

Configurazione dell'assegnazione dinamica della VLAN con ISE e Catalyst 9800 Wireless LAN Controller

Sommario

[Introduzione](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Assegnazione dinamica di VLAN con server RADIUS](#)

[Configurazione](#)

[Esempio di rete](#)

[Procedura di configurazione](#)

[Cisco ISE Configuration](#)

[Passaggio 1. Configurare il WLC di Catalyst come client AAA sul server Cisco ISE](#)

[Passaggio 2. Configurazione degli utenti interni su Cisco ISE](#)

[Passaggio 3. Configurare gli attributi RADIUS \(IETF\) utilizzati per l'assegnazione dinamica della VLAN](#)

[Configurazione dello switch per più VLAN](#)

[Catalyst 9800 WLC Configuration](#)

[Passaggio 1. Configurare il WLC con i dettagli del server di autenticazione](#)

[Passaggio 2. Configurazione delle VLAN](#)

[Passaggio 3. Configurare le WLAN \(SSID\)](#)

[Passaggio 4. Configurare il profilo dei criteri](#)

[Passaggio 5. Configurazione del tag dei criteri](#)

[Passaggio 6. Assegnare il codice di matricola a un punto di accesso](#)

[Flexconnect](#)

[Configurazione dello switch per più VLAN](#)

[Configurazione profilo criteri Flexconnect](#)

[Assegnare il profilo dei criteri Flexconnect a una WLAN e a un tag dei criteri](#)

[Configurazione del profilo Flex](#)

[Configurazione tag Flex Site](#)

[Assegnare il criterio e il tag del sito a un punto di accesso.](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare Catalyst 9800 WLC e Cisco ISE per assegnare una LAN wireless (WLAN).

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscere a fondo le funzionalità di Wireless LAN Controller (WLC) e Lightweight Access Point (LAP).
- Avere una conoscenza funzionale del server AAA, ad esempio Identity Services Engine (ISE).
- Conoscere a fondo le reti wireless e i problemi di sicurezza wireless.
- Conoscenza funzionale dell'assegnazione di VLAN (Virtual LAN) dinamiche.
- Conoscenze base di Controllo e provisioning per CAPWAP (Wireless Access Point).

Componenti usati

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

- Cisco Catalyst 9800 WLC (Catalyst 9800-CL) con firmware versione 16.12.4a.
- Cisco serie 2800 LAP in modalità locale.
- Suppliant Windows 10 nativo.
- Cisco ISE con versione 2.7.
- Cisco serie 3850 switch con firmware versione 16.9.6.

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

Assegnazione dinamica di VLAN con server RADIUS

In questo documento viene descritto il concetto di assegnazione dinamica di VLAN e viene spiegato come configurare il controller LAN wireless Catalyst 9800 (WLC) e Cisco Identity Service Engine (ISE) in modo da assegnare una LAN wireless (WLAN) ai client wireless.

Nella maggior parte dei sistemi WLAN (Wireless Local Area Network), ogni WLAN dispone di un criterio statico che viene applicato a tutti i client associati a un SSID (Service Set Identifier). Sebbene potente, questo metodo presenta delle limitazioni in quanto richiede ai client di associarsi a SSID diversi per ereditare criteri QoS e di sicurezza diversi.

Tuttavia, la soluzione Cisco WLAN supporta le reti di identità. In questo modo la rete può annunciare un singolo SSID e consentire a utenti specifici di ereditare criteri QoS o di sicurezza diversi in base alle credenziali utente.

L'assegnazione dinamica della VLAN è una di queste funzionalità che permette a un utente wireless di accedere a una VLAN specifica in base alle credenziali fornite dall'utente. L'attività di

assegnazione degli utenti a una VLAN specifica viene gestita da un server di autenticazione RADIUS, ad esempio Cisco ISE. Questa funzione può essere utilizzata, ad esempio, per fare in modo che l'host wireless rimanga sulla stessa VLAN su cui si sposta all'interno della rete di un campus.

Pertanto, quando un client tenta di associarsi a un LAP registrato con un controller, il WLC passa le credenziali dell'utente al server RADIUS per la convalida. Una volta completata l'autenticazione, il server RADIUS passa all'utente alcuni attributi IETF (Internet Engineering Task Force). Questi attributi RADIUS determinano l'ID VLAN che deve essere assegnato al client wireless. L'SSID del client non ha importanza perché l'utente è sempre assegnato a questo ID VLAN predeterminato.

Gli attributi utente RADIUS utilizzati per l'assegnazione dell'ID VLAN sono:

- IETF 64 (Tipo tunnel) - Impostare questa opzione su VLAN.
- IETF 65 (Tunnel Medium Type) - Impostato su 802.
- IETF 81 (Tunnel Private Group ID) - Imposta su VLAN ID.

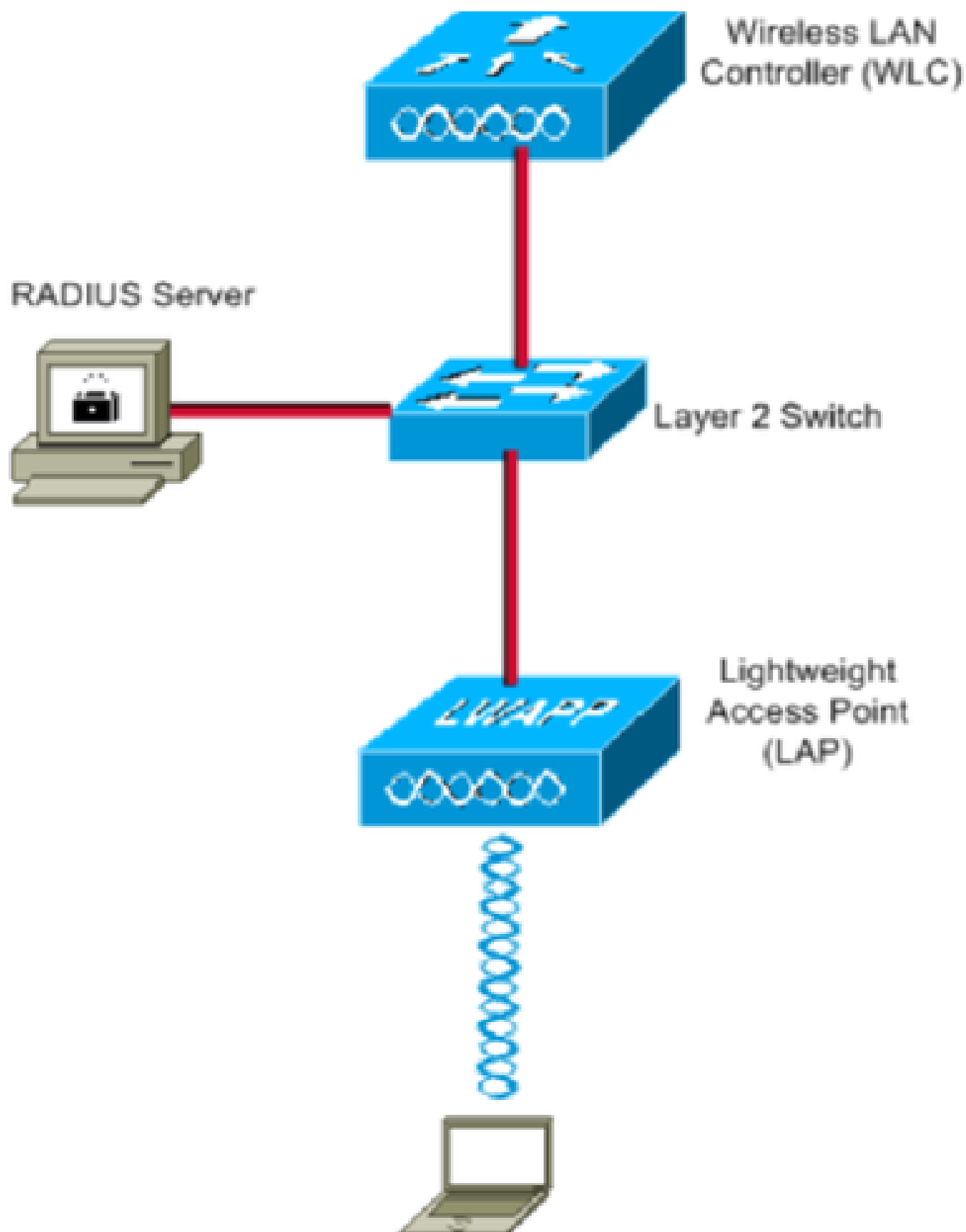
L'ID VLAN è a 12 bit e assume un valore compreso tra 1 e 4094 inclusi. Poiché Tunnel-Private-Group-ID è di tipo stringa, come definito nella [RFC2868](#) per l'utilizzo con IEEE 802.1X, il valore intero dell'ID VLAN viene codificato come stringa. Quando questi attributi del tunnel vengono inviati, è necessario immetterli nel campo Tag.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Il documento usa la seguente configurazione di rete:



Di seguito sono riportati i dettagli di configurazione dei componenti utilizzati nel diagramma:

- L'indirizzo IP del server Cisco ISE (RADIUS) è 10.10.1.24.
- L'indirizzo dell'interfaccia di gestione del WLC è 10.10.1.17.
- Il server DHCP interno sul controller viene utilizzato per assegnare l'indirizzo IP ai client

wireless.

- Nel documento viene usato 802.1x con PEAP come meccanismo di sicurezza.
- Nell'intera configurazione, viene utilizzata la VLAN102. Il nome utente smith -102 è configurato per essere inserito nella VLAN102 dal server RADIUS.

Procedura di configurazione

Questa configurazione è suddivisa in tre categorie:

- Cisco ISE Configuration.
- Configurare lo switch per più VLAN.
- Catalyst 9800 WLC Configuration.

Cisco ISE Configuration

Questa configurazione richiede i seguenti passaggi:

- Configurare il Catalyst WLC come client AAA sul server Cisco ISE.
- Configurare gli utenti interni su Cisco ISE.
- Configurare gli attributi RADIUS (IETF) utilizzati per l'assegnazione dinamica della VLAN su Cisco ISE.

Passaggio 1. Configurare il WLC di Catalyst come client AAA sul server Cisco ISE

In questa procedura viene spiegato come aggiungere il WLC come client AAA sul server ISE in modo che il WLC possa passare le credenziali dell'utente ad ISE.

Attenersi alla seguente procedura:

1. Dalla GUI di ISE, selezionare **Administration > Network Resources > Network Devices** e passare a **Add**.
2. Completare la configurazione con l'indirizzo IP di gestione WLC e il segreto condiviso RADIUS tra WLC e ISE, come mostrato nell'immagine:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MD

Network Devices List > **New Network Device**

Network Devices

* Name

Description

IP Address * IP : /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

☒ **RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol

* Shared Secret

Use Second Shared Secret ☐

CoA Port

Passaggio 2. Configurazione degli utenti interni su Cisco ISE

In questa procedura viene spiegato come aggiungere gli utenti al database interno di Cisco ISE.

