Configurazione dell'autenticazione 802.1X su Catalyst serie 9800 Wireless Controller

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazione WLC](#)
[Configurazione AAA su 9800 WLC](#)
[Configurazione profilo WLAN](#)
[Configurazione del profilo di policy](#)
[Configurazione del tag di policy](#)
[Assegnazione tag criteri](#)
[Configurazione di ISE](#)
[Dichiarare il WLC su ISE](#)
[Creazione di un nuovo utente in ISE](#)
[Creazione del profilo di autorizzazione](#)
[Crea set di criteri](#)
[Crea criterio di autenticazione](#)
[Crea criterio di autorizzazione](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Risoluzione dei problemi sul WLC](#)
[Risoluzione dei problemi con ISE](#)

Introduzione

Questo documento descrive come configurare una WLAN con sicurezza 802.1X su un controller wireless Cisco Catalyst serie 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 802.1X

Componenti usati

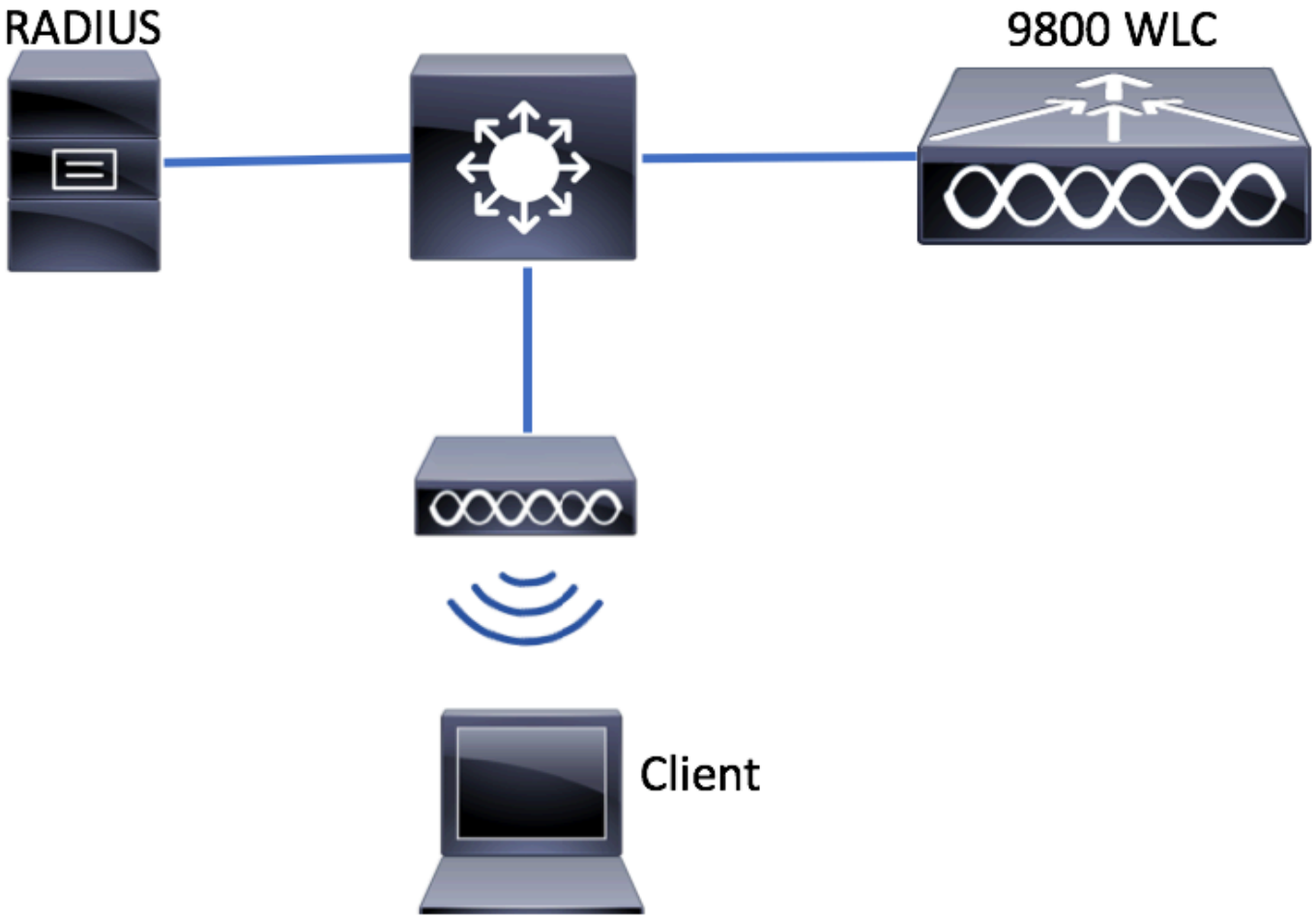
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst serie 9800 Wireless Controller (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

