

# Override di FlexConnect WLAN con 802.1x AAA sui controller wireless Catalyst 9800

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione AAA sui controller 9800 WLC](#)

[Configurazione della WLAN](#)

[Imposta AP come modalità FlexConnect](#)

[Configurazione degli switch](#)

[Configurazione del profilo di policy](#)

[Configurazione del tag di policy](#)

[Assegnazione tag criteri](#)

[Configurazione di ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto come configurare un controller LAN wireless elastico (9800 WLC) con punti di accesso in modalità FlexConnect e una rete WLAN (Wireless Local Area Network) 802.1x a commutazione locale con override dell'autenticazione, dell'autorizzazione e dell'accounting (VLAN).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- modalità di configurazione 9800 WLC
- FlexConnect

### Componenti usati

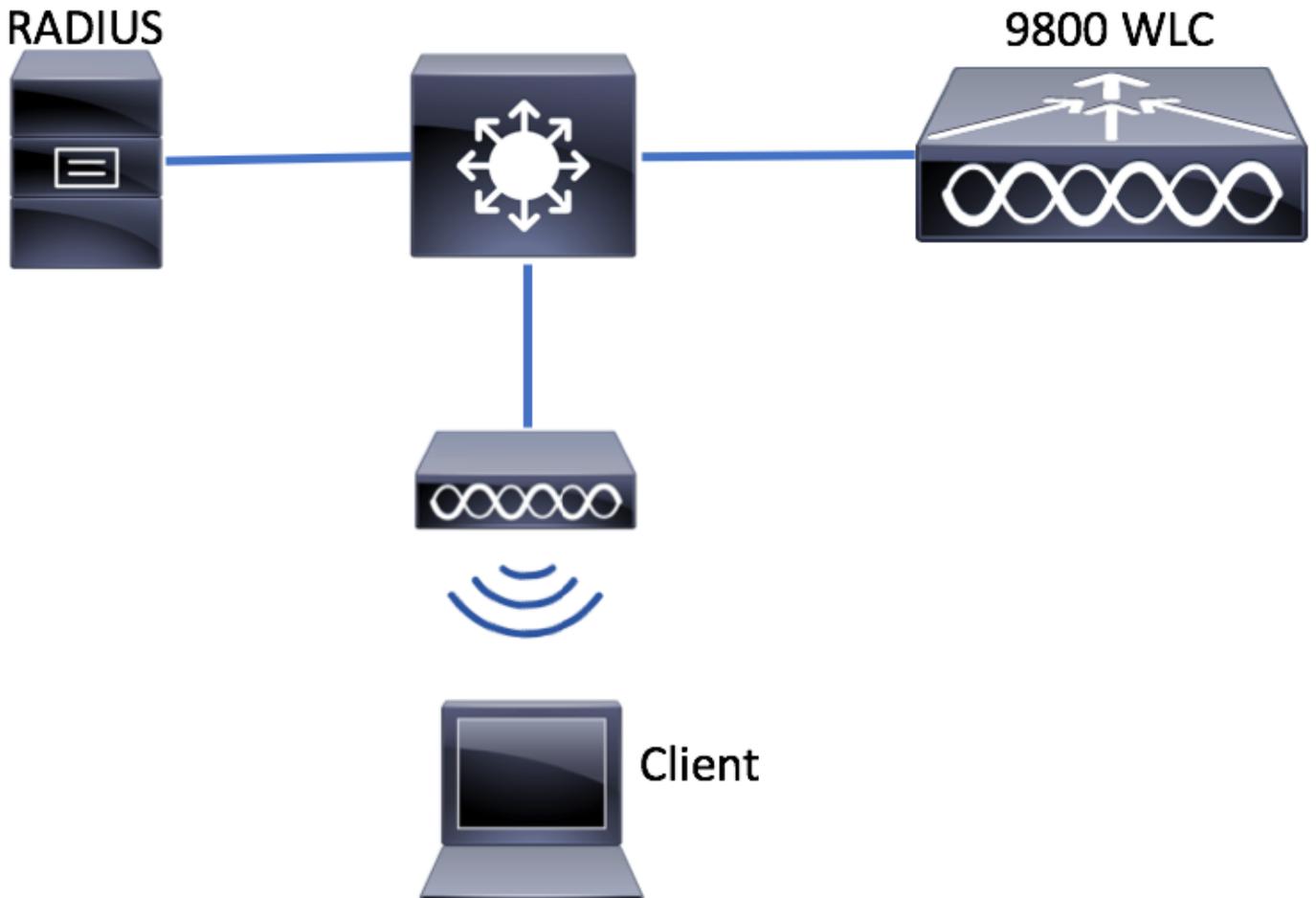
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 9800 WLC v16.10

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.