Attenersi alla seguente procedura:

1. Dalla GUI di ISE, selezionare **Administration > Identity Management > Identities** e passare a **Add**.
2. Completare la configurazione con il nome utente, la password e il gruppo di utenti, come mostrato nell'immagine:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Network Access Users List > New Network Access User

Users

Latest Manual Network Scan Results

Network Access User

* Name

Status ☒ Enabled

Email

Passwords

Password Type:

Password

Enable Password

User Information

First Name

Last Name

Account Options

Description

Change password on next login ☐

Account Disable Policy

☐ Disable account if date exceeds

(yyyy-mm-dd)

User Groups

Passaggio 3. Configurare gli attributi RADIUS (IETF) utilizzati per l'assegnazione dinamica della VLAN

In questa procedura viene illustrato come creare un profilo di autorizzazione e un criterio di autenticazione per gli utenti wireless.

Attenersi alla seguente procedura:

1. Dalla GUI di ISE, selezionare **Policy > Policy Elements > Results > Authorization > Authorization profiles** e passare **Add a** per creare un nuovo profilo.
2. Completare la configurazione del profilo di autorizzazione con le informazioni sulla VLAN per il gruppo corrispondente. In questa immagine vengono illustrate le impostazioni di configurazione del **jonathga-VLAN-102** gruppo.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > jonathga-VLAN-102

Authorization Profile

* Name: jonathga-VLAN-102

Description: Dynamic-Vlan-Assignment

Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: ☐

Track Movement: ☐

Passive Identity Tracking: ☐

Common Tasks

☐ DACL Name

☐ ACL (Filter-ID)

☐ Security Group

☒ VLAN Tag ID 1 Edit Tag ID/Name 102

Advanced Attributes Settings

Select an item =

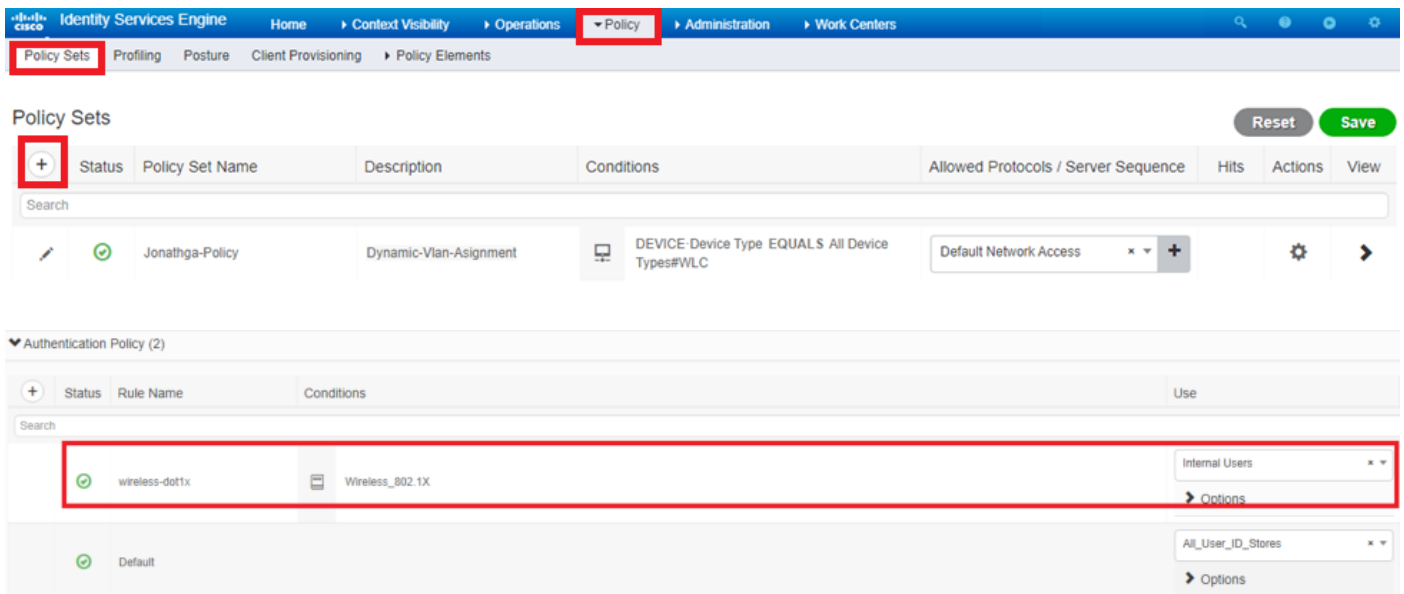
Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:102
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Save Reset

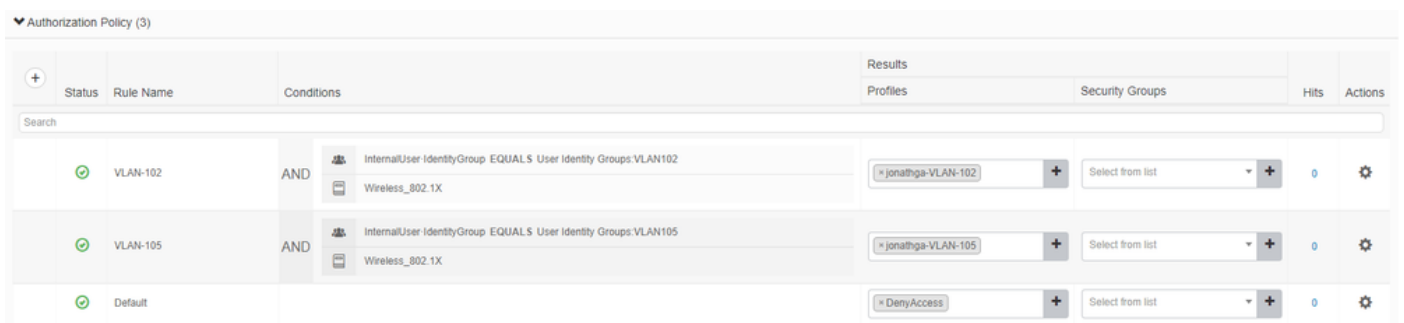
Dopo aver configurato i profili di autorizzazione, è necessario creare un criterio di autenticazione per gli utenti wireless. È possibile utilizzare un nuovo Custom criterio o modificare il set di Default criteri. In questo esempio viene creato un profilo personalizzato.

3. Individuare Policy > Policy Sets e selezionare Add per creare un nuovo criterio, come mostrato nell'immagine:



A questo punto è necessario creare criteri di autorizzazione per gli utenti per assegnare un profilo di autorizzazione corrispondente in base all'appartenenza ai gruppi.

5. Aprire la **Authorization policy** sezione e creare i criteri per soddisfare tale requisito, come mostrato nell'immagine:



Configurazione dello switch per più VLAN

Per consentire l'uso di più VLAN sullo switch, è necessario usare questi comandi per configurare la porta dello switch connessa al controller:

```
<#root>
```

```
Switch(config-if)#
```

```
switchport mode trunk
```

```
<#root>
```

```
Switch(config-if)#
```

switchport trunk encapsulation dot1q

 Nota: Per impostazione predefinita, la maggior parte degli switch consente tutte le VLAN create sullo switch tramite la porta trunk. Se allo switch è collegata una rete cablata, è possibile applicare la stessa configurazione alla porta dello switch che si connette alla rete cablata. Ciò consente la comunicazione tra le stesse VLAN nella rete cablata e wireless.

Catalyst 9800 WLC Configuration

Questa configurazione richiede i seguenti passaggi:

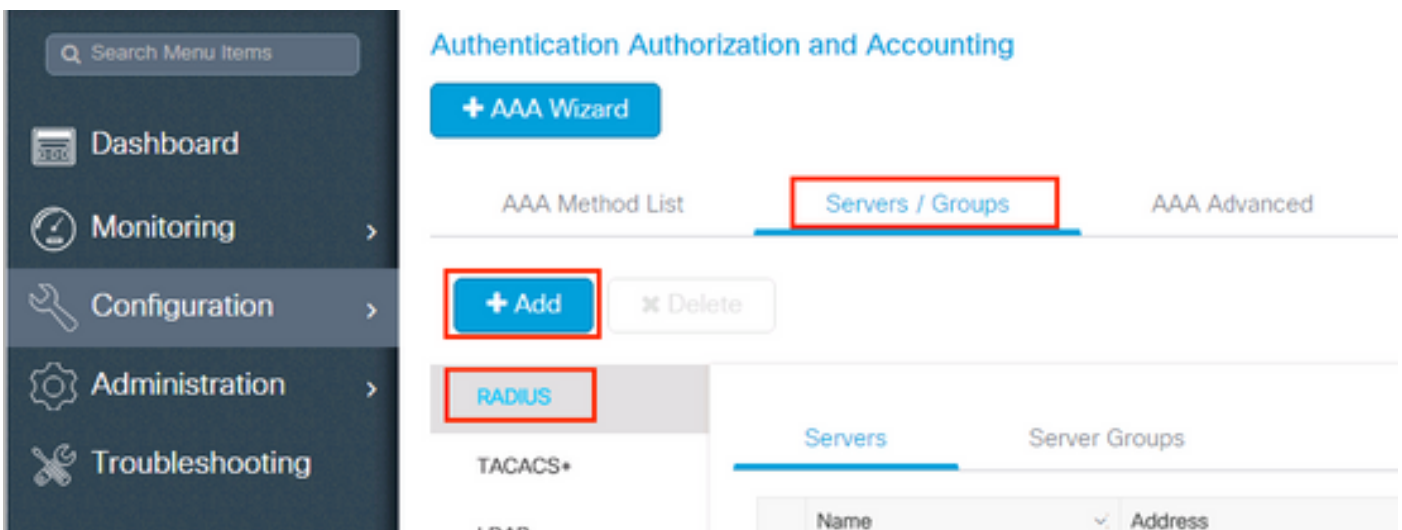
- Configurare il WLC con i dettagli del server di autenticazione.
- Configurare le VLAN.
- Configurare le WLAN (SSID).
- Configurare il profilo dei criteri.
- Configurare il tag Criteri.
- Assegnare il tag Policy a un punto di accesso.

Passaggio 1. Configurare il WLC con i dettagli del server di autenticazione

È necessario configurare il WLC in modo che possa comunicare con il server RADIUS per autenticare i client.

