

Configurazione di Mesh sui controller LAN wireless Catalyst 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Caso di studio 1: modalità Bridge](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Case study 2: Flex + Bridge](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto un esempio di configurazione di base per collegare un punto di accesso mesh al controller WLC (Catalyst 9800 Wireless LAN Controller).

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 di un server DHCP esterno
- Configurazione degli switch Cisco

Componenti usati

In questo esempio viene usato un Lightweight Access Point (1572AP e 1542) che può essere configurato come Root AP (RAP) o Mesh AP (MAP) per collegarsi a Catalyst 9800 WLC. La procedura è identica per i punti di accesso 1542 o 1562. Il dispositivo RAP è collegato al Catalyst 9800 WLC tramite uno switch Cisco Catalyst.

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

- C9800-CL v16.12.1
- Cisco Layer 2 Switch
- Cisco Aironet serie 1572 Lightweight External Access Point per la sezione Bridge
- Cisco Aironet 1542 per la sezione Flex+Bridge

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

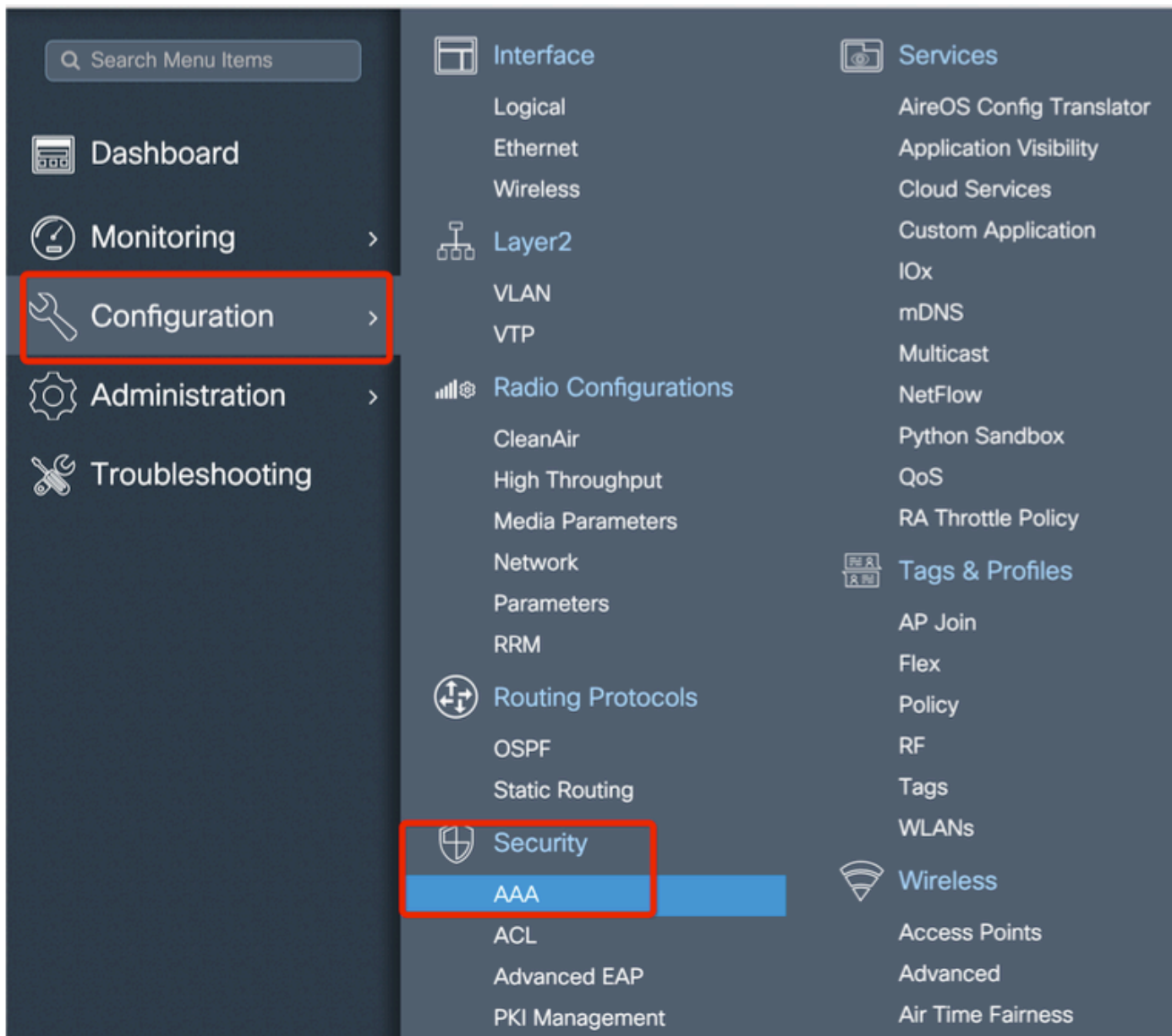
Caso di studio 1: modalità Bridge

Configurazioni


Affinché si colleghi al controller 9800, è necessario autenticare un punto di accesso mesh. In questo caso di studio si considera che l'access point viene collegato in modalità locale prima al WLC e quindi convertito in modalità mesh Bridge (alias a). Per evitare l'assegnazione di profili di join AP, utilizzare questo esempio ma configurare il metodo di download delle credenziali di autorizzazione aaa predefinito in modo che qualsiasi access point mesh possa unirsi al controller.

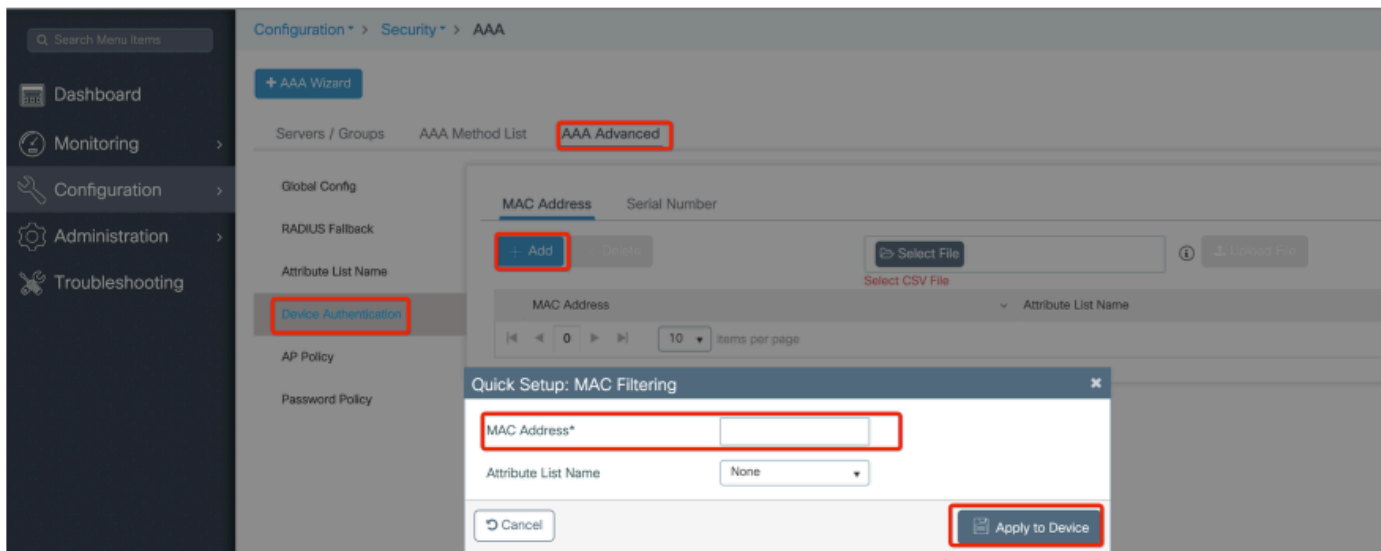
Passaggio 1: configurare gli indirizzi MAC RAP/MAP in Autenticazione dispositivo.