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



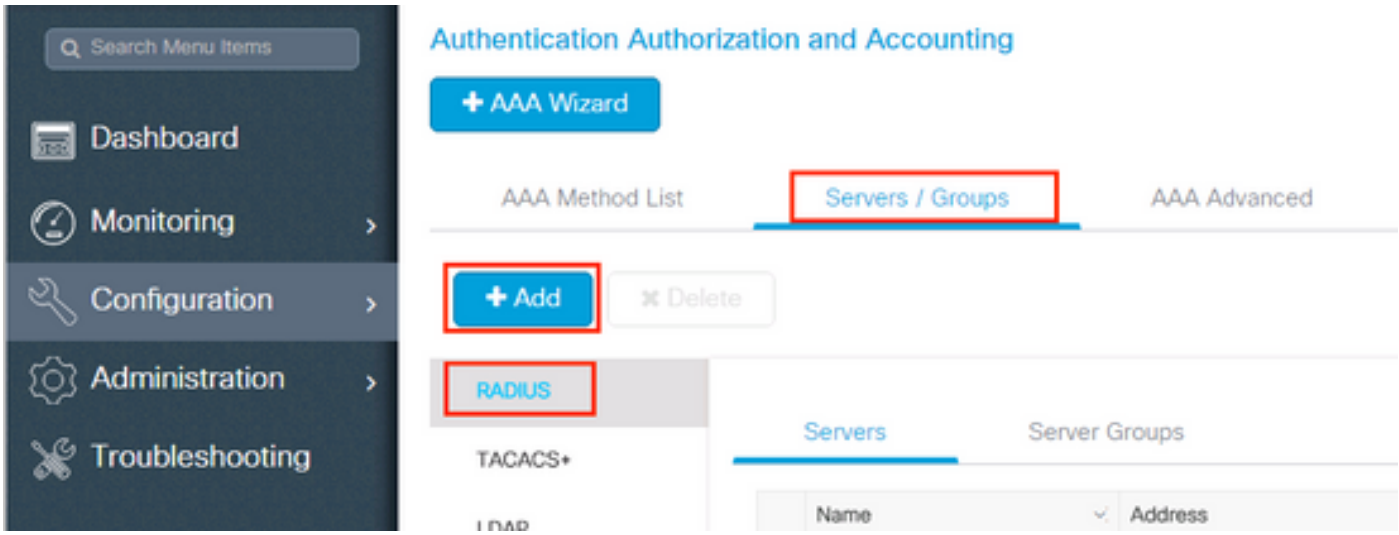
Configurazione WLC

Configurazione AAA su 9800 WLC

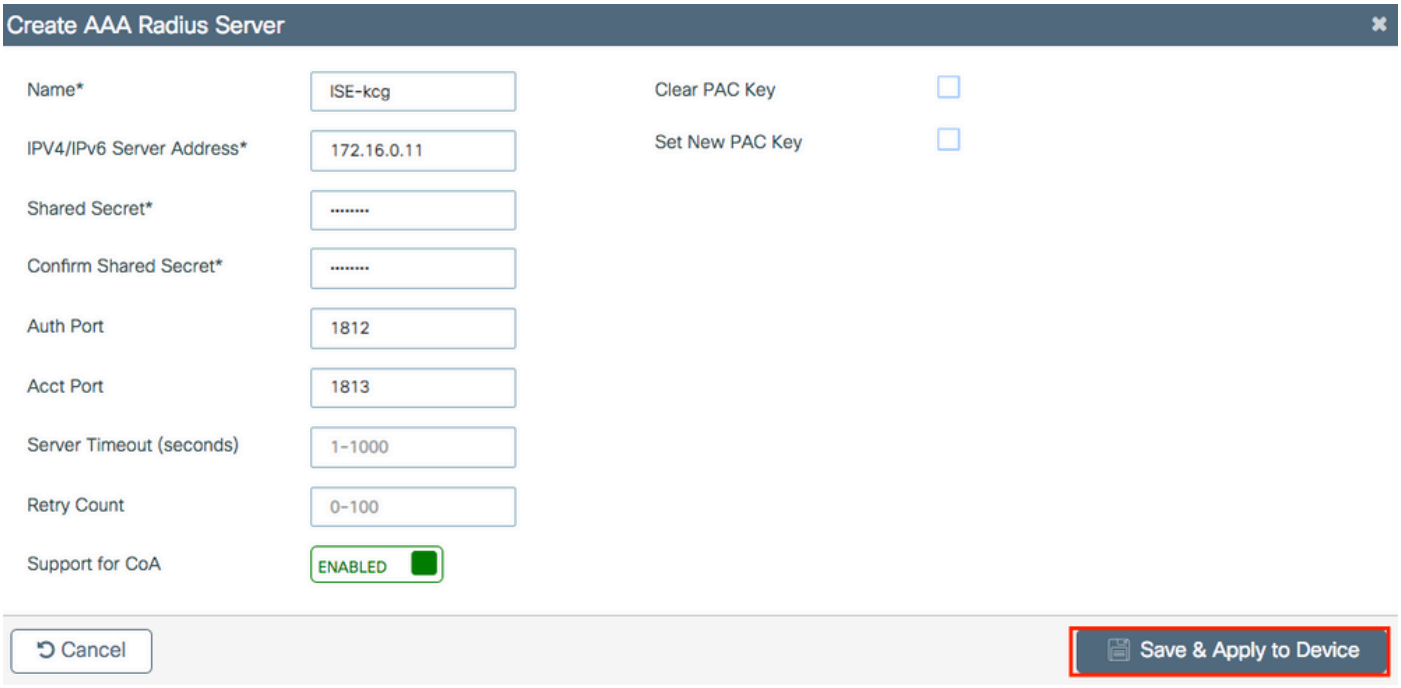
GUI:

Passaggio 1. Dichiarare il server RADIUS. Passa a **Configuration > Security > AAA > Servers / Groups >**

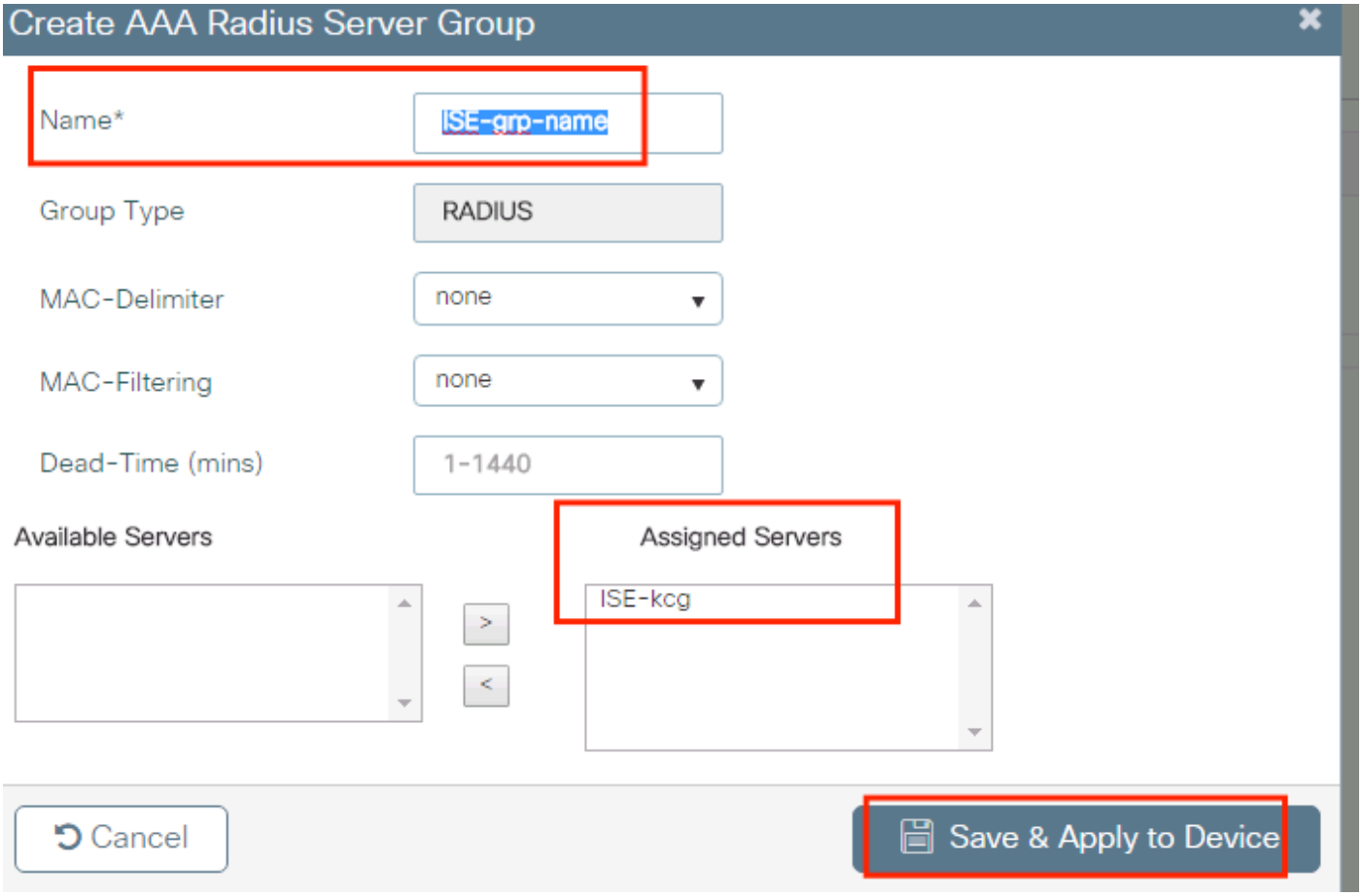
RADIUS > Servers > + Add e immettere le informazioni sul server RADIUS.



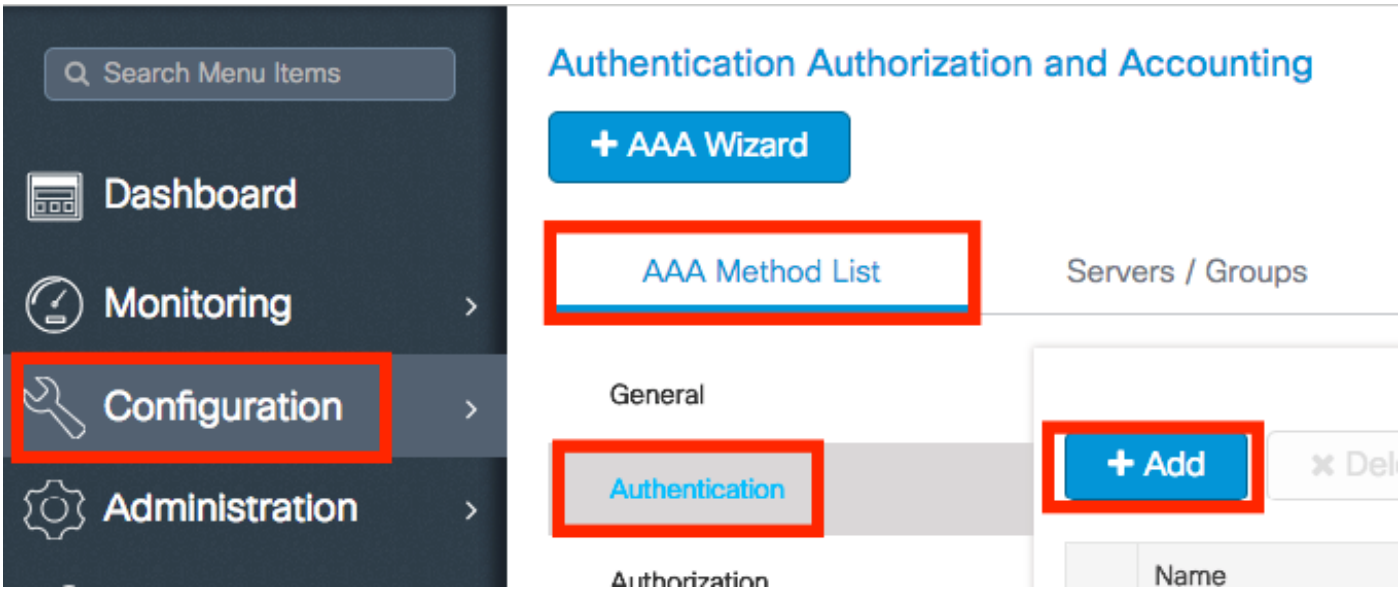
verificare che il **supporto per CoA** sia abilitato se si intende utilizzare l'autenticazione Web centrale (o qualsiasi tipo di protezione che richieda la modifica dell'autorizzazione [CoA]) in futuro.



