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

Sommario

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

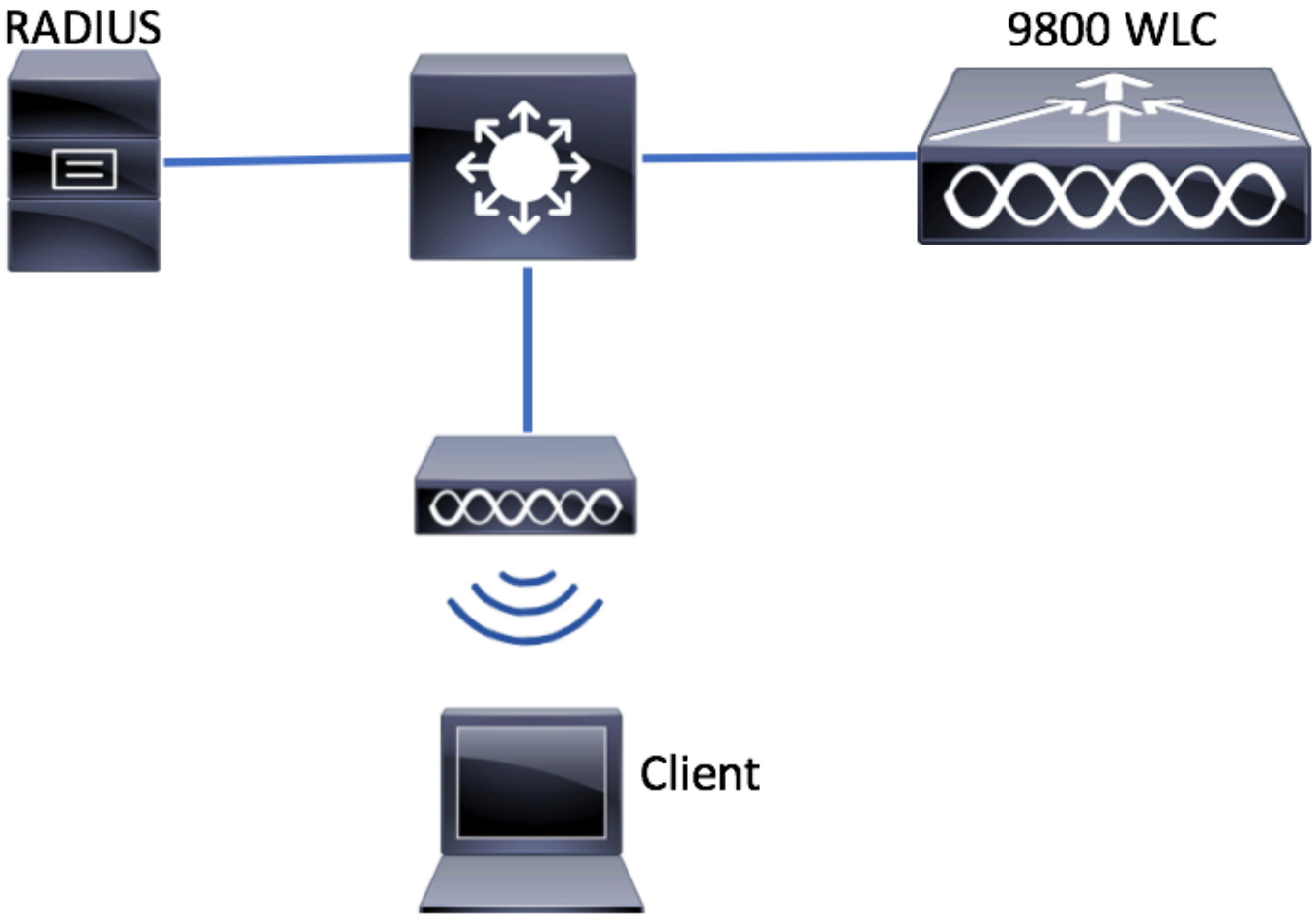
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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

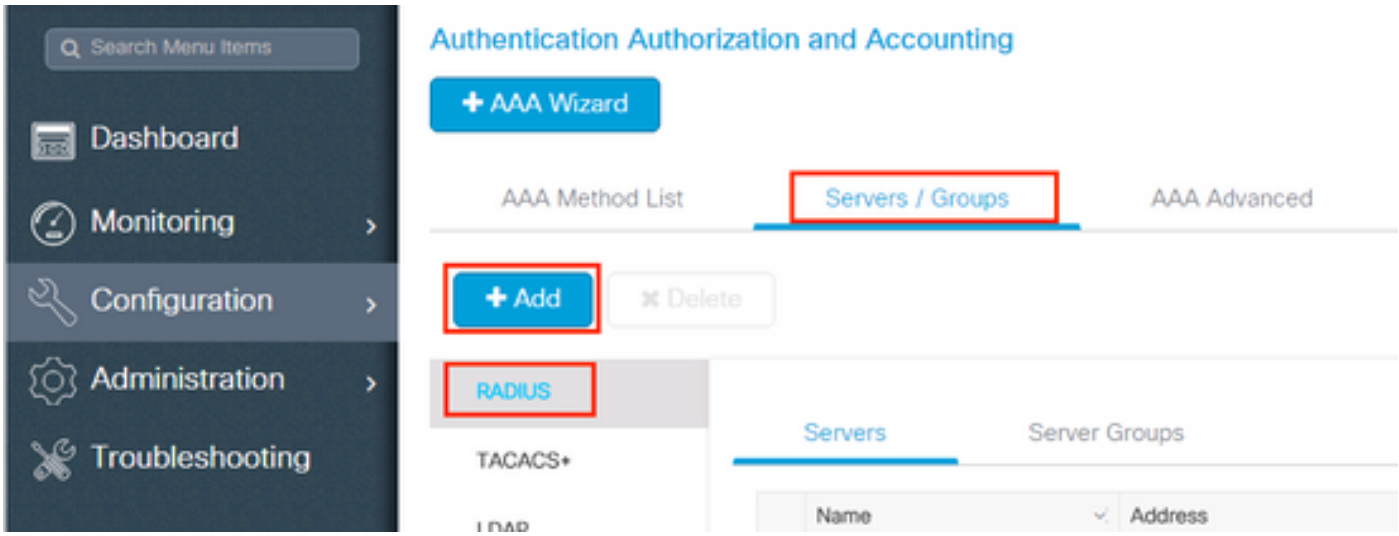


Configurazione WLC

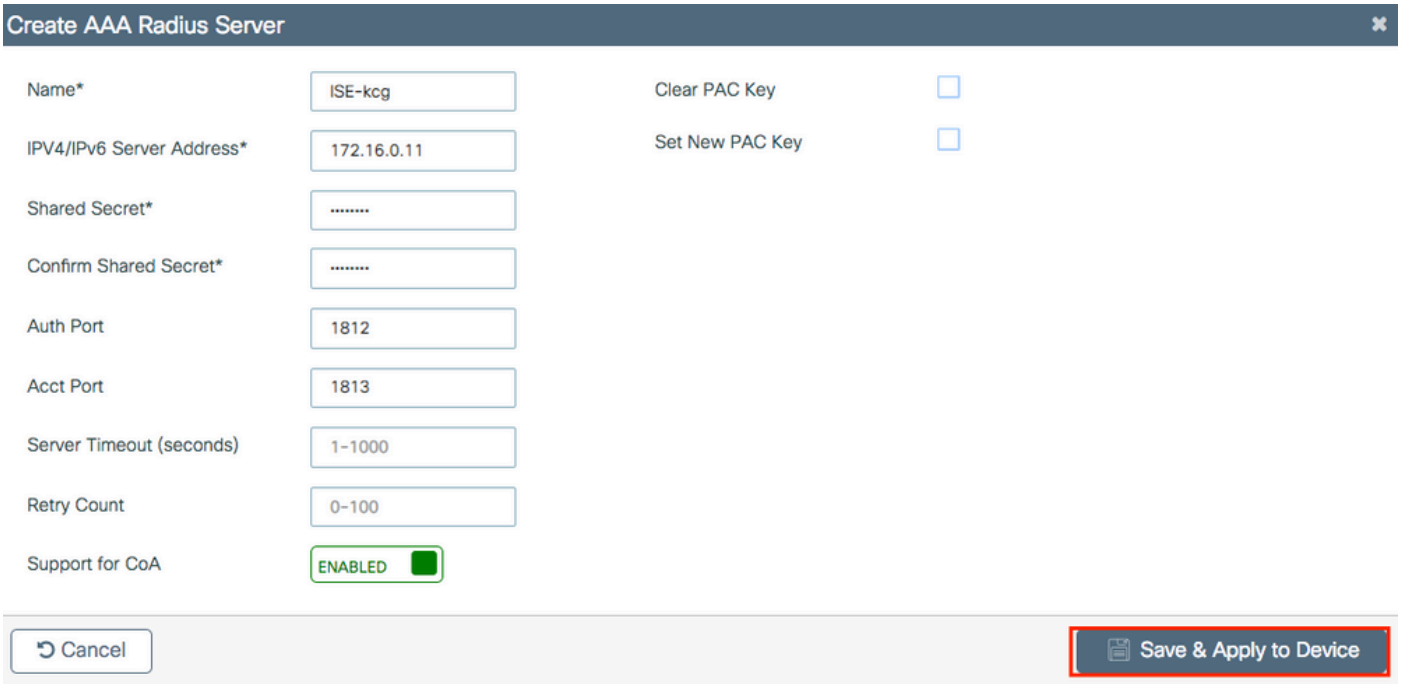
Configurazione AAA su 9800 WLC

GUI:

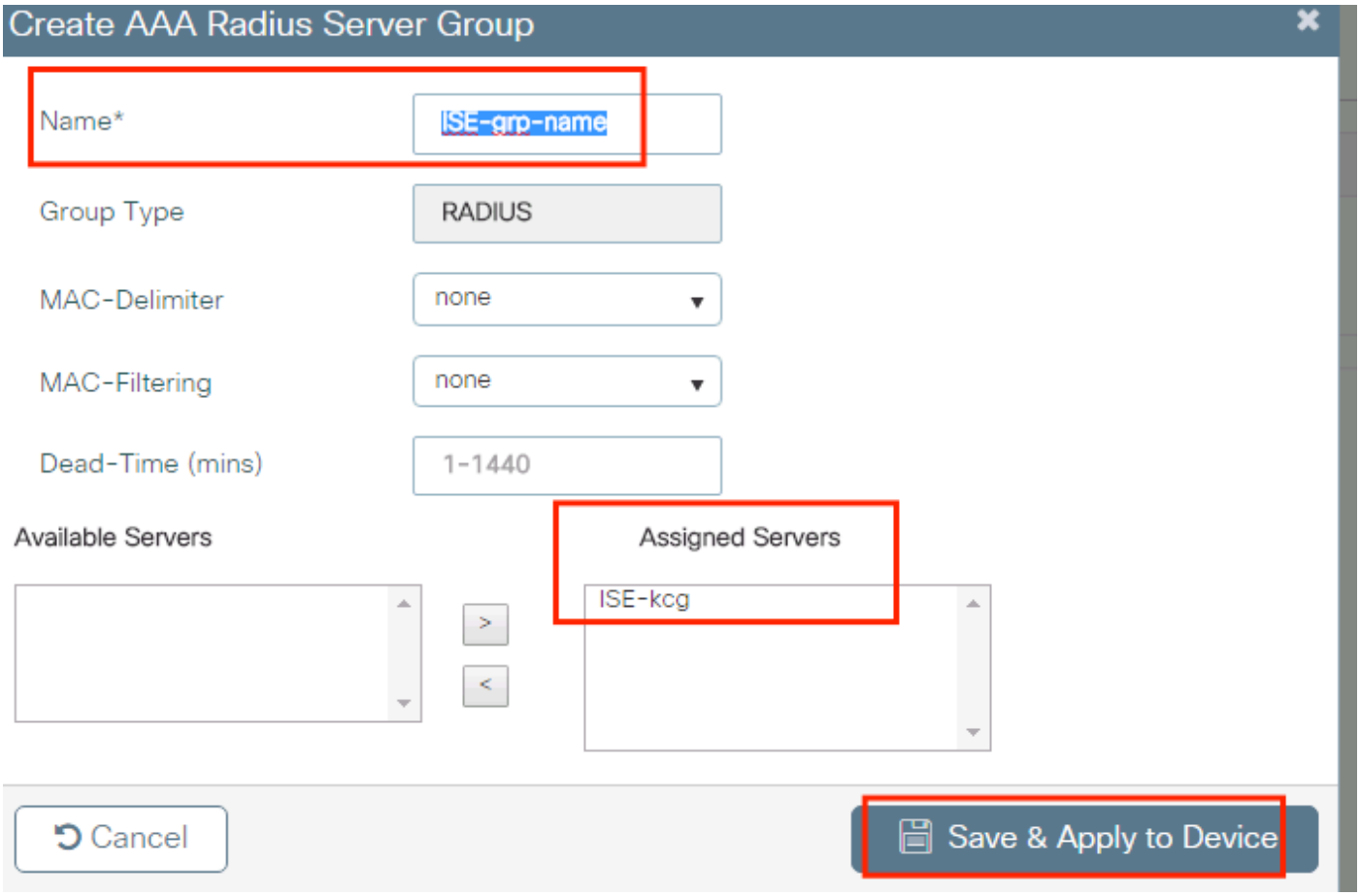
Passaggio 1. Dichiarare il server RADIUS. Individuare **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** e immettere le informazioni sul server RADIUS.