Selezionare Configuration > AAA > AAA Advanced > Device Authentication (Configurazione > AAA > Avanzate AAA > Autenticazione dispositivo).



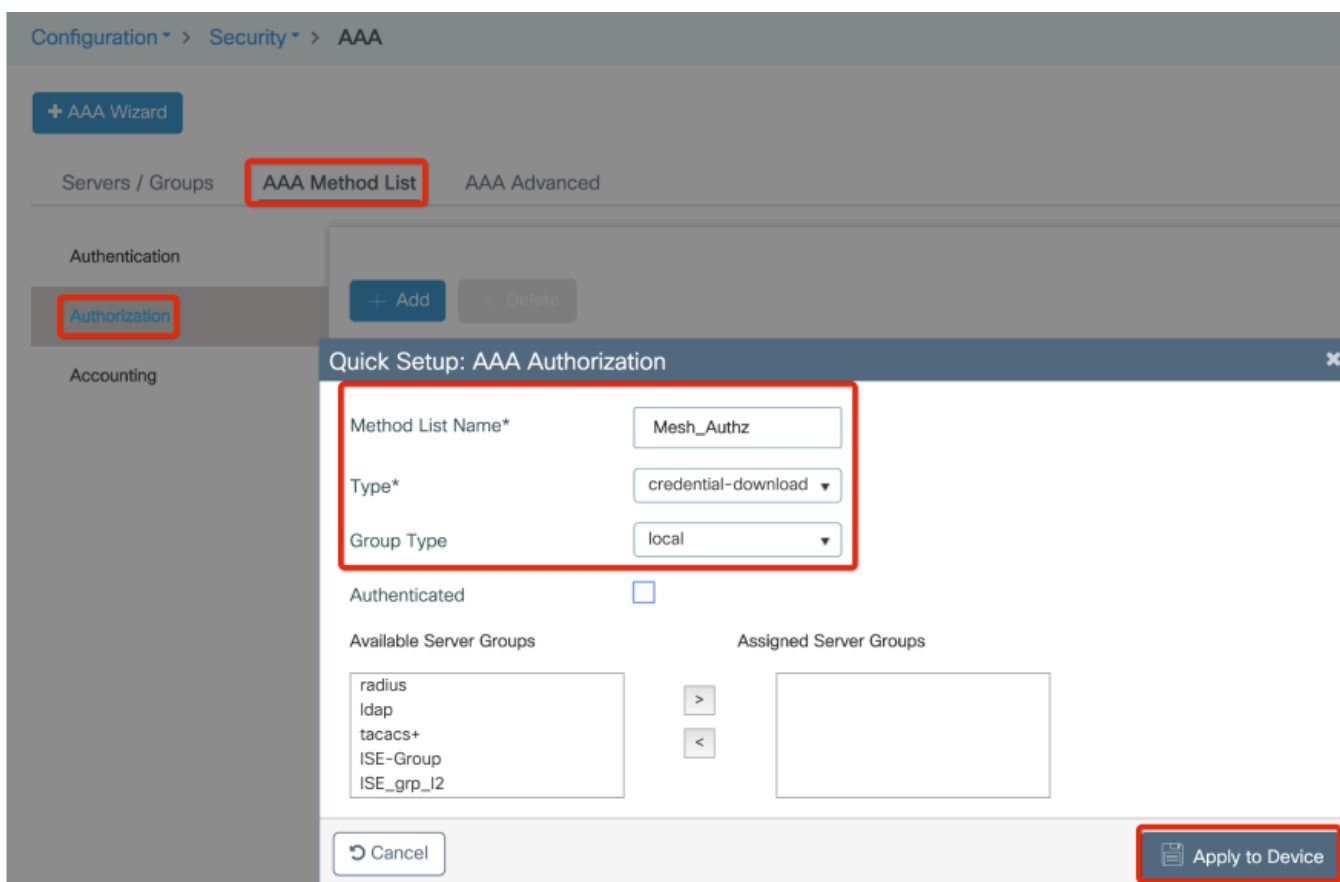
Aggiungere l'indirizzo MAC Ethernet di base dei punti di accesso alla rete. Aggiungerlo senza caratteri speciali, senza '.' o ':'

 Nota: a partire dalla versione 17.3.1, se vengono aggiunti delimitatori di indirizzo mac come '.', ':' o '-', l'access point non è in grado di unirsi. A tale scopo, sono attualmente disponibili 2 miglioramenti: ID bug Cisco [CSCvv43870](#) e ID bug Cisco [CSCvr07920](#). In futuro, 9800 accetterà tutti i formati di indirizzo MAC.



Passaggio 2: configurare l'elenco dei metodi di autenticazione e autorizzazione.

Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione e creare l'elenco dei metodi di autenticazione e l'elenco dei metodi di autorizzazione.



Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization

Accounting

+ Add Delete

Quick Setup: AAA Authentication

Method List Name* Mesh_Authentication

Type* dot1x

Group Type local

Available Server Groups Assigned Server Groups

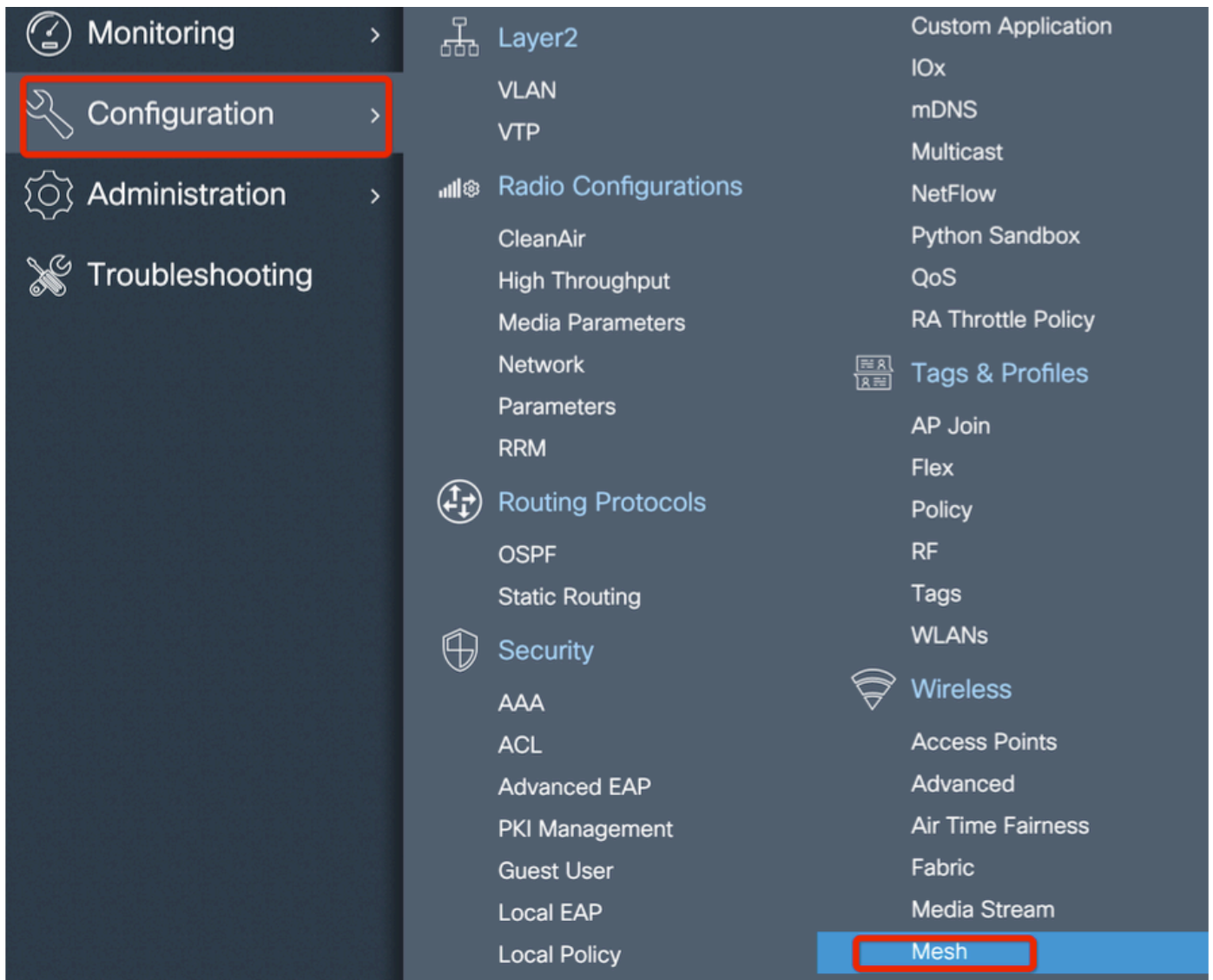
radius
ldap
tacacs+
ISE-Group
ISE_grp_I2

>
<

Cancel Apply to Device

Passo 3: configurare i parametri mesh globali.