Attenersi alla seguente procedura:

1. Dalla GUI del controller, individuare **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** e immettere le informazioni sul server RADIUS, come mostrato nell'immagine:



Create AAA Radius Server

Name*
Cisco-ISE

Server Address*
10.10.1.24

PAC Key
☐

Key Type
Clear Text

Key* ⓘ

Confirm Key*

Auth Port
1812

Acct Port
1813

Server Timeout (seconds)
1-1000

Retry Count
0-100

Support for CoA
ENABLED ☒ ⓘ

CoA Server Key Type
Clear Text

CoA Server Key ⓘ

Confirm CoA Server Key

Automate Tester
☐

Cancel

Apply to Device

2. Per aggiungere il server RADIUS a un gruppo RADIUS, passare alla **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** sezione come mostrato nell'immagine:

Create AAA Radius Server Group ✕

Name*

ISE-SERVER

Group Type

RADIUS

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

☐ DISABLED

Source Interface VLAN ID

none

Available Servers

server-2019

Assigned Servers

Cisco-ISE

Cancel

Apply to Device

3. Per creare un elenco di metodi di autenticazione, passare **Configuration > Security > AAA > AAA Method List > Authentication > + Add** a come mostrato nelle immagini:

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List

Servers / Groups

General

Authentication

Authorization

+ Add

✕ Del

Name

Quick Setup: AAA Authentication

Method List Name*

ISE-SERVER

Type*

dot1x

Group Type

group

Fallback to local

☐

Available Server Groups

radius
ldap
tacacs+
radgrp_SykesLab
server2019
tacacgrp_SykesLab

>
<
>>
<<

Assigned Server Groups

ISE-SERVER

⏮
⏪
⏩
⏭

Cancel

Apply to Device

Passaggio 2. Configurazione delle VLAN

In questa procedura viene spiegato come configurare le VLAN sul Catalyst 9800 WLC. Come spiegato in precedenza in questo documento, l'ID VLAN specificato nell'attributo Tunnel-Private-Group ID del server RADIUS deve esistere anche nel WLC.

Nell'esempio, l'utente smith-102 viene specificato con il Tunnel-Private-Group ID of 102 (VLAN =102) sul server RADIUS.

1. Passare a, **Configuration > Layer2 > VLAN > VLAN > + Add** come mostrato nell'immagine:

Q Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

VLAN

SVI

VLAN

VLAN Group

+ Add

× Delete

	VLAN ID	Name
☐	1	default
☐	100	VLAN
☐	210	VLAN
☐	2602	VLAN

2. Immettere le informazioni necessarie come illustrato nell'immagine:

Create VLAN

Create a single VLAN

VLAN ID*

102

Name

State

ACTIVATED

IGMP Snooping

DISABLED

ARP Broadcast

DISABLED

Port Members

Available (2)

Gi1

Gi2

Associated (0)

No Associated Members

Create a range of VLANs

VLAN Range*

-

(Ex:5-7)

Cancel

Apply to Device

 Nota: Se non si specifica un nome, alla VLAN viene assegnato automaticamente il nome VLAN XXXX, dove XXXX è l'ID della VLAN.

Ripetere i passaggi 1 e 2 per tutte le VLAN necessarie, quindi continuare con il passaggio 3.

3. Verificare che le VLAN siano consentite nelle interfacce dati.

- Se è in uso un canale porta, passare a **Configuration > Interface > Logical > PortChannel name > General**. Se la configurazione è stata visualizzata al termine della **Allowed VLAN = All** configurazione. In questo caso, aggiungere le VLAN necessarie e **Allowed VLAN = VLANs** quindi selezionare **Update & Apply to Device**.
- Se il canale della porta non è in uso, passare a **Configuration > Interface > Ethernet > Interface Name > General**. Se la configurazione è stata visualizzata al termine della **Allowed VLAN = All** configurazione. In questo caso, aggiungere le VLAN necessarie e **Allowed VLAN = VLANs** quindi selezionare **Update & Apply to Device**.

Nelle immagini viene mostrata la configurazione relativa all'impostazione dell'interfaccia se si usano tutti gli ID VLAN o ID VLAN specifici.

General	Advanced
Interface	GigabitEthernet3
Description	(1-200 Characters)
Admin Status	UP 
Port Fast	disable ▼
Enable Layer 3 Address	☐ DISABLED
Switchport Mode	trunk ▼
Allowed Vlan	☒ All ☐ Vlan IDs
Native Vlan	▼

General

Advanced

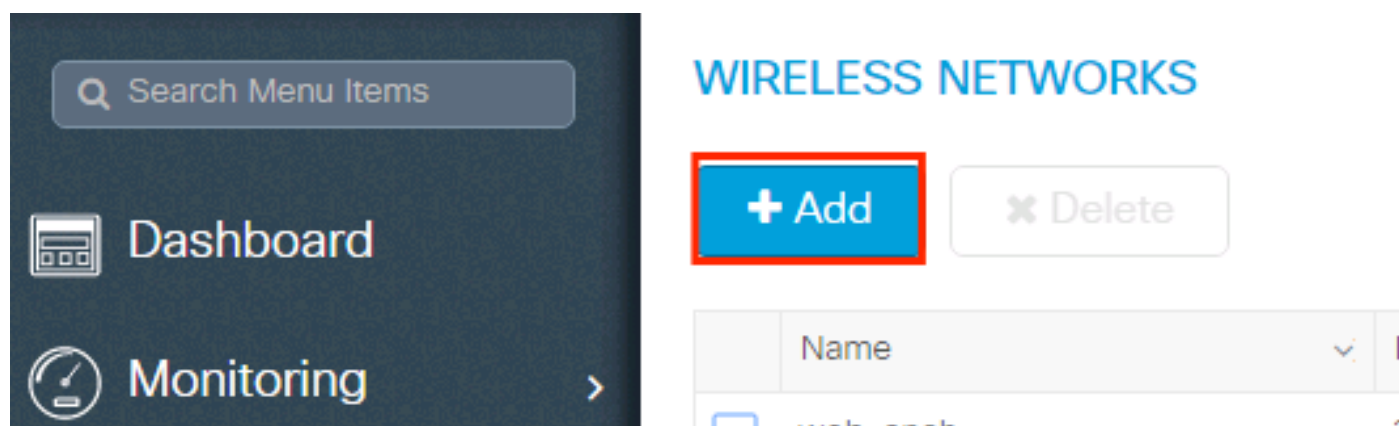
Interface	GigabitEthernet1	
Description		(1-200 Characters)
Speed	1000 ▼	
Admin Status	UP 	
Enable Layer 3 Address	☐ DISABLED	
Switchport Mode	trunk ▼	
Allowed Vlan	☐ All ☒ Vlan IDs	
Vlan IDs	551,102,105	(e.g. 1,2,4,6-10)
Native Vlan	551 ▼	

Passaggio 3. Configurare le WLAN (SSID)

In questa procedura viene spiegato come configurare le WLAN nel WLC.

Attenersi alla seguente procedura:

1. Per creare la WLAN. Passare alla **Configuration > Wireless > WLANs > + Add** rete e configurarla come necessario, come mostrato nell'immagine:



2. Immettere le informazioni sulla WLAN come mostrato nell'immagine:

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. A red rectangle highlights the following fields:

- Profile Name*: Dinamyc-VLAN
- SSID*: Dinamyc-VLAN
- WLAN ID*: 6
- Status: ENABLED (with a green toggle switch)

Other visible fields include:

- Radio Policy: All (dropdown)
- Broadcast SSID: ENABLED (with a green toggle switch)

At the bottom, there are two buttons: 'Cancel' and 'Apply to Device' (the latter is highlighted with a red rectangle).

3. Passare alla Security scheda e selezionare il metodo di protezione necessario. In questo caso, WPA2 + 802.1x come mostrato nelle immagini:

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. The 'Layer2' sub-tab is also selected. A red rectangle highlights the 'Layer 2 Security Mode' dropdown menu, which is set to 'WPA + WPA2'.

Other visible fields include:

- MAC Filtering: ☐
- Protected Management Frame: ☐
- PMF: Disabled (dropdown)
- WPA Parameters: ☐
- WPA Review: ☐
- Fast Transition: Adaptive Enab... (dropdown)
- Over the DS: ☒
- Reassociation Timeout: 20 (input field)

At the bottom, there are two buttons: 'Cancel' and 'Save & Apply to Device'.

Add WLAN

PMF Disabled

WPA Parameters

WPA Policy ☐

WPA2 Policy ☒

WPA2 Encryption

AES(CCMP128)	☒
CCMP256	☐
GCMP128	☐
GCMP256	☐

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

Dalla **Security** > AAA scheda, selezionare il metodo di autenticazione creato al passaggio 3 dalla **Configure the WLC with the Details of the Authentication Server** sezione come mostrato nell'immagine:

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List ISE-SERVER ⓘ

Local EAP Authentication ☐

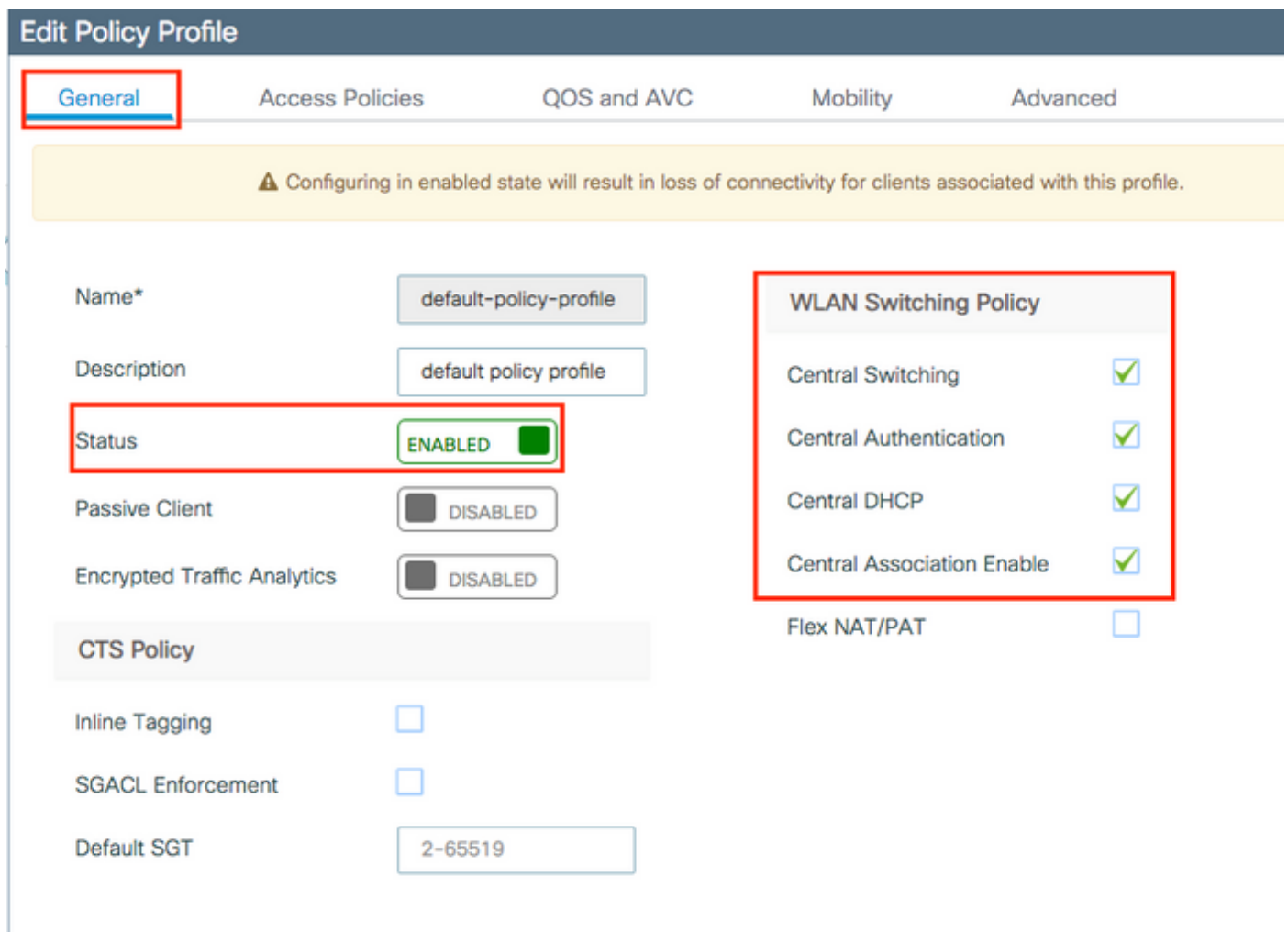
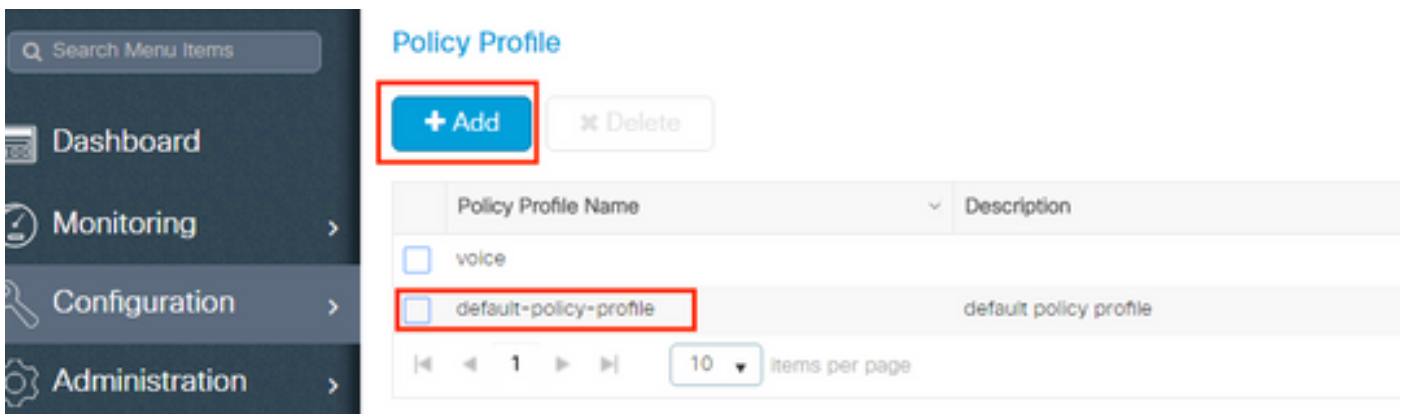
Cancel Apply to Device

Passaggio 4. Configurare il profilo dei criteri

In questa procedura viene spiegato come configurare il profilo dei criteri nel WLC.

Attenersi alla seguente procedura:

1. Individuare **Configuration > Tags & Profiles > Policy Profile** e configurare il file `default-policy-profile` o crearne uno nuovo, come mostrato nelle immagini:



2. Dalla **Access Policies** scheda assegnare la VLAN a cui sono assegnati i client wireless quando si connettono a questa WLAN per impostazione predefinita, come mostrato nell'immagine:

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Local Profiling

HTTP TLV Caching

☐

RADIUS Profiling

☐

DHCP TLV Caching

☐

Local Subscriber Policy Name

Search or Select

▼

VLAN

VLAN/VLAN Group

VLAN2602

▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select

▼

IPv6 ACL

Search or Select

▼

URL Filters

Pre Auth

Search or Select

▼

Post Auth

Search or Select

▼

 Nota: Nell'esempio fornito, dopo l'autenticazione, il server RADIUS deve assegnare un client wireless a una VLAN specifica. Pertanto, la VLAN configurata nel profilo della policy può essere una VLAN buca nera, il server RADIUS ignora questo mapping e assegna l'utente che passa attraverso tale WLAN alla VLAN specificata nel campo user Tunnel-Group-Private-ID nel server RADIUS.

3. Dalla **Advance** scheda, abilitare la casella di controllo per **Allow AAA Override** ignorare la configurazione WLC quando il server RADIUS restituisce gli attributi necessari per posizionare il client sulla VLAN corretta, come mostrato nell'immagine:

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

1800

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

☒

60

DHCP

IPv4 DHCP Required

☒

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

☒

NAC State

☐

Policy Name

default-aaa-policy x

Fabric Profile

☐

Search or Select

Umbrella Parameter Map

Not Configured

mDNS Service Policy

default-mdns-service

Clear

WLAN Flex Policy

VLAN Central Switching

☐

Split MAC ACL

Search or Select

Air Time Fairness Policies

2.4 GHz Policy

Search or Select

5 GHz Policy

Search or Select

Cancel

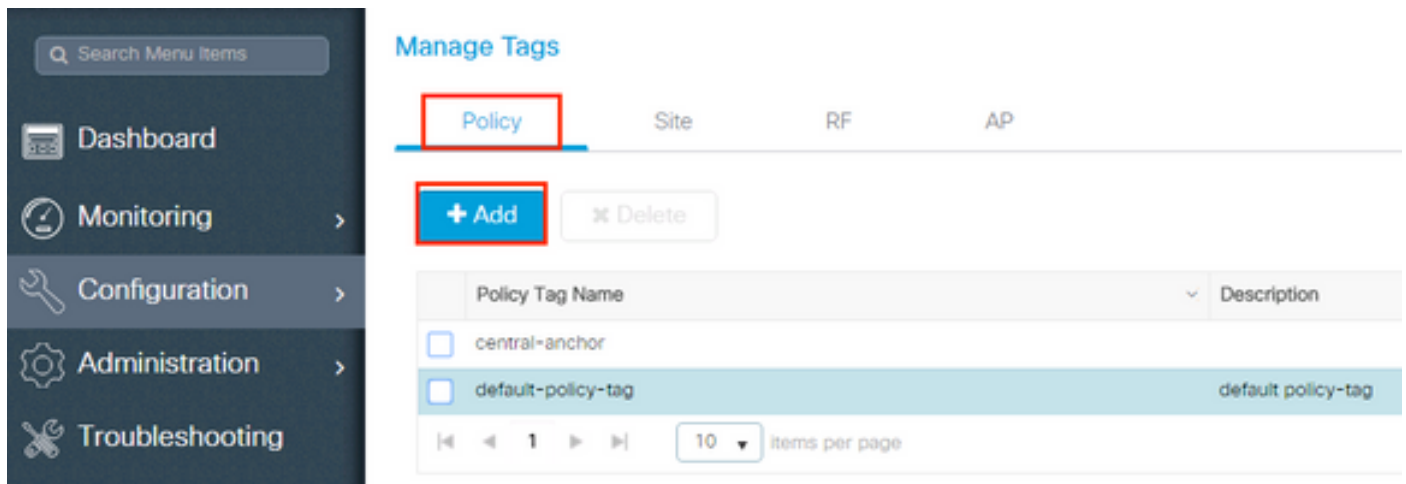
Update & Apply to Device

Passaggio 5. Configurazione del tag dei criteri

In questa procedura viene spiegato come configurare il tag Policy nel WLC.

Attenersi alla seguente procedura:

1. Se necessario, individuare **Configuration > Tags & Profiles > Tags > Policy** e aggiungere un nuovo file, come mostrato nell'immagine:



2. Aggiungere un nome al tag dei criteri e selezionare +Add, come mostrato nell'immagine:

3. Collegare il profilo WLAN al profilo di policy desiderato, come mostrato nelle immagini:

Add Policy Tag

Name*

Dynamic-VLAN

Description

Enter Description

WLAN-POLICY Maps: 0

+ Add

× Delete

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile*

Dinamyc-VLAN

Policy Profile*

default-policy-profil

×

✓

Add Policy Tag

Name*

Dynamic-VLAN

Description

Enter Description

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
☐ Dinamyc-VLAN	default-policy-profile

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

RLAN-POLICY Maps: 0

Cancel

Apply to Device

Passaggio 6. Assegnare il tag di criterio a un punto di accesso

In questa procedura viene spiegato come configurare il tag Policy nel WLC.

Attenersi alla seguente procedura:

1. Individuare **Configuration > Wireless > Access Points > AP Name > General Tags** e assegnare il tag di criterio appropriato, quindi selezionare **Update & Apply to Device** come mostrato nell'immagine:

Edit AP

General Interfaces High Availability Inventory ICap Advanced

General

AP Name* AP2802I-B-K9

Location* default location

Base Radio MAC 10b3.d677.a8c0

Ethernet MAC 084f.a9a2.8ed4

Admin Status **ENABLED**

AP Mode Local

Operation Status Registered

Fabric Status Disabled

LED State **ENABLED**

LED Brightness Level 8

CleanAir NSI Key

Tags

Policy Dynamic-VLAN

Site default-site-tag

Version

Primary Software Version 16.12.4.31

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.1.2.4

IOS Version 16.12.4.31

Mini IOS Version 0.0.0.0

IP Config

CAPWAP Preferred Mode IPv4

DHCP IPv4 Address 10.10.102.101

Static IP (IPv4/IPv6)