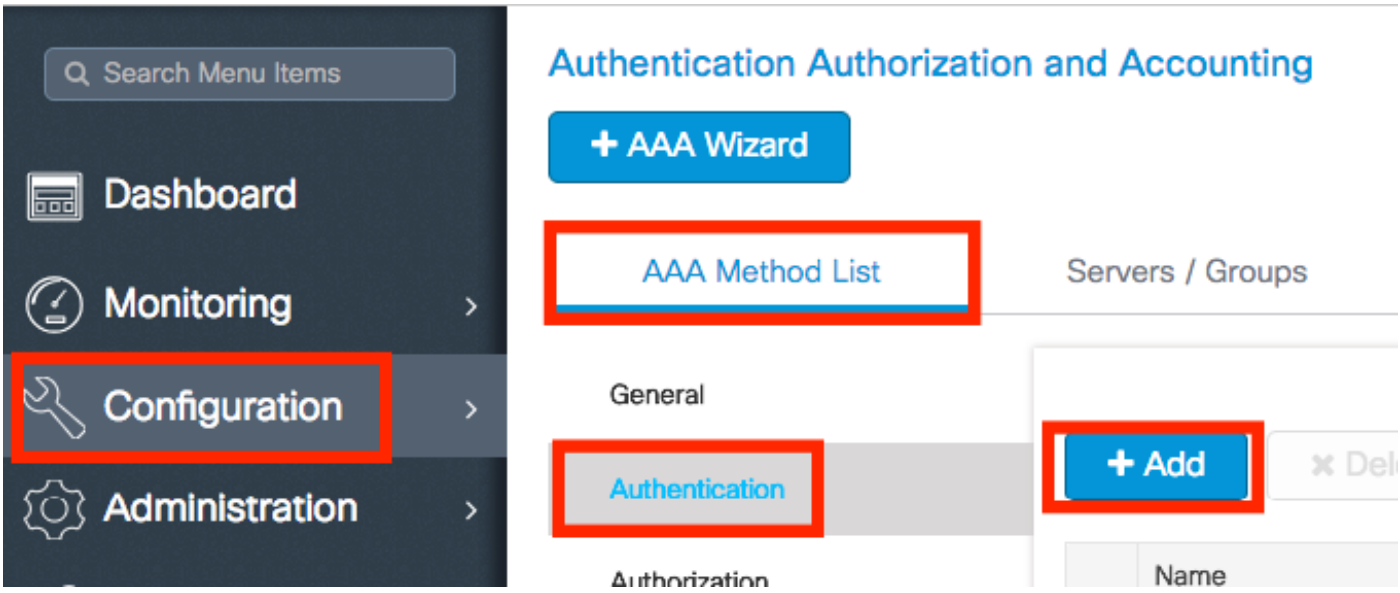
verificare che il **supporto per CoA** sia abilitato se si intende utilizzare l'autenticazione Web centrale (o qualsiasi tipo di protezione che richieda la modifica dell'autorizzazione [CoA]) in futuro.



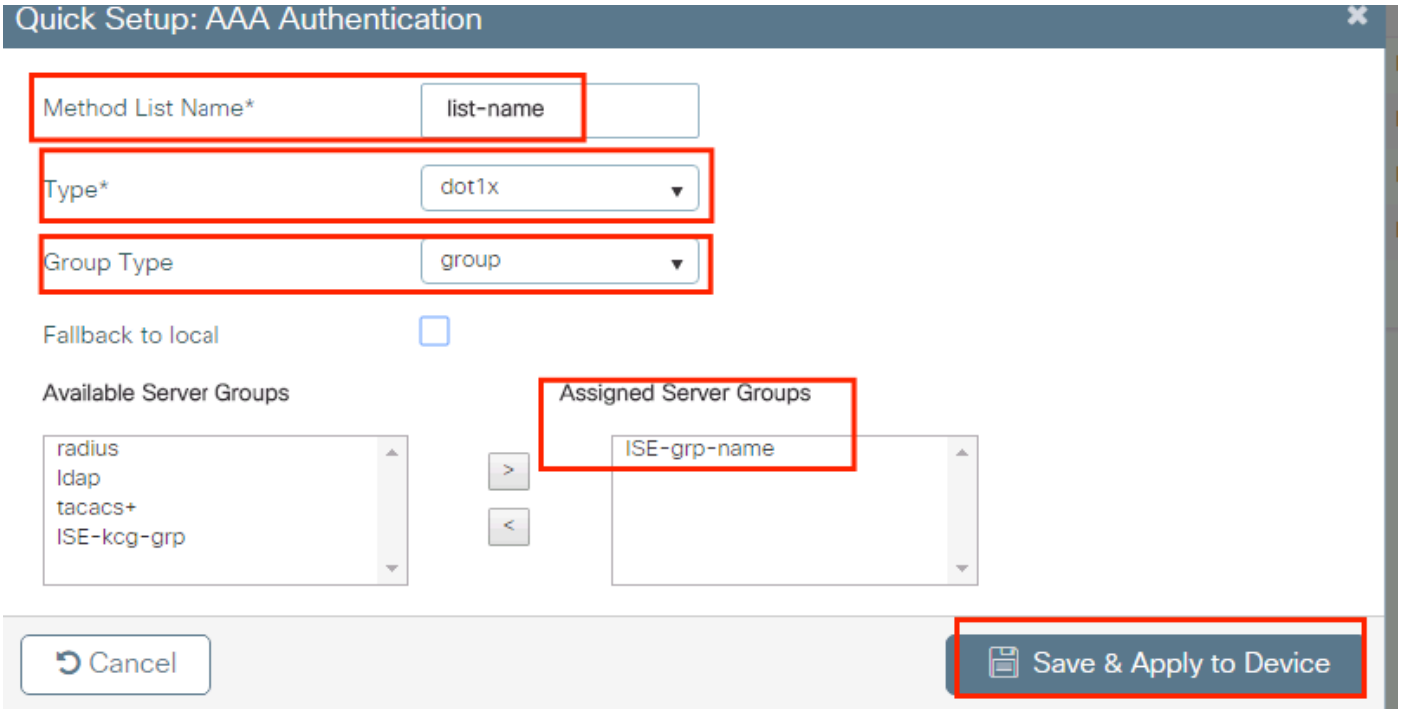
Passaggio 2. Aggiungere il server RADIUS a un gruppo RADIUS. Passare a **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.** Assegnare un nome al gruppo e spostare il server creato in precedenza nell'elenco di **Assigned Servers**.