Passare a Configurazione> Mesh> Parametri globali. Inizialmente è possibile mantenere questi valori predefiniti.



Passo 4: creazione di un nuovo profilo di rete in Configurazione > Rete > Profilo > +Aggiungi.

Global Config **Profiles**

+ Add Delete

Number of Profiles : 1

Add Mesh Profile

General Advanced

Name*	Mesh_Profile	Backhaul amsdu	<input checked="" type="checkbox"/>
Description	Enter Description	Backhaul Client Access	<input type="checkbox"/>
Range (Root AP to Mesh AP)	12000	Battery State for an AP	<input checked="" type="checkbox"/>
Multicast Mode	In-Out	Full sector DFS status	<input checked="" type="checkbox"/>
IDS (Rogue/Signature Detection)	<input type="checkbox"/>		
Convergence Method	Standard		
Background Scanning	<input type="checkbox"/>		
Channel Change Notification	<input type="checkbox"/>		
LSC	<input type="checkbox"/>		

Cancel Apply to Device

Fate clic sul profilo mesh creato per modificare le impostazioni generali e avanzate per il profilo mesh.

Nel diagramma come mostrato, è necessario mappare il profilo di autenticazione e autorizzazione creato prima al profilo Mesh.

Configuration > Wireless > Mesh

Global Config Profiles

Number of Profiles : 1

default-mesh-profile

Add Mesh Profile

General **Advanced**

Security

Method: EAP

Authentication Method: Mesh_Authentication

Authorization Method: Mesh_Authz

Ethernet Bridging

VLAN Transparent:

Ethernet Bridging:

Bridge Group

Bridge Group Name: Enter Name

Strict Match:

5 GHz Band Backhaul

Rate Types: auto

2.4 GHz Band Backhaul

Rate Types: auto

Cancel Apply to Device

Passaggio 5: Creare un nuovo profilo di join AP. Passare a Configura > Tag e profili: AP Join.

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Interface

Logical

Ethernet

Wireless

Layer2

VLAN

VTP

Radio Configurations

CleanAir

High Throughput

Media Parameters

Network

Parameters

RRM

Routing Protocols

OSPF

Static Routing

Security

AAA

ACL

Services

AireOS Config Translator

Application Visibility

Cloud Services

Custom Application

IOx

mDNS

Multicast

NetFlow

Python Sandbox

QoS

RA Throttle Policy

Tags & Profiles

AP Join

Flex

Policy

RF

Tags

WLANs

Wireless

Access Points

Configuration > Tags & Profiles > AP Join

+ Add - Delete

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

Add AP Join Profile

General Client CAPWAP AP Management Rogue AP ICap

Name* Mesh_AP_Join_Profile

Description Enter Description

LED State

LAG Mode

NTP Server 0.0.0.0

Cancel Apply to Device

Applicare il profilo Mesh configurato in precedenza e configurare l'autenticazione AP-EAP:

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

Add AP Join Profile ✕

General Client CAPWAP **AP** Management Rogue AP ICap

General Hyperlocation BLE Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Code

