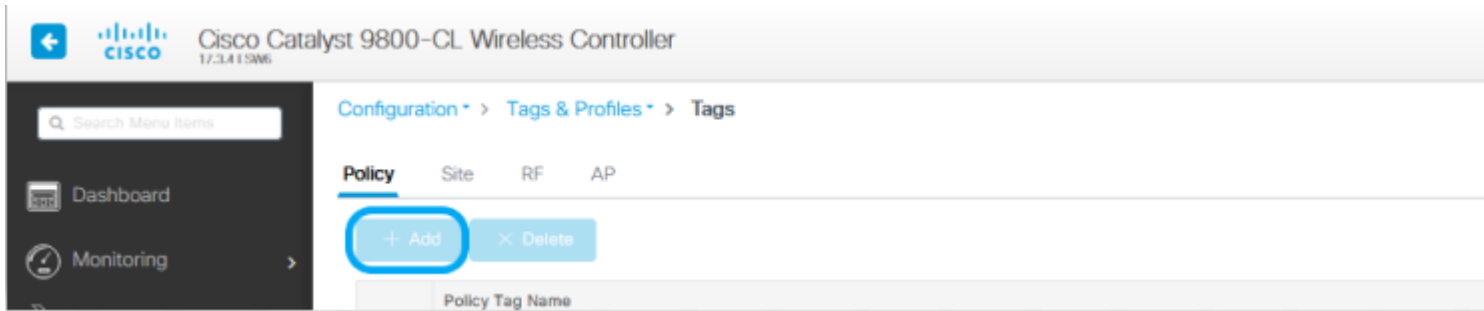
EoGRE Tunnel Profiles

↶ Cancel

↶ Update & Apply to Device

Configurazione del tag di policy

Passaggio 1. **Dalla GUI:** selezionare Configurazione > Tag e profili > Tag > Criterio > +Aggiungi.



Passaggio 2. Assegnare un nome ed eseguire il mapping del Profilo criteri e del Profilo WLAN creati in precedenza.

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

Configurazione profilo Flex

Passaggio 1. **Dalla GUI:** selezionare Configurazione > Tag e profili > Flex e fare clic su +Add per crearne uno nuovo.

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 ▼

Nota: l'ID VLAN nativo si riferisce alla VLAN utilizzata dagli access point che possono assegnare questo profilo Flex e deve essere lo stesso ID VLAN configurato come nativo sulla porta dello switch a cui sono connessi gli access point.

Passaggio 2. Nella scheda VLAN, aggiungere le VLAN necessarie, quelle assegnate per impostazione predefinita alla WLAN tramite un profilo criteri o quelle sottoposte a push da un server RADIUS. Quindi fare clic su Aggiorna e applica al dispositivo.

Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

Umbrella

+ Add

× Delete

VLAN Name	ID	ACL Name
No items to display		

VLAN Name*

VLAN76

VLAN Id*

76

ACL Name

Select ACL

✓ Save

↻ Cancel

↻ Cancel

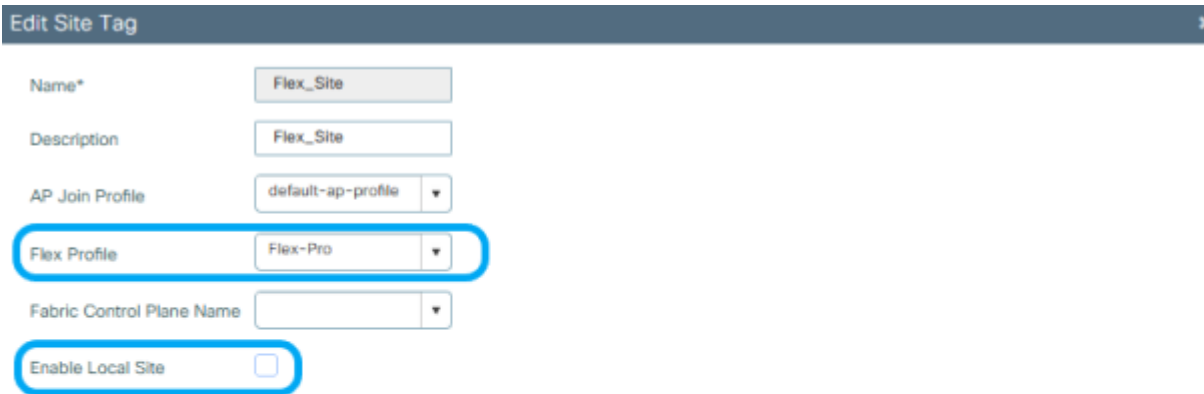
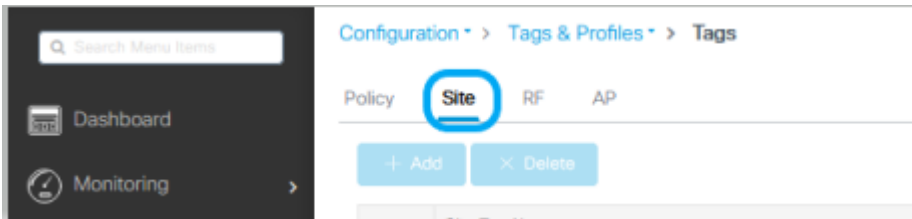
⏪ Upd

