

# Configurazione dei punti di accesso alla rete per il bridging dei dati locali in modalità Flex e Bridge

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Aggiungi punto di accesso al database locale del controller](#)

[Elenco metodi AAA per autenticazione](#)

[Elenco metodi AAA per autorizzazione](#)

[Profilo mesh](#)

[Profilo di join AP](#)

[Profilo Flex](#)

[Profilo criterio](#)

[Tag WLAN](#)

[Tag criteri](#)

[Tag sito](#)

[Configurazione dei punti di accesso](#)

[Switch Port Configuration](#)

[Verifica](#)

---

## Introduzione

Questo documento descrive la configurazione delle MAPPE in modalità Flex e Bridge per il bridging dei dati dei client locali, ignorando il RAP.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst Wireless 9800 modello di configurazione
- Configurazione dei LAP
- Controllo e fornitura di punti di accesso wireless (CAPWAP)
- Configurazione degli switch Cisco

## Componenti usati

In questo esempio vengono utilizzati punti di accesso leggeri (modelli 9124AP), che possono essere configurati come punto di accesso principale (RAP) o punto di accesso Mesh (MAP) per l'integrazione con il controller Catalyst 9800 Wireless LAN Controller (WLC).

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

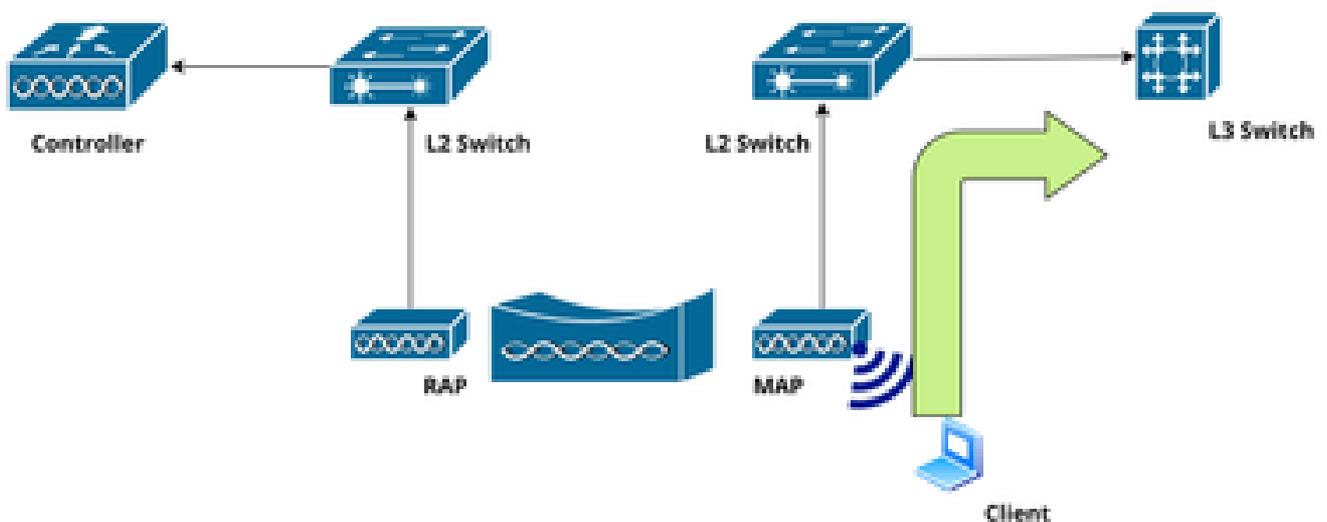
- C9800-L v17.12.5
- Cisco Catalyst 3850 Switch
- Access point Cisco Catalyst serie 9124AX