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

Extended Module

Enable

AP EAP Auth Configuration

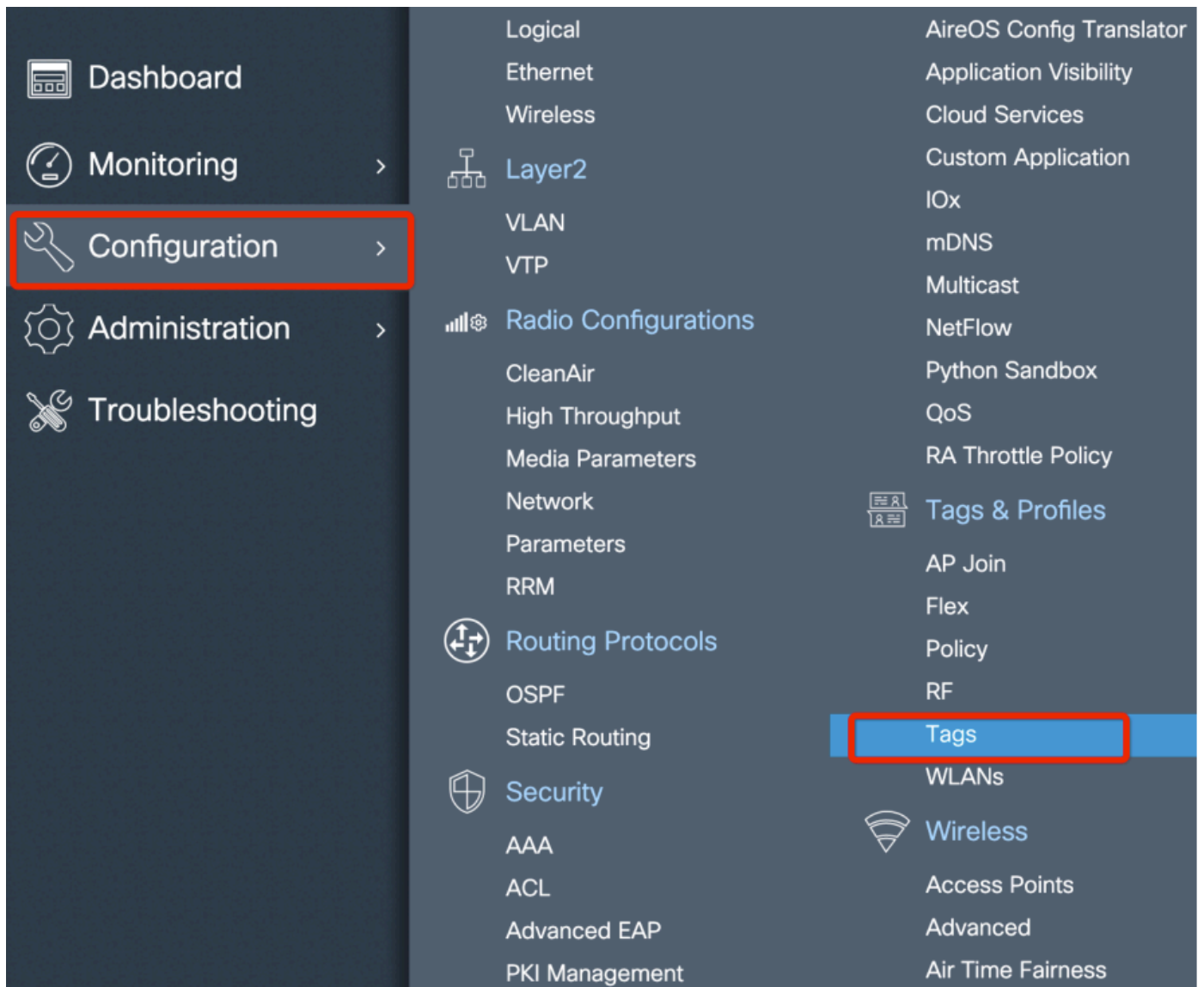
EAP Type

AP Authorization Type

Mesh

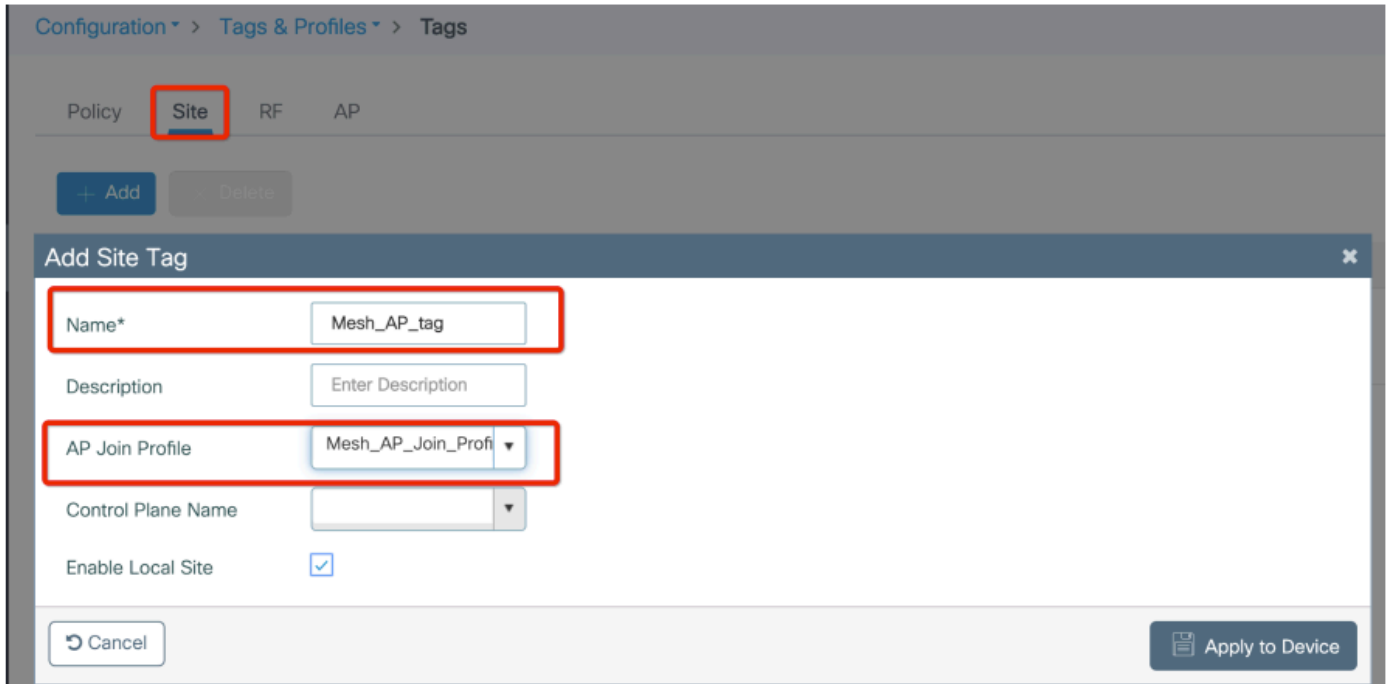
Profile Name [Clear](#)

Passo 6: creare un tag di posizione mesh come mostrato.



Configura Fare clic sul tag di posizione Mesh creato nel Passaggio 6 per configurarlo.

Passare alla scheda Sito e applicarvi il profilo di join Mesh AP precedentemente configurato:



Passaggio 7. Convertire il punto di accesso in modalità Bridge.

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address
AP2C33-110E-6B66	AIR-AP1562E-E-K9	2	✓	109.129.49.9

10 items per page

- > 5 GHz Radios
- > 2.4 GHz Radios
- > Dual-Band Radios

Edit AP

General | Interfaces | High Availability | Inventory | Mesh | Advanced | Support Bundle

General		Version	
AP Name*	AP2C33-110E-6B66	Primary Software Version	17.3.0.17
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	7070.8bb4.9200	Predownloaded Version	N/A
Ethernet MAC	2c33.110e.6b66	Next Retry Time	N/A
Admin Status	ENABLED	Boot Version	1.1.2.4
AP Mode	Bridge	IOS Version	17.3.0.17
Operation Status	Monitor	Mini IOS Version	0.0.0.0
Fabric Status	Sniffer	IP Config	
LED State	Bridge	CAPWAP Preferred Mode	IPv4
	Clear		

Tramite CLI, è possibile utilizzare questo comando sull'access point:

```
capwap ap mode bridge
```

L'access point si riavvia e si unisce nuovamente come modalità Bridge.

Passaggio 8. È ora possibile definire il ruolo dell'access point: punto di accesso radice o punto di accesso mesh.

L'access point principale è quello con una connessione cablata al WLC, mentre l'access point con rete si unisce al WLC tramite la radio che tenta di connettersi a un access point principale. Un

punto di accesso mesh può unirsi al WLC tramite l'interfaccia cablata se non riesce a trovare un punto di accesso radice tramite la radio, a scopo di provisioning. Non dimenticare di specificare la vlan nativa del trunk nelle impostazioni dell'access point nel caso sia diversa dalla VLAN predefinita 1.

The screenshot shows the 'Edit AP' configuration page for a mesh access point. The 'Mesh' tab is selected, and the 'Ethernet Port Configuration' section is visible. The 'VLAN Trunking Native' is set to 1, and the 'Role' is set to Mesh. The 'Backhaul Radio Type' is 5ghz, 'Backhaul Slot ID' is 1, and 'Rate Types' is auto. The 'Update & Apply to Device' button is visible at the bottom right.

Verifica

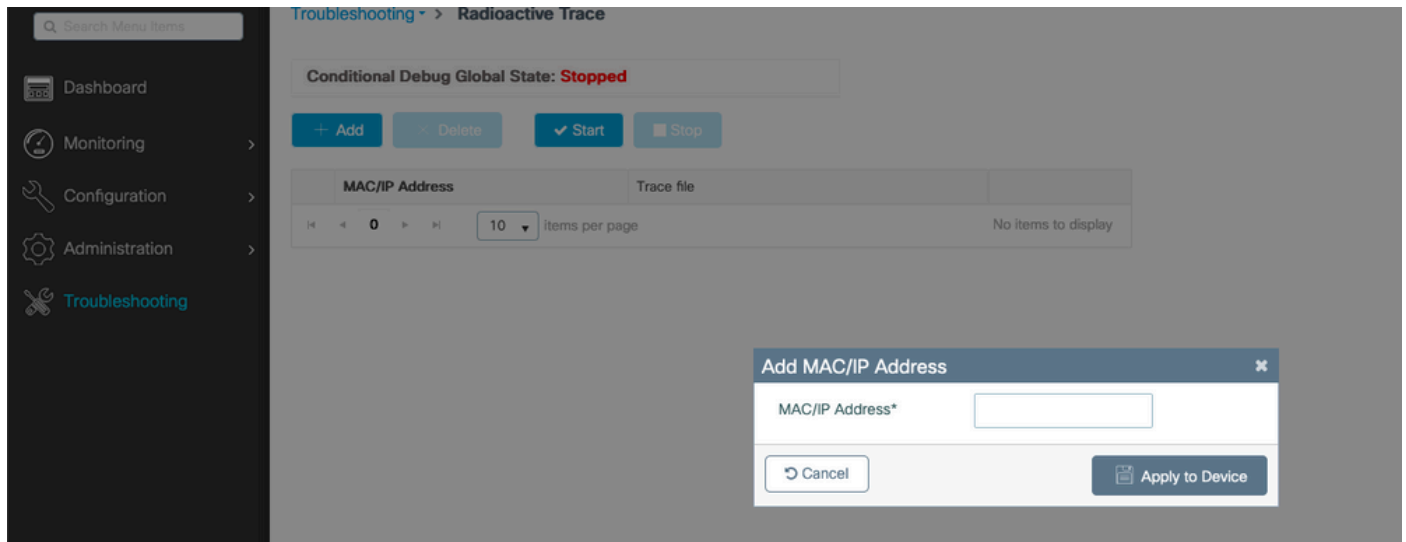
```

aaa new-model
aaa local authentication default authorization default
!
!
aaa authentication dot1x default local
aaa authentication dot1x Mesh_Authentication local
aaa authorization network default local
aaa authorization credential-download default local
aaa authorization credential-download Mesh_Authz local
username 111122223333 mac
wireless profile mesh Mesh_Profile
  method authentication Mesh_Authentication
  method authorization Mesh_Authz
wireless profile mesh default-mesh-profile
  description "default mesh profile"
wireless tag site Mesh_AP_Tag
  ap-profile Mesh_AP_Join_Profile
ap profile Mesh_AP_Join_Profile
  hyperlocation ble-beacon 0
  hyperlocation ble-beacon 1
  hyperlocation ble-beacon 2
  hyperlocation ble-beacon 3
  hyperlocation ble-beacon 4
  mesh-profile Mesh_Profile