Time Statistics

Up Time 0 days 0 hrs 4 mins 52 secs

Controller Association Latency 1 min 36 secs

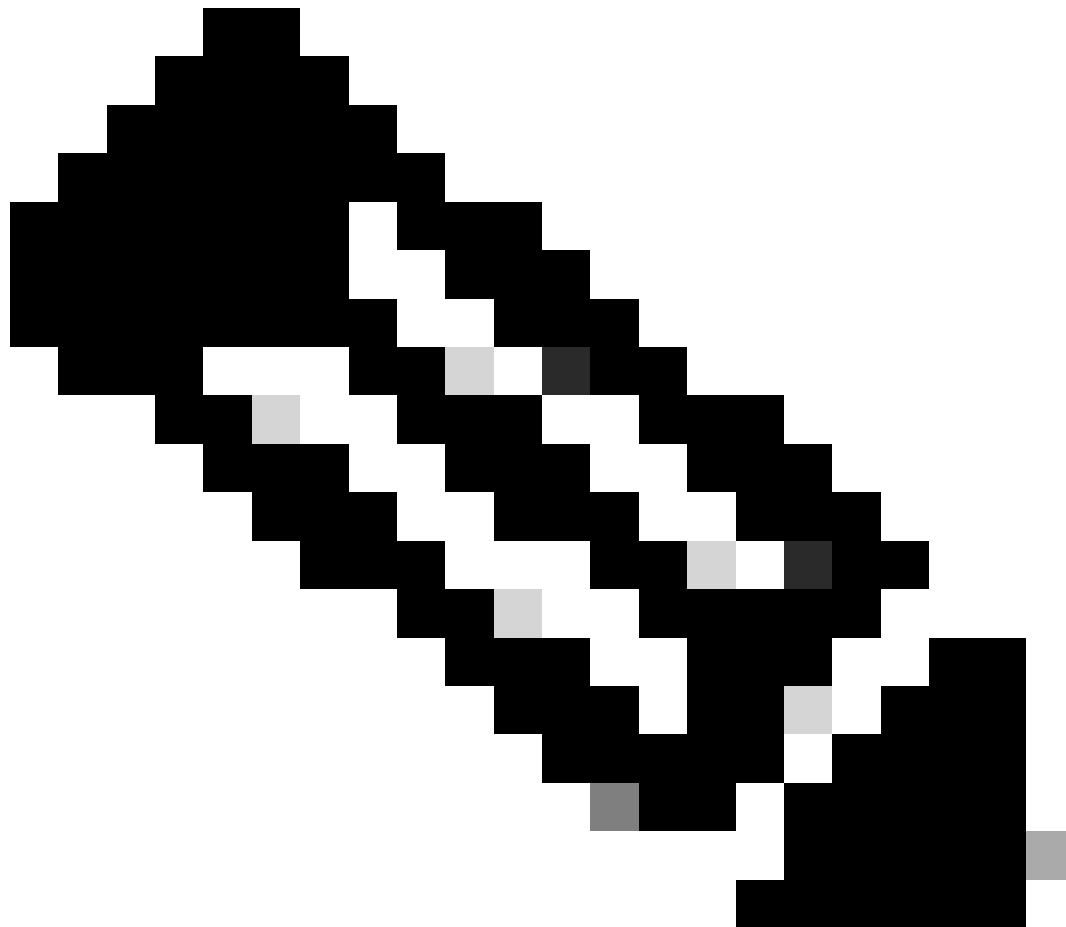
Cancel **Update & Apply to Device**

⚠ Attenzione: Tenere presente che la modifica del tag dei criteri in un access point comporta la disconnessione e la riconnessione dell'access point dal WLC.

Flexconnect

La funzione Flexconnect consente ai punti di accesso di inviare i dati dei client wireless in uscita tramite la porta LAN del punto di accesso quando sono configurati come trunk. Questa modalità, nota come switching locale Flexconnect, consente all'access point di separare il traffico dei client assegnando tag alle VLAN separate dall'interfaccia di gestione. In questa sezione vengono fornite

istruzioni su come configurare l'assegnazione della VLAN dinamica per lo scenario di switching locale.

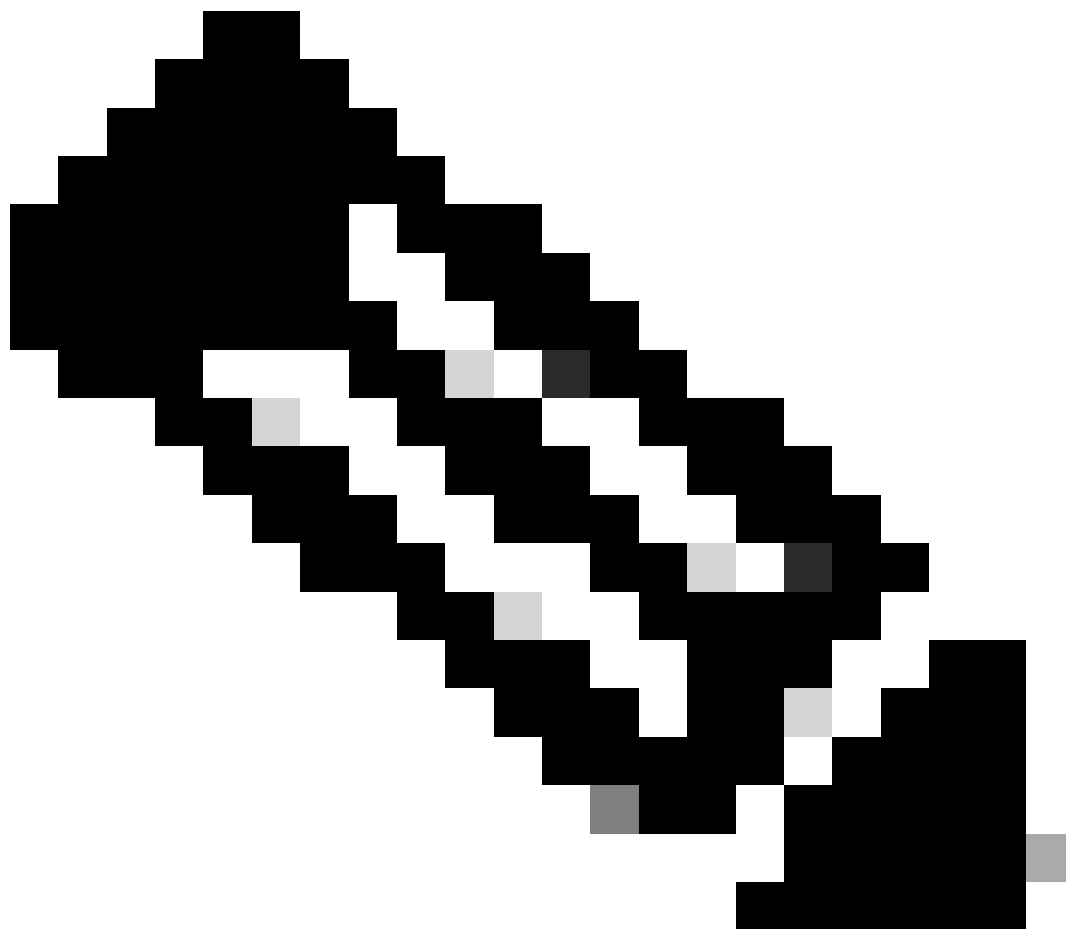


Nota: I passaggi descritti nella sezione precedente sono applicabili anche allo scenario Flexconnect. Per completare la configurazione di Flexconnect, effettuare le operazioni aggiuntive descritte in questa sezione.

Configurazione dello switch per più VLAN

Per consentire l'uso di più VLAN sullo switch, è necessario usare i comandi successivi per configurare la porta dello switch collegata all'access point:

1. Switch(config-if)#switchport mode trunk
2. Switch(config-if)#switchport trunk encapsulation dot1q



Nota: Per impostazione predefinita, la maggior parte degli switch consente tutte le VLAN create sullo switch tramite la porta trunk.

Profilo criteri Flexconnect configurazione

1. Passare a Configurazione > Tag e profili > Profilo criterio > +Aggiungi e creare un nuovo criterio.
2. Aggiungere il nome e deselezionare la casella di controllo Cambio centralizzato e DHCP centrale. Con questa configurazione, il controller gestisce l'autenticazione del client, mentre il punto di accesso FlexConnect commuta i pacchetti di dati del client e DHCP localmente.

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

⚠

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Name*

Flexconnect-Policy

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

Nota: A partire dal codice 17.9.x, l'aspetto del profilo della policy è stato aggiornato come illustrato nella figura.

WLAN Switching Policy

Central Switching

☐ DISABLED

Central Authentication

ENABLED ☒

Central DHCP

☐ DISABLED

Flex NAT/PAT

☐ DISABLED

3. Dalla scheda Criteri di accesso assegnare la VLAN a cui sono assegnati i client wireless quando si connettono a questa WLAN per impostazione predefinita.

Edit Policy Profile

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

Search or Select ▼

VLAN

VLAN/VLAN Group

103 ▼

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

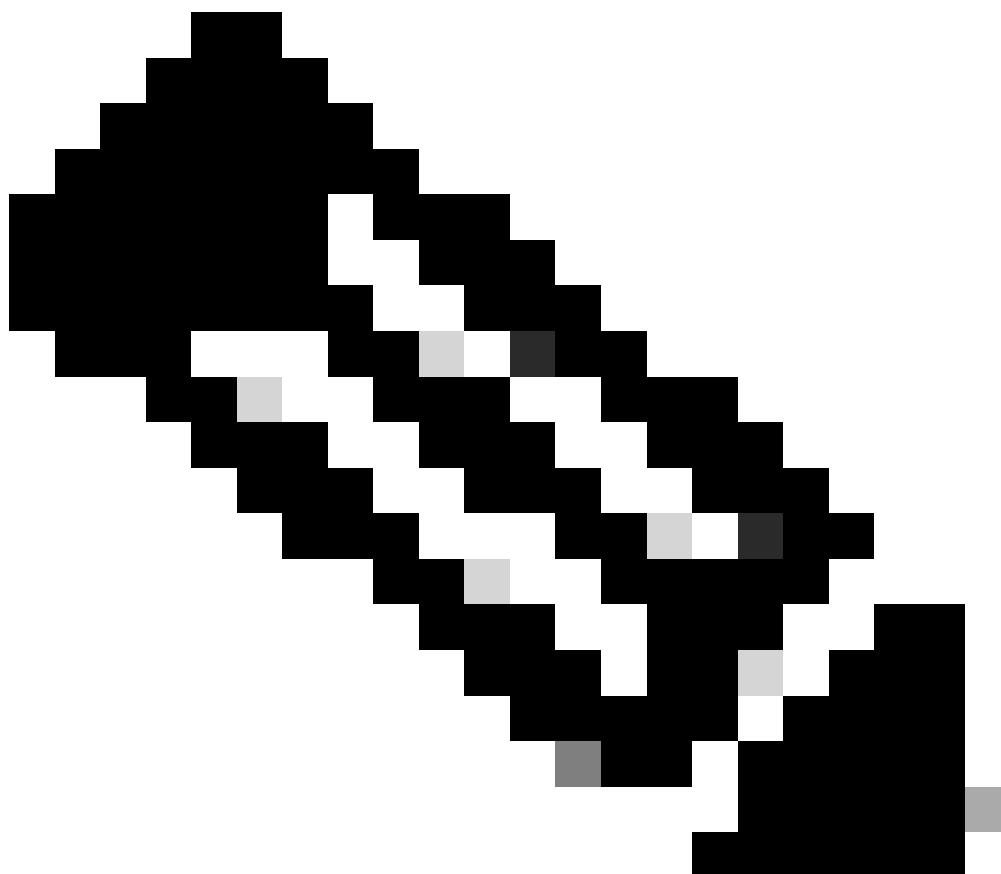
URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼



Nota: la VLAN configurata in questo passaggio non deve necessariamente essere presente nell'elenco delle VLAN del WLC. Le VLAN necessarie vengono aggiunte successivamente al Flex-Profile, che crea le VLAN sull'access point stesso.