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

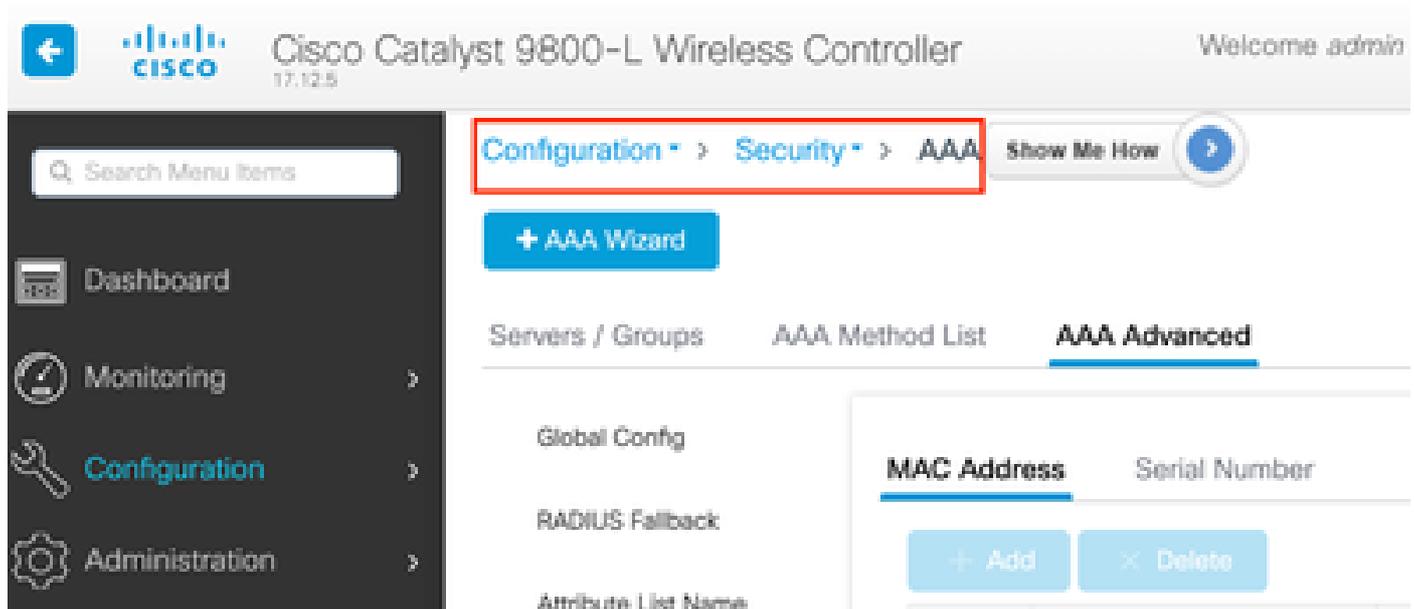
In questa sezione viene descritta la configurazione dei punti di accesso Mesh (MAP) che operano in modalità Mesh + Bridge, consentendo il bridging diretto dei dati client locali allo switch uplink e ignorando il punto di accesso radice (RAP).