```

Risoluzione dei problemi

In Risoluzione dei problemi > Pagina UI Web di Traccia radioattiva, fare clic su aggiungi e immettere l'indirizzo MAC dell'access point.



Fare clic su Start e attendere che l'access point tenti di unirsi nuovamente al controller. Al termine, fare clic su Genera e scegliere un periodo di tempo per la raccolta dei log (ad esempio, gli ultimi 10 o 30 minuti).

Fare clic sul nome del file di traccia per scaricarlo dal browser.

Di seguito è riportato un esempio di access point non collegato perché è stato definito un nome di metodo di autorizzazione aaa errato:

```
2019/11/28 13:08:38.269 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [23388]: (info): DTLS record type: 23, appli
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (info): 00a3.8e95.6c40 Ap auth p
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): Failed to initialize auth
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): 00a3.8e95.6c40 Auth requ
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get wtp r
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get ap ta
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (ERR): Session-IP: 192.168.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (info): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.289 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [23038]: (debug): instance :0 port:38932MAC
```

Lo stesso può essere visto più facilmente nel dashboard dell'interfaccia utente Web quando si fa clic su AP non uniti. Autenticazione app in sospeso è il suggerimento che punta all'autenticazione dell'access point stesso:

The screenshot shows the 'Join Statistics' dashboard. On the left, there are filters for 'Number of AP(s): 2' and a search for 'Status "Is equal to" NOT JOINED'. A table lists APs, with 'NA' selected. The main area displays two statistics tables: 'Join phase statistics' and 'Data DTLS Statistics'.

Join phase statistics			
Join requests received	1		
Successful join responses sent	0		
Unsuccessful join request processing	0		
Reason for last unsuccessful join attempt	Ap auth pending		
Time at last successful join attempt	NA		
Time at last unsuccessful join attempt	NA		

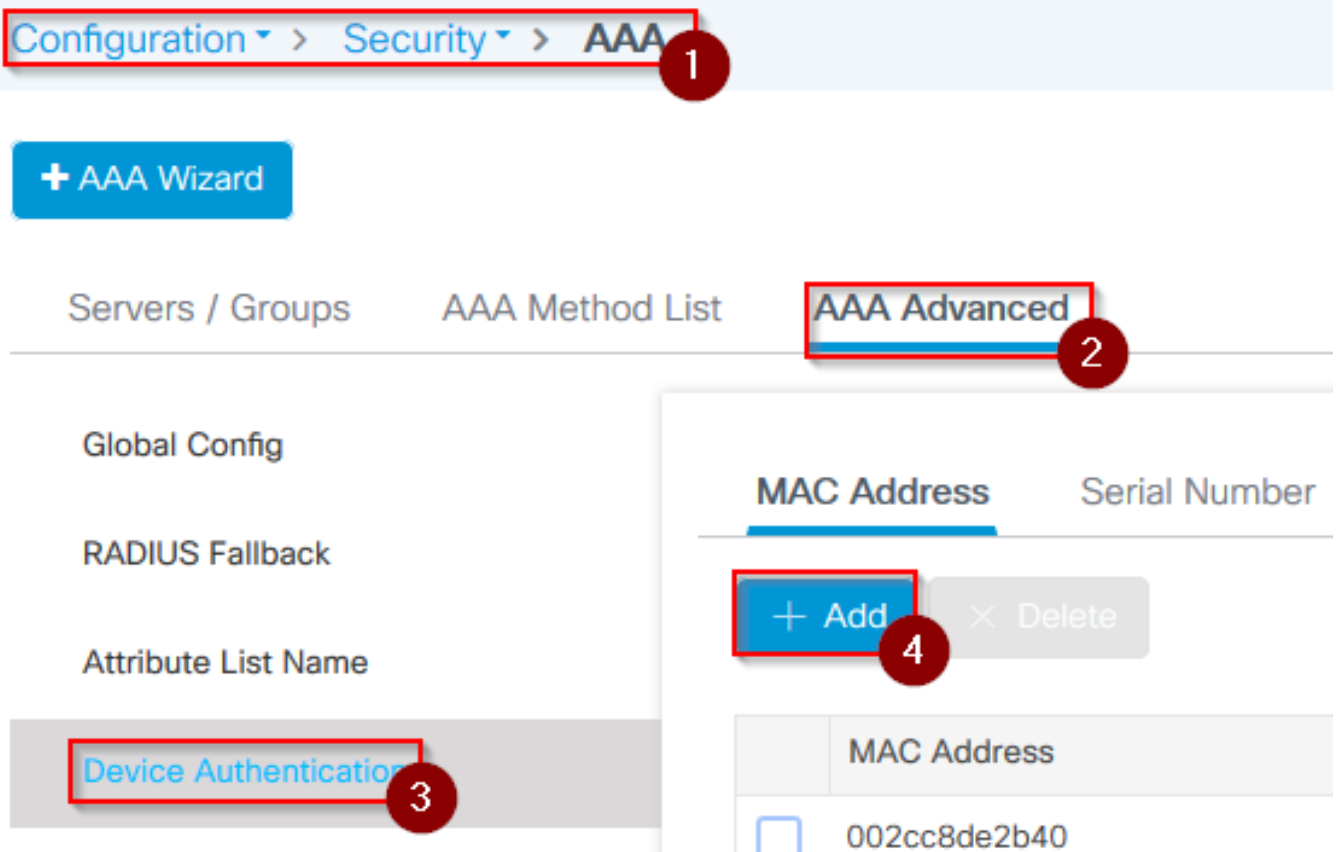
Data DTLS Statistics			
DTLS Session request received	0	Configuration requests received	0
Established DTLS session	0	Successful configuration responses sent	0
Unsuccessful DTLS session	0	Unsuccessful configuration request processing	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success	Reason for last unsuccessful configuration attempt	NA
Time at last successful DTLS session	Mon, 17 Feb 2020 09:15:41 GMT	Time at last successful configuration attempt	NA
Time at last unsuccessful DTLS session	NA	Time at last unsuccessful configuration attempt	NA

Case study 2: Flex + Bridge

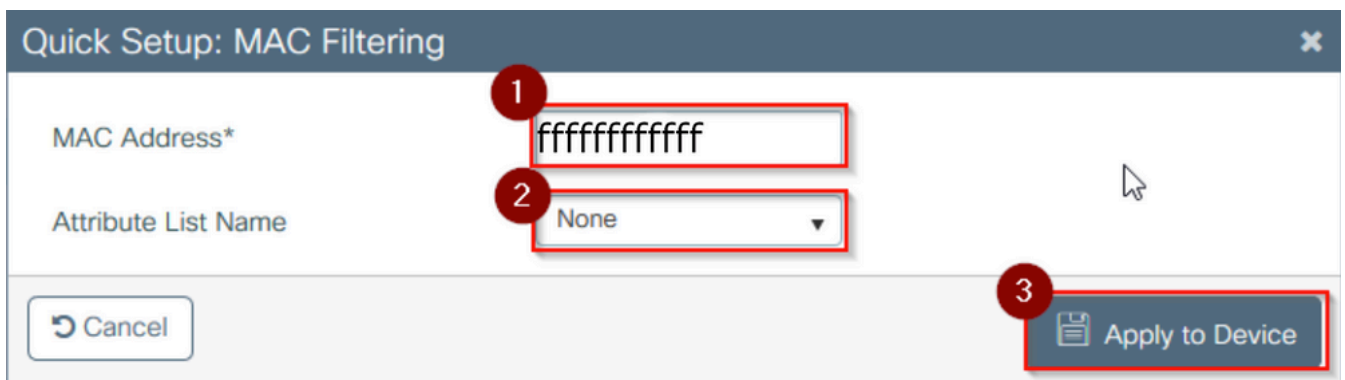
In questa sezione viene evidenziato il processo di join di un access point serie 1542 in modalità Flex+bridge con autenticazione EAP eseguita in locale sul WLC.