## Configurazione

### Esempio di rete



### Configurazione

#### Configurazione AAA sui controller 9800 WLC

È possibile seguire le istruzioni di questo collegamento:

[Configurazione AAA sui controller 9800 WLC](#)

#### Configurazione della WLAN

È possibile seguire le istruzioni di questo collegamento:

[Configurazione della WLAN](#)

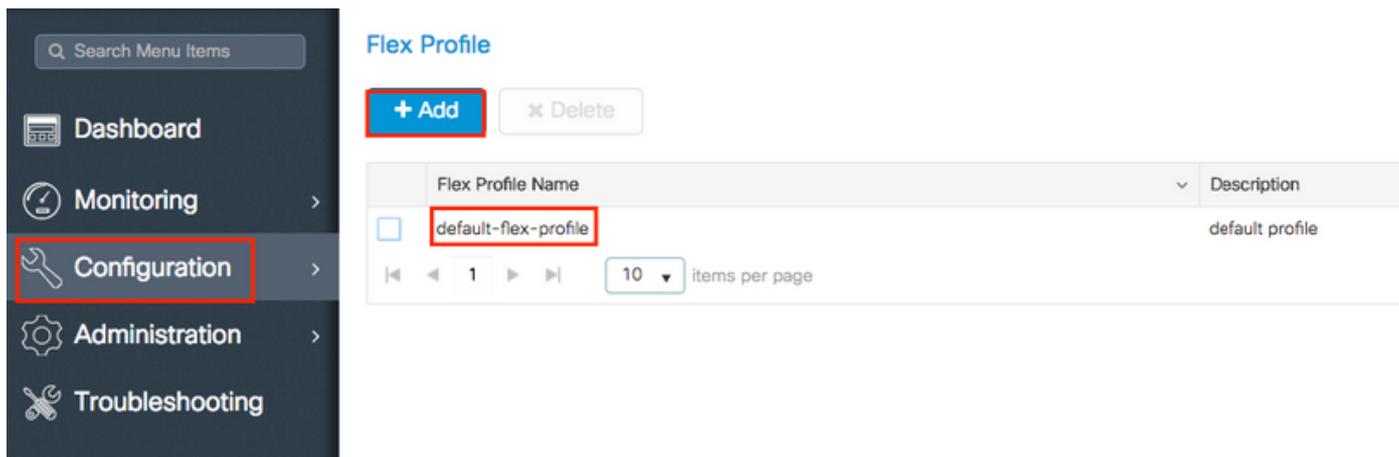
## Imposta AP come modalità FlexConnect

A differenza della configurazione AireOS, sullo switch 9800 WLC non è possibile configurare l'access point in modalità locale o flexconnect direttamente dall'access point. Per configurare un access point in modalità FlexConnect, attenersi alla seguente procedura.