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 # retransm
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) : cur
```

È possibile configurare sia il **dead criteria**, router che il router **deadtime** sul WLC, in particolare se si utilizzano più server RADIUS.

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

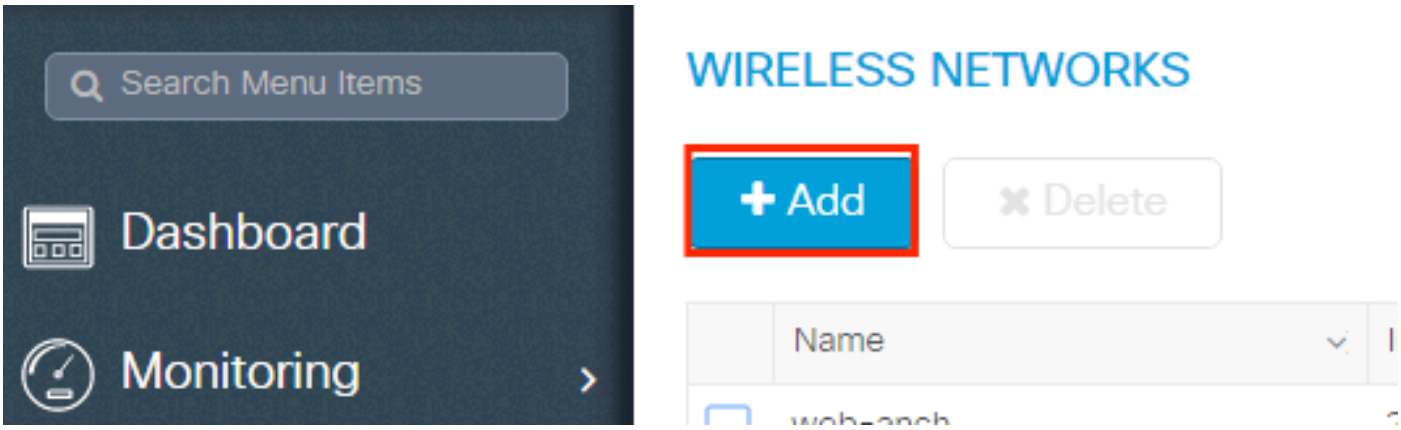
Nota: **dead criteria** è il criterio utilizzato per contrassegnare un server RADIUS come inattivo. Si compone di: 1. Un timeout (in secondi) che rappresenta il periodo di tempo che deve trascorrere tra il momento in cui il controller ha ricevuto per ultimo un pacchetto valido dal server RADIUS e il 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: **deadtime** specifica per quanto tempo (in minuti) 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.

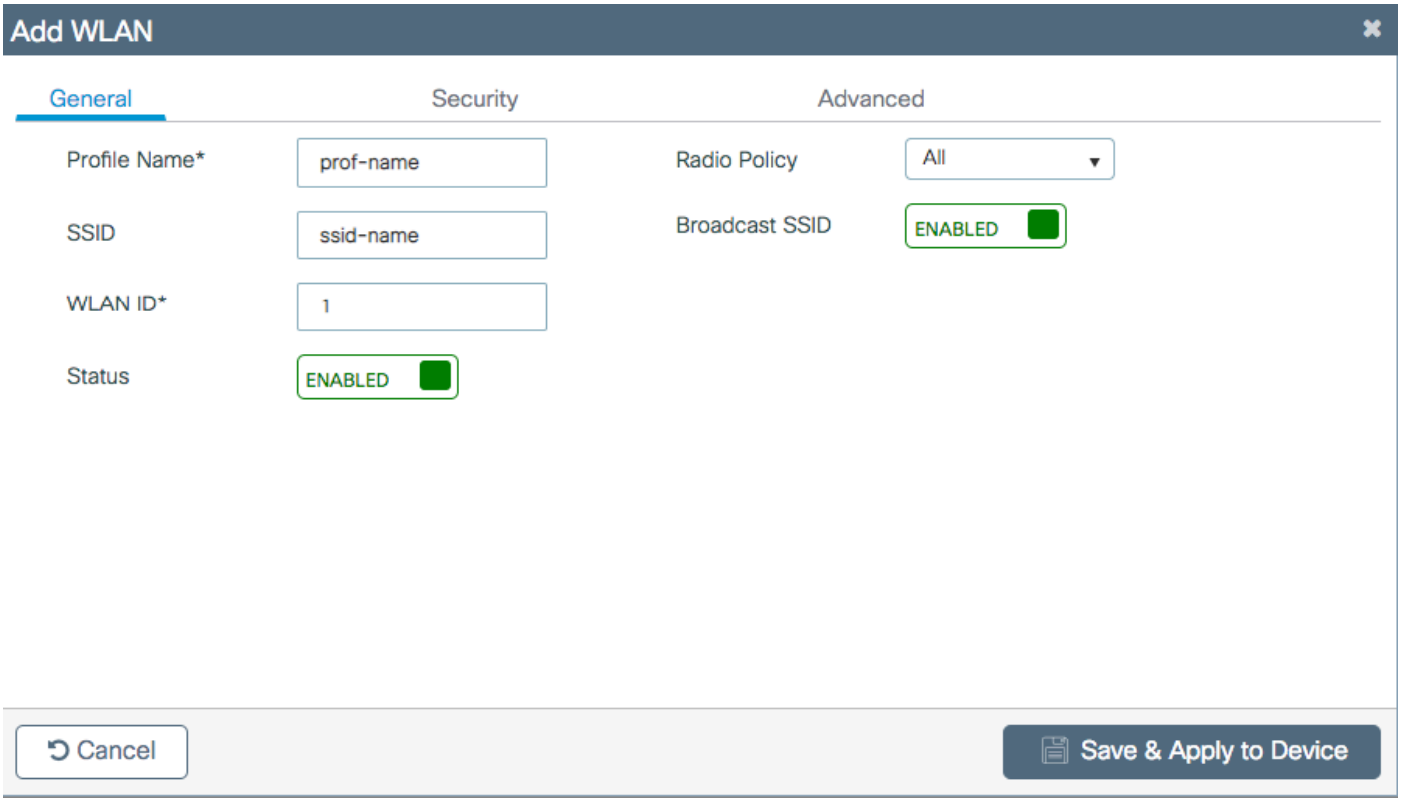
Configurazione profilo WLAN

GUI:

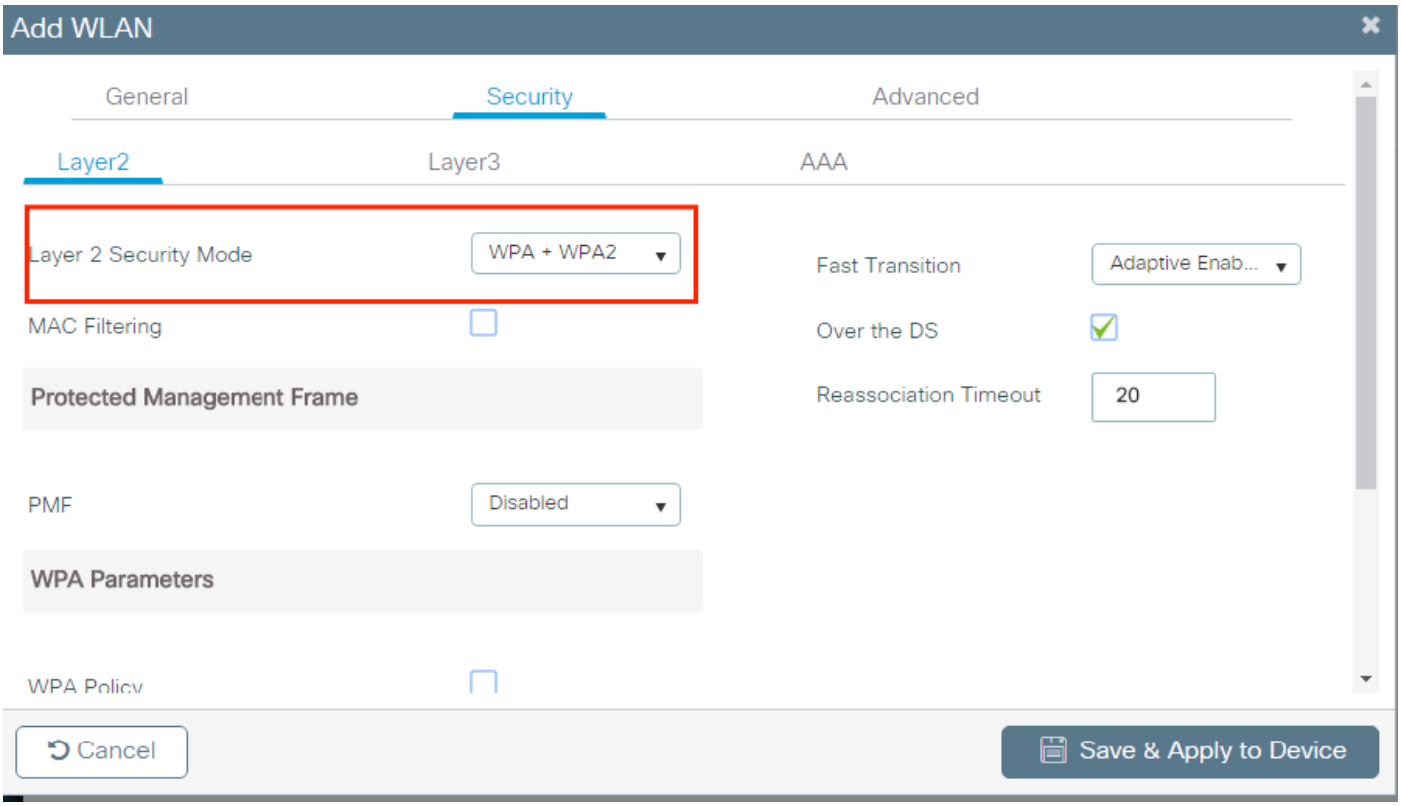
Passaggio 1. Creare la WLAN. Selezionare **Configurazione** > **Wireless** > **WLAN** > **+ Aggiungi** e configura la rete come necessario.

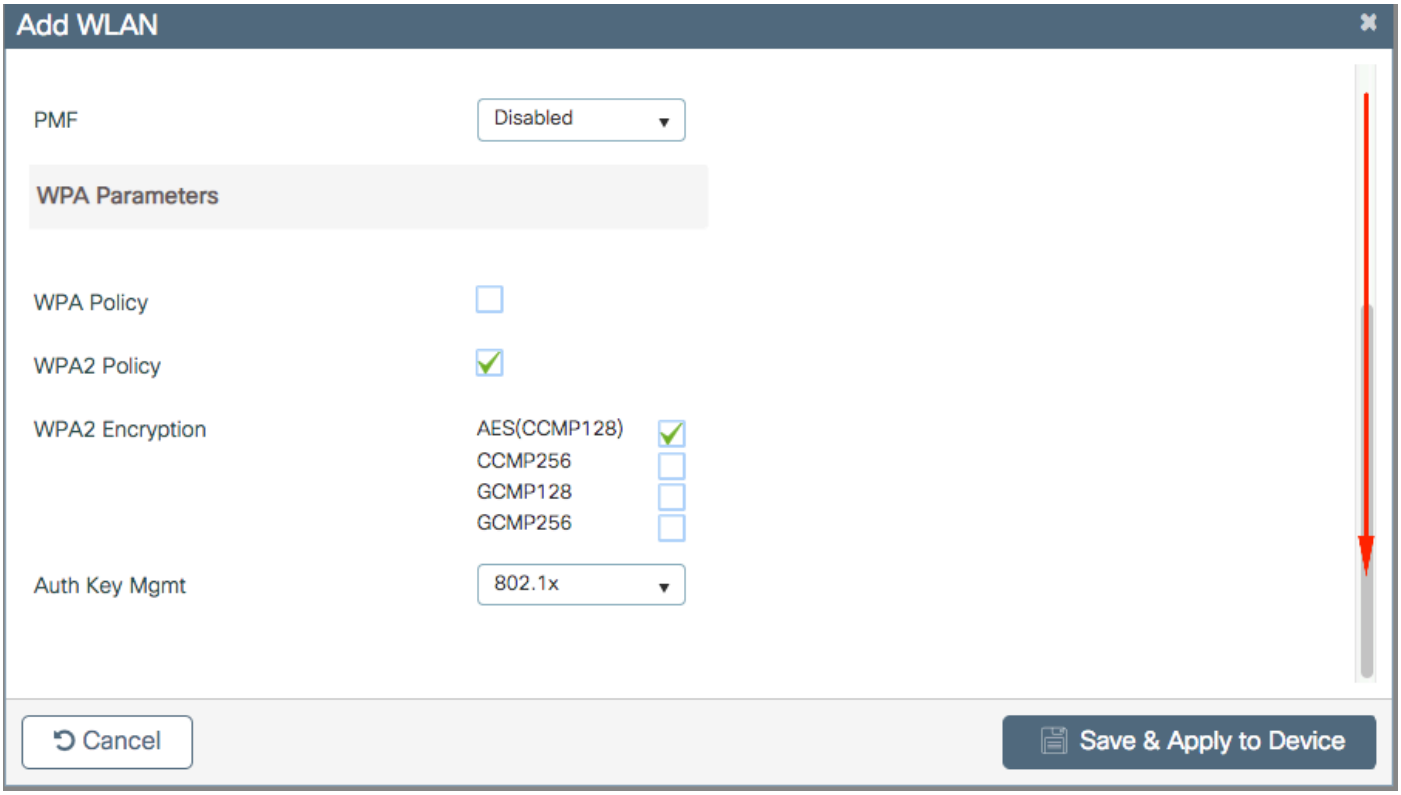


Passaggio 2. Immettere le informazioni sulla WLAN

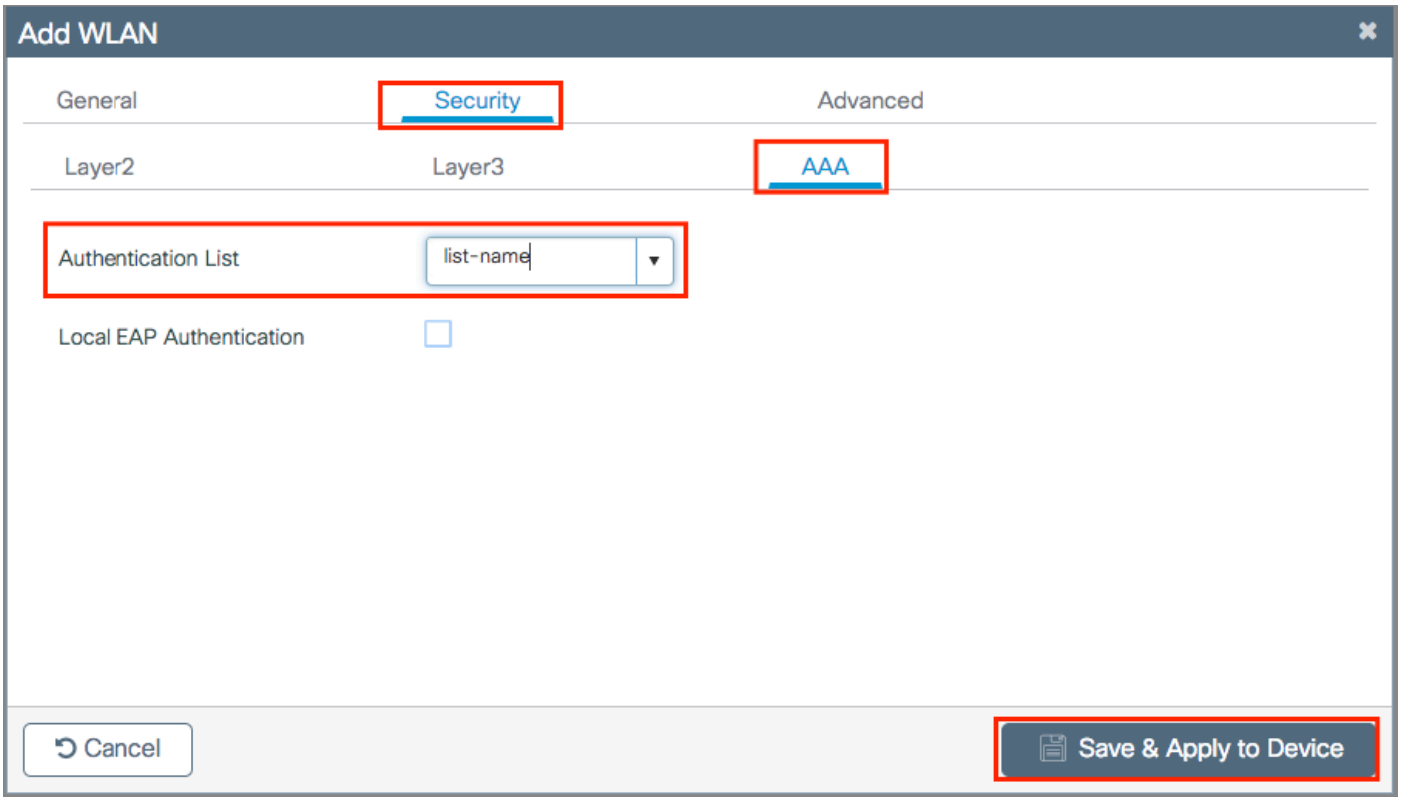


Passaggio 3. Passare alla scheda Protezione e selezionare il metodo di protezione desiderato. In questo caso, **WPA2 + 802.1x**.





Passaggio 4. Dalla **Security** > **AAA** scheda, selezionare il metodo di autenticazione creato al passo 3 dalla sezione Configurazione AAA su 9800 WLC.



CLI:

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

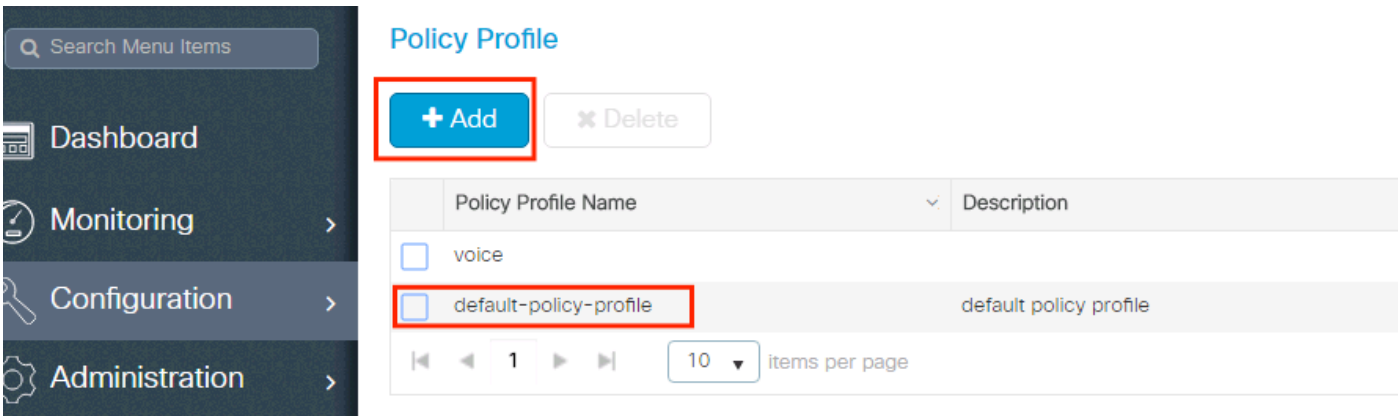
Configurazione del profilo di policy

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).

È possibile utilizzare il profilo dei criteri predefinito oppure creare un nuovo profilo.

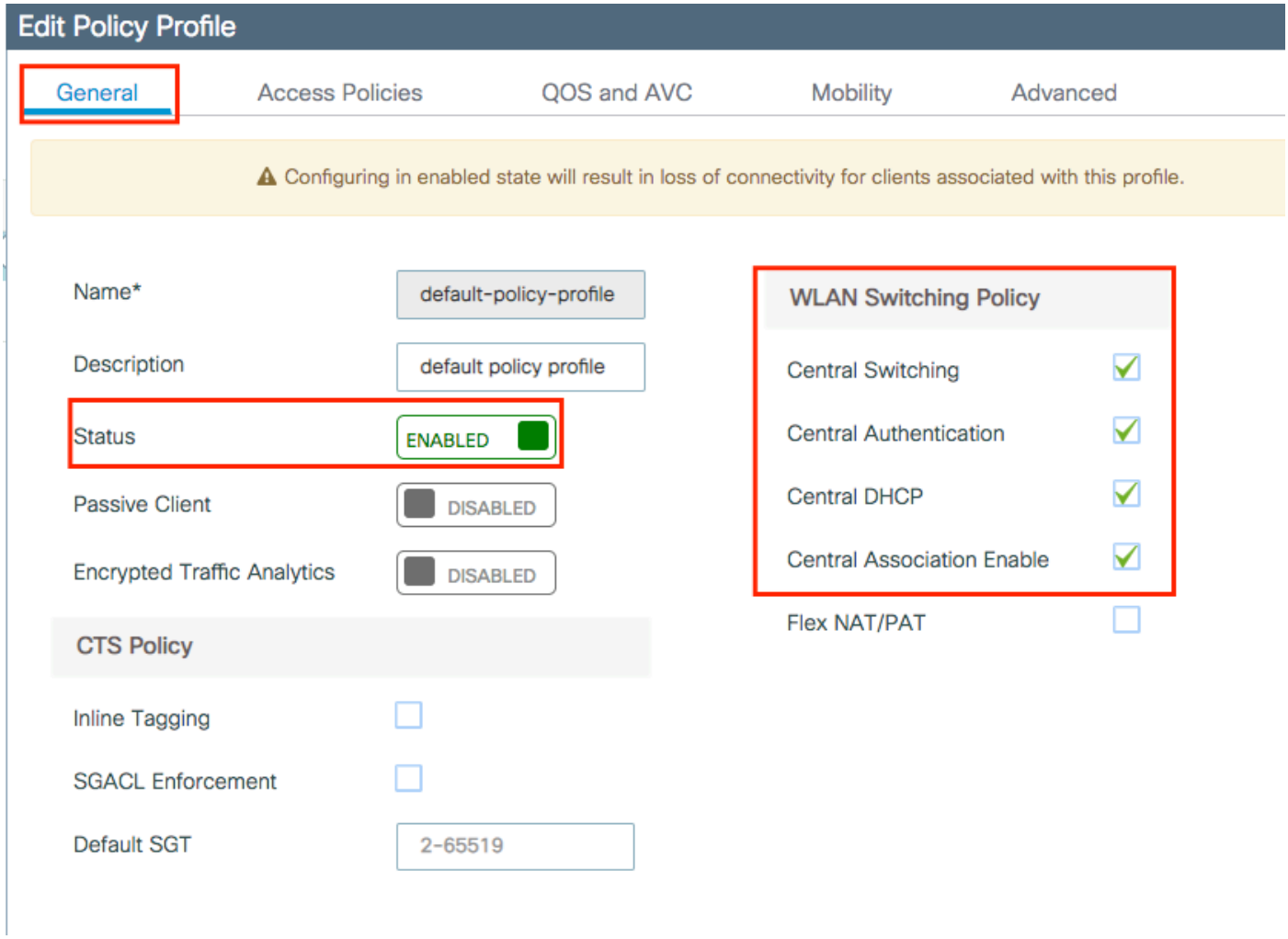
GUI:

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

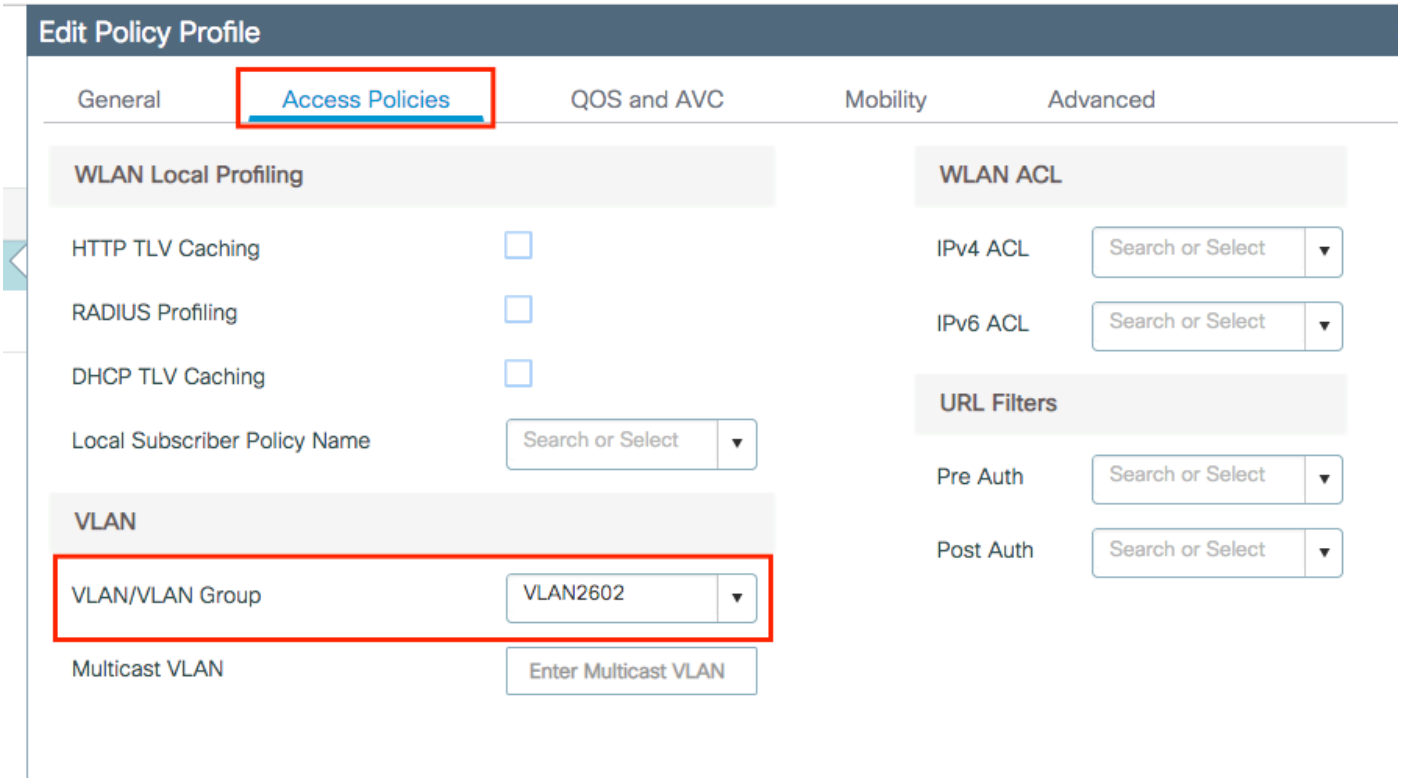


Verificare che il profilo sia abilitato.

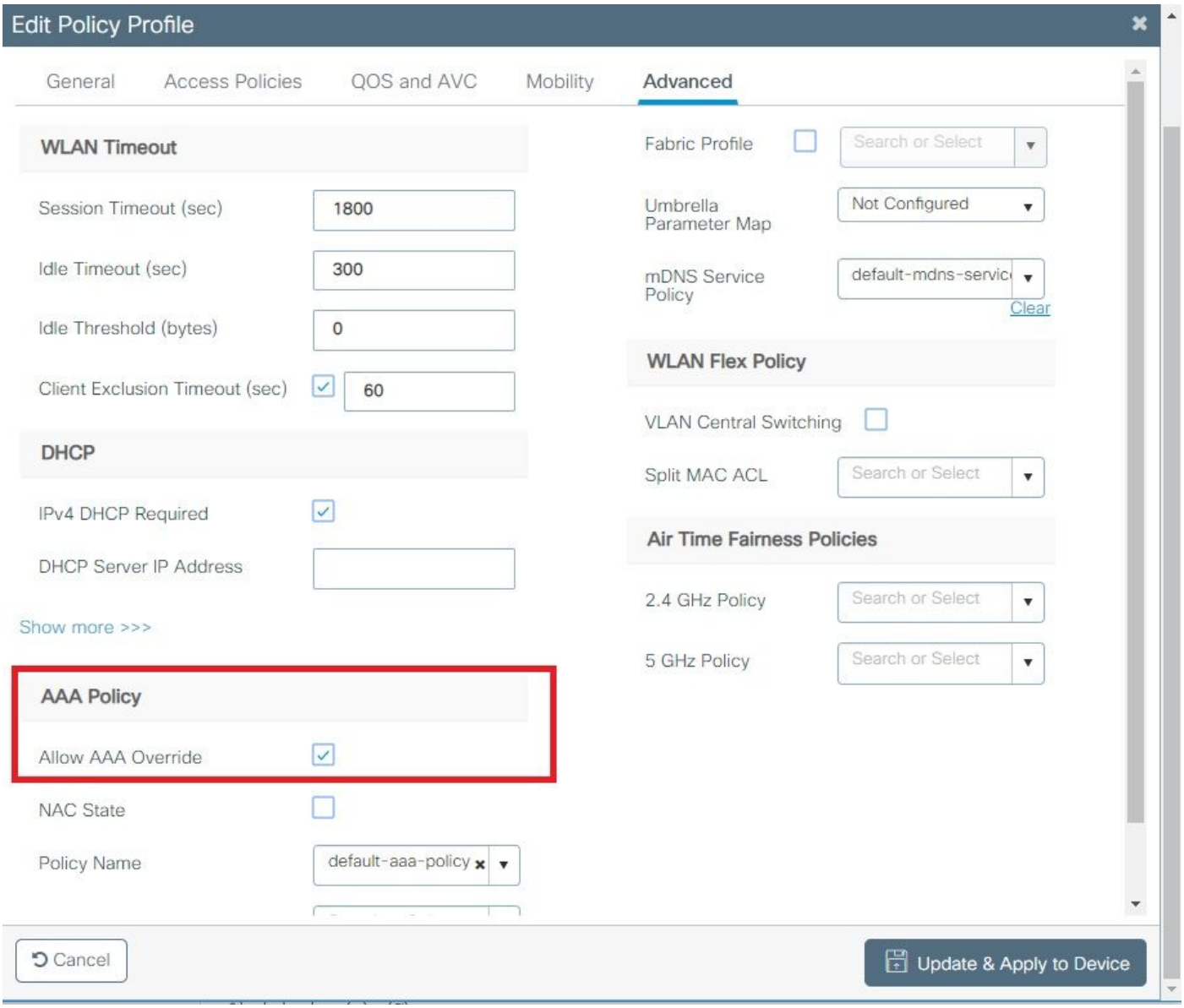
Inoltre, se il punto di accesso è in modalità locale, verificare che nel profilo della policy siano attivate le opzioni **Cambio centrale** e **Autenticazione centrale**.



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



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



CLI:

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

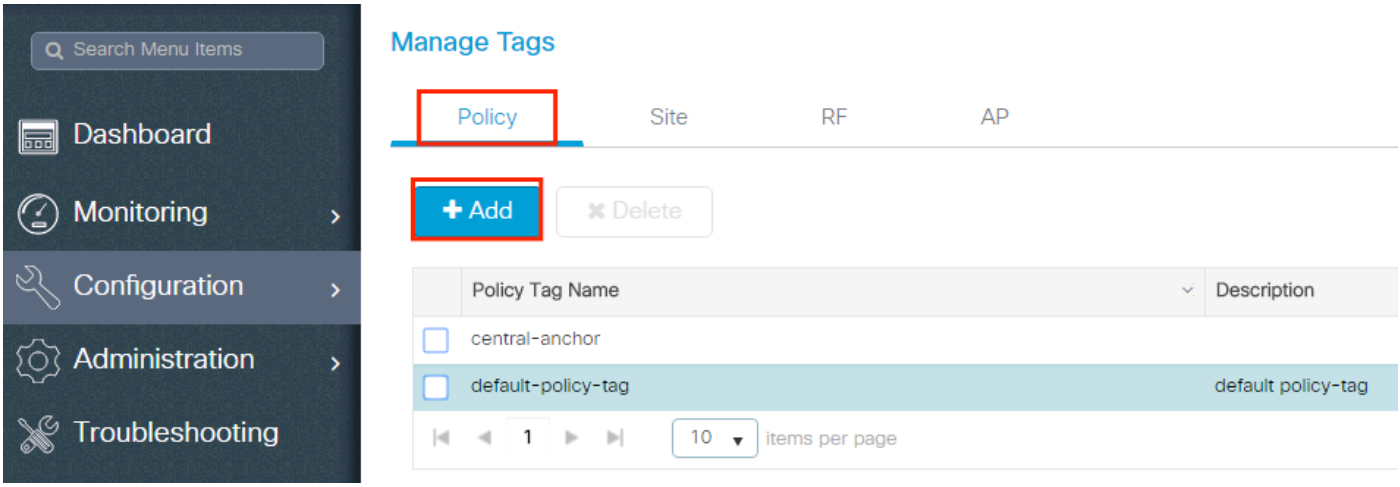
Configurazione del tag di policy

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.

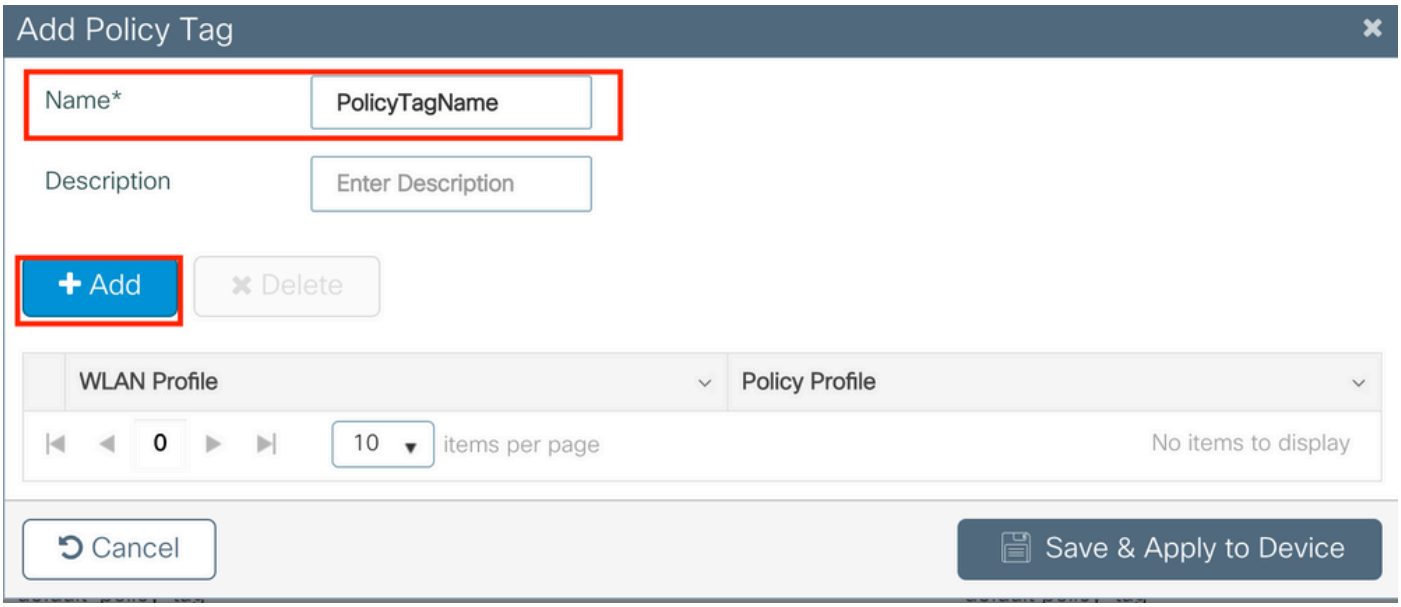
Nota: il tag default-policy-tag mappa automaticamente qualsiasi SSID con ID WLAN compreso tra 1 e 16 al profilo default-policy-profile. Non può essere né modificata né eliminata. Se si dispone di una WLAN con ID 17 o superiore, non è possibile utilizzare il tag default-policy.

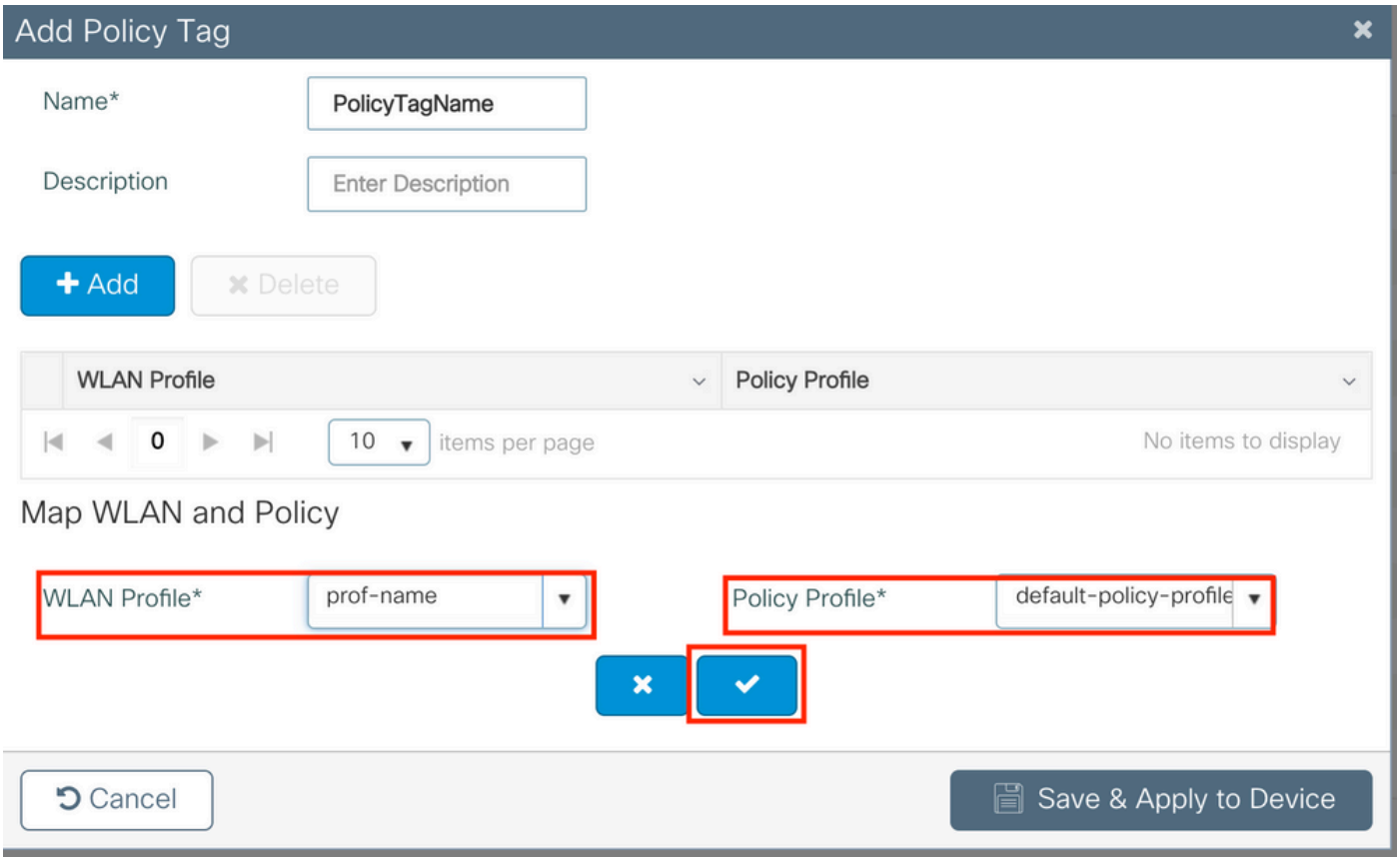
GUI:

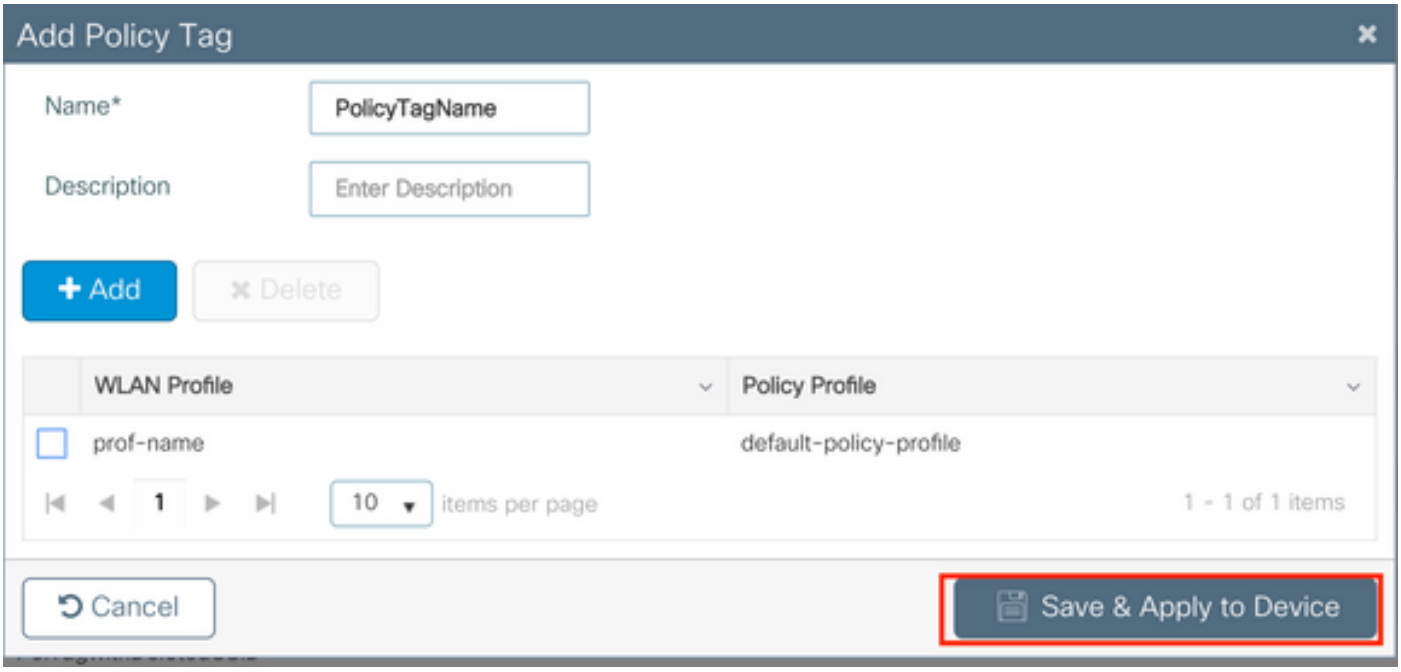