## Esempio di rete

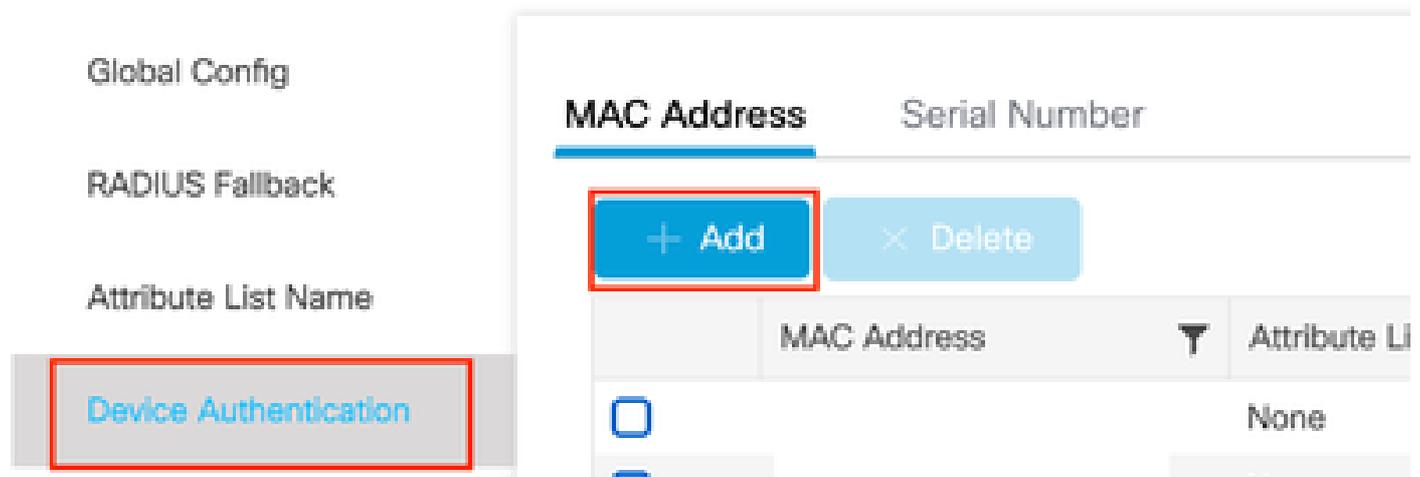


## Aggiungi punto di accesso al database locale del controller

Passaggio 1: Passare a Configurazione > Sicurezza > AAA > AAA Avanzate.



Passaggio 2. Selezionare Device Authentication (Autenticazione dispositivo) e selezionare Add (Aggiungi).



Passaggio 3. Digitare l'indirizzo MAC Ethernet di base dell'access point per collegarsi al WLC. Lasciare vuoto il campo Nome elenco attributi e selezionare Applica a dispositivo.

MAC Address*	<input type="text" value="3a5f1c8e729b"/>
Attribute List Name	<input type="text" value="None"/>
Description	<input type="text"/>
WLAN Profile Name	<input type="text" value="Select a value"/>

## Elenco metodi AAA per autenticazione

Passaggio 1: Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione e selezionare Aggiungi.

[Configuration](#) > [Security](#) > [AAA](#)

[Servers / Groups](#) **[AAA Method List](#)** [AAA Advanced](#)

**[Authentication](#)**

Authorization

Passaggio 2: Definire il nome dell'elenco di metodi. Selezionare dot1x dall'elenco a discesa Tipo\* e local per il Tipo di gruppo. Selezionare Applica a dispositivo per salvare la configurazione.



+ AAA Wizard

Servers / Groups

**AAA Method List**

AAA Advanced

Authentication

**Authorization**

Accounting

+ Add

× Delete

	Name	Type
	default	exec

Passaggio 2: Definire il nome dell'elenco di metodi, selezionare download credenziali dall'elenco a discesa Type\* e locale per il tipo di gruppo. Fare clic su Applica alla periferica.

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+
- HTTSGROUP
- ISE\_DD\_Group
- ISE\_HA
- Test



Assigned Server Groups



 Cancel

 Update & Apply to Device

## Profilo mesh

Passaggio 1: Passare a Configurazione > Wireless > Mesh > Profili e selezionare Aggiungi.

Configuration ▾ > Wireless ▾ > Mesh

Global Config **Profiles**

+ Add

× Delete

Passaggio 2: Nella scheda Generale, definire un nome e una descrizione (facoltativa) per il profilo Mesh.

**General** Advanced

Name\*

MESH-Profile

Description

Enter Description

Range (Root AP to Mesh AP)

12000

Multicast Mode

In-Out ▾

IDS (Rogue/Signature Detection)

Passaggio 3: Nella scheda Avanzate, impostare il campo Metodo su EAP, quindi selezionare i profili Autorizzazione e Autenticazione creati in precedenza dai menu a discesa. Infine, abilitare la casella di controllo Ethernet Bridging e selezionare Aggiorna e applica.

General

**Advanced**

## Security

Method

EAP

Authentication Method

MESH

Authorization Method

MESH-Authorizati...

## Ethernet Bridging

VLAN Transparent

Ethernet Bridging

## Profilo di join AP

Passaggio 1: Selezionare Configurazione > Tag e profili > Join AP > Profilo, quindi fare clic su Aggiungi.

**Configuration** > **Tags & Profiles** > **AP Join**

+ Add

× Delete

Clone

AP Join Profile Name

Passaggio 2: Definire il nome e la descrizione del profilo (facoltativo).