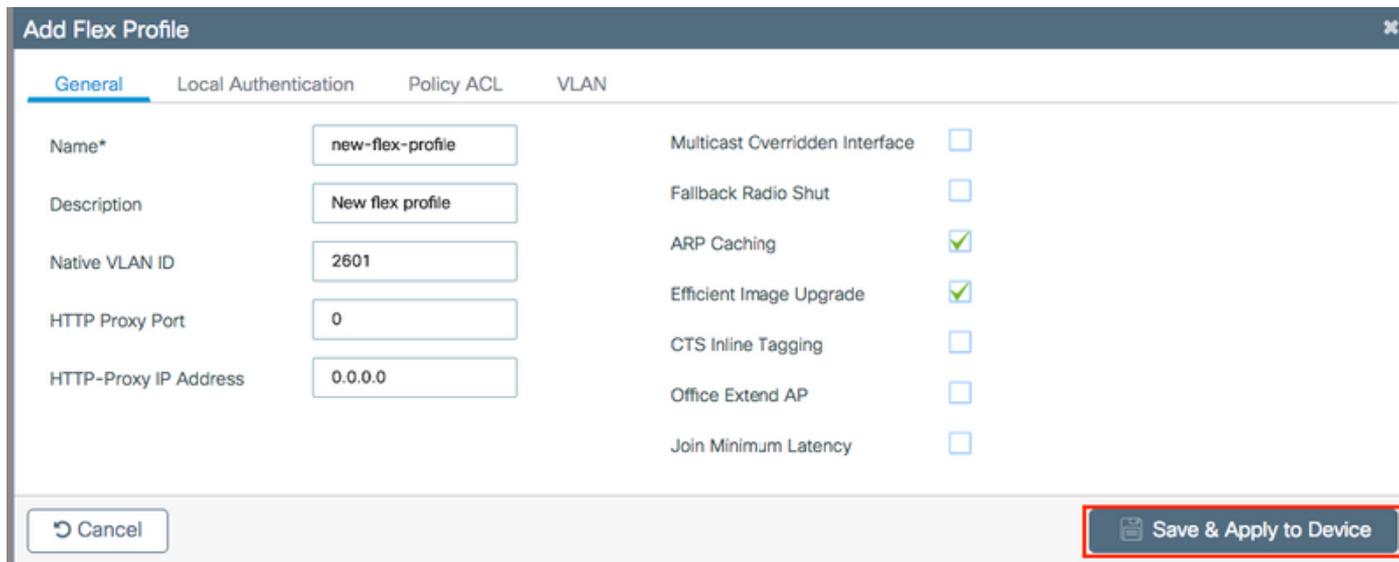
GUI

Passaggio 1. Configurare un profilo Flex.

Passa a **Configurazione > Tag e profili > Flex** e modificare il profilo **default-flex-profile** o fare clic su **+Aggiungi** per crearne uno nuovo.



The screenshot shows the 'Flex Profile' configuration page. On the left, a dark sidebar contains a search bar and navigation items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area is titled 'Flex Profile' and features a '+ Add' button (highlighted in red) and a 'Delete' button. Below these is a table with two columns: 'Flex Profile Name' and 'Description'. The table contains one entry: 'default-flex-profile' with the description 'default profile'. The 'default-flex-profile' text in the table is highlighted with a red box. At the bottom of the table, there are navigation icons and a dropdown menu set to '10 items per page'.



The screenshot shows the 'Add Flex Profile' configuration form. The 'General' tab is selected, and the form is divided into two columns. The left column contains input fields for 'Name\*' (new-flex-profile), 'Description' (New flex profile), 'Native VLAN ID' (2601), 'HTTP Proxy Port' (0), and 'HTTP-Proxy IP Address' (0.0.0.0). The right column contains checkboxes for 'Multicast Overridden Interface', 'Fallback Radio Shut', 'ARP Caching' (checked), 'Efficient Image Upgrade' (checked), 'CTS Inline Tagging', 'Office Extend AP', and 'Join Minimum Latency'. At the bottom of the form, there is a 'Cancel' button on the left and a 'Save & Apply to Device' button (highlighted in red) on the right.

Passaggio 2. Aggiungere le VLAN necessarie (sia le VLAN predefinite della WLAN che le VLAN estese da ISE).

**Nota:** al passaggio 3 della sezione **Configurazione del profilo delle policy**, è possibile selezionare 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.

## Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

+ Add

✕ Delete

VLAN Name	ID	ACL Name
-----------	----	----------

◀ ◁ 0 ▷ ▶ 10 items per page

No items to display

Facoltativamente, è possibile aggiungere ACL specifici per ciascuna VLAN.

VLAN Name\*

vlan2602

VLAN Id\*

2602

ACL Name

Select ACL

✓ Save

↺ Cancel

Facoltativamente, assegnare un gruppo di server Radius per consentire ai punti di accesso FlexConnect di eseguire l'autenticazione locale.

## Edit Flex Profile

General **Local Authentication** Policy ACL VLAN

Radius Server Group **ISE-kcg-grp** LEAP

EAP Fast Profile Select Profile PEAP

TLS

**RADIUS**

Users

**+ Add**

Username

10 items per page

No items to display

Passaggio 3. Configurare un tag del sito.