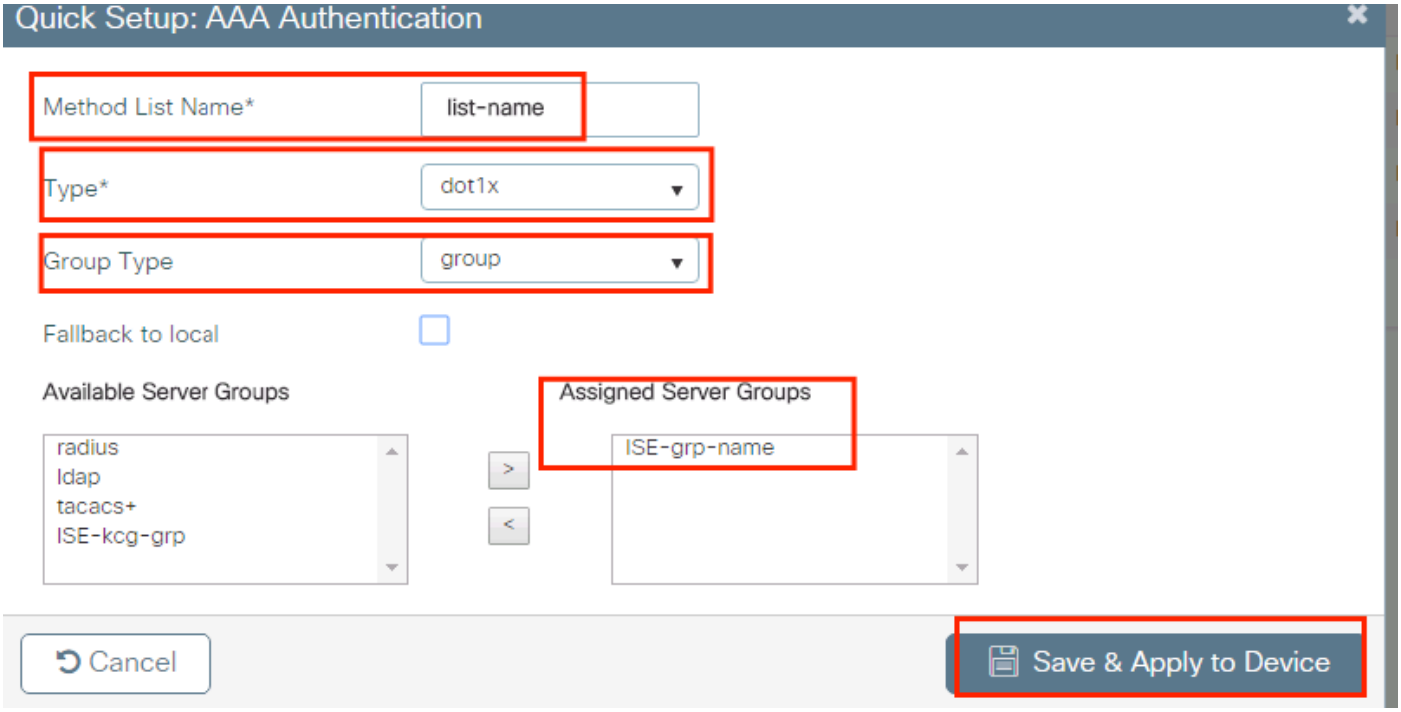
Passaggio 2. Aggiungere il server RADIUS a un gruppo RADIUS. Passa a **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.** Assegnare un nome al gruppo e spostare il server creato in precedenza nell'elenco **Assigned Servers**.



Passaggio 3. Creare un elenco di metodi di autenticazione. Passa a **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.



Immettere le informazioni:



CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

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

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Nota sul rilevamento di server inattivi AAA

Dopo aver configurato il server RADIUS, è possibile verificare se è considerato "ATTIVO":

```
#show aaa servers | s WNCD Platform State from WNCD (1) : current UP Platform State from WNCD
(2) : current UP Platform State from WNCD (3) : current UP Platform State from WNCD (4) :
current UP ...
```

Èpossibile configurare il **dead criteria**, nonché **deadtime** sul WLC, in particolare se si utilizzano più server RADIUS.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

> **Nota**: la **dead criteria** Criteri utilizzati per contrassegnare un server RADIUS come inattivo. Si compone di: 1. Un timeout (in secondi) che rappresenta il periodo di tempo che deve trascorrere tra il momento in cui il controller ha ricevuto per ultimo un pacchetto valido dal

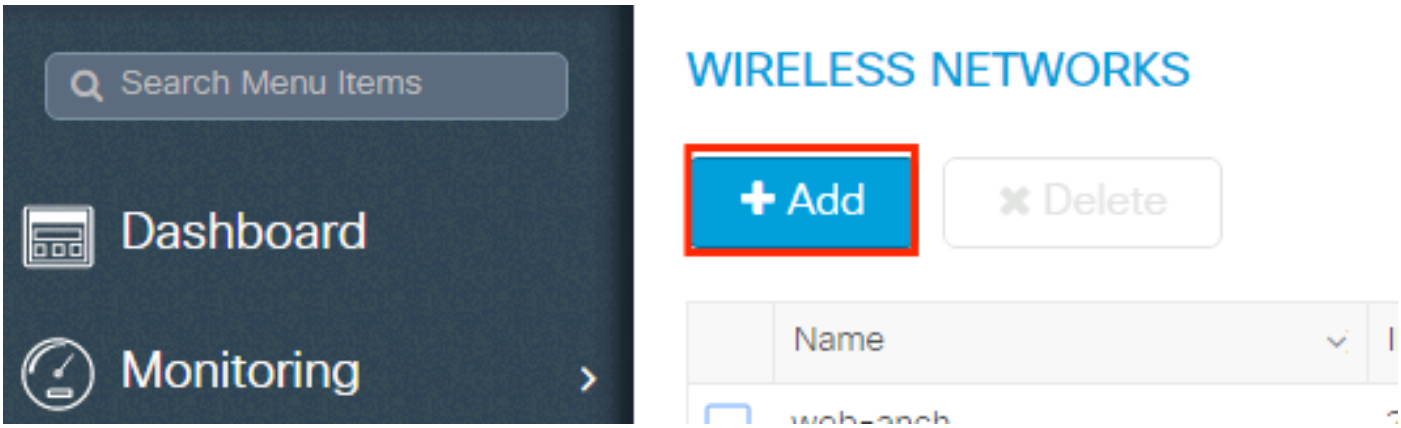
server RADIUS e il momento in cui il server viene contrassegnato come inattivo. 2. Un contatore, che rappresenta il numero di timeout consecutivi che devono verificarsi sul controller prima che il server RADIUS venga contrassegnato come inattivo.

Nota: la **deadtime** specifica il periodo di tempo (in minuti) durante il quale il server rimane nello stato inattivo dopo che i criteri inattivo lo contrassegnano come inattivo. Alla scadenza del tempo di inattività, il controller contrassegna il server come ATTIVO (ALIVE) e notifica ai client registrati la modifica dello stato. Se il server è ancora irraggiungibile dopo che lo stato è contrassegnato come ATTIVO e se i criteri non attivi sono soddisfatti, il server viene nuovamente contrassegnato come non attivo per l'intervallo di tempo morto.