Name\*

Mesh-AP-Join

Description

Enter Description

Country Code

IN



Time Zone



Not Configured



Use-Controller



Delta from WLC

Passo 3: passare alla scheda AP, selezionare il profilo Mesh dall'elenco a discesa Nome profilo Mesh, impostare EAP-FAST per il tipo EAP e CAPWAP DTLS per il tipo di autorizzazione AP, quindi fare clic su Applica a dispositivo.

**Edit AP Join Profile**

General Client CAPWAP **AP** Management Security ICap QoS Geolocation

**General** Power Management Hyperlocation AP Statistics

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type Unknown

Injector Switch MAC 0000.0000.0000

**AP EAP Auth Configuration**

EAP Type EAP-FAST

AP Authorization Type CAPWAP DTLS

**Client Statistics Reporting Interval**

5 GHz (sec) 90

2.4 GHz (sec) 90

**Extended Module**

Enable

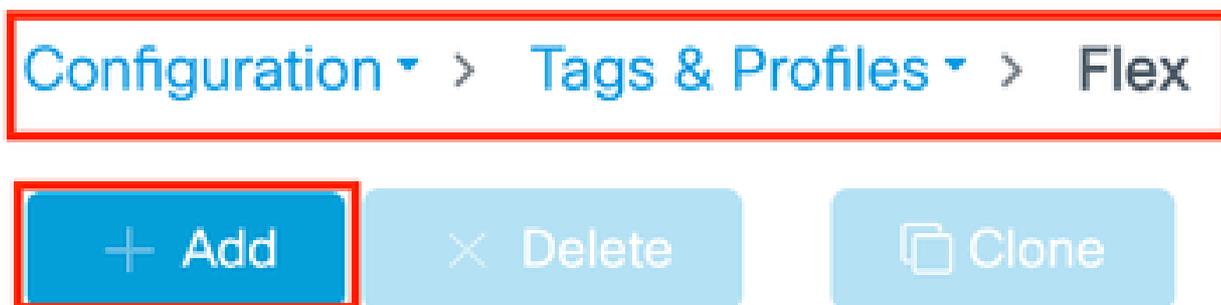
**Mesh**

Profile Name MESH-Profile

Cancel Update & Apply to Device

## Profilo Flex

Passaggio 1: Configurazione > Tag e profili > Flex, quindi fare clic su Aggiungi.



Passaggio 2: Definire un nome per il profilo Flex.

**General**

Local Authentication

Policy ACL

VLAN

DNS Layer Security

Name\*

Mesh-Flex

Fallback Radio Shut

Description

Enter Description

Flex Resilient

Passaggio 3: Passare alla scheda vlan e configurare il nome e l'ID della VLAN per il bridging locale del traffico client wireless, quindi fare clic su Salva.

General

Local Authentication

Policy ACL

**VLAN**

DNS Layer Security

+ Add

< Delete

VLAN Name	ID	Ingress ACL	Egress ACL
0	10		

No items to display

VLAN Name\*

Bridge-VLAN

VLAN ID\*

100

ACL

Unidirectional  Bidirectional

Ingress ACL

Select ACL

Egress ACL

Select ACL

Save

Cancel

Cancel

Update & Apply to Device

## Profilo criterio

Passaggio 1: Passare a Configurazione > Tag e profili > Criterio e fare clic su Aggiungi.