Passare a **Configurazione > Tag e profili > Tag > Sito**. Modificare il tag **predefinito del sito** (ovvero il tag assegnato per impostazione predefinita a tutti gli access point) o crearne uno nuovo (fare clic su **+Aggiungi** per crearne uno nuovo).

Search Menu Items

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

### Manage Tags

Policy **Site** RF AP

**+ Add**

Site Tag Name
<input type="checkbox"/> <b>default-site-tag</b>

10 items per page

Assicuratevi di disabilitare l'opzione **Abilita sito locale** altrimenti l'opzione **Flex Profile** non sarà disponibile.

**Add Site Tag**

Name\*

Description

AP Join Profile

Flex Profile

Enable Local Site

**Nota:** Qualsiasi access point che ottiene un tag del sito con l'opzione **Abilita sito locale** abilitata, è configurato come modalità locale. Analogamente, qualsiasi access point che ottiene un tag del sito con l'opzione **Abilita sito locale** disabilitata, viene configurato come modalità flexconnect.

Passaggio 4. Associare un access point al WLC 9800 e assegnare il tag Site configurato nel passaggio 2.

Passare a **Configurazione > Wireless > Access Point > Nome punto di accesso** e impostare il tag del sito. Quindi fare clic su **Aggiorna e applica al dispositivo** per impostare la modifica.

**Access Points**

Number of AP(s): 1

AP Name	AP Model	Base Radio MAC	AP Mode	Adm. Stat.
AP1702-05	AIR-CAP1702I-A-K9	00:c0:00:00:00:00	Local	En

**Edit AP**

General | Interfaces | High Availability | Inventory | Advanced

**General**

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status

AP Mode

Operation Status

Fabric Status

**Tags**

Policy

Site

RF

**Version**

Primary Software Version 16.8.1.5

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 15.3.0.0

IOS Version 15.0(201000001.205348)S

Mini IOS Version 0.0.0.0

**IP Config**

IP Address 172.16.0.200

Static IP

**Time Statistics**

Up Time 0 days 19 hrs 8 mins 11 secs

Controller Associated Time 0 days 18 hrs 57 mins 16 secs

Controller Association Latency 0 days 0 hrs 10 mins 44 secs

**Nota:** dopo aver modificato il tag su un access point, quest'ultimo perde l'associazione al WLC 9800 e si ricongiunge entro circa 1 minuto.

## Passaggio 5. Una volta che l'access point si è unito, la modalità dell'access point è Flex

The screenshot displays the network management interface. On the left is a dark sidebar with navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is titled 'Access Points' and shows a table with one AP listed: AP1702-05, model AIR-CAP1702I-A-K9, Base Radio MAC 00:c8:8b:26:2c:d0, and AP Mode Flex (highlighted with a red box). Below the table are expandable sections for 'Radios 802.11a/n/ac', 'Radios 802.11b/g/n', and 'Dual-Band Radios'. On the right, the 'Edit AP' panel is open, showing the 'General' tab. The 'AP Mode' dropdown menu is set to 'Flex' and is also highlighted with a red box. Other fields include AP Name (AP1702-05), Location (default location), Base Radio MAC (00:c8:8b:26:2c:d0), Ethernet MAC (00:f2:8b:89:c2:ac), Admin Status (Enabled), Operation Status (Registered), and Fabric Status (Disabled).

### CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                               : FlexConnect
```

### Configurazione degli switch

Configurare l'interfaccia dello switch a cui è connesso l'access point.

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

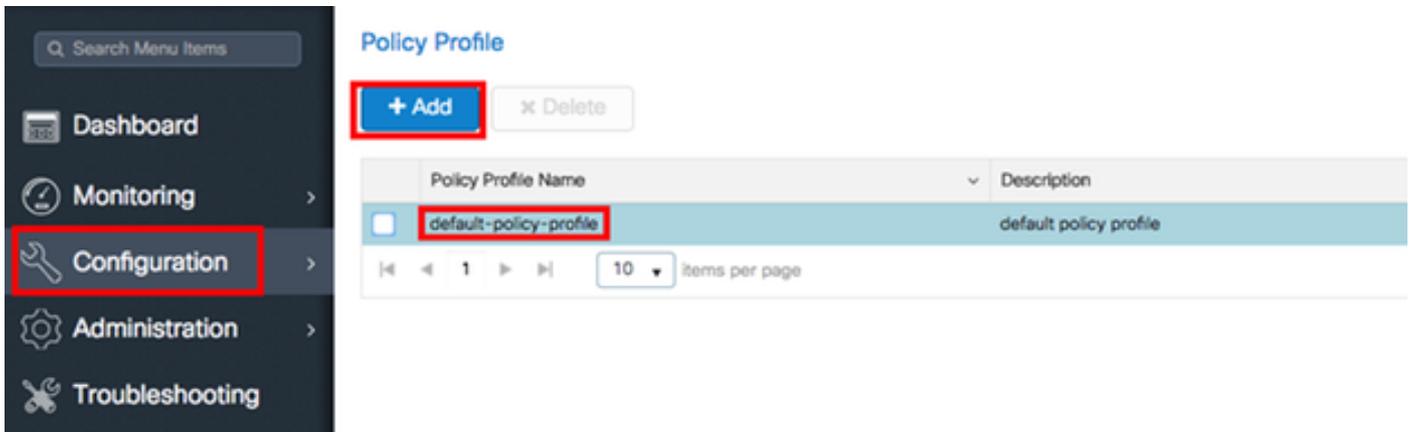
### Configurazione del profilo di policy

All'interno di un profilo di policy, è possibile decidere a quale VLAN assegnare i client, tra le altre impostazioni (come Access Controls List [ACLs], Quality of Service [QoS], Mobility Anchor, Timer e così via).

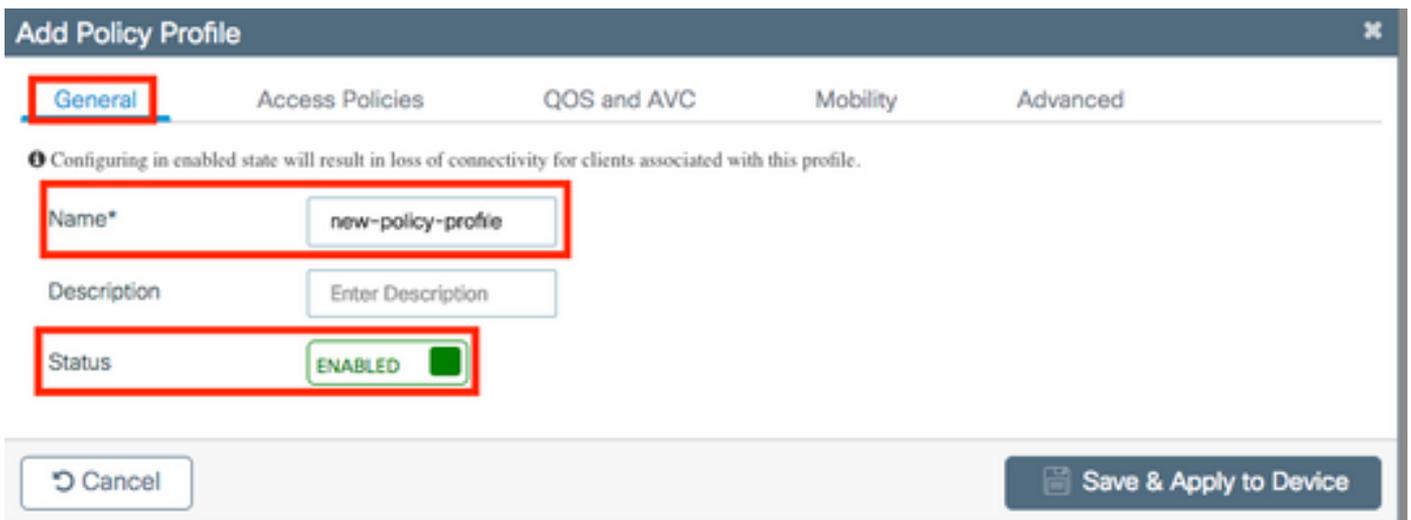
### GUI

Passaggio 1. Configurare il profilo dei criteri da assegnare alla WLAN.

Passare a **Configurazione > Tag e profili > Criterio** e crearne uno nuovo o modificare il **profilo predefinito-criterio**.



Passaggio 2. Dalla **scheda Generale**, assegnare un nome al Profilo criterio e modificarne lo stato in **ABILITATO**.



Passaggio 3. Dalla scheda **Access Policies** (Criteri di accesso), assegnare la VLAN a cui sono assegnati i client wireless quando si connettono alla WLAN per impostazione predefinita.

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

**Nota:** se si seleziona un nome di vlan dall'elenco a discesa, verificare che corrisponda al nome di vlan usato nel passaggio 2 della sezione **Impostare AP come modalità FlexConnect**.

### Add Policy Profile

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

**WLAN Local Profiling**

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**VLAN**

VLAN/VLAN Group

o

### Edit Policy Profile

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

**WLAN Local Profiling**

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

**VLAN**

VLAN/VLAN Group

Passaggio 4. Passare alla scheda **Advanced** e abilitare le opzioni **Central Authentication Enable** e **Allow AAA Override**. La **commutazione centrale** deve essere disabilitata.

Se si desidera che il processo di autenticazione venga eseguito a livello centrale dal WLC 9800, è necessario abilitare l'**autenticazione centrale**. Disattivarla se si desidera che i punti di accesso FlexConnect autenticchino i client wireless.

# Edit Policy Profile



General

Access Policies

QOS and AVC

Mobility

**Advanced**

## WLAN Timeout

Session Timeout (sec)\*

Idle Timeout (sec)\*

Idle Threshold (bytes)\*

Client Exclusion Timeout (sec)\*

## DHCP

DHCP Enable

DHCP Server IP Address

DHCP Opt82 Enable

DHCP Opt82 Ascii

DHCP Opt82 RID

DHCP Opt82 Format

DHCP AP MAC

DHCP SSID

DHCP AP ETH MAC

DHCP AP NAME

DHCP Policy Tag

DHCP AP Location

DHCP VLAN ID

## AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile

## WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

## WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Cancel

Update & Apply to Device

## CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
```