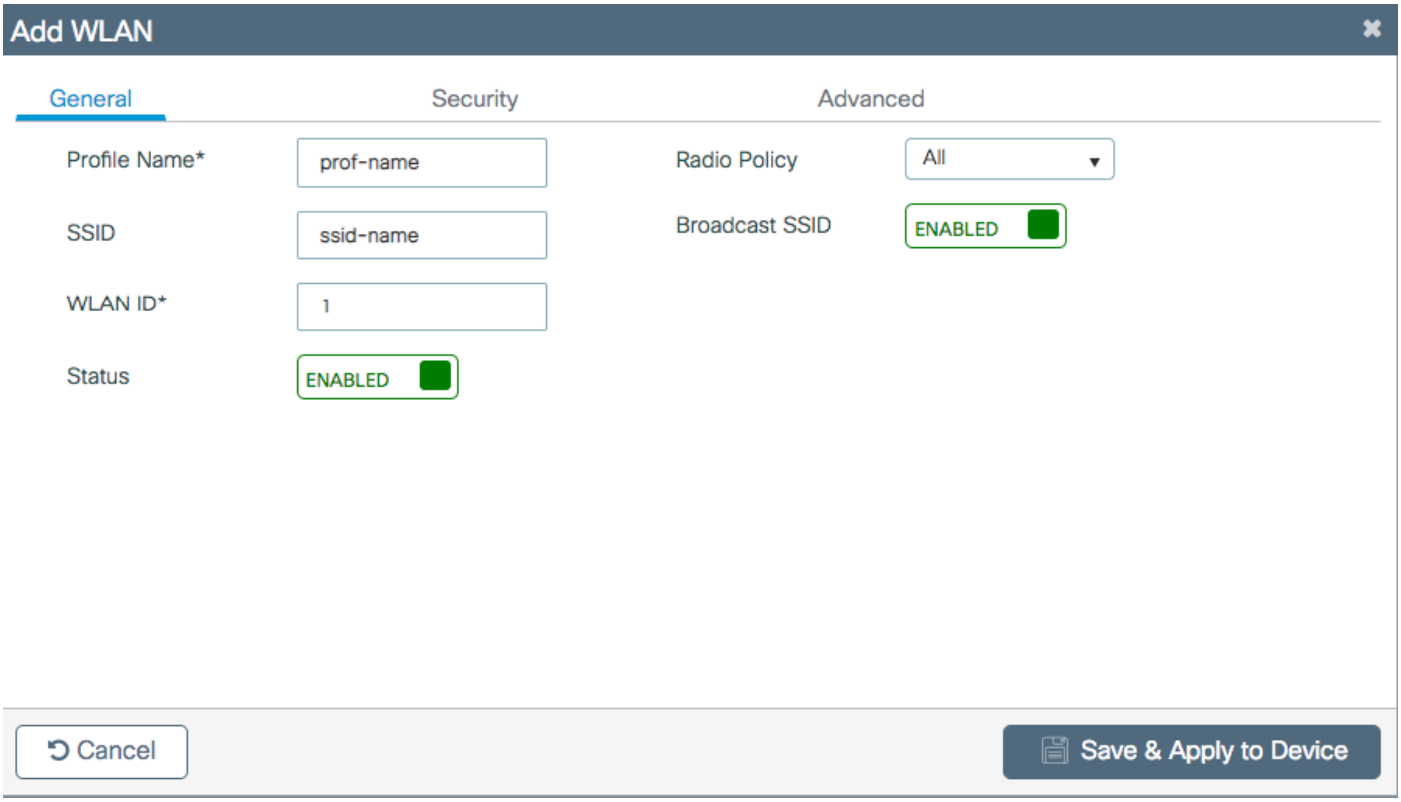
Configurazione profilo WLAN

GUI:

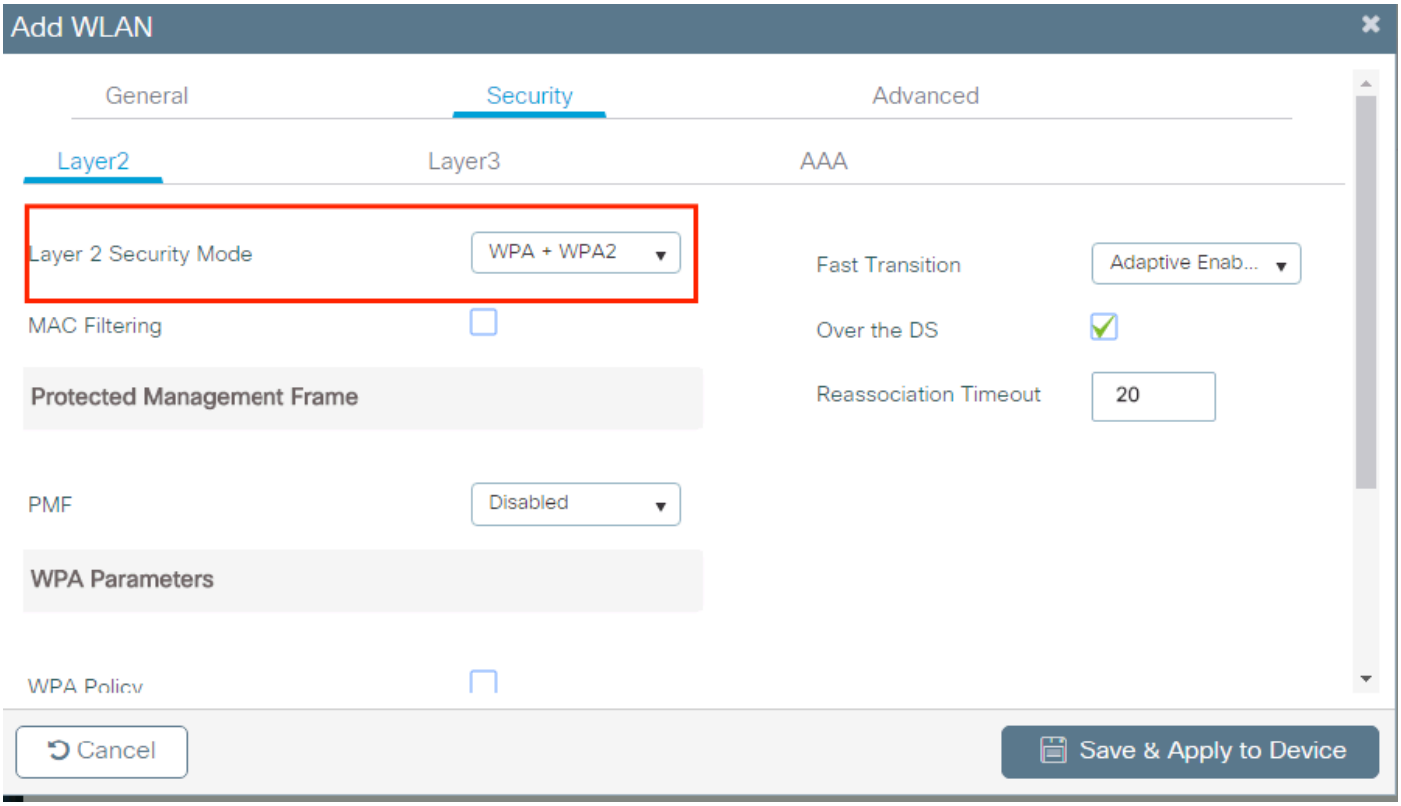
Passaggio 1. Creare la WLAN. Selezionare **Configurazione > Wireless > WLAN > + Aggiungi** e configura la rete come necessario.