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Clone

Admin  
Status

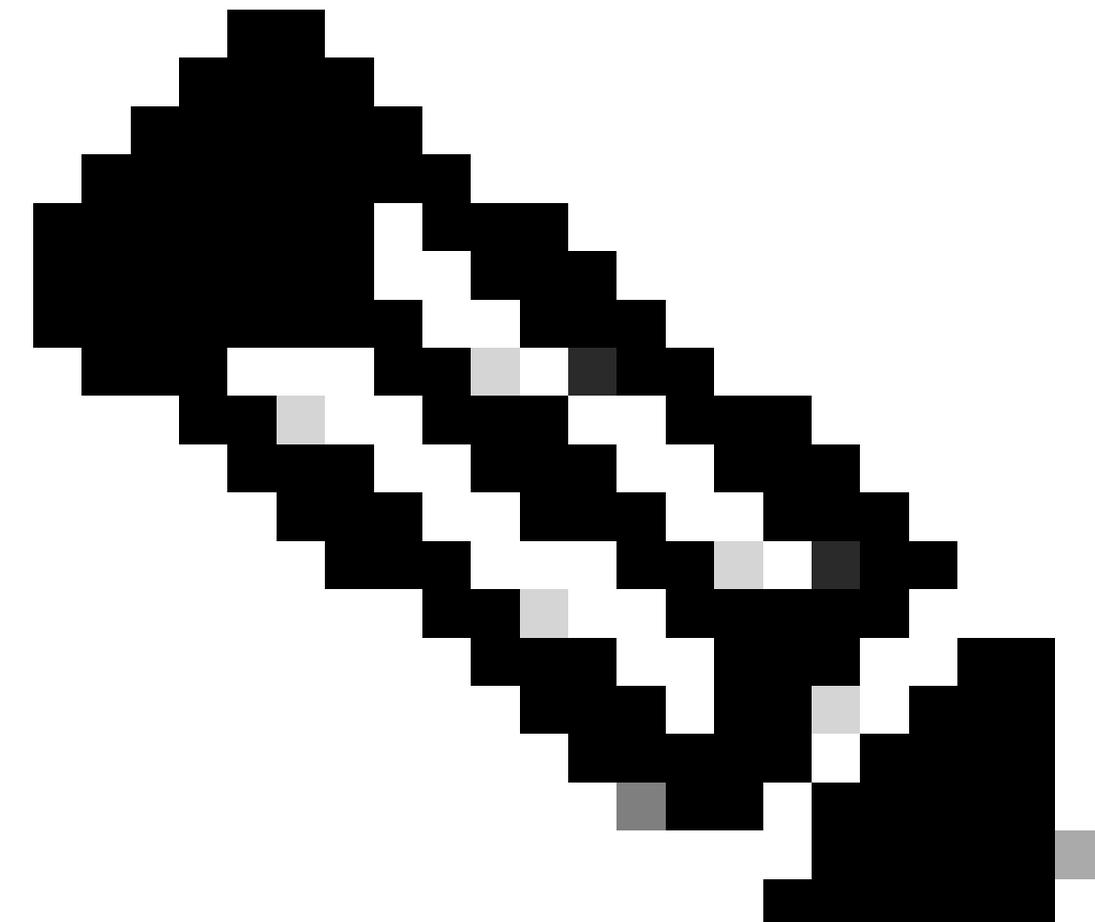


Associated  
Policy Tags



Policy Profile Name

Passaggio 2: Nella scheda Generale, definire il nome del profilo, impostare Status su Enabled e Disable Central Switching.



Nota: Per abilitare il bridging locale del traffico client, è necessario disabilitare la commutazione centrale. In base alla configurazione SSID, è possibile abilitare o

disabilitare altre opzioni in base alle esigenze.

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

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

Passaggio 3: Configurare la VLAN specificata nella scheda VLAN di AP Flex Profile, quindi fare clic su Aggiorna e applica.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name  ⓘ