# no shutdown

## Configurazione del tag di policy

Il tag dei criteri viene utilizzato per collegare l'SSID al profilo dei criteri. È possibile creare un nuovo tag o utilizzare il tag predefinito.

**Nota:** il tag default-policy-tag mappa automaticamente qualsiasi SSID con ID WLAN compreso tra 1 e 16 al profilo default-policy-profile. Non può essere modificata né eliminata. Se si dispone di una WLAN con ID 17 o superiore, non è possibile utilizzare il tag default-policy.

GUI:

Passare a **Configurazione > Tag e profili > Tag > Criteri** e aggiungerne uno nuovo, se necessario.

The screenshot shows the 'Manage Tags' interface. On the left is a navigation sidebar with options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is titled 'Manage Tags' and has tabs for 'Policy', 'Site', 'RF', and 'AP'. The 'Policy' tab is selected. Below the tabs are '+ Add' and 'x Delete' buttons. A table lists policy tags with columns 'Policy Tag Name' and 'Description'. The table contains two entries: 'central-anchor' and 'default-policy-tag' (highlighted in blue). Below the table is a pagination control showing '1' items per page.

Associare il profilo WLAN al profilo di policy desiderato.

The screenshot shows the 'Add Policy Tag' dialog box. It has a title bar with a close button. The form contains a 'Name\*' field with the value 'PolicyTagName' and a 'Description' field with the placeholder 'Enter Description'. Below the form are '+ Add' and 'x Delete' buttons. At the bottom, there are two dropdown menus: 'WLAN Profile' and 'Policy Profile'. Below these is a pagination control showing '0' items per page and the text 'No items to display'. At the very bottom are 'Cancel' and 'Save & Apply to Device' buttons.