4. Dalla scheda Advance, abilitare la casella di controllo Allow AAA Override per sostituire le configurazioni WLC con il server RADIUS.

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

IPv4 DHCP Required ☒

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override ☒

Fabric Profile ☐

Umbrella Parameter Map

mDNS Service Policy [Clear](#)

WLAN Flex Policy

VLAN Central Switching ☐

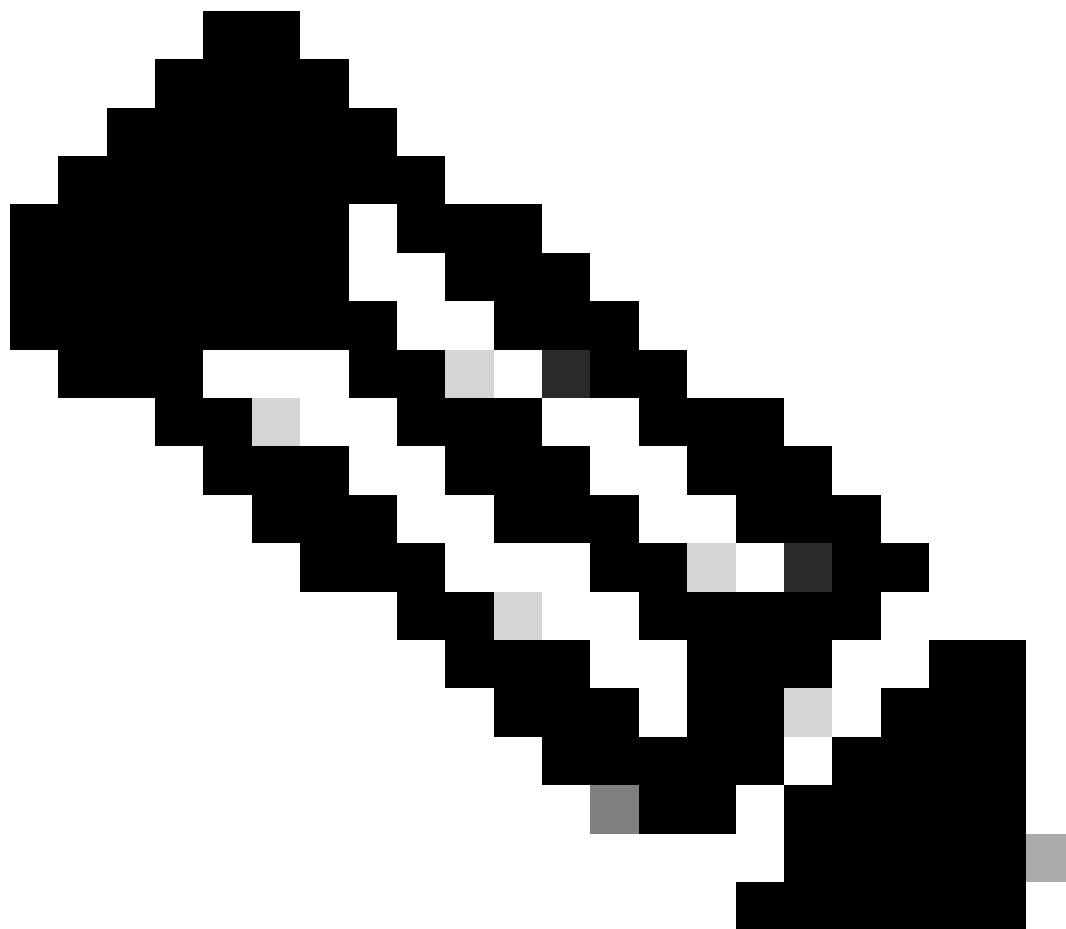
Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

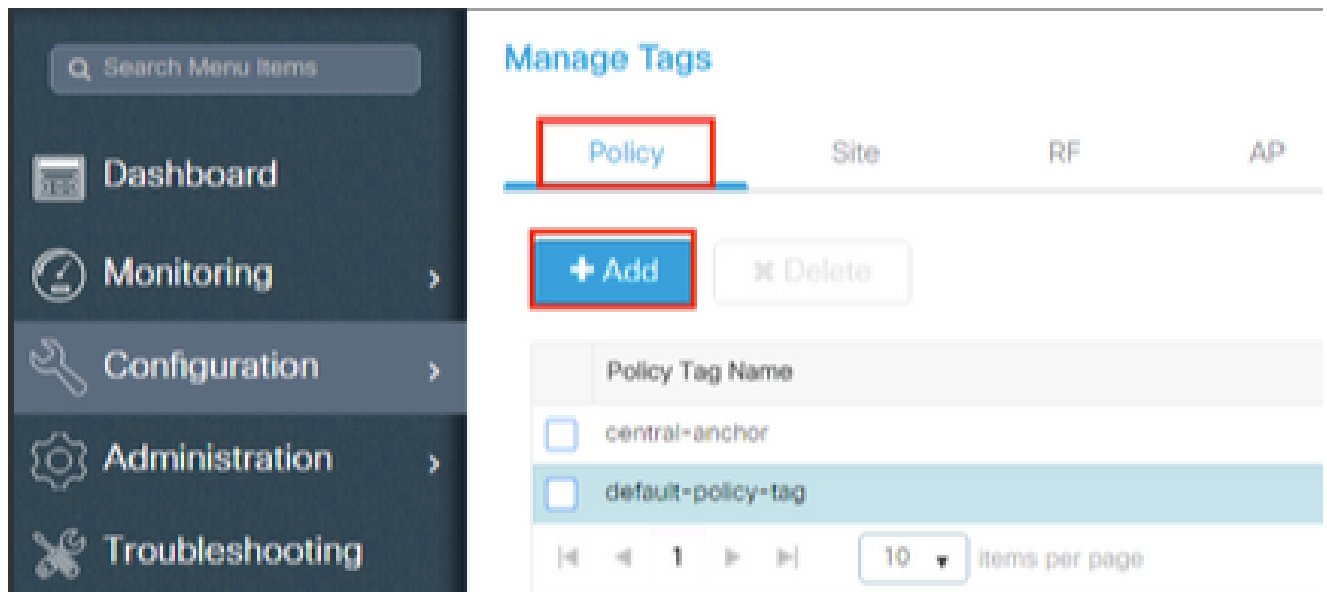
5 GHz Policy

Assegnare il profilo dei criteri Flexconnect a una WLAN e a un tag dei criteri

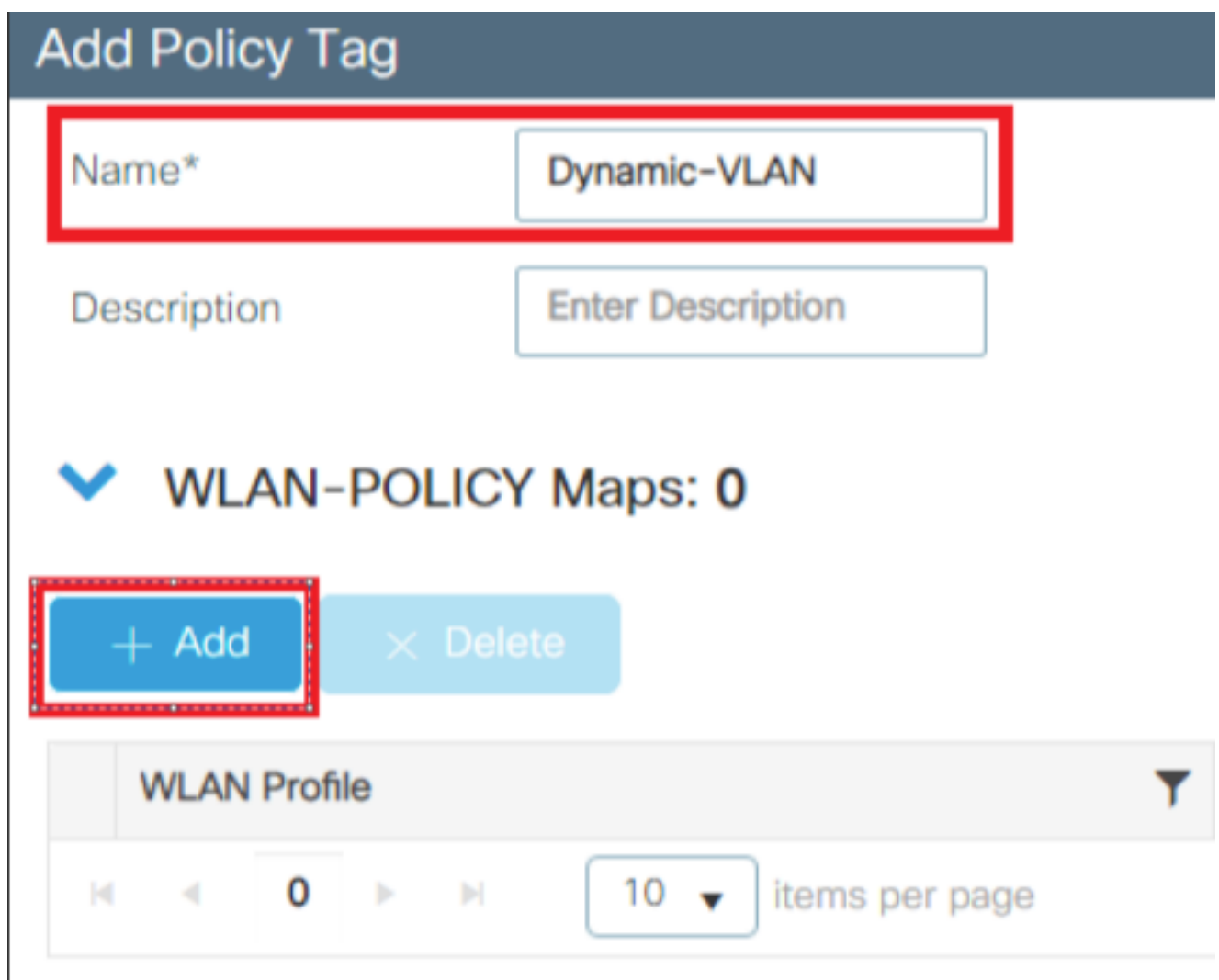


Nota: Un tag di policy viene utilizzato per collegare la WLAN al profilo di policy. È possibile creare un nuovo tag o utilizzare il tag predefinito.