Configurazione

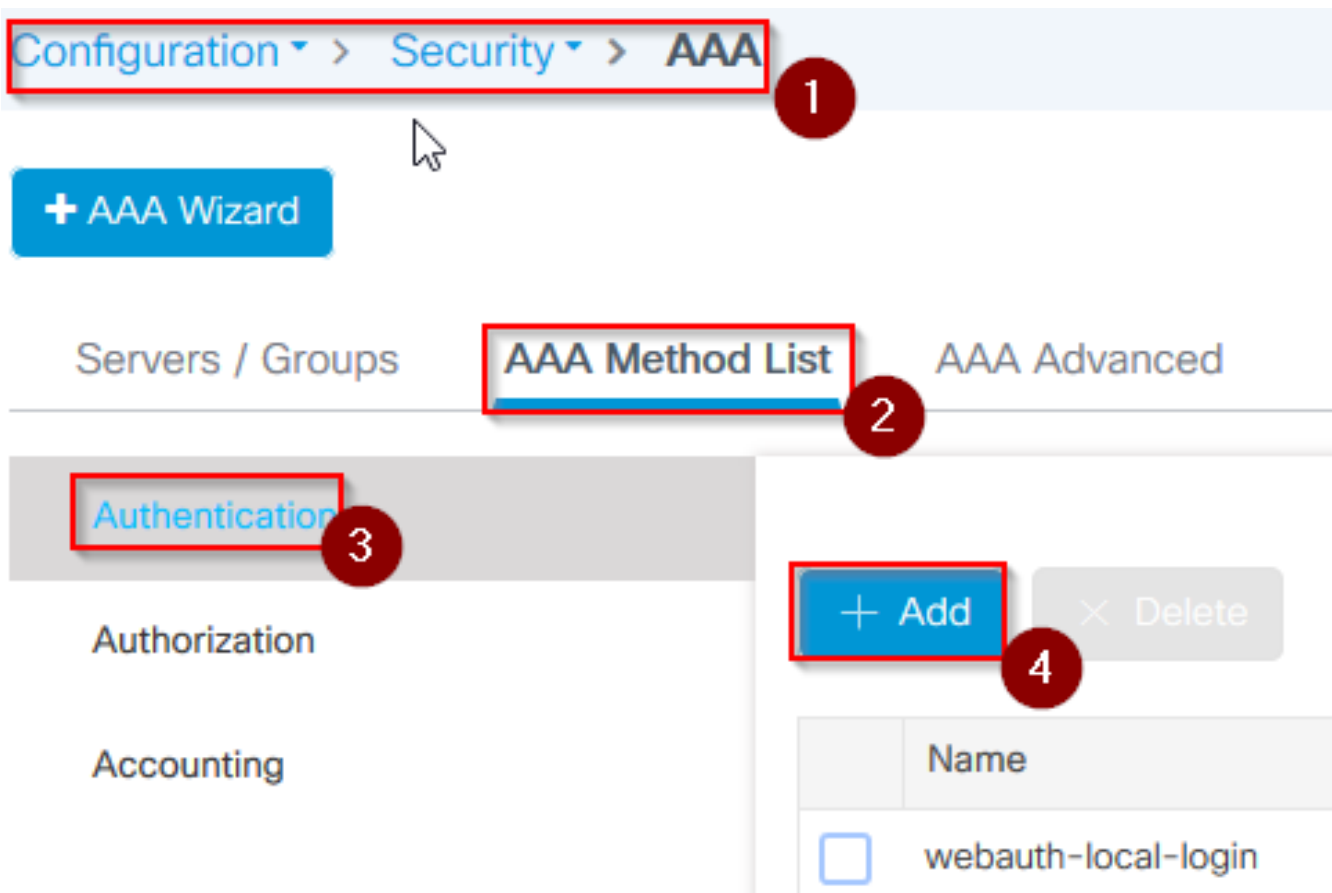
- Passaggio 1. Selezionare Configuration > Security > AAA > AAA Advanced > Device Authentication (Configurazione > Sicurezza > AAA > Avanzate AAA > Autenticazione dispositivo).



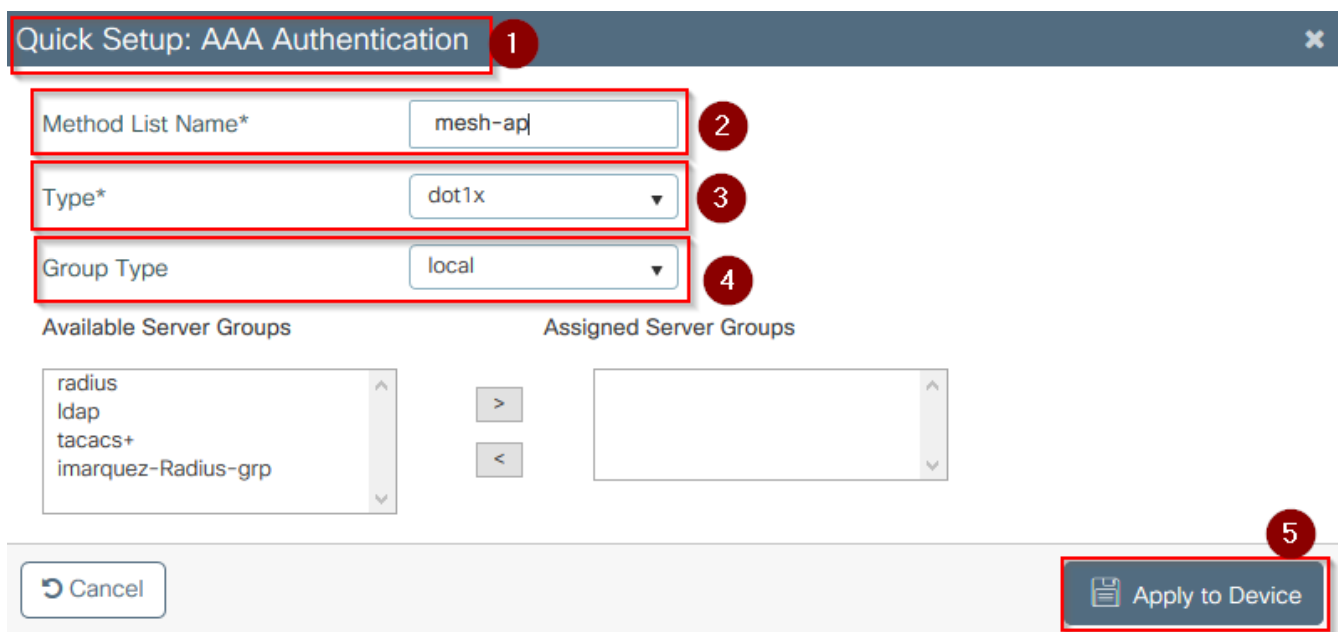
- Passaggio 2. Selezionare Device Authentication (Autenticazione dispositivo), quindi Add (Aggiungi).
- Passaggio 3. Digitare l'indirizzo MAC Ethernet di base dell'access point per collegarsi al WLC. Lasciare vuoto il campo Nome elenco attributi e selezionare Applica al dispositivo.