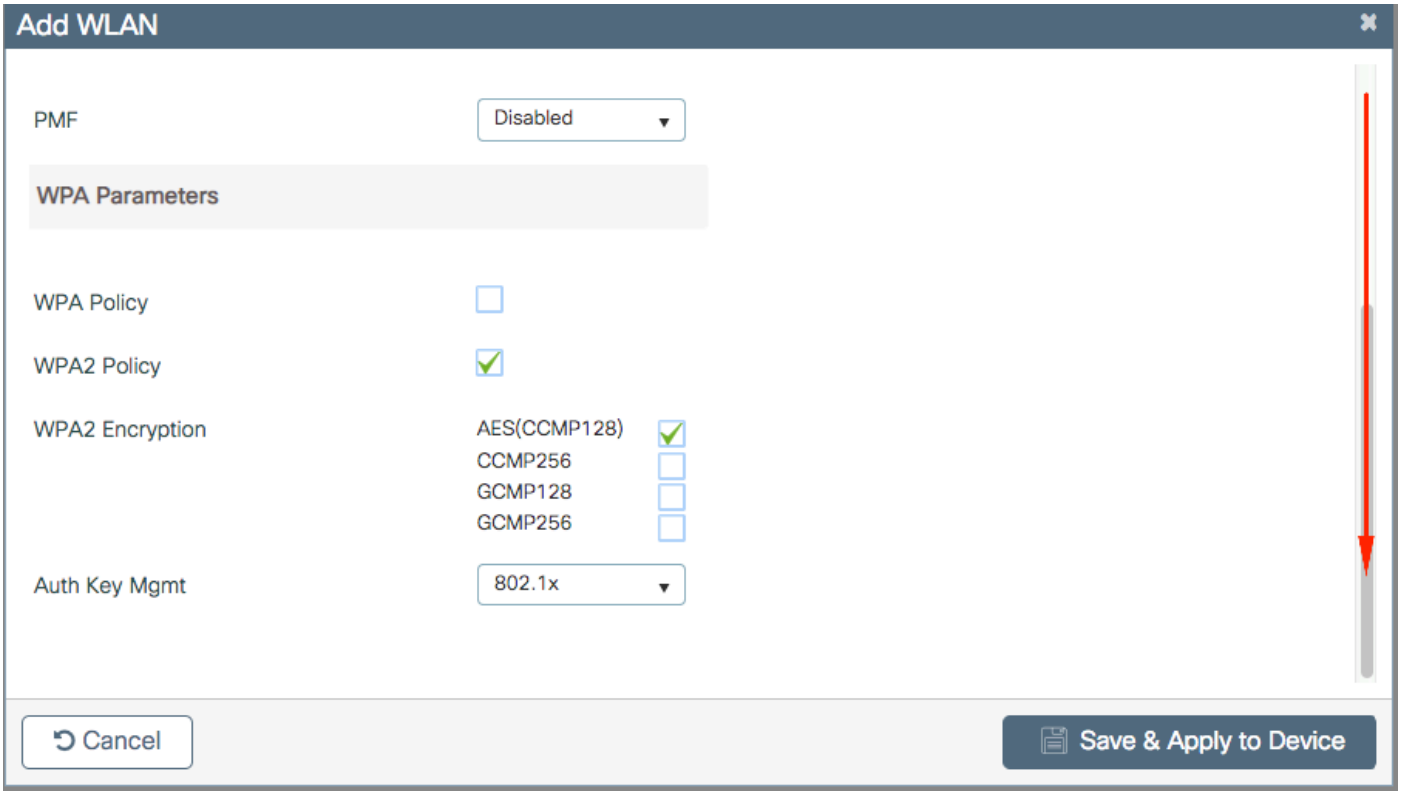


Passaggio 2. Immettere le informazioni sulla WLAN

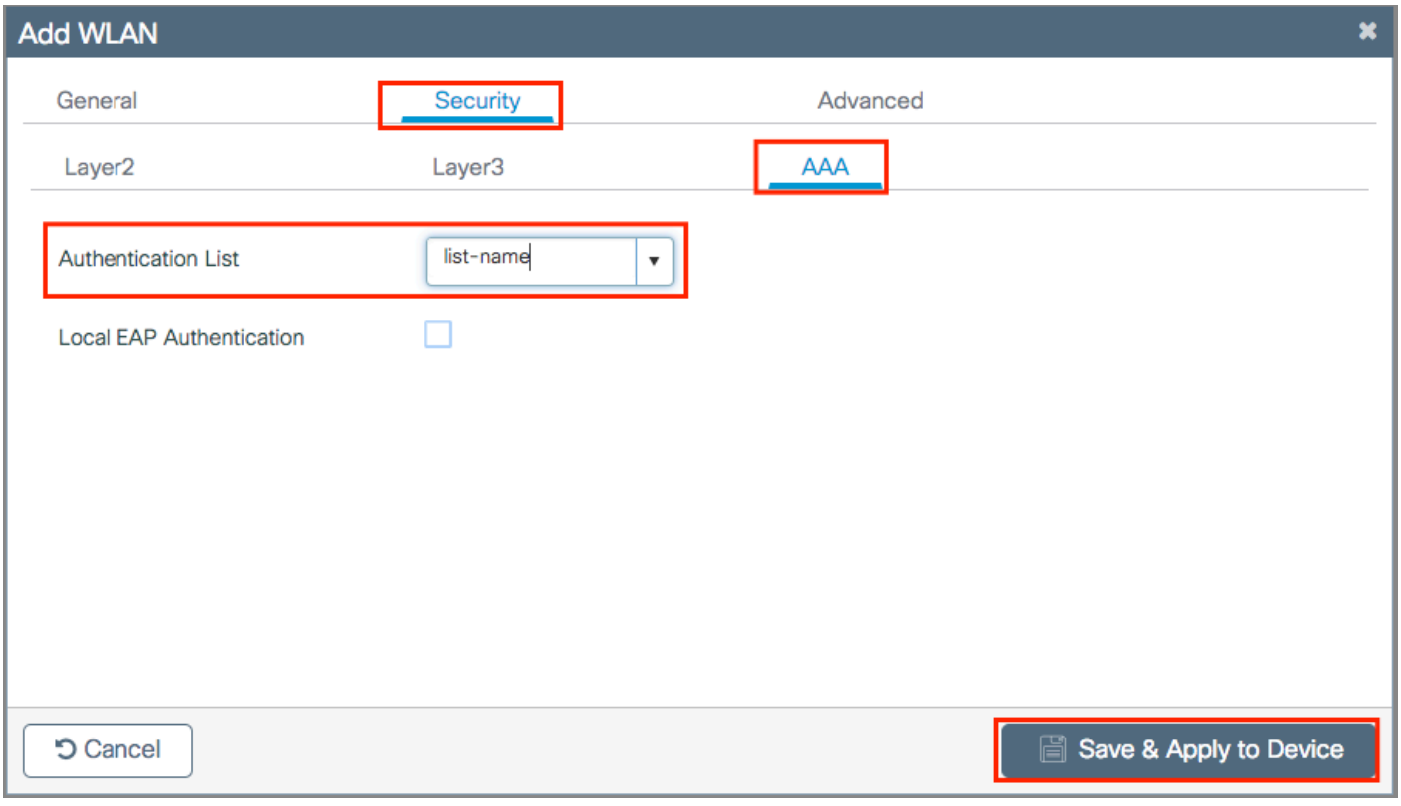


Passaggio 3. Passare alla Scheda **Protezione** e selezionare il metodo di protezione necessario. In questo caso, **WPA2 + 802.1x**.





Passaggio 4. Dal **Security > AAA** selezionare il metodo di autenticazione creato nel passaggio 3 dalla sezione AAA Configuration on 9800 WLC.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

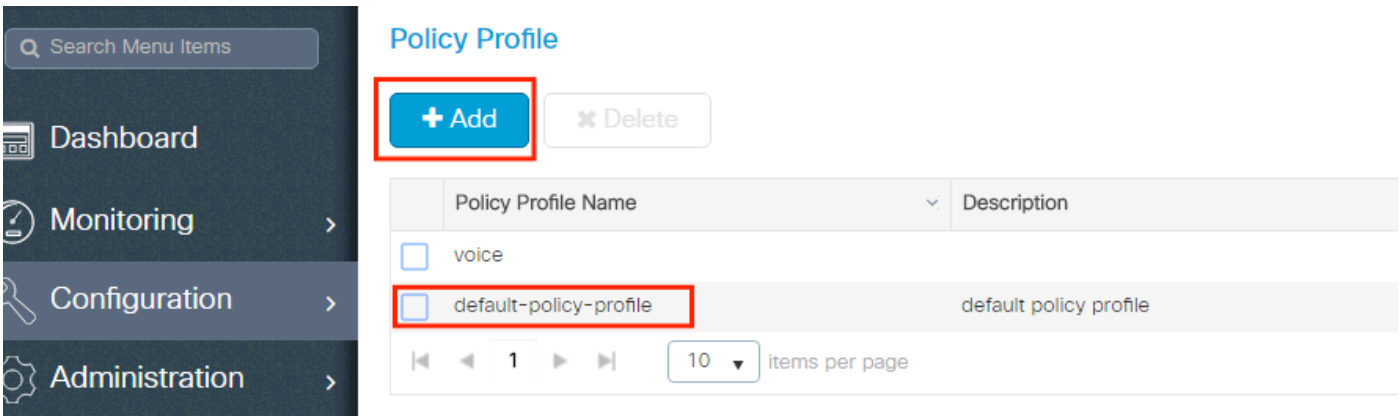
Configurazione del profilo di policy

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

Èpossibile utilizzare il profilo dei criteri predefinito oppure creare un nuovo profilo.

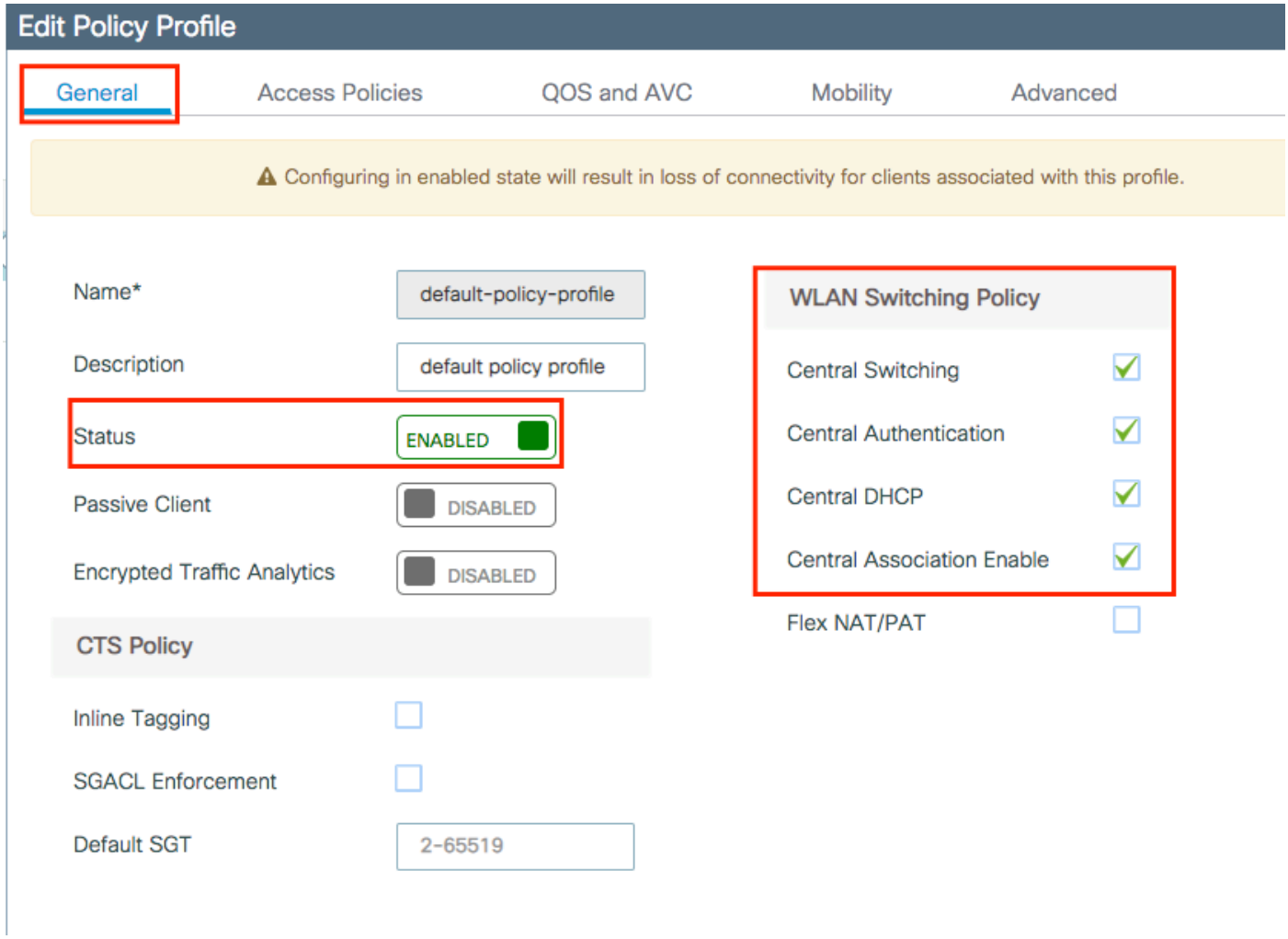
GUI:

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

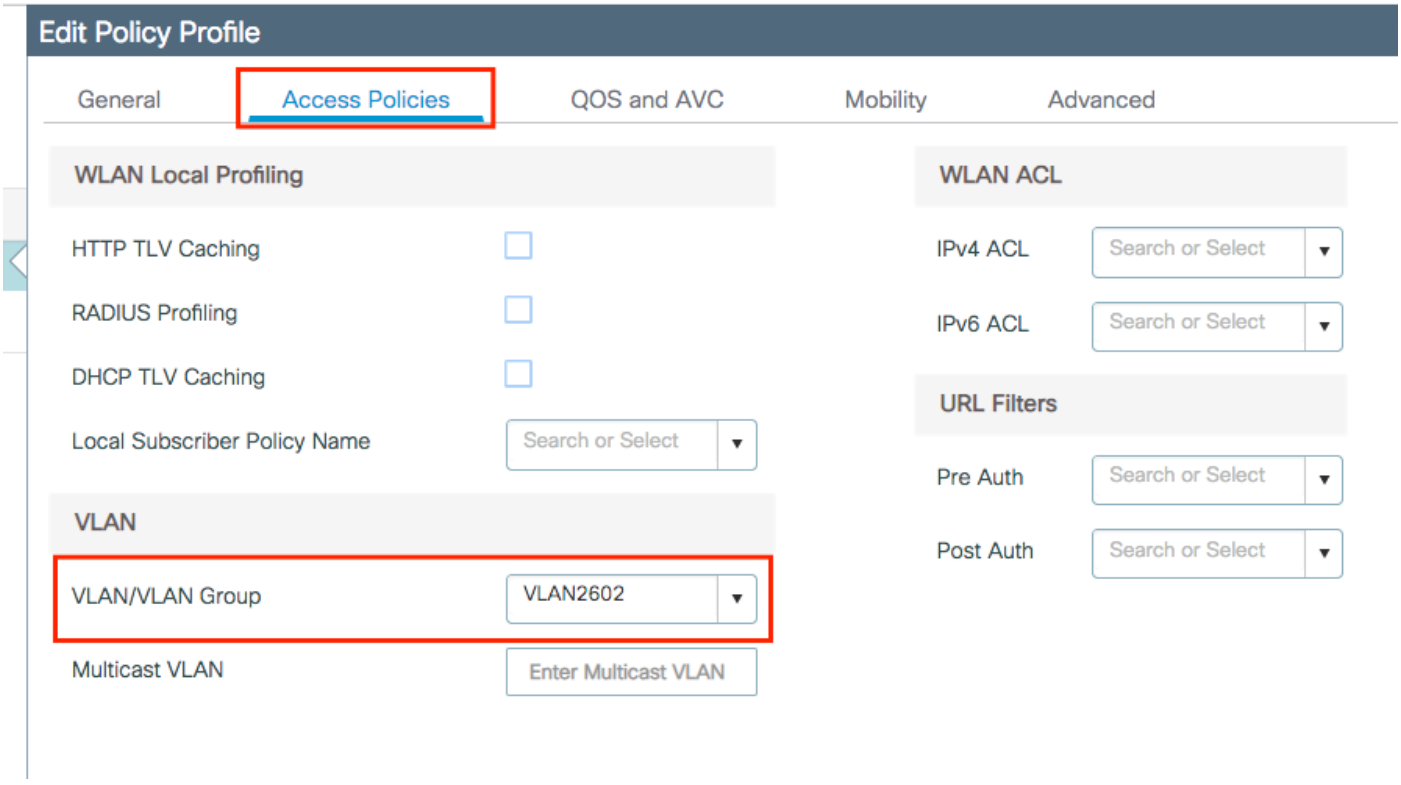


Verificare che il profilo sia abilitato.

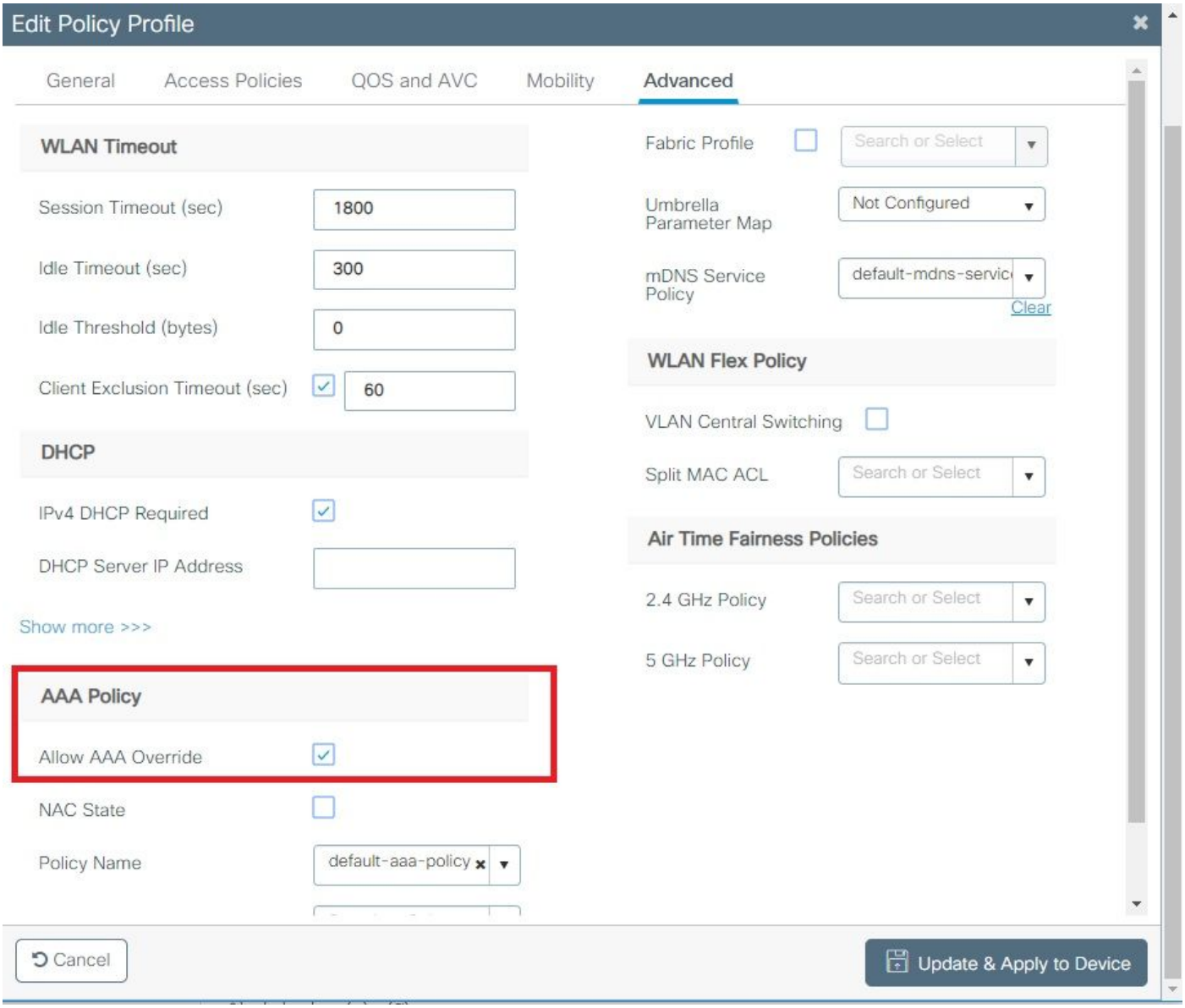
Inoltre, se il punto di accesso è in modalità locale, verificare che nel profilo della policy siano attivate le opzioni **Cambio centrale** e **Autenticazione centrale**.