VLAN

VLAN/VLAN Group  ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

URL Filters ⓘ

Pre Auth  ⓘ

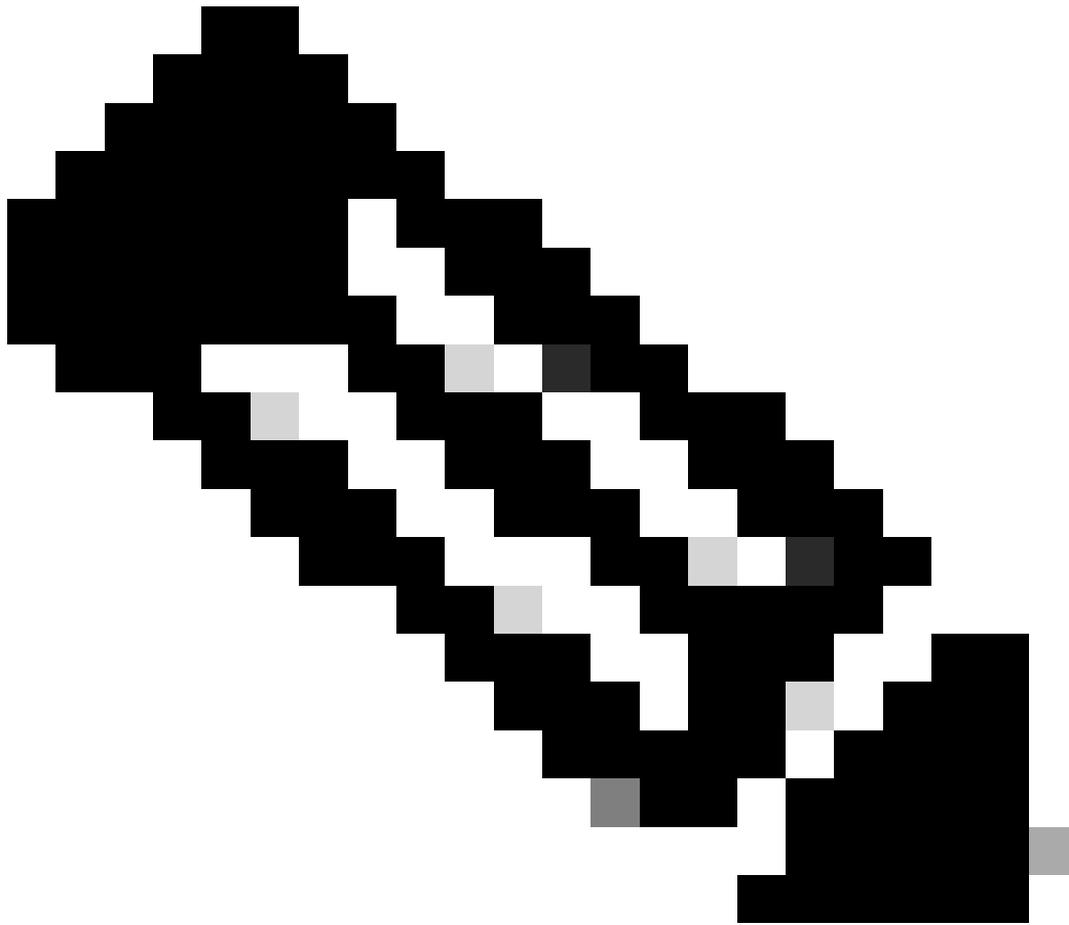
Post Auth  ⓘ

## Tag WLAN

Passaggio 1: Selezionare Configurazione > Tag e profili > WLAN e selezionare Aggiungi.

Passaggio 2: Nella scheda Generale, configurare Nome profilo, SSID e impostare lo stato su Abilitato.

Passaggio 3: Selezionare la scheda Protezione, Abilita WAP+WPA2 e configurare una chiave già condivisa.



Nota: La configurazione di SSID dipende interamente dai requisiti dell'utente. Per questo esempio, è configurato un SSID basato su PSK.

---

**General**

Security

Advanced

Add To Policy Tags

Profile Name\*

Bridge

R

SSID\*

Bridge-SSID

WLAN ID\*

6

6

St

Status

ENABLED



Broadcast SSID

ENABLED



5

St

General **Security** Advanced Add To Policy Tags**Layer2** Layer3 AAA WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP NoneMAC Filtering Lobby Admin Access 

## WPA Parameters

WPA Policy WPA2 Policy GTK Randomize OSEN Policy 

## WPA2 Encryption

AES(CCMP128) CCMP256 GCMP128 GCMP256 

## Protected Management Frame

PMF

Disabled

## Fast Transition

Status

Disabled

Over the DS 

Reassociation Timeout \*

20

## Auth Key Mgmt

802.1X PSK Easy-PSK OAKM  FT + 802.1X FT + PSK 802.1X-  
SHA256 PSK-SHA256 

PSK Format

ASCII

PSK Type

AES



Pre-Shared Key\*

.....

Cancel

Update &amp; Apply to Device

## Tag criteri

Passaggio 1: Passare a Configurazione > Tag e profili > Tag > Scheda Criteri, quindi fare clic su Aggiungi.