Nota: per Policy Profile, quando si seleziona la VLAN predefinita assegnata all'SSID. se si usa un nome VLAN in questo passaggio, verificare di usare lo stesso nome VLAN nella configurazione del profilo Flex, altrimenti i client non saranno in grado di connettersi alla WLAN.

Nota: per configurare un ACL per FlexConnect con override, occorre configurarlo solo su "ACL di criterio". Se l'ACL è assegnato a una VLAN specifica, aggiungere l'ACL su quando si aggiunge la VLAN, quindi aggiungere l'ACL su "ACL di criterio".

Configurazione tag sito

Passaggio 1. **Dalla GUI:** selezionare Configurazione > Tag e profili > Tag > Sito e fare clic su +Aggiungi per creare un nuovo tag Sito. Deselezionare la casella Abilita sito locale per consentire ai punti di accesso di commutare il traffico di dati client localmente e aggiungere il profilo Flex creato in precedenza.

The 'Edit Site Tag' form contains the following fields:

- 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)

Nota: se l'opzione Abilita sito locale è disabilitata, è possibile configurare i punti di accesso a cui viene assegnato questo tag del sito in modalità FlexConnect.

Passaggio 2. **Dalla GUI:** selezionare Configurazione > Wireless > Access Point > Nome access point per aggiungere il tag del sito e il tag dei criteri a un access point associato. In questo caso, l'access point può riavviare il tunnel CAPWAP e tornare al WLC 9800.

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

Una volta che l'access point si è unito nuovamente, l'access point è ora in modalità FlexConnect.

▼ 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

Autenticazione locale con server RADIUS esterno

Passaggio 1. Aggiungere il punto di accesso come dispositivo di rete al server RADIUS. Per un esempio, vedere [Come utilizzare Identity Service Engine \(ISE\) come server RADIUS](#)

Passaggio 2. Creare una WLAN.

La configurazione può essere uguale a quella configurata in precedenza.

Add WLAN ✕

General Security Advanced

Profile Name*

SSID*

WLAN ID*

Status ENABLED

Radio Policy

Broadcast SSID ENABLED

↶ Cancel

▶ Apply to Device

Passaggio 3. Configurazione del profilo di policy.

È possibile crearne uno nuovo o utilizzare quello configurato in precedenza. In questo caso, deselezionare le caselle Switching centrale, Autenticazione centrale, DHCP centrale e Abilitazione associazione centrale.

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

Passaggio 4. Configurazione del tag di policy.

Associare la WLAN configurata e il profilo criteri creato.

Passaggio 5. Configurazione profilo Flex.

Creare un profilo Flex, passare alla scheda Autenticazione locale, configurare il gruppo di server Radius e selezionare la casella 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

Select CSV File



Upload

Username

0 10 items per page

No items to display

Cancel

Update

Passaggio 6. Configurazione tag sito.

Configurare il profilo Flex configurato nel passaggio 5 e deselezionare la casella Abilita sito locale.

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 D

Verifica

Dalla GUI: passare a **Monitoraggio > Wireless > Client** e confermare lo **stato di Policy Manager** e i parametri di FlexConnect.