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<span>◀◀ 0 ▶▶</span> <input style="width: 50px;" type="text" value="10"/> items per page <span style="float: right;">No items to display</span>	

Map WLAN and Policy

WLAN Profile\* 
Policy Profile\*

✕
✓

↶ Cancel
Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
<span>◀◀ 1 ▶▶</span> <input style="width: 50px;" type="text" value="10"/> items per page <span style="float: right;">1 - 1 of 1 items</span>	

↶ Cancel
Save & Apply to Device

CLI:

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

### Assegnazione tag criteri

Assegnare il tag Policy all'access point

## GUI

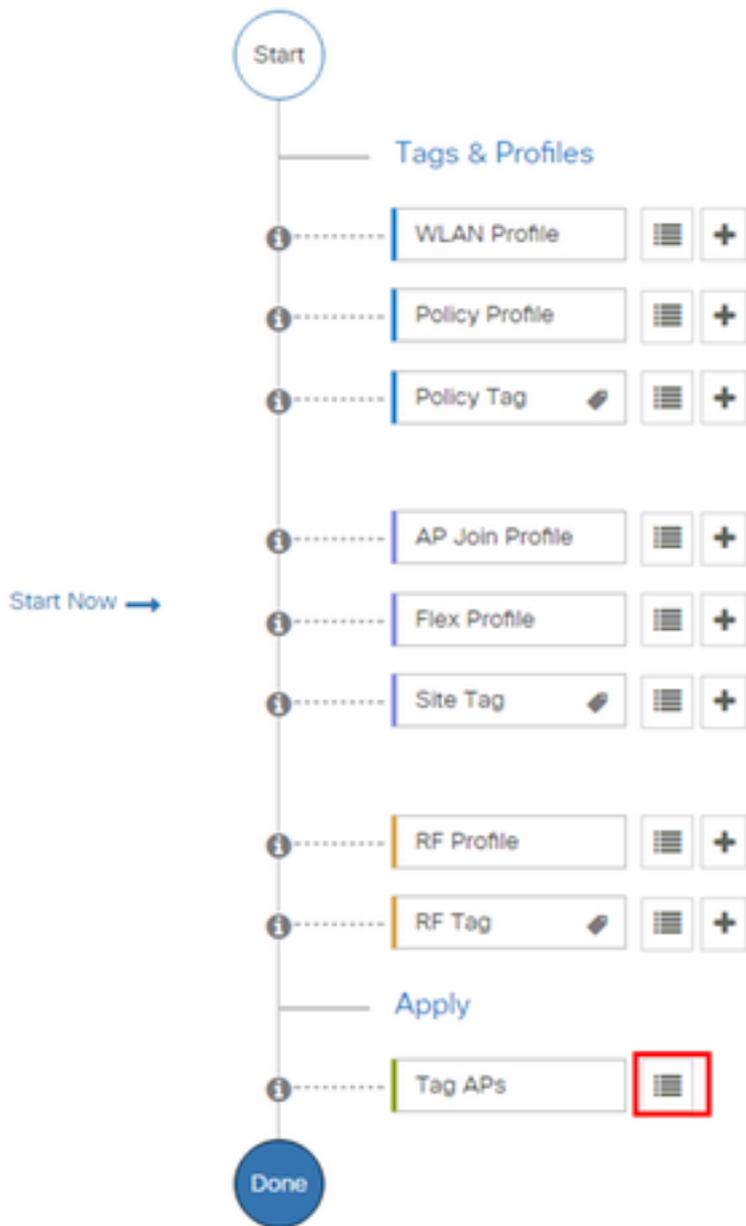
Per assegnare il tag a un punto di accesso, selezionare **Configurazione > Wireless > Access Point > Nome punto di accesso > Tag generali**, effettuare l'assegnazione necessaria e fare clic su **Aggiorna e applica al dispositivo**.

The screenshot shows the 'Edit AP' configuration window with the following details:

Section	Field	Value
General	AP Name*	AP1702-05
	Location*	default location
	Base Radio MAC	00:c1:00:00:00:00
	Ethernet MAC	00:c1:00:00:00:00
	Admin Status	Enabled
	AP Mode	Flex
	Operation Status	Registered
	Fabric Status	Disabled
Tags	Policy	new-policy-tag
	Site	new-flex-site
	RF	default-rf-tag
Version	Primary Software Version	16.0.0.0
	Predownloaded Status	N/A
	Predownloaded Version	N/A
	Next Retry Time	N/A
IP Config	IP Address	172.16.0.200
	Static IP	<input type="checkbox"/>
	Time Statistics	
Time Statistics	Up Time	1 days 1 hrs 44 mins 59 secs
	Controller Associated Time	0 days 5 hrs 32 mins 5 secs
	Controller Association Latency	0 days 20 hrs 11 mins 24 secs

**Nota:** tenere presente che dopo aver modificato il tag di criterio in un access point, l'associazione al WLC 9800 viene persa e l'utente torna indietro entro 1 minuto.