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



2. Immettere un nome per il tag del criterio e fare clic sul pulsante "aggiungi".



3. Associare il profilo WLAN al profilo di policy desiderato.

Add Policy Tag

Name*

Dynamic-VLAN

Description

Enter Description

▼

WLAN-POLICY Maps: 0

+ Add

× Delete

WLAN Profile

▼

Policy Profile

▼

◀◀

0

▶▶

10

items per page

No items to display

Map WLAN and Policy

WLAN Profile*

Dinamyc-VLAN

▼

Policy Profile*

Flexconnect-Policy

▼

×

✓

➤

RLAN-POLICY Maps: 0

↺ Cancel

📄 Apply to Device

4. Fare clic sul pulsante Applica al dispositivo.

Add Policy Tag

Name*

Dynamic-VLAN

Description

Enter Description

▼

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile

▼

Policy Profile

▼

☐

Dinamyc-VLAN

Flexconnect-Policy

◀◀

1

▶▶

10

items per page

1 - 1 of 1 items

➤

RLAN-POLICY Maps: 0

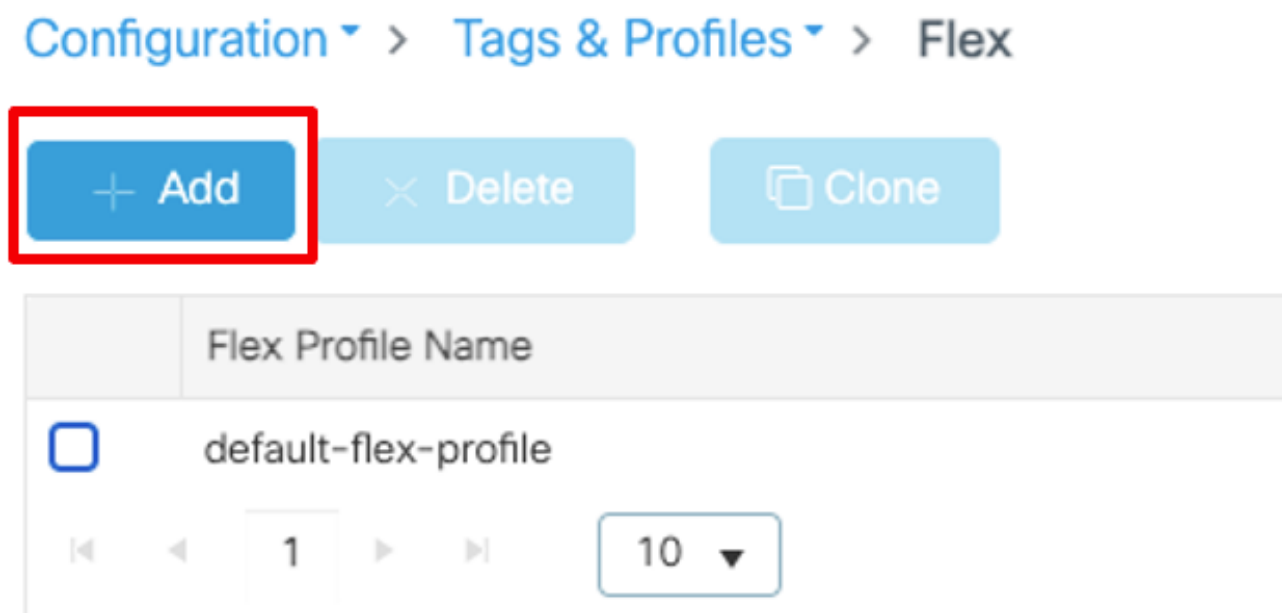
↺ Cancel

📄 Apply to Device

Configurazione del profilo Flex

Per assegnare dinamicamente un ID VLAN tramite RADIUS su un access point FlexConnect, è necessario che l'ID VLAN menzionato nell'attributo Tunnel-Private-Group ID della risposta RADIUS sia presente sui punti di accesso. Le VLAN sono configurate sul profilo Flex.

1. Selezionare Configurazione > Tag e profili > Flex > + Aggiungi.



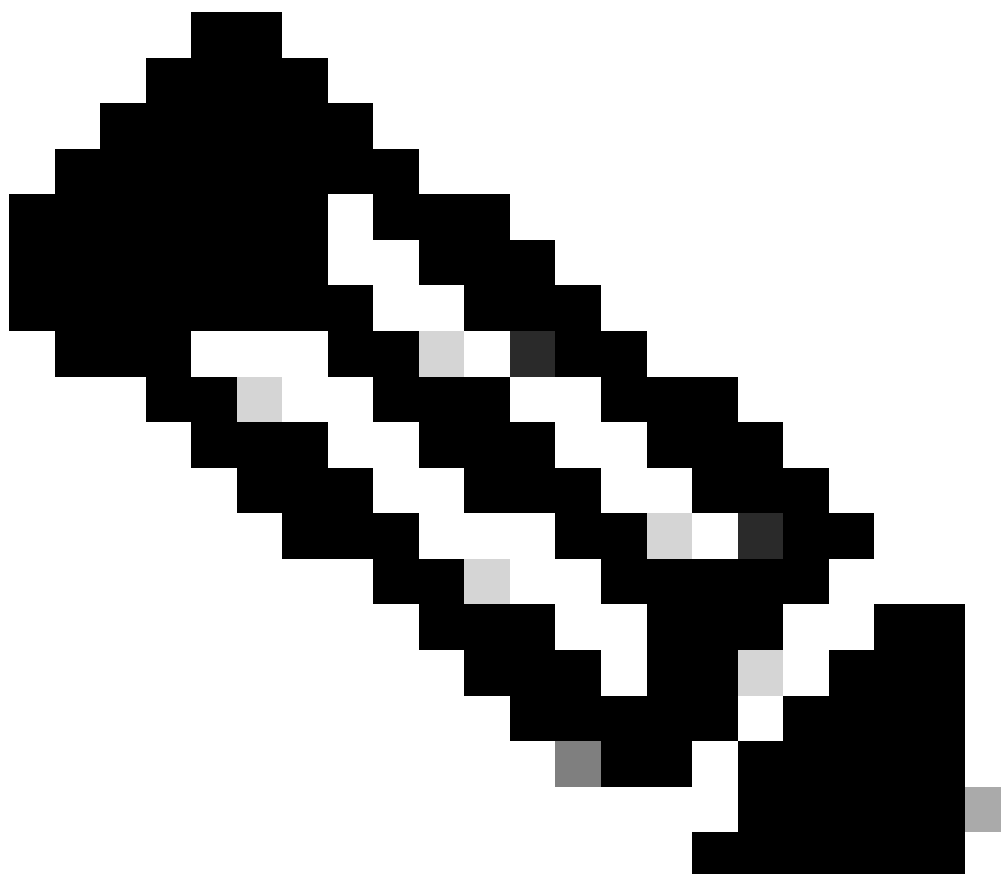
2. Fare clic sulla scheda General (Generale), assegnare un nome al profilo Flex e configurare un ID VLAN nativo per l'access point.

Add Flex Profile

General Local Authentication Policy ACL VLAN Umbrella

Name*	Dynamic-VLAN-Flex	Fallback Radio Shut	☐
Description	Enter Description	Flex Resilient	☐
Native VLAN ID	103	ARP Caching	☒
HTTP Proxy Port	0	Efficient Image Upgrade	☒
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP	☐
CTS Policy		Join Minimum Latency	☐
Inline Tagging	☐	IP Overlap	☐
SGACL Enforcement	☐	mDNS Flex Profile	Search or Select ▼
CTS Profile Name	default-sxp-profile x ▼		

Cancel Apply to Device



Nota: L'ID VLAN nativo fa riferimento alla VLAN di gestione dell'access point, quindi deve corrispondere alla configurazione VLAN nativa dello switch a cui è connesso l'access point

-
3. Selezionare la scheda VLAN e fare clic sul pulsante "Add" (Aggiungi) per immettere tutte le VLAN necessarie.

Add Flex Profile

General

Local Authentication

Policy ACL

VLAN

Umbrella

+ Add

× Delete

VLAN Name	ID	Ingress ACL	Egress ACL
VLAN102	102		

10 items per page1 - 1 of 1 items

VLAN Name*

VLAN105

VLAN Id*

105

ACL

Unidirectional

Bidirectional

Ingress ACL

Select ACL

Egress ACL

Select ACL

✓ Save

Cancel

Cancel

Apply to Device

Nota: Nel passaggio 3 della sezione Configurazione del profilo dei criteri di connessione flessibile, è stata configurata 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.

Configurazione tag Flex Site

1. Passare a Configurazione > Tag e profili > Tag > Sito > +Aggiungi, per creare un nuovo tag del sito.
2. 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 nella sezione Configurazione profilo Flex.

The screenshot shows the 'Add Site Tag' configuration window. The 'Name*' field is set to 'DynamicVLAN-FlexTag'. The 'Flex Profile' dropdown is set to 'Dynamic-VLAN-Flex'. The 'Enable Local Site' checkbox is unchecked. The 'Apply to Device' button is highlighted with a red border.

Assegnare il criterio e il tag del sito a un punto di accesso.

1. Selezionare Configurazione > Wireless > Access Point > Nome access point > Tag generali, assegnare la policy e il tag del sito appropriati e fare clic su Aggiorna e applica alla periferica.