Se necessario, individuare **Configugation > Tags & Profiles > Tags > Policy** e aggiungere un nuovo elemento.



Associare il profilo WLAN al profilo di policy desiderato.







CLI:

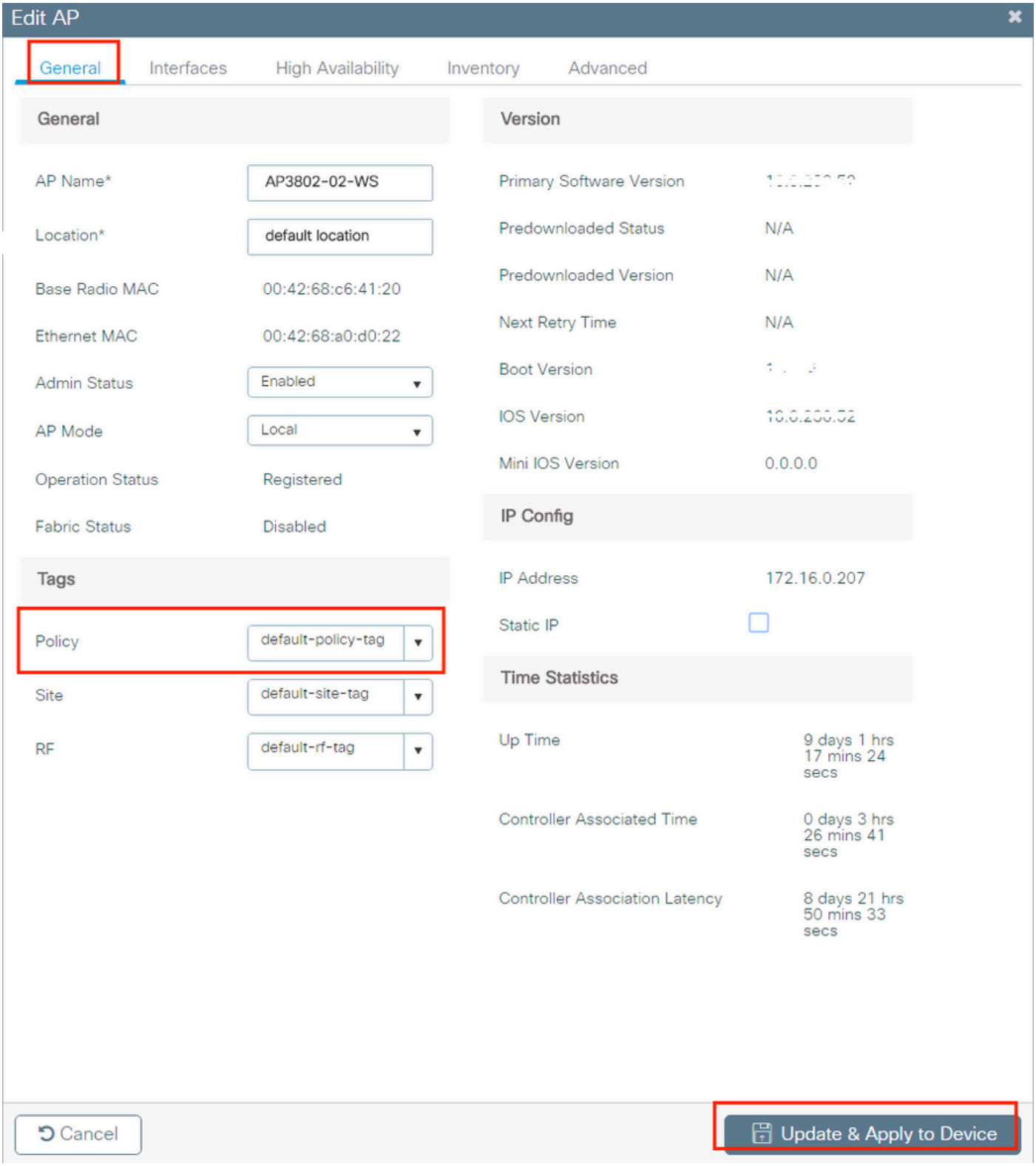
config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>

Assegnazione tag criteri

Assegnare il tag di policy agli access point desiderati.

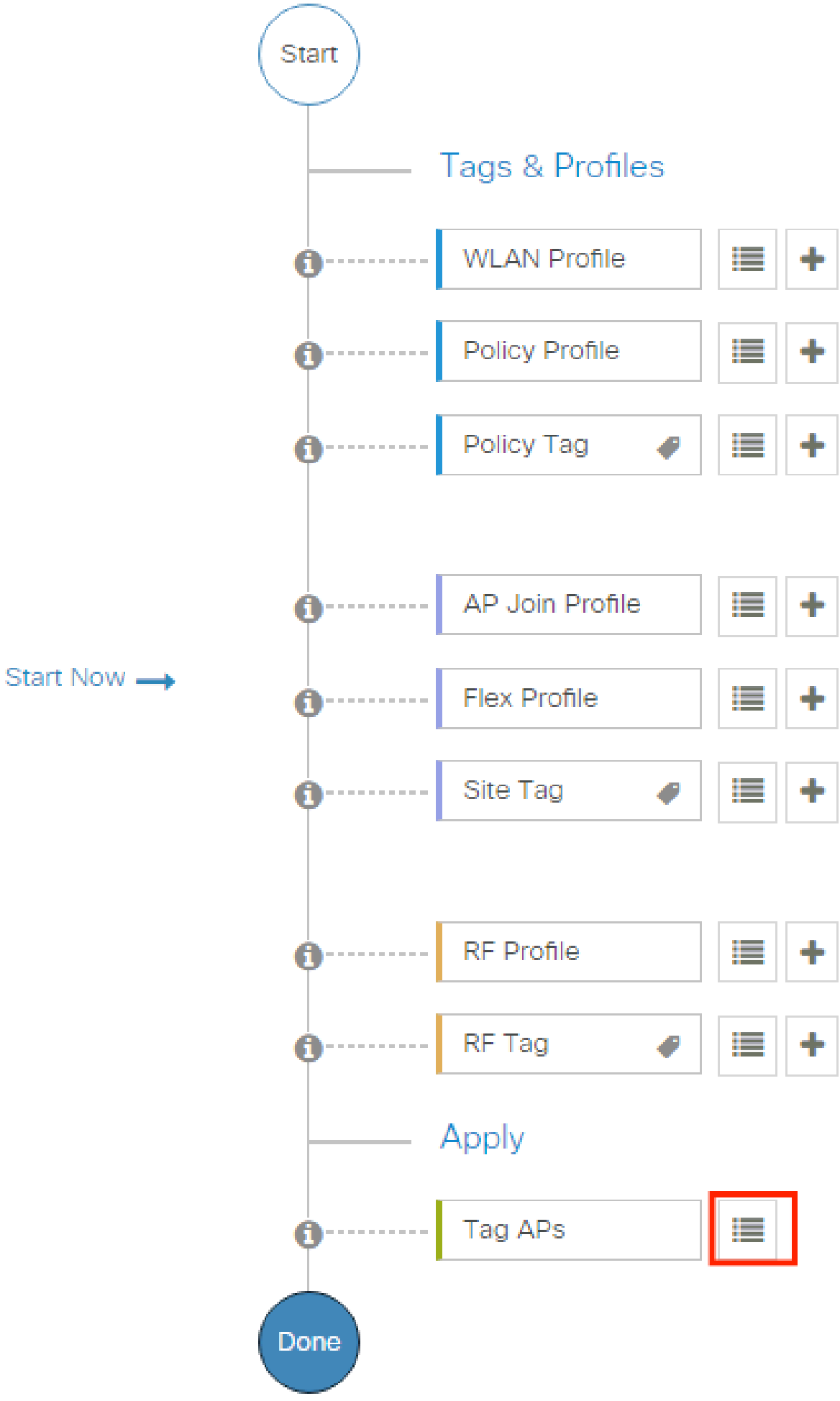
GUI:

Per assegnare il tag a un punto di accesso, spostarsi per **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.

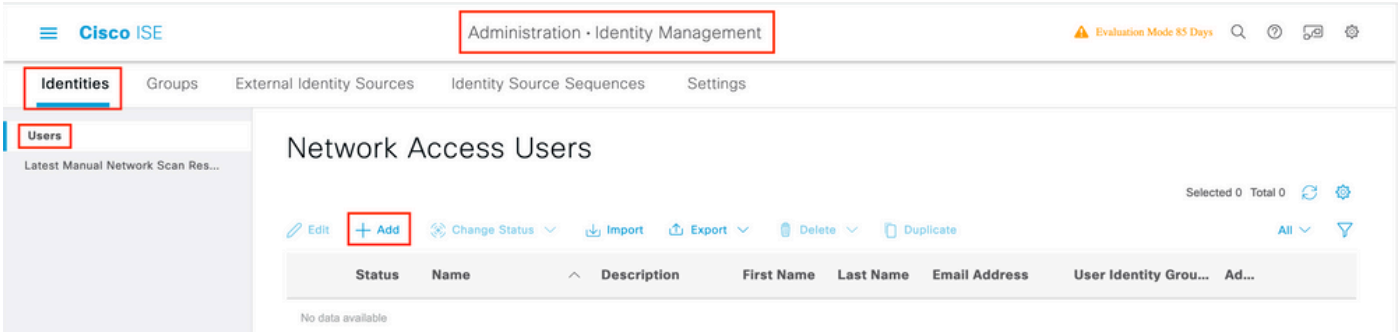
Per assegnare lo stesso tag criteri a più access point, passare a **Configuration > Wireless Setup > Advanced > Start Now > Apply**.


Start
Tags & Profiles
WLAN Profile
Policy Profile
Policy Tag
AP Join Profile
Start Now
Flex Profile
Site Tag
RF Profile
RF Tag
Apply
Tag APs
Done

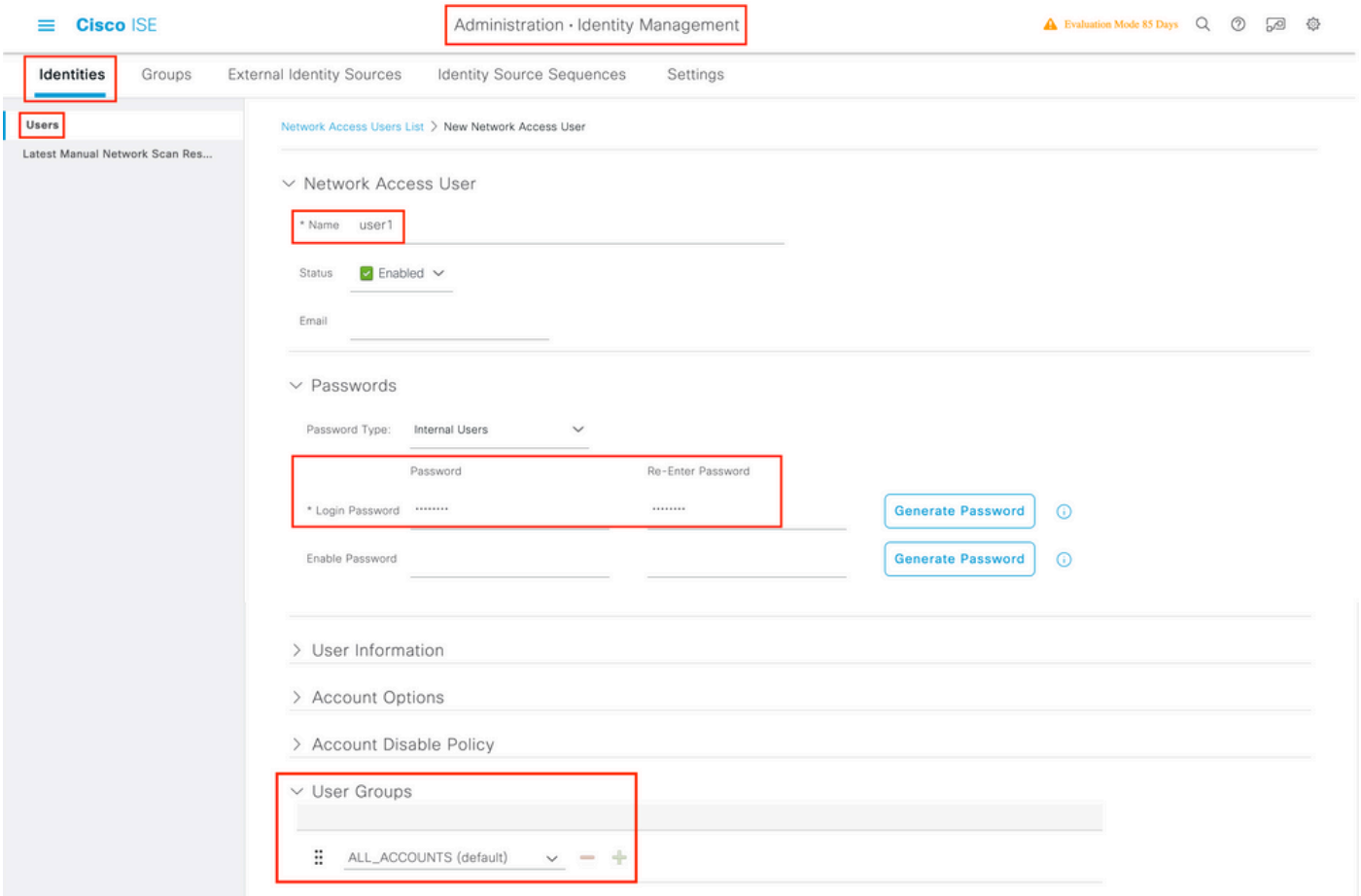
su questo argomento, vedere il capitolo relativo alla gestione dei dispositivi di rete nel manuale Cisco Identity Services Engine Administrator Guide, : Network Device Groups

Creazione di un nuovo utente in ISE

Passaggio 1. Spostarsi **Administration > Identity Management > Identities > Users > Add** tra i punti come mostrato nell'immagine:



Passaggio 2. Immettere le informazioni per l'utente. In questo esempio, l'utente appartiene a un gruppo denominato ALL_ACCOUNTS, ma può essere modificato in base alle esigenze, come mostrato nell'immagine:

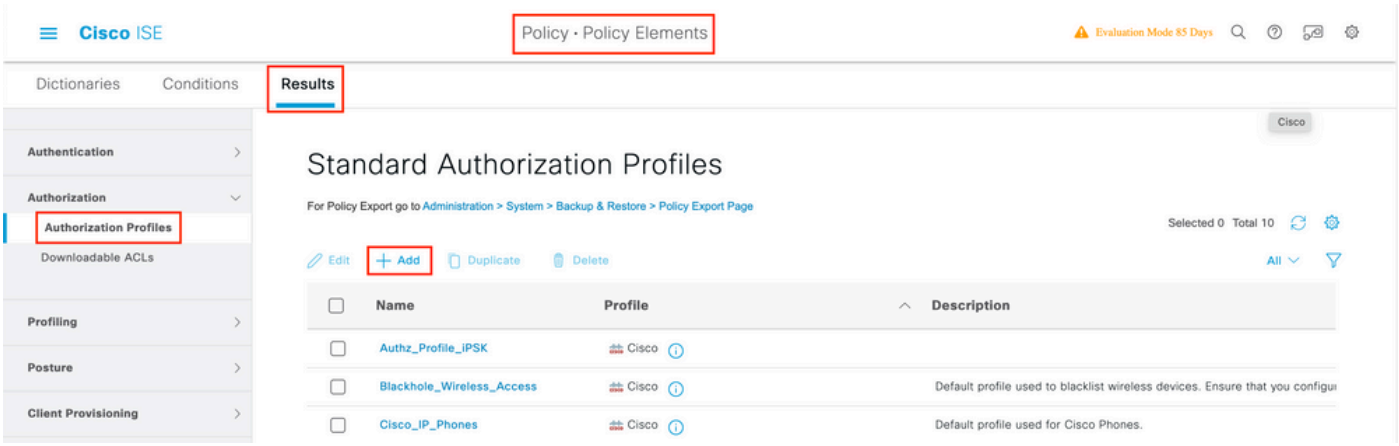


Creazione del profilo di autorizzazione

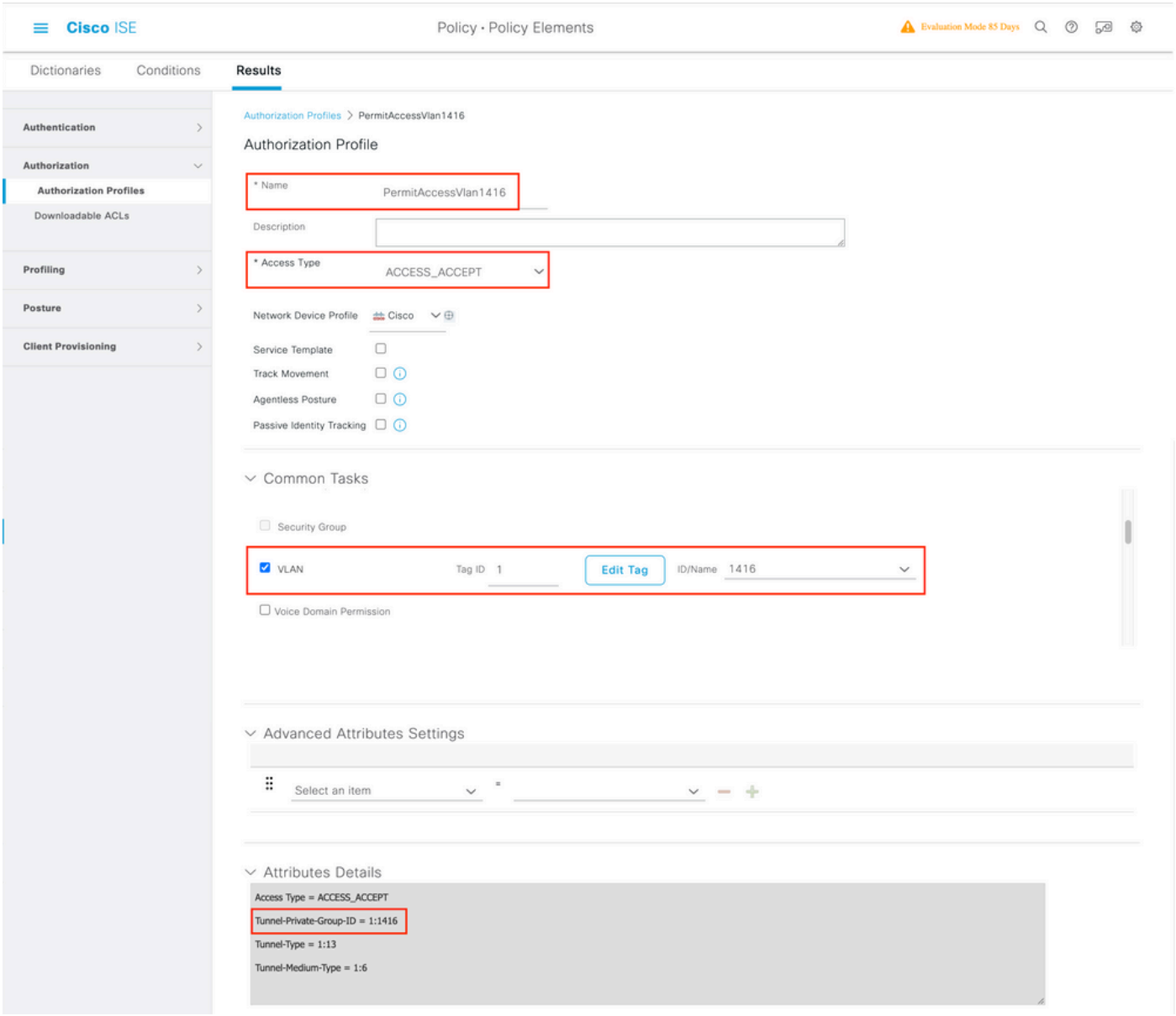
L' **Authorization Profile** oggetto è costituito da un set di attributi che vengono restituiti quando una condizione viene soddisfatta. Il profilo di autorizzazione determina se il client ha accesso o meno alla rete, esegue il push degli Access Control Lists (ACL), esegue l'override della VLAN

o di qualsiasi altro parametro. Il profilo di autorizzazione mostrato in questo esempio invia un'autorizzazione di accesso per il client e assegna il client alla VLAN 1416.

Passaggio 1. Individuare **Policy > Policy Elements > Results > Authorization > Authorization Profiles** e fare clic sul **Add** pulsante.

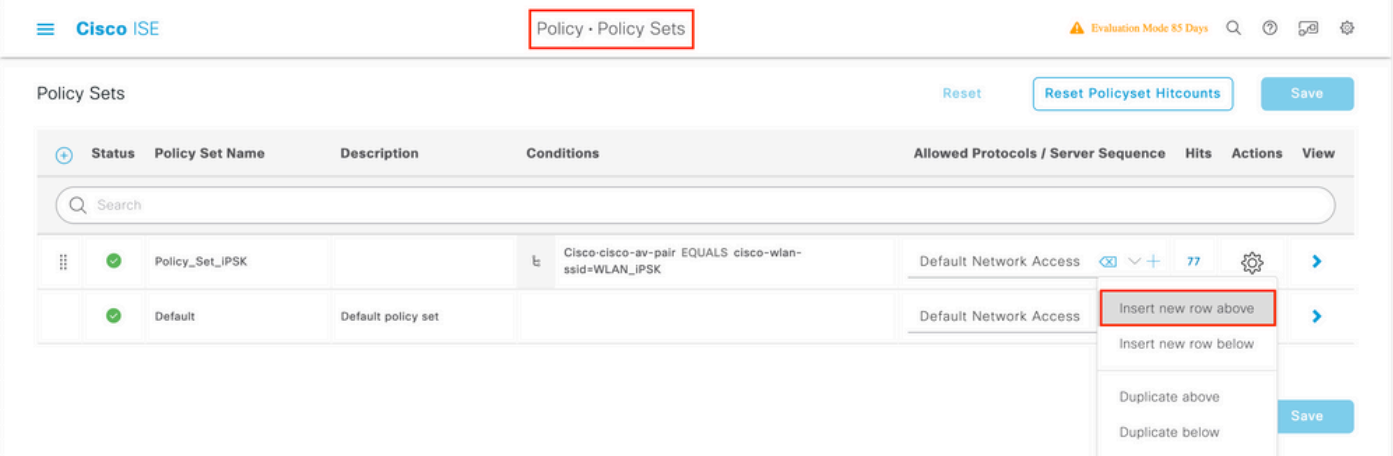


Passaggio 2. Immettete i valori come mostrato nell'immagine. In questa sezione è possibile restituire gli attributi di override AAA, ad esempio VLAN. La WLC 9800 accetta gli attributi del tunnel 64, 65, 81 che usano l'ID VLAN o il nome e accetta anche l'uso dell' **AirSpace-Interface-Name** attributo.



Crea set di criteri

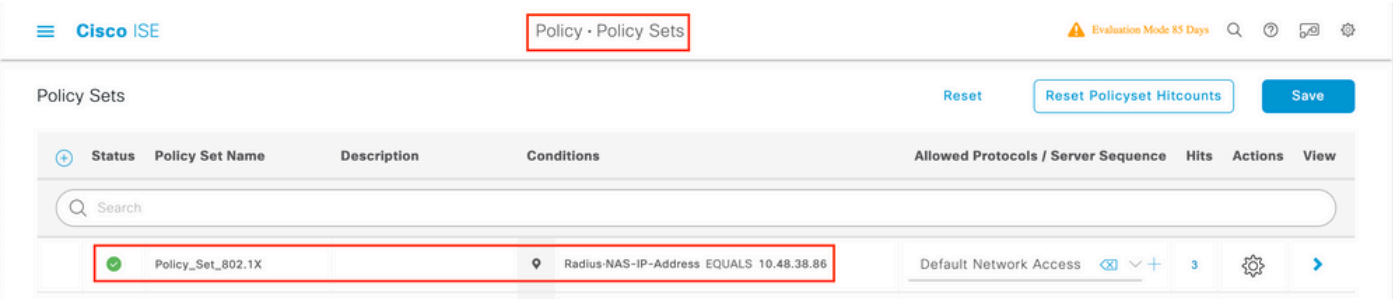
Un set di criteri definisce un insieme di regole di autenticazione e autorizzazione. Per crearne uno, andare a **Policy > Policy Sets**, fare clic sull'ingranaggio del primo set di criteri nell'elenco e selezionare **Insert new row above** come mostrato in questa immagine:



Configurare un nome e creare una condizione per questo set di criteri. Nell'esempio, la condizione specifica che il traffico proveniente dal WLC corrisponde:

```
Radius:NAS-IP-Address EQUALS X.X.X.X // X.X.X.X is the WLC IP address
```

Assicurarsi che **Default Network Access** sia selezionato in **Allowed Protocols / Server Sequence**.



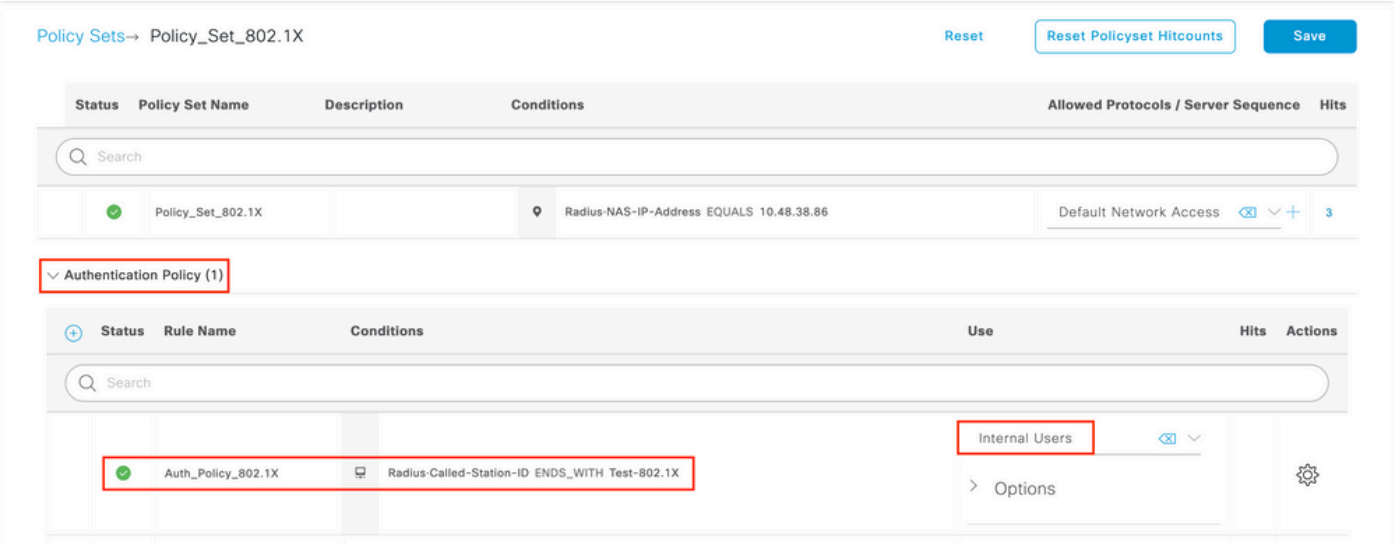
Crea criterio di autenticazione

Per configurare i criteri di autenticazione e autorizzazione, è necessario immettere la configurazione del set di criteri. A tale scopo, fare clic sulla freccia blu a destra della **Policy Set** riga:

I **criteri di autenticazione** vengono utilizzati per verificare se le credenziali degli utenti sono corrette (verificare se l'utente è effettivamente l'utente a cui è associato). In **Authenticaton Policy**, creare un criterio di autenticazione e configurarlo come illustrato nell'immagine. La condizione per il criterio utilizzato in questo esempio è:

```
RADIUS:Called-Station-ID ENDS_WITH <SSID> // <SSID> is the SSID of your WLAN
```

Scegliere inoltre **la scheda Utenti interni** nella **Use** scheda di questi criteri di autenticazione.

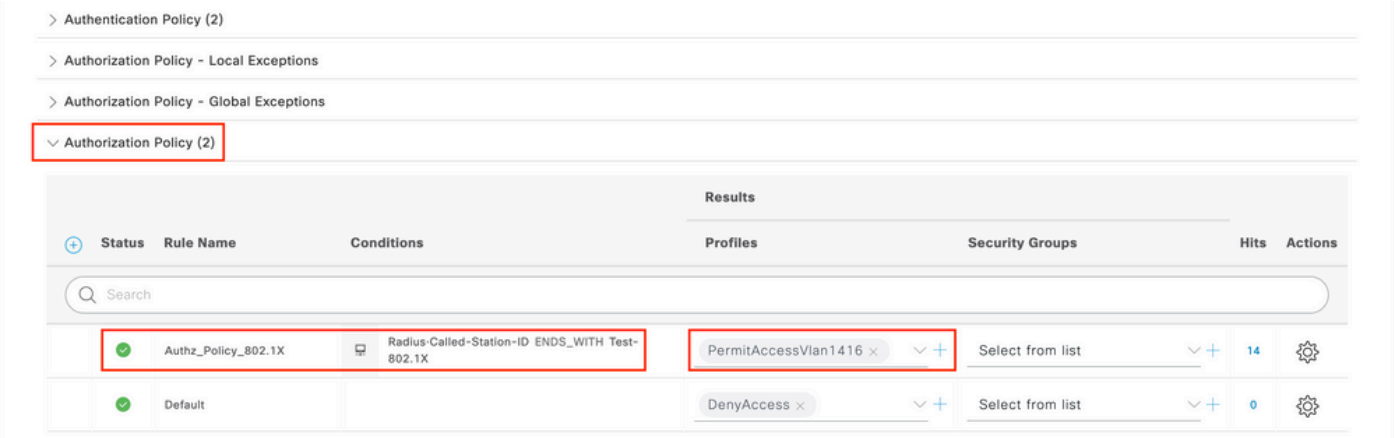


Crea criterio di autorizzazione

Nella stessa pagina crearne una **Authorization Policy** . La condizione per questo criterio di autorizzazione è:

```
RADIUS:Called-Station-ID ENDS_WITH <SSID> // <SSID> is the SSID of your WLAN
```

Nella **Result > Profiles** scheda di questo criterio, selezionare la **Authorization Profile** scheda creata in precedenza. In questo modo, ISE invierà gli attributi corretti al WLC se l'utente è autenticato.



A questo punto, se tutta la configurazione per il WLC e l'ISE è completa, è possibile provare a connettersi con un client.

Per ulteriori informazioni sui criteri ISE Allow Protocols, vedere il capitolo: Manage Authentication Policies nel manuale Cisco Identity Services Engine Administrator Guide. [Manage Authentication Policies]

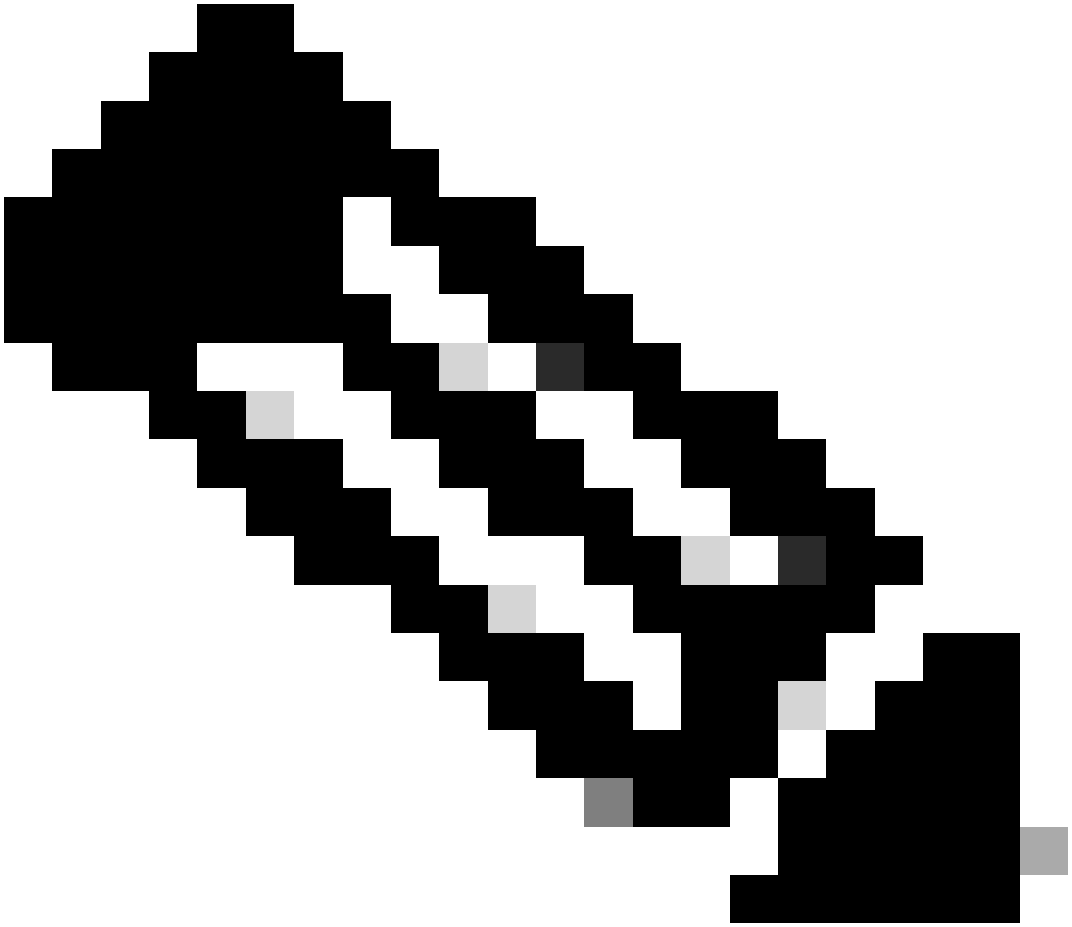
Per ulteriori informazioni su ISE Identity Sources, consultare il capitolo: Manage Users and External Identity Sources nel manuale Cisco Identity Services Engine Administrator Guide: Identity Sources

Verifica

È possibile utilizzare questi comandi per verificare la configurazione corrente:

show run wlan // WLAN configuration # show run aaa // AAA configuration (server, server group, methods) # show aaa servers // Configured AAA serve
show ap tag summary // Tag information for AP'S
show wlan { summary | id | name | all } // WLAN details
show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
show wireless profile policy detailed <policy-profile name>// Detailed information on given policy profile

Risoluzione dei problemi



Nota: l'utilizzo dei servizi di bilanciamento del carico esterni è corretto. Verificare tuttavia che il servizio di bilanciamento del carico funzioni per client utilizzando l'attributo RADIUS id stazione chiamante. L'utilizzo della porta di origine UDP non è un meccanismo supportato per il bilanciamento delle richieste RADIUS provenienti da 9800.

Risoluzione dei problemi sul WLC

WLC 9800 offre funzionalità di traccia ALWAYS-ON. In questo modo, tutti gli errori, gli avvisi e i messaggi relativi alla connettività del client vengono registrati costantemente ed è possibile visualizzare i registri di un evento imprevisto o di una condizione di errore dopo che si è verificato.

Dipende dal volume dei registri generati, ma in genere è possibile tornare indietro di alcune ore o diversi giorni.

Per visualizzare le tracce raccolte per impostazione predefinita dal protocollo 9800 WLC, è possibile connettersi al protocollo 9800 WLC in modalità SSH/Telnet e procedere come segue: (accertarsi di registrare la sessione su un file di testo).

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

show clock

Passaggio 2. Raccogliere i syslog dal buffer WLC o dal syslog esterno, in base alla configurazione del sistema. In questo modo è possibile visualizzare rapidamente lo stato di integrità del sistema ed eventuali errori.

show logging

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

show debugging IOSXE Conditional Debug Configs: Conditional Debug Global State: Stop IOSXE Packet Tracing Configs: Packet Infra debugs: Ip Add

Nota: se nell'elenco viene visualizzata una condizione, le tracce vengono registrate a livello di debug per tutti i processi che soddisfano le condizioni abilitate (indirizzo MAC, indirizzo IP e così via). In questo modo si aumenta il volume dei registri. È pertanto consigliabile cancellare tutte le condizioni quando non si esegue il debug attivo.

Passaggio 4. Si supponga che l'indirizzo MAC in test non sia stato elencato come condizione nel passaggio 3, raccogliere le tracce del livello di avviso always on per l'indirizzo MAC specifico:

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

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

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Debug condizionale e traccia Radioactive (RA)

Se le tracce sempre attive non forniscono informazioni sufficienti per determinare il trigger del problema in esame, è possibile abilitare il debug condizionale e acquisire la traccia Radio attiva (RA), che fornisce le tracce a livello di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client). È possibile farlo tramite la GUI o la CLI.

CLI:

Per abilitare il debug condizionale, effettuare le seguenti operazioni:

Passaggio 5. Verificare che non vi siano condizioni di debug abilitate.