Per assegnare lo stesso tag di policy a più access point, selezionare **Configurazione > Wireless > Wireless Setup > Start Now > Apply (Configurazione wireless > Impostazione wireless > Avvia ora > Applica)**.



Selezionare gli access point ai quali si desidera assegnare il tag e fare clic su **+ Tag AP**

**+ Tag APs**

Number of APs: 3  
Selected Number of APs: 3

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag
<input checked="" type="checkbox"/>	AP3802-02-WS	AIR-AP3802I-A-K9	C0-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-01	AIR-AP3802I-B-K9	20-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-02	AIR-AP3802I-B-K9	40-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag

10 items per page      1 - 3 of 3 items

Selezionare il tag desiderato e fare clic su **Salva e applica al dispositivo**

**Tag APs** [X]

Tags

Policy: default-policy-tag [v]

Site: SiteTag1 [v]

RF: default-rf-tag [v]

[Cancel]      [Save & Apply to Device]

## CLI

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

## Configurazione di ISE

Per la configurazione di ISE v1.2, controllare questo collegamento:

[Configurazione di ISE](#)

## Verifica

È possibile utilizzare questi comandi per verificare la configurazione corrente

```
# 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 relativi alla connettività dei client, le avvertenze e i messaggi di avviso vengono costantemente registrati e, dopo che si è verificato un incidente o un errore, è possibile visualizzare i vari log.

**Nota:** A seconda del volume di log generati, è possibile tornare da alcune ore a diversi giorni.

Per visualizzare le tracce raccolte dal controller 9800 WLC per impostazione predefinita, è possibile collegarsi in modalità SSH/Telnet al controller 9800 WLC e seguire questa procedura (verificare di registrare la sessione in un file di testo).

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

```
# show clock
```

Passaggio 2. Recuperare i messaggi syslog dal buffer del controller o dal syslog esterno come richiesto dalla configurazione del sistema. In questo modo è possibile visualizzare rapidamente lo stato di integrità del sistema ed eventuali errori.

```
# show logging
```

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

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:

Packet Infra debugs:
```

```
Ip Address _____ | _____ Port
```

**Nota:** se le condizioni vengono visualizzate, le tracce sono registrate al livello di debug per tutti i processi che soddisfano le condizioni abilitate (indirizzo MAC, indirizzo IP, ecc.). Ciò aumenta le dimensioni dei log. Pertanto, si consiglia di cancellare tutte le condizioni quando non si effettua attivamente il debug.

Passaggio 4. Supponendo che l'indirizzo MAC da verificare non sia elencato come condizione nel Passaggio 3, raccogliere le tracce del livello di avviso always-on per l'indirizzo MAC specifico.

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

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

```
# 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 Radioactive (RA)

Se le tracce always-on non forniscono informazioni sufficienti per determinare la causa del problema, è possibile abilitare il debug condizionale e acquisire la traccia Radioactive (RA) che fornisce informazioni su tutti i processi interessati dalla condizione specifica (in questo caso, indirizzo MAC del client). Per abilitare il debug condizionale, attenersi alla seguente procedura.

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

```
# 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.

```
# 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 indirizzo MAC.

**Nota:** l'output dell'attività del client nella sessione terminale non viene visualizzato, in quanto tutto viene memorizzato internamente nel buffer 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 scaduto.

```
# 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. Raccogliere il file dell'attività dell'indirizzo MAC. È possibile copiare il file di tracce .log in un server esterno o visualizzare l'output direttamente sullo schermo.

Controllare il nome del file delle tracce RA

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

Copiare il file su un server esterno:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

Visualizzare il contenuto:

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

Passaggio 10. Se non è stato possibile individuare la causa principale del problema, raccogliere i log interni che contengono informazioni più dettagliate dei log di debug. Non è necessario eseguire di nuovo il debug del client, in quanto vengono esaminati in dettaglio solo i log di debug già raccolti e archiviati internamente.

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

**Nota:** questo output del comando restituisce tracce per tutti i livelli di registrazione di 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:

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

Visualizzare il contenuto:

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

Passaggio 11. Rimuovere le condizioni di debug.

```
# clear platform condition all
```

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