Edit AP

General Interfaces High Availability Inventory ICap Advanced Support Bundle

General

AP Name* AIR-AP3802I-A-K9

Location* default location

Base Radio MAC 4ce1.7544.4000

Ethernet MAC 4ce1.751c.91c8

Admin Status **ENABLED** ☒

AP Mode Local ▾

Operation Status Registered

Fabric Status Disabled

LED

State **ENABLED** ☒

Brightness Level 8 ▾

Flash  **ENABLED** ☒

Flash Duration (sec) ⓘ * 0

Tags

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

Policy Dynamic-VLAN ▾

Site DynamicVLAN-FlexT ▾

RF default-rf-tag ▾

Write Tag Config to AP ☐

Version

Primary Software Version 17.4.1.6

Predownloaded Status N/A

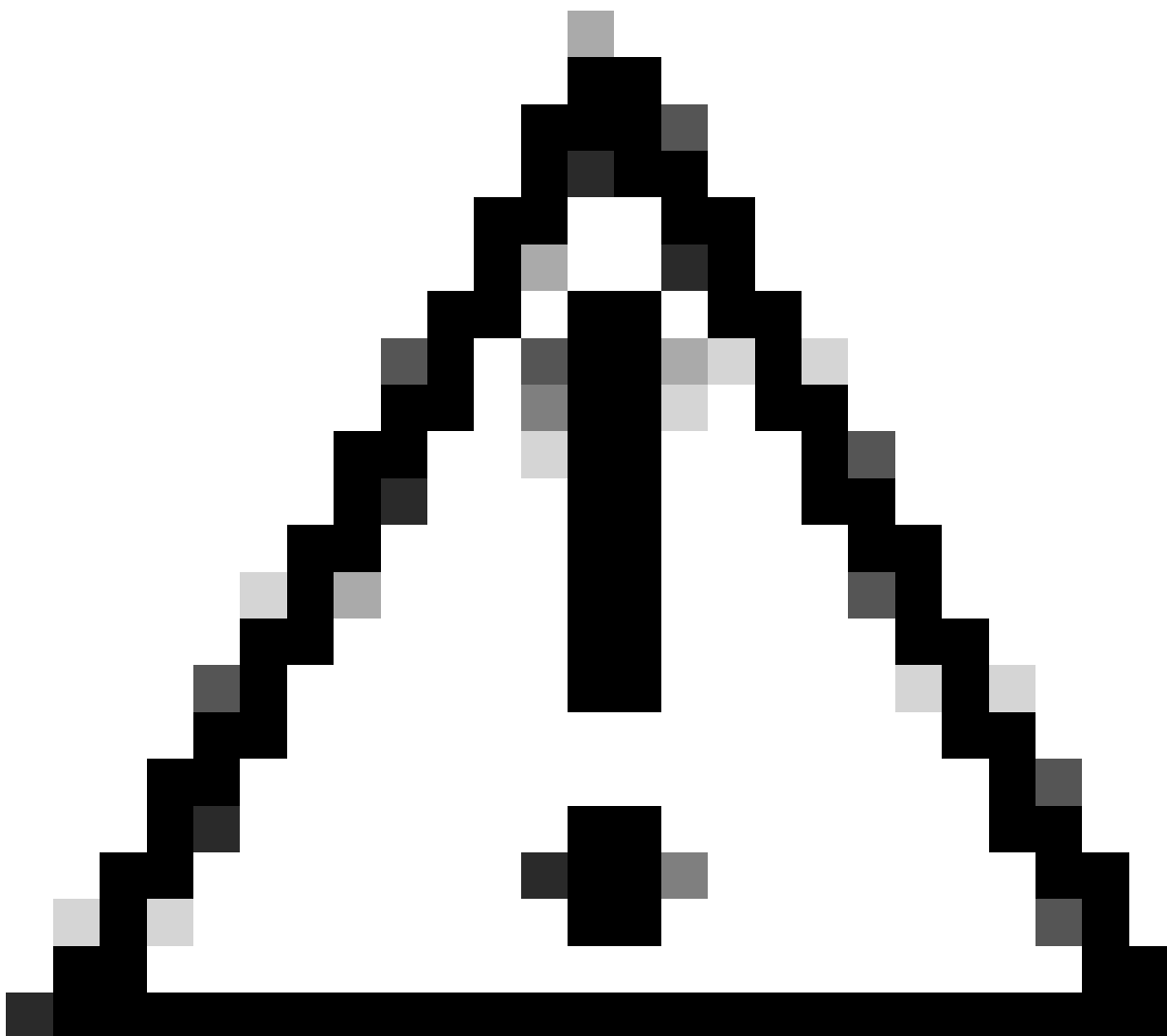
Predownloaded Version N/A

Next Retry Time N/A

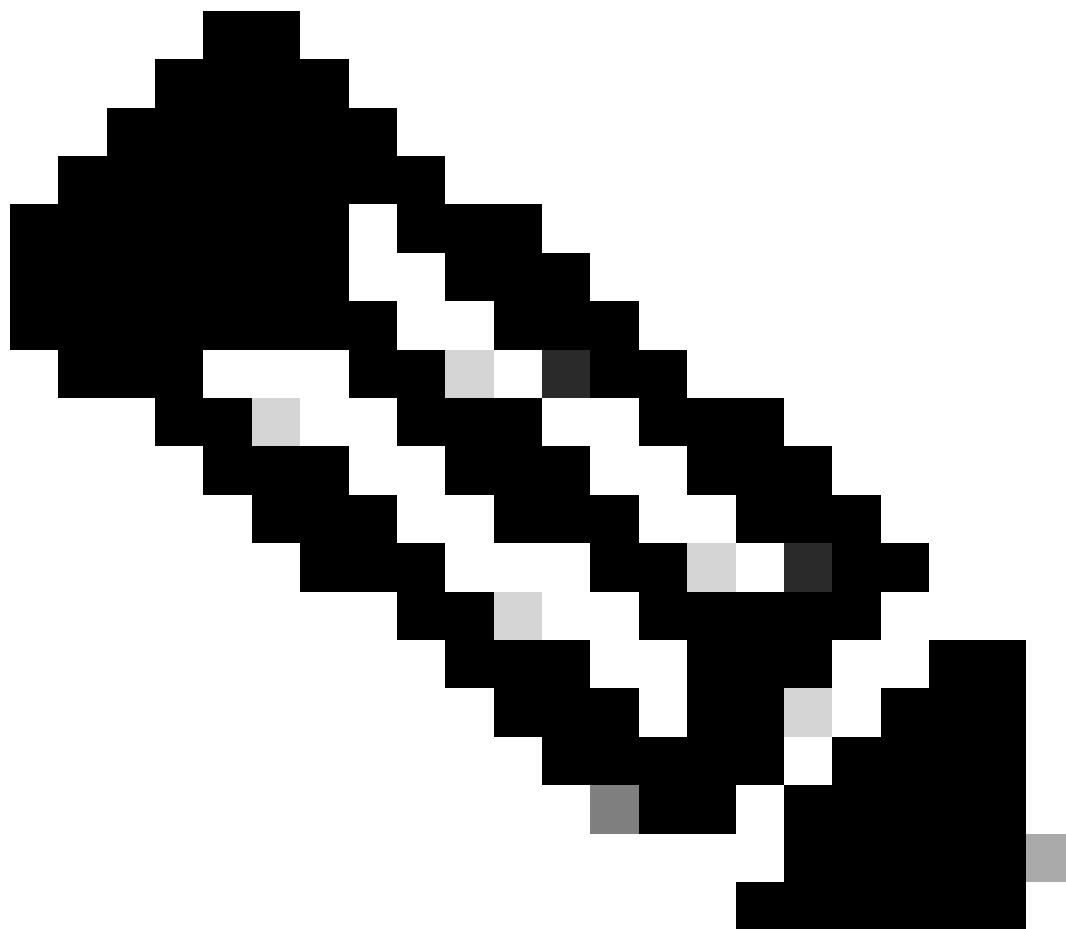
Boot Version 1.1.2.4

Cancel

 Update & Apply to Device



Attenzione: Tenere presente che la modifica dei criteri e del tag del sito in un access point comporta la disconnessione e la riconnessione dell'access point dal WLC.



Nota: Se l'access point è configurato in modalità Locale (o in qualsiasi altra modalità) e viene visualizzato un tag del sito con l'impostazione "Abilita sito locale" disabilitata, l'access point si riavvia e torna in modalità FlexConnect

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Configurare il profilo SSID del client di test utilizzando il protocollo EAP appropriato e le credenziali definite in ISE che possono restituire un'assegnazione di VLAN dinamica. Dopo aver richiesto un nome utente e una password, immettere le informazioni dell'utente mappato su una VLAN su ISE.

Nell'esempio precedente, lo smith-102 è assegnato alla VLAN102 come specificato nel server RADIUS. In questo esempio viene utilizzato questo nome utente per ricevere l'autenticazione e per essere assegnato a una VLAN dal server RADIUS:

Al termine dell'autenticazione, è necessario verificare che il client sia assegnato alla VLAN corretta in base agli attributi RADIUS inviati. Per eseguire questa operazione, completare i seguenti passaggi:

1. Dalla GUI del controller, selezionare **Monitoring > Wireless > Clients > Select the client MAC address > General > Security Information** e cercare il campo VLAN, come mostrato nell'immagine:

The screenshot displays the Cisco Wireless Controller GUI. The breadcrumb navigation is **Monitoring > Wireless > Clients**. Under the **Clients** tab, the **Client** details for MAC address **b88a.6010.3c60** are shown. The **General** tab is selected, and the **Security Information** sub-tab is active. The **Server Policies** section shows the client is assigned to **VLAN 102**.

Client	360 View	General	QOS Statistics	ATF Statistics
Client Properties				
AP Properties				
Security Information				
IIF ID	0x90000008			
Authorized	TRUE			
Common Session ID	33020A0A0000003			
Acct Session ID	0x00000000			
Auth Method Status List				
Method	Dot1x			
SM State	AUTHENTICATED			
SM Bend State	IDLE			
Protocol Map	0x000001 (OUI)			
Local Policies				
Service Template	wlan_svc_default-f			
Absolute Timer	1800			
Server Policies				
VLAN	102			
Resultant Policies				
VLAN Name	VLAN0102			
VLAN	102			

Da questa finestra è possibile osservare che il client è assegnato alla VLAN102 in base agli attributi RADIUS configurati sul server RADIUS.

Dalla CLI è possibile usare **show wireless client summary detail** per visualizzare le stesse informazioni mostrate nell'immagine:

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1
```

MAC Address	SSID	AP Name	Connected	State	IP Address	Device-type	VLAN
BSSID	Auth Method	Created		Protocol	Channel Width		
b88a.6010.3c60	Dynamyc-VLAN	AIR-AP2802I-A-K9	06	Run	10.10.105.200	Intel-Device	105
44.4000	[802.1x]	05		11n(2.4) 1	20/20 Y/Y 1/1 24.0	jonathga-105	

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1
```

MAC Address	SSID	AP Name	Connected	State	IP Address	Device-type	VLAN
BSSID	Auth Method	Created		Protocol	Channel Width		
b88a.6010.3c60	Dynamyc-VLAN	AIR-AP2802I-A-K9	55	Run	10.10.102.121	Intel-Device	102
44.4000	[802.1x]	54		11n(2.4) 1	20/20 Y/Y 1/1 m5	jonathga-102	

2. È possibile abilitare il **Radioactive traces** router per garantire il corretto trasferimento degli attributi RADIUS al WLC. A tale scopo, eseguire la procedura seguente:

1. Dalla GUI del controller, passare a **Troubleshooting > Radioactive Trace > +Add**.
2. Immettere l'indirizzo Mac del client wireless.
3. Selezionare **Start**.
4. Collegare il client alla rete WLAN.
5. Passare a **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log**.

Questa parte dell'output di traccia garantisce la corretta trasmissione degli attributi RADIUS:

<#root>

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id 1812/60 10

Access-Accept

, len 352

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: authenticator e5 5e 58 fa

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}:

[radius] [25253]: (info): RADIUS: User-Name [1] 13 "smith-102

"

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: State [24]

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Class [25]

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:

2021/03/21 22:22:45.236

{wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Type [64] 6 VLAN

[13]

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:

2021/03/21 22:22:45.236

{wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Medium-Type [65] 6 ALL_802

[6]

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Message [79]

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Message-Authenticator[80]

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:

2021/03/21 22:22:45.236

{wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Private-Group-Id[81] 6 "102"

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Key-Name [102]

2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Send-Key [16]

2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Recv-Key [17]

2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method name: PEAP

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[Applied attribute : username 0 "smith-102"]

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute :

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[Applied attribute : tunnel-type 1 13 [vlan]]

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[Applied attribute : tunnel-medium-type 1 6 [ALL_802]]

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info):

[Applied attribute :tunnel-private-group-id 1 "102"]

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [Applied attribute :

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info): [0000.0000.0000:unk

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- [Guida per l'utente finale](#)
- [Supporto tecnico Cisco e download](#)

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).