- Passaggio 4. Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione.
- Passaggio 5. Selezionare Aggiungi. Viene visualizzata la schermata di autenticazione AAA.

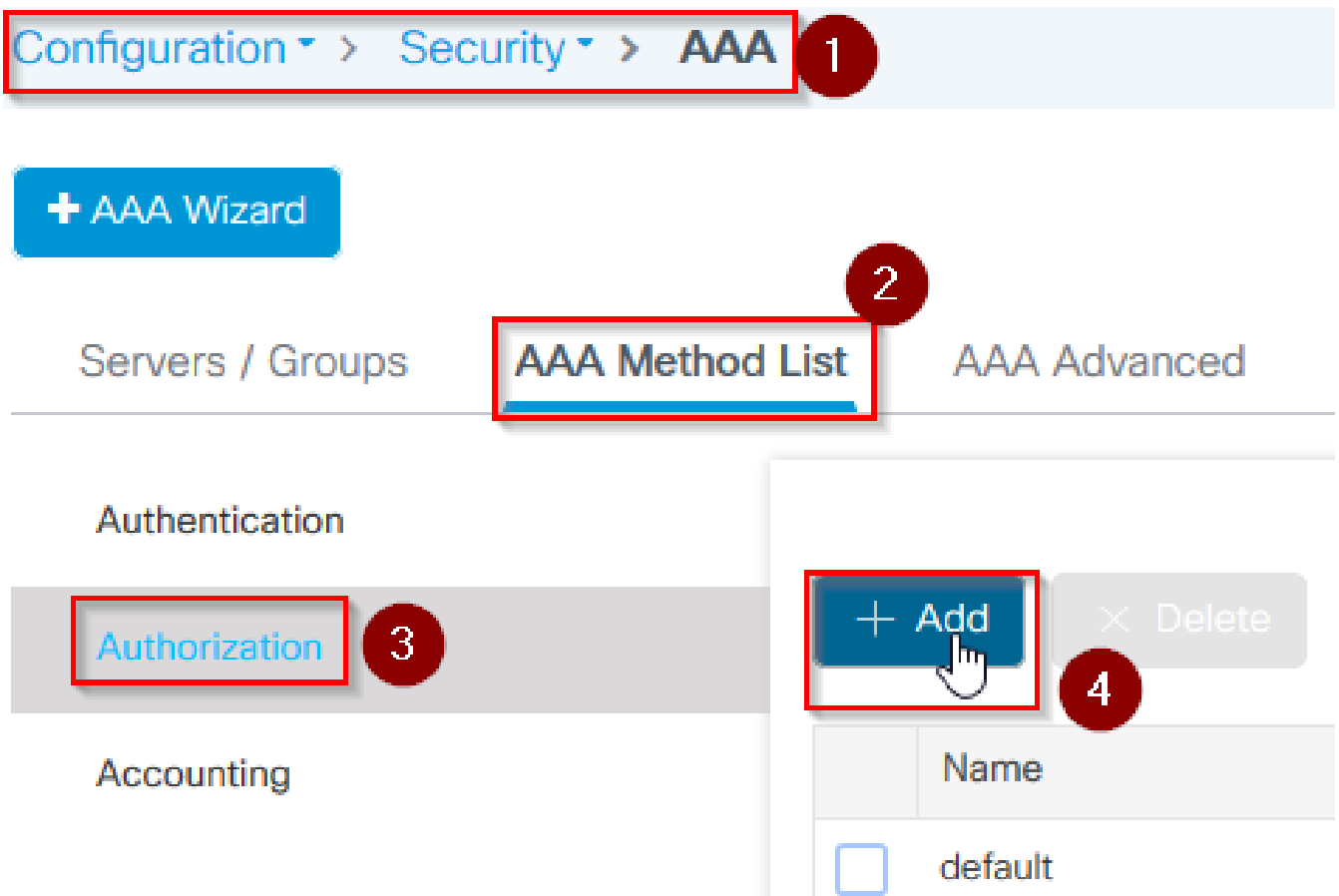


- Passaggio 6. Digitare un nome in Nome elenco metodi. Selezionare 802.1x dall'elenco a discesa Type* e local per il Group Type. Infine, selezionare Applica al dispositivo.



- Passaggio 6b. Se i punti di accesso vengono collegati direttamente in modalità Bridge e non sono stati assegnati un tag di sito e criteri in precedenza, ripetere il passaggio 6 ma per il metodo predefinito.
- Configurare un metodo di autenticazione aaa dot1x che punta a locale (autenticazione AAA CLI predefinita dot1x locale).

- Passaggio 7. Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione.
- Passaggio 8. Selezionare Aggiungi. Viene visualizzata la schermata di popup AAA Authorization (Autorizzazione AAA).



- Passaggio 9. Digitare un nome in Nome elenco metodi, selezionare download credenziali dall'elenco a discesa Tipo* e locale per Tipo gruppo. Infine, selezionare Applica al dispositivo.

Quick Setup: AAA Authorization ✕

Method List Name* 1

Type* 2

Group Type 3

Authenticated

Available Server Groups Assigned Server Groups

4

- Passaggio 9b. Se l'access point si unisce direttamente in modalità bridge, ovvero non si unisce prima in modalità locale, ripetere il passaggio 9 per il metodo di download delle credenziali predefinito (CLI `aaa authorization credential-download default local`).
- Passaggio 10. Selezionare Configurazione > Wireless > Mesh > Profili.
- Passaggio 11. Selezionare Aggiungi. Viene visualizzato il popup Aggiungi profilo di rete.

Configuration ▾ > Wireless ▾ > Mesh

1

Global Config **Profiles** 2

3

- Passaggio 12. Nella scheda Generale, impostare un nome e una descrizione per il profilo Mesh.

Add Mesh Profile

General

Advanced

Name*

mesh-profile|

Description

mesh-profile

- Passaggio 13. Nella scheda Avanzate, selezionare EAP per il campo Metodo.
- Passaggio 14. Selezionare il profilo di autorizzazione e autenticazione definito nei passaggi 6 e 9, quindi selezionare Applica al dispositivo.

Add Mesh Profile

General **Advanced**

Security

Method: EAP

Authentication Method: mesh-ap

Authorization Method: mesh-ap

Ethernet Bridging

VLAN Transparent:

Ethernet Bridging:

Bridge Group

Bridge Group Name: Enter Name

Strict Match:

5 GHz Band Backhaul

Rate Types: auto

2.4 GHz Band Backhaul

Rate Types: auto

Cancel **Apply to Device**

- Passaggio 15. Selezionare Configurazione > Tag e profili > Join AP > Profilo.
- Passaggio 16. Selezionare Aggiungi. Viene visualizzata la schermata di popup Profilo di join AP. Impostare un nome e una descrizione per il profilo di join AP.

Configuration > Tags & Profiles > AP Join

1

+ Add

× Delete

2

AP Join Profile Name

Add AP Join Profile

General

Client

CAPWAP

AP

Management

Rogue AP

ICap

Name*

mes-ap-join

Description

mesh-ap-join

LED State



LAG Mode



NTP Server

0.0.0.0

- Passaggio 17. Passare alla scheda AP e selezionare il profilo di rete creato nel passo 12 dall'elenco a discesa Nome profilo di rete.
- Passaggio 18. Verificare che EAP-FAST e CAPWAP DTLS siano impostati per i campi Tipo EAP e Tipo di autorizzazione AP rispettivamente.
- Passaggio 19. Selezionare Applica alla periferica.