Passaggio 2: creare un tag criteri definendo un nome e associando la WLAN e il profilo criteri.

**Add Policy Tag** ✕

Name\*

Description

▼ **WLAN-POLICY Maps: 0**

WLAN Profile	Policy Profile
No items to display	

**Map WLAN and Policy**

WLAN Profile\*   Policy Profile\*

➤ **RLAN-POLICY Maps: 0**

## Tag sito

Passaggio 1: Passare a Configurazione > Tag e profili > Tag > Sito e fare clic su Aggiungi.

**Configuration** ▾ > **Tags & Profiles** ▾ > **Tags**

Policy **Site** RF AP

Passo 2: configurare il nome del tag, disabilitare l'opzione Abilita sito locale e associare sia il profilo di aggiunta AP che il profilo Flex.

**Edit Site Tag**

Name\* Mesh-Site-Tag

Description Enter Description

AP Join Profile Mesh-AP-Join

Flex Profile Mesh-Flex

Fabric Control Plane Name

Enable Local Site

Load\* @

Cancel Update & Apply to Device

## Configurazione dei punti di accesso

In questo caso di studio si presume che il punto di accesso (AP) sia prima unito al controller WLC (Wireless LAN Controller) in modalità locale e quindi passato alla modalità Flex+Bridge.

Passaggio 1: Selezionare Configuration > Wireless > Access Point (Configurazione > Wireless > Punti di accesso) e selezionare il punto di accesso (AP).

Passaggio 2: Assegnare il tag del sito e il tag dei criteri ai punti di accesso.



Nota: Il punto di accesso (AP) si riavvia, stabilisce la connessione con il controller in modalità Flex+Bridge ed è disponibile la scheda Mesh.

General		Tags	
AP Name*	AP34B8.8314.A204	<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>	
Location*	default location		
Base Radio MAC	34b8.831d.05a0	Policy	Mesh-Policy-Tag
Ethernet MAC	34b8.8314.a204	Site	Mesh-Site-Tag
Admin Status	ENABLED		

Passaggio 3: Nella scheda Rete, selezionare il ruolo da radice

**Edit AP**

General Interfaces High Availability Inventory Geolocation **Mesh** Advanced Support Bundle

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

Role

Ethernet Port Configuration

**!** Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully

Port

Mode

VLAN ID\*

Passaggio 4: Ripetere i passaggi 1 e 2 per il punto di accesso designato come punto di accesso mesh per portarlo online in modalità Flex+Bridge. Passare alla scheda Rete e configurare il ruolo come Rete.

Passaggio 5: Il punto di accesso Mesh è collegato allo switch sulla porta 0, configurata in modalità trunk, con i punti di accesso e la VLAN impostata come VLAN nativa. Verificare che le VLAN consentite includano la VLAN client specificata nel profilo Flex.

Passaggio 6: Fare clic su Aggiorna e applica.

General Interfaces High Availability Inventory Geolocation **Mesh** Advanced Support Bundle

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

Role

Remove PSK 

Ethernet Port Configuration

**!** Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully

Port

Mode

Native VLAN ID\*

Allowed VLAN IDs

## Switch Port Configuration

```
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 100
switchport mode trunk
end
```

## Verifica

Mesh associazione punto di accesso a punto di accesso radice:

```
#show wireless mesh ap summary
AP Name AP Model BVI MAC BGN AP Role
-----
AP34B8.8314.A204 C9124AXI-ROW 34b8.8314.a204 Default Root AP
APC828.E536.D47C C9124AXI-ROW c828.e536.d47c Default Mesh AP
Number of Flex+Bridge APs : 2
Number of Flex+Bridge RAPs : 1
Number of Flex+Bridge MAPs : 1
```

```
#show wireless mesh ap tree
=====
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=====
[Sector 1]
-----
AP34B8.8314.A204 [0, 0, Default, (36,40), 0000.0000.0000, 5%, 0]
|-APC828.E536.D47C [1, 68, Default, (36,40), 0000.0000.0000, 6%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1
```