Selezionare la VLAN a cui assegnare i client nella scheda **Criteri di accesso**.



Se si intende avere gli attributi ISE restituiti nell'assegnazione Access-Accept come VLAN, abilitare l'override AAA nell'assegnazione **Advanced** scheda:



CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

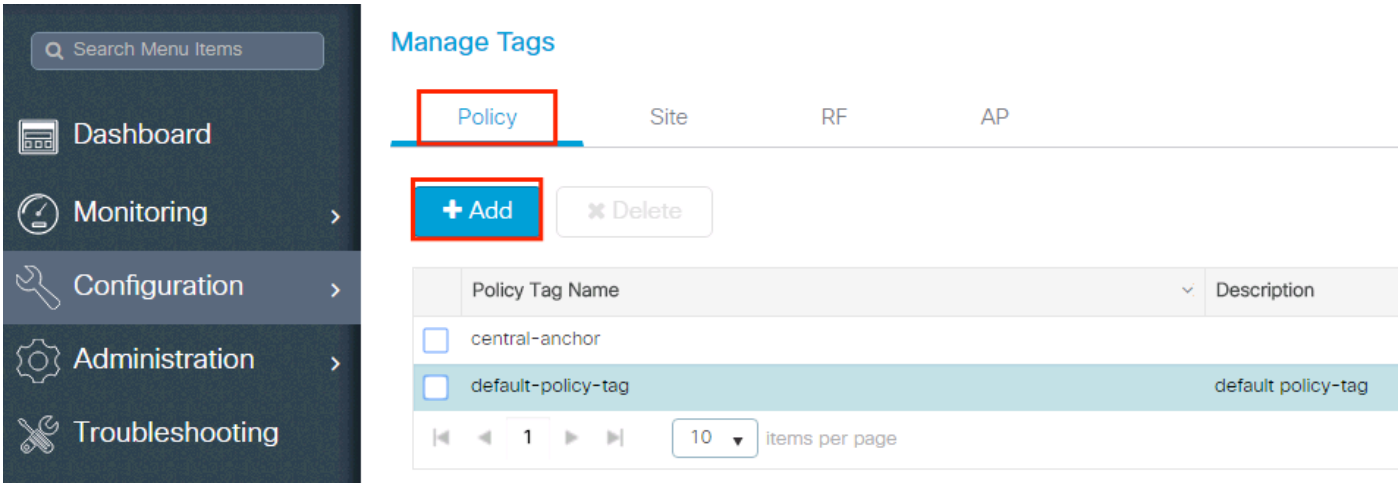
Configurazione del tag di policy

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.

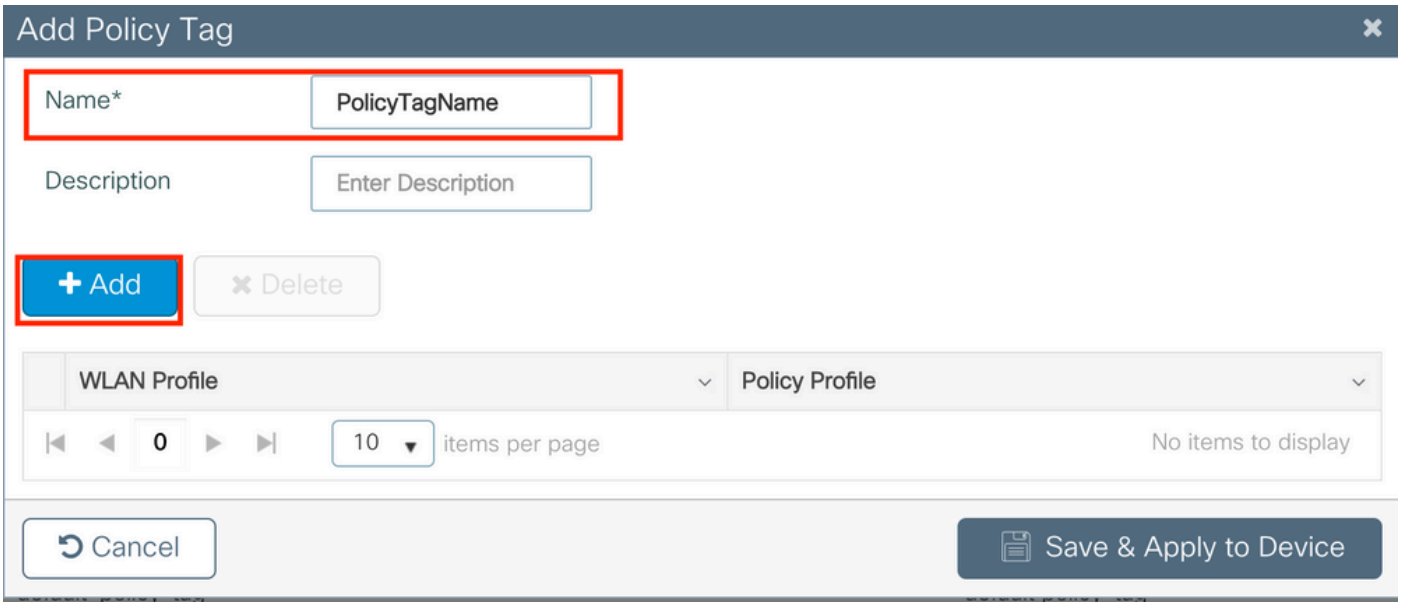
> **Nota**: il tag default-policy-tag mappa automaticamente qualsiasi SSID con ID WLAN compreso tra 1 e 16 al profilo default-policy-profile. Non può essere né modificata né eliminata. Se si dispone di una WLAN con ID 17 o superiore, non è possibile utilizzare il tag default-policy.

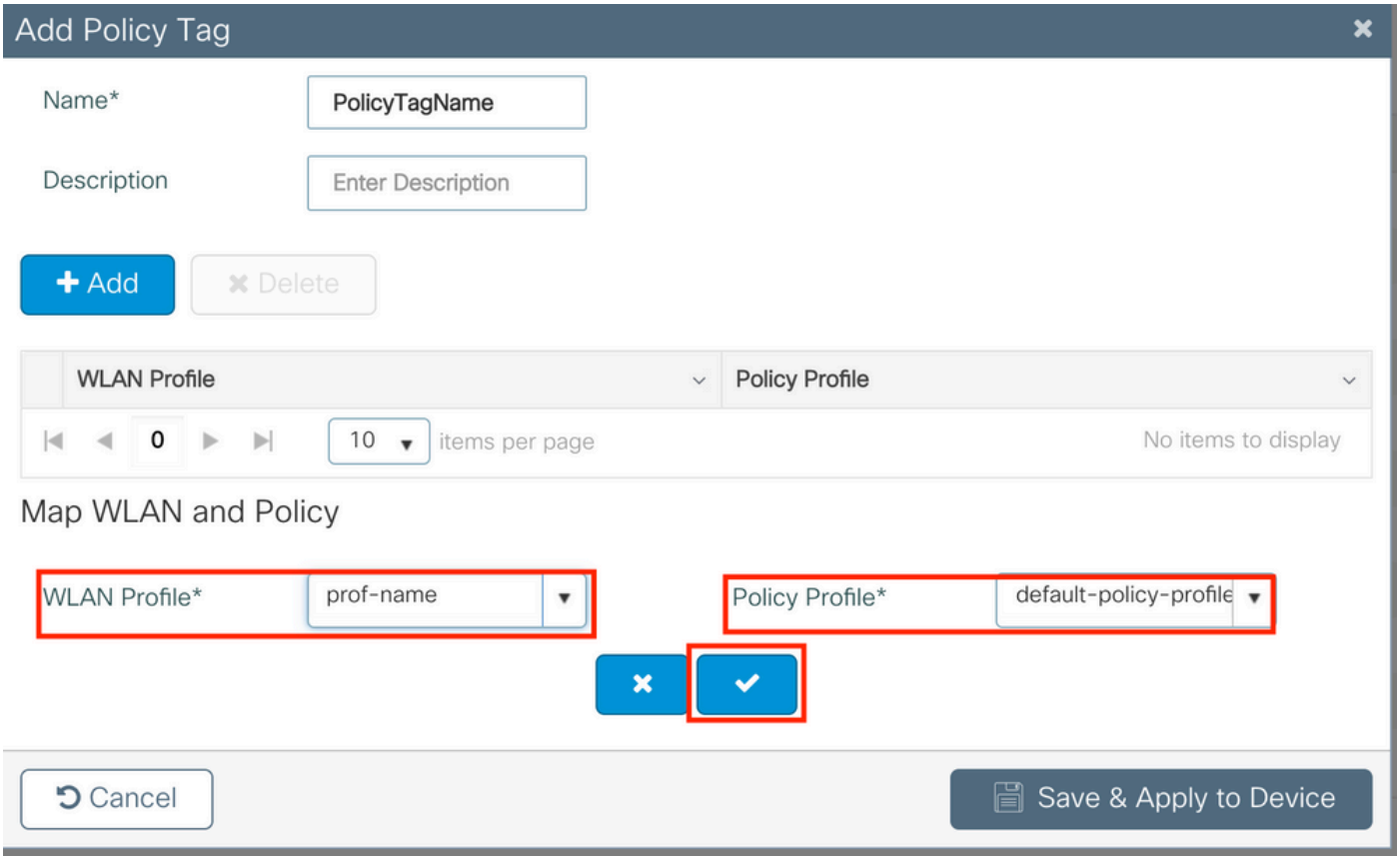
GUI:

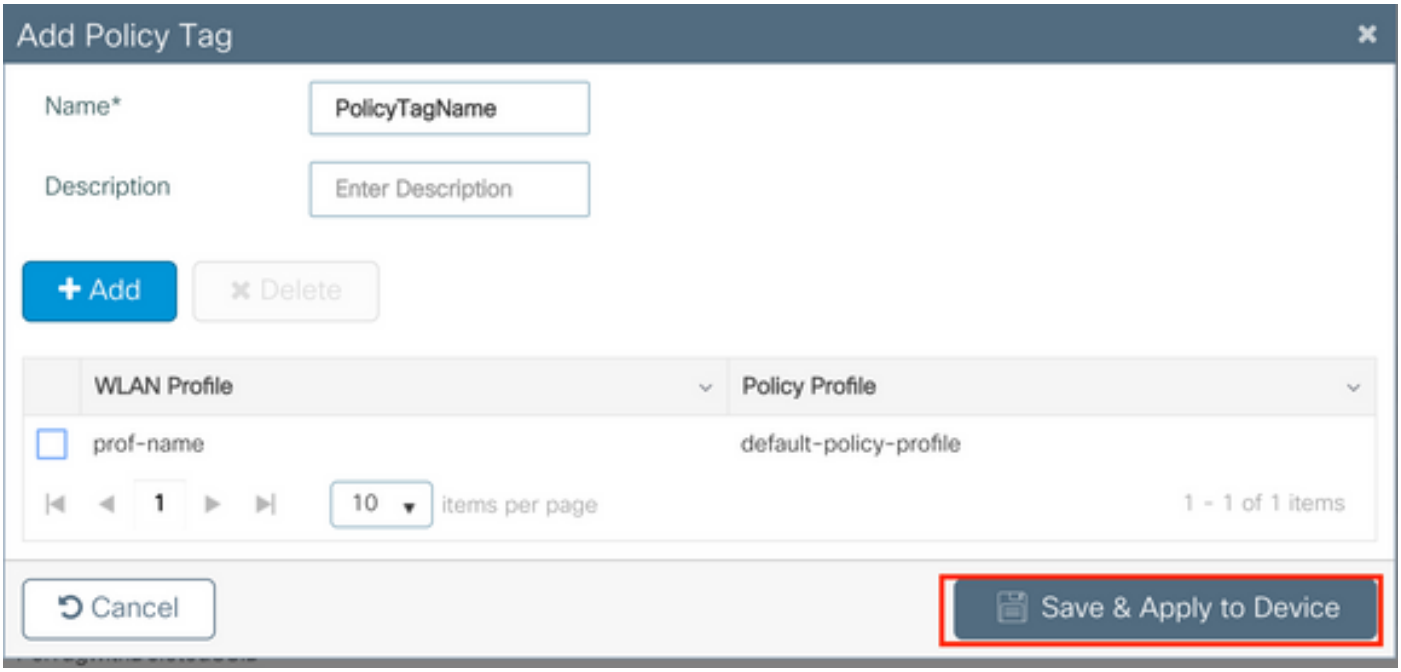
Passa a **Configugation > Tags & Profiles > Tags > Policy** e aggiungerne uno nuovo, se necessario.



Associare il profilo WLAN al profilo di policy desiderato.







CLI:

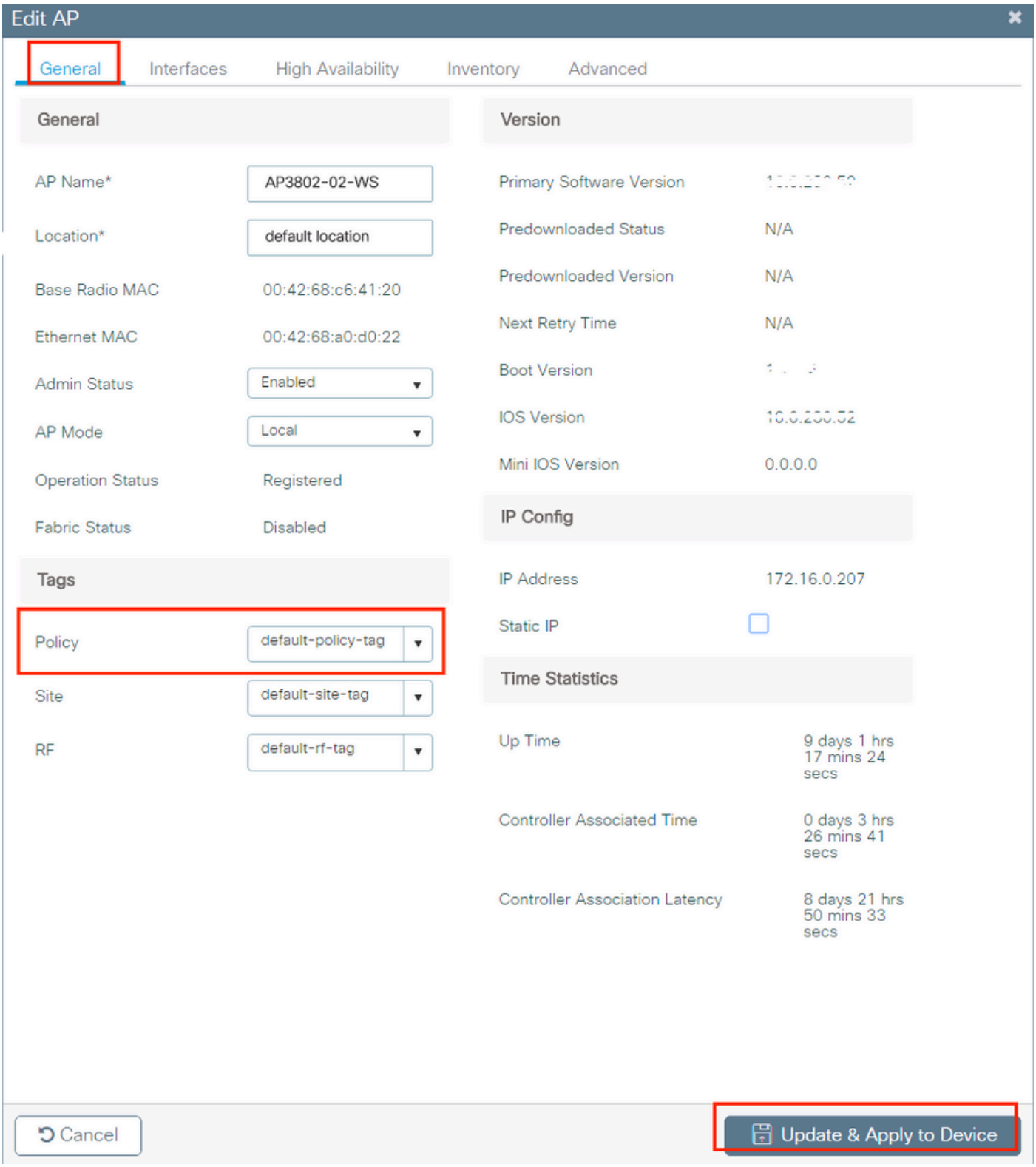
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Assegnazione tag criteri

Assegnare il tag di policy agli access point desiderati.

GUI:

Per assegnare il tag a un punto di accesso, passare a **Configuration > Wireless > Access Points > AP Name > General Tags**, assegnare il tag di criterio appropriato e fare clic su **Update & Apply to Device**.



Nota: quando si modifica il tag di policy su un access point, l'associazione viene interrotta al WLC 9800 e si unisce nuovamente qualche istante dopo.

Per assegnare lo stesso tag criteri a più access point, passare a **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

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).