```
# clear platform condition all
```

Passaggio 6. Abilitare la condizione di debug per l'indirizzo MAC del client wireless che si desidera monitorare.

Questo comando avvia il monitoraggio dell'indirizzo MAC fornito per 30 minuti (1800 secondi). È possibile aumentare il tempo fino a 2085978494 secondi.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Nota: per monitorare più client alla volta, eseguire il comando debug wireless mac <aaa.bbbb.ccc> per ogni indirizzo MAC.

Nota: non è possibile visualizzare l'output dell'attività del client in una sessione terminale, in quanto tutto viene memorizzato internamente nel buffer per essere visualizzato successivamente.

Passaggio 7. Riprodurre il problema o il comportamento che si desidera monitorare.

Passaggio 8. Interrompere i debug se il problema viene riprodotto prima che scada il tempo del monitor predefinito o configurato.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Una volta trascorso il tempo di monitoraggio o interrotto il debug wireless, il controller 9800 WLC genera un file locale con il nome:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Passaggio 9. Recuperare il file dell'attività dell'indirizzo MAC. È possibile copiare il file trace.log su un server esterno oppure visualizzare l'output direttamente sullo schermo.

Controllare il nome del file delle tracce RA:

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

Copiare il file su un server esterno:

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

Visualizzare il contenuto:

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

Passaggio 10. Se la causa principale non è ancora ovvia, raccogliere i log interni, che offrono una visualizzazione più dettagliata dei log del livello di debug. Non è necessario eseguire di nuovo il debug del client per ulteriori dettagli sui log di debug già raccolti e archiviati internamente.

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

Nota: questo output del comando restituisce tracce per tutti i livelli di log per tutti i processi ed è piuttosto voluminoso. Contattare Cisco TAC per analizzare queste tracce.

È possibile copiare il file ra-internal-FILENAME.txt su un server esterno o visualizzare l'output direttamente sullo schermo.

Copiare il file su un server esterno:

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

Visualizzare il contenuto:

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

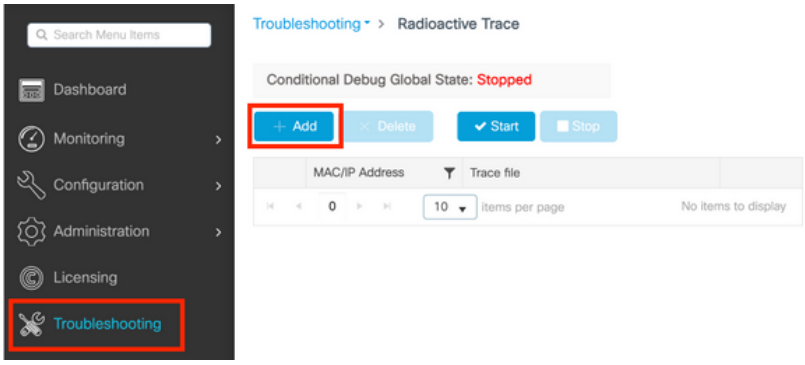
Passaggio 11. Rimuovere le condizioni di debug.

clear platform condition all

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

GUI:

Passaggio 1. Accedere a **Troubleshooting > Radioactive Trace > + Add** e specificare l'indirizzo MAC/IP dei client per i quali si desidera risolvere i problemi.

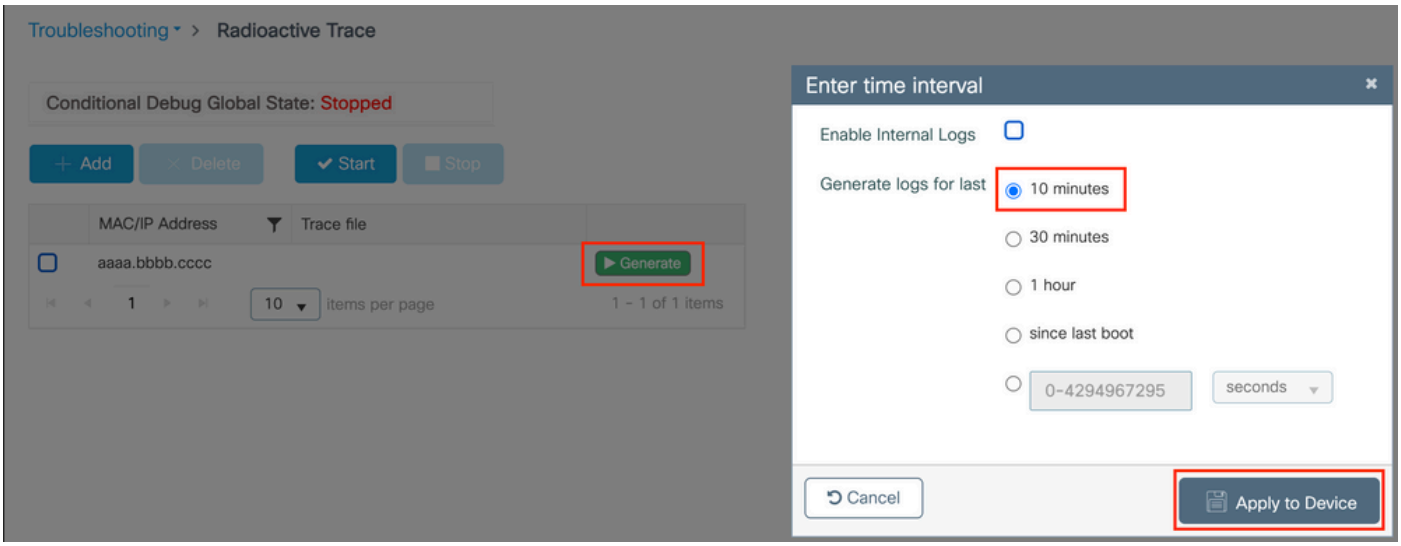


Passaggio 2. Fare clic su **Start**.

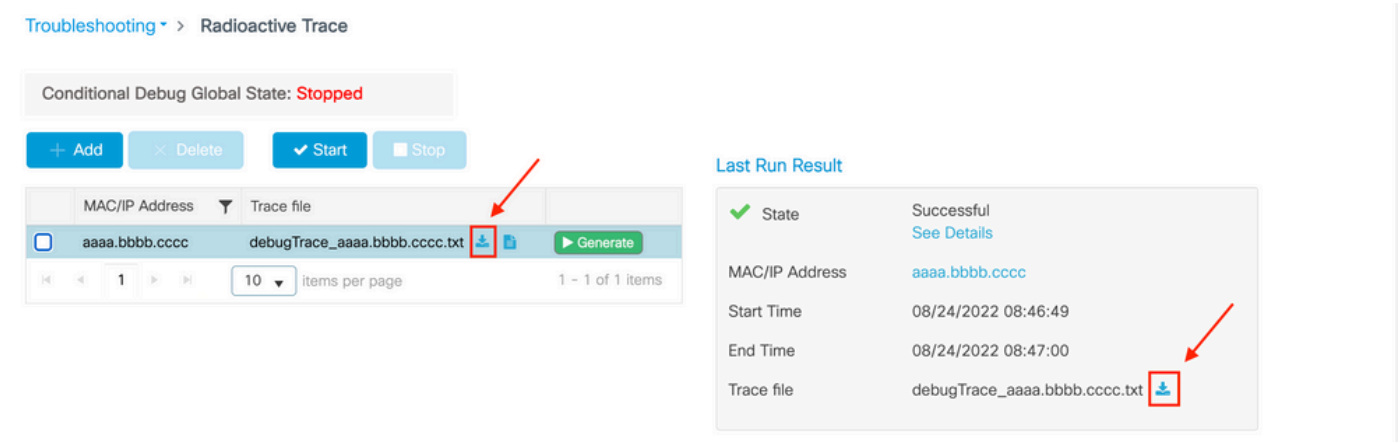
Passaggio 3. Riprodurre il problema.

Passaggio 4. Fare clic su **Stop**.

Passaggio 5. Fare clic sul **Generate** pulsante, selezionare l'intervallo di tempo per il quale si desidera ottenere i registri e fare clic su **Apply to Device**. In this example, the logs for the last 10 minutes are requested.