Add AP Join Profile ✕

General Client CAPWAP **AP** Management Rogue AP ICap

General Hyperlocation BLE Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type Unknown ▾

Injector Switch MAC 00:00:00:00:00:00

Code

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

Extended Module

Enable

Mesh

Profile Name mesh-profile ▾ Clear

AP EAP Auth Configuration

EAP Type EAP-FAST ▾

AP Authorization Type CAPWAP DTLS ▾

↶ Cancel

Apply to Device ➤

- Passaggio 20. Selezionare Configurazione > Tag e profili > Tag > Sito.
- Passaggio 21. Selezionare Aggiungi. Viene visualizzato il tag del sito.

Configuration ▾ > Tags & Profiles ▾ > Tags

Policy **Site** RF AP

+ Add × Delete

- Passaggio 22. Digitare un nome e una descrizione per il tag del sito.

Add Site Tag

1

Name*

mesh-ap-site

Description

mesh-ap-site

AP Join Profile

mesh-ap-join-profile

2

- Passaggio 23. Selezionare il Profilo di join AP creato nel passaggio 16 dall'elenco a discesa Profilo di join AP.
- Passaggio 24. Nella parte inferiore del popup relativo al tag del sito, deselezionare la casella di controllo Abilita sito locale per abilitare l'elenco a discesa Profilo flessibile.
- Passaggio 35. Dall'elenco a discesa Profilo flessibile, selezionare il profilo flessibile che si desidera utilizzare per l'access point.

Add Site Tag

x

Name*

mesh-ap-site

Description

mesh-ap-site

AP Join Profile

mesh-ap-join-profile

Flex Profile

imarquez-FlexLocal

2

Control Plane Name

Enable Local Site

1

Cancel

Apply to Device

3

- Passaggio 36. Collegare l'access point alla rete e verificare che sia in modalità locale.
- Passaggio 37. Per verificare che l'access point sia in modalità locale, usare il comando capwap ap mode local.

L'access point deve essere in grado di trovare il controller, sia che si tratti di una trasmissione L2, di un'opzione DHCP 43, di una risoluzione DNS o di una configurazione manuale.

- Passaggio 38. L'access point si unisce al WLC. Accertarsi che sia elencato nell'elenco dei punti di accesso. Selezionare Configurazione > Wireless > Access Point > Tutti i punti di accesso.

All Access Points

Number of AP(s): 2

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mode	Operation Status
	2	✓			Flex+Bridge	Registered
	2	✓			Local	Registered

- Passaggio 39. Selezionare l'access point. Viene visualizzato il popup AP.
- Passaggio 40. Selezionare il tag del sito creato nel passo 22 in Generale > Tag > scheda Sito all'interno del popup AP, selezionare Aggiorna e Applica al dispositivo.

Edit AP

General **1** Interfaces High Availability Inventory Mesh Advanced

General		Version	
AP Name*	[input field]	Primary Software Version	16.12.1.139
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	[input field]	Predownloaded Version	N/A
Ethernet MAC	[input field]	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Flex-Bridge	IOS Version	16.12.1.139
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	[input field]
CleanAir NSI Key	[input field]	Static IP (IPv4/IPv6)	<input type="checkbox"/>
Tags		Time Statistics	
Policy	imarquez-FlexLocal	Up Time	4 days 3 hrs 2 mins 6 secs
Site	Mesh-AP-Tag 2	Controller Association Latency	20 secs
RF	default-rf-tag		

Cancel **3** Update & Apply to Device

- Passaggio 41. L'access point si riavvia e deve collegarsi nuovamente al WLC in modalità Flex + Bridge.

Questo metodo unisce innanzitutto l'access point in modalità locale (in cui non esegue l'autenticazione dot1x) per applicare il tag del sito con il profilo mesh e quindi passare all'access point in modalità bridge.

Per aggiungere un access point bloccato in modalità bridge (o Flex+Bridge), configurare i metodi predefiniti (autenticazione aaa dot1x predefinita locale e cred di autorizzazione aaa locale predefinita).

L'access point è quindi in grado di autenticarsi e successivamente è possibile assegnare i tag.

Verifica

Assicurarsi che la modalità AP sia visualizzata come Flex + Bridge, come mostrato nell'immagine.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 2

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mode	Operation Status
	2	✓	AIR-AP1542I-A-K9		Flex+Bridge	Registered

Eseguire questi comandi dalla CLI del WLC 9800 e cercare l'attributo AP Mode. Deve essere elencato come Flex+Bridge.

```
aaa authorization credential-download mesh-ap local
aaa authentication dot1x mesh-ap local
wireless profile mesh default-mesh-profile
  description "default mesh profile"
wireless tag site meshsite
  ap-profile meshapjoin
  no local-site
ap profile meshapjoin
  hyperlocation ble-beacon 0
  hyperlocation ble-beacon 1
  hyperlocation ble-beacon 2
  hyperlocation ble-beacon 3
  hyperlocation ble-beacon 4
mesh-profile mesh-profile
```

Risoluzione dei problemi

Verificare che i comandi aaa authentication dot1x default local e aaa authorization cred default local siano presenti. Sono necessarie se l'access point non è stato pre-aggiunto in modalità locale. Il dashboard 9800 principale dispone di un widget che visualizza gli access point che non possono essere collegati. Fare clic su di esso per ottenere un elenco di access point che non riescono a unirsi:

Monitoring > Wireless > AP Statistics

General Join Statistics

Clear Clear All

Number of AP(s): 2

Status "Is equal to" NOT JOINED

Status	Base Radio MAC	Ethernet MAC	AP Name	IP Address
✗	10b3.c622.5d80	2cf8.9b21.18b0	AP2CF8.9B21.18B0	87.66.46.211
✗	7070.8bb4.9200	2c33.110e.6b66	AP2C33.110E.6B66	87.66.46.211

Fare clic sull'access point specifico per visualizzare il motivo per cui non è stato unito. In questo caso, si verifica un problema di autenticazione (autenticazione AP in sospeso) perché il tag del sito non è stato assegnato all'access point.

Pertanto, lo switch 9800 non ha scelto il metodo di autenticazione/autorizzazione indicato per autenticare l'access point:

Join Statistics ✕			
General		Statistics	
Control DTLS Statistics		Configuration phase statistics	
DTLS Session request received	179	Configuration requests received	173
Established DTLS session	179	Successful configuration responses sent	4
Unsuccessful DTLS session	0	Unsuccessful configuration request processing	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success	Reason for last unsuccessful configuration attempt	Regulatory domain check failed
Time at last successful DTLS session	Thu, 19 Dec 2019 13:03:19 GMT	Time at last successful configuration attempt	Thu, 19 Dec 2019 12:36:10 GMT
Time at last unsuccessful DTLS session	NA	Time at last unsuccessful configuration attempt	NA
Join phase statistics		Data DTLS Statistics	
Join requests received	179	DTLS Session request received	0
Successful join responses sent	173	Established DTLS session	0
Unsuccessful join request processing	0	Unsuccessful DTLS session	0
Reason for last unsuccessful join attempt	Ap auth pending	Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful join attempt	Thu, 19 Dec 2019 12:36:10 GMT	Time at last successful DTLS session	NA
Time at last unsuccessful join attempt	NA	Time at last unsuccessful DTLS session	NA

Per una risoluzione dei problemi più avanzata, passare alla pagina [Risoluzione dei problemi](#) > Traccia radioattiva sull'interfaccia utente Web. Se si immette l'indirizzo MAC dell'access point, è possibile generare immediatamente un file per ottenere i log sempre attivi (a livello di avviso) dell'access point che tenta di unirsi. Fare clic su Start per abilitare il debug avanzato per l'indirizzo MAC. Alla successiva generazione dei log, generare i log, i log a livello di debug per il join AP, come mostrato.



Search Menu Items

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

Troubleshooting > Radioactive Trace

[← Back to Troubleshooting Menu](#)

Conditional Debug Global State: **Stopped**

[+ Add](#) [x Delete](#) [✓ Start](#) [■ Stop](#)

MAC/IP Address	Trace file	
<input type="checkbox"/> 2c33.110e.6b66	debugTrace_2c33.110e.6b66.txt ↓	▶ Generate

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

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).