Autenticazione centrale:

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

Autenticazione locale:

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		

Usare questi comandi per verificare la configurazione corrente:

Dalla 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>
```

Risoluzione dei problemi

WLC 9800 offre funzionalità di traccia ALWAYS-ON. In questo modo, tutti gli errori, gli avvisi e i messaggi relativi alla connettività del client vengono costantemente registrati ed è possibile visualizzare i registri di un evento imprevisto o di una condizione di errore dopo che si è verificato.

Nota: in base al volume dei log generati, è possibile tornare indietro di alcune ore a diversi giorni.

Per visualizzare le tracce raccolte per impostazione predefinita dal 9800 WLC, è possibile connettersi al 9800 WLC tramite SSH/Telnet e seguire la procedura descritta (accertarsi di registrare la sessione su un file di testo).

Passaggio 1. Controllare l'ora corrente del controller in modo da poter tenere traccia dei log nel tempo che intercorre tra il momento in cui si è verificato il problema.

Dalla CLI:

```
# show clock
```

Passaggio 2. Raccogliere syslog dal buffer del controller o dal syslog esterno in base alla configurazione del sistema. In questo modo è possibile visualizzare rapidamente lo stato del sistema e gli eventuali errori.

Dalla CLI:

```
# show logging
```

Passaggio 3. Verificare se sono abilitate le condizioni di debug.

Dalla CLI:

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

Ip Address	Port
-----	-----

Nota: se si trova una delle condizioni elencate, le tracce vengono registrate a livello di debug per tutti i processi che soddisfano le condizioni abilitate (indirizzo MAC, indirizzo IP e così via). Ciò aumenta le dimensioni dei log. Pertanto, si consiglia di cancellare tutte le condizioni quando non si effettua attivamente il debug.

Passaggio 4. Se si presume che l'indirizzo MAC in fase di test non sia stato elencato come condizione nel passaggio 3, raccogliere le tracce del livello di avviso sempre attive per l'indirizzo MAC specifico.

Dalla CLI:

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

È possibile visualizzare il contenuto della sessione oppure copiare il file su un server TFTP esterno.

Dalla CLI:

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

Debug condizionale e traccia attiva radio

Se le tracce sempre attive non forniscono informazioni sufficienti per determinare il trigger del problema in esame, è possibile abilitare il debug condizionale e acquisire la traccia Radio attiva (RA), che può fornire le tracce dei livelli di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client). Per abilitare il debug condizionale, eseguire la procedura seguente.

Passaggio 5. Accertarsi che non vi siano condizioni di debug abilitate.

Dalla CLI:

```
# clear platform condition all
```

Passaggio 6. Abilitare la condizione di debug per l'indirizzo MAC del client wireless che si desidera monitorare.

Questo comando avvia il monitoraggio dell'indirizzo MAC fornito per 30 minuti (1800 secondi). È possibile aumentare questo tempo fino a 2085978494 secondi.

Dalla CLI:

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

Nota: per monitorare più client alla volta, eseguire il comando `debug wireless mac <aaa.bbbb.ccc>` per ogni indirizzo MAC.

Nota: non si visualizza l'output dell'attività del client nella sessione terminale, in quanto tutto viene memorizzato internamente per essere visualizzato successivamente.

Passaggio 7. Riprodurre il problema o il comportamento che si desidera monitorare.

Passaggio 8. Interrompere i debug se il problema viene riprodotto prima che il tempo di monitoraggio predefinito o configurato sia attivo.

Dalla CLI:

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

Una volta trascorso il tempo di monitoraggio o interrotto il debug wireless, il controller 9800 WLC genera un file locale con il nome:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 9. Recuperare il file dell'attività dell'indirizzo MAC. È possibile copiare la traccia RA .log su un server esterno o visualizzare l'output direttamente sullo schermo.

Controllare il nome del file delle tracce RA

Dalla CLI:

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

Copiare il file su un server esterno:

Dalla CLI:

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

Visualizzare il contenuto:

Dalla CLI:

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

Passaggio 10. Se la causa principale non è ancora ovvia, raccogliere i log interni che offrono una visualizzazione più dettagliata dei log del livello di debug. non è necessario eseguire di nuovo il debug del client perché sono stati esaminati in dettaglio i log di debug già raccolti e archiviati internamente.

Dalla CLI:

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

Nota: questo output del comando restituisce tracce per tutti i livelli di registrazione per tutti i processi ed è piuttosto voluminoso. Contattare Cisco TAC per analizzare queste tracce.

È possibile copiare il file ra-internal-FILENAME.txt su un server esterno o visualizzare l'output direttamente sullo schermo.

Copiare il file su un server esterno:

Dalla CLI:

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

Visualizzare il contenuto:

Dalla CLI:

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

Passaggio 11. Rimuovere le condizioni di debug.

Dalla CLI:

```
# clear platform condition all
```

Nota: assicurarsi di rimuovere sempre le condizioni di debug dopo una sessione di risoluzione dei problemi.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).