Associazione client nell'access point Mesh:

```
#show flexconnect client
Flexconnect Clients:
mac radio vap aid state encr aaa-vlan aaa-acl aaa-ipv6-acl assoc auth switching key-method roam key-pro
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 none none none Local Central Local Other regular No Yes No 0

#show controllers dot11Radio 0 client
mac radio vap aid state encr Maxrate Assoc Cap is_wgb_wired wgb_mac_addr
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 MCS92SS HE HE false 00:00:00:00:00:00
```

```
#show flexconnect client aaa-override
```

```
Flexconnect Clients:
```

```
mac vlan qos acl ipv6-acl vlan-name avgdtids avgrtdtds bstdtds bstrtdtds avgdtus avgrtdtus bstdtus bstrtdtus  
52:95:C7:EE:B7:E5 none none none none Bridge-VLAN 0 0 0 0 0 0 0 0
```

Il traffico proveniente dal punto di accesso Mesh (MAP) viene collegato direttamente allo switch uplink, ignorando il punto di accesso radice (RAP):

```
<#root>
```

```
DHCP:
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2883] [ 62081:607119] [APC828.E536.D47C]
```

```
[U:C] DHCP_REQUEST : TransId 0x3bcb0a7b
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2884] chatter: dhcp_req_local_sw_nonat: 1
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] [ 62081:607245] [APC828.E536.D47C]
```

```
[U:C] DHCP_REQUEST : TransId 0x3bcb0a7b
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] chatter: dhcp_reply_nonat: 1748579
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613080] [APC828.E536.D47C]
```

```
[D:C] DHCP_ACK : TransId 0x3bcb0a7b
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613123] [APC828.E536.D47C]
```

```
[D:W] DHCP_ACK : TransId 0x3bcb0a7b
```

ARP:

May 30 04:31:44 APC828.E536.D47C kernel: [\*05/30/2025 04:31:44.0572] [ 62464:537183] [APC828.E536.D47C]

[U:W] ARP\_QUERY : Sender 100.0.0.2 TargIp 100.0.0.1

May 30 04:31:44 APC828.E536.D47C kernel: [\*05/30/2025 04:31:44.0572] [ 62464:537219] [APC828.E536.D47C]

[U:C] ARP\_QUERY : Sender 100.0.0.2 TargIp 100.0.0.1

May 30 04:31:44 APC828.E536.D47C kernel: [\*05/30/2025 04:31:44.0573] chatter: ethertype\_cl1: 1748579504

May 30 04:31:44 APC828.E536.D47C kernel: [\*05/30/2025 04:31:44.0628] [ 62464:542842] [APC828.E536.D47C]

[D:C] ARP\_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:44 APC828.E536.D47C kernel: [\*05/30/2025 04:31:44.0629] chatter: fromdevs\_arp\_resp: arp resp

May 30 04:31:44 APC828.E536.D47C kernel: [\*05/30/2025 04:31:44.0629] [ 62464:542971] [APC828.E536.D47C]

[D:C] ARP\_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:44 APC828.E536.D47C kernel: [\*05/30/2025 04:31:44.0630] [ 62464:543018] [APC828.E536.D47C]

[D:W] ARP\_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:45 APC828.E536.D47C kernel: [\*05/30/2025 04:31:45.4301] [ 62465:910100] [APC828.E536.D47C]

[D:A] ARP\_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

ICMP:

May 30 04:32:09 APC828.E536.D47C kernel: [\*05/30/2025 04:32:09.3059] [ 62489:785903] [APC828.E536.D47C]

[U:W] ICMP\_ECHO : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [\*05/30/2025 04:32:09.3059] [ 62489:785938] [APC828.E536.D47C]

[U:C] ICMP\_ECHO : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [\*05/30/2025 04:32:09.3104] [ 62489:790444] [APC828.E536.D47C]

[D:C] ICMP\_ECHO\_REPLY : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [\*05/30/2025 04:32:09.3105] [ 62489:790534] [APC828.E536.D47C]

[D:C] ICMP\_ECHO\_REPLY : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [\*05/30/2025 04:32:09.3105] [ 62489:790583] [APC828.E536.D47C]

[D:W] ICMP\_ECHO\_REPLY : Id 39016 Seq 0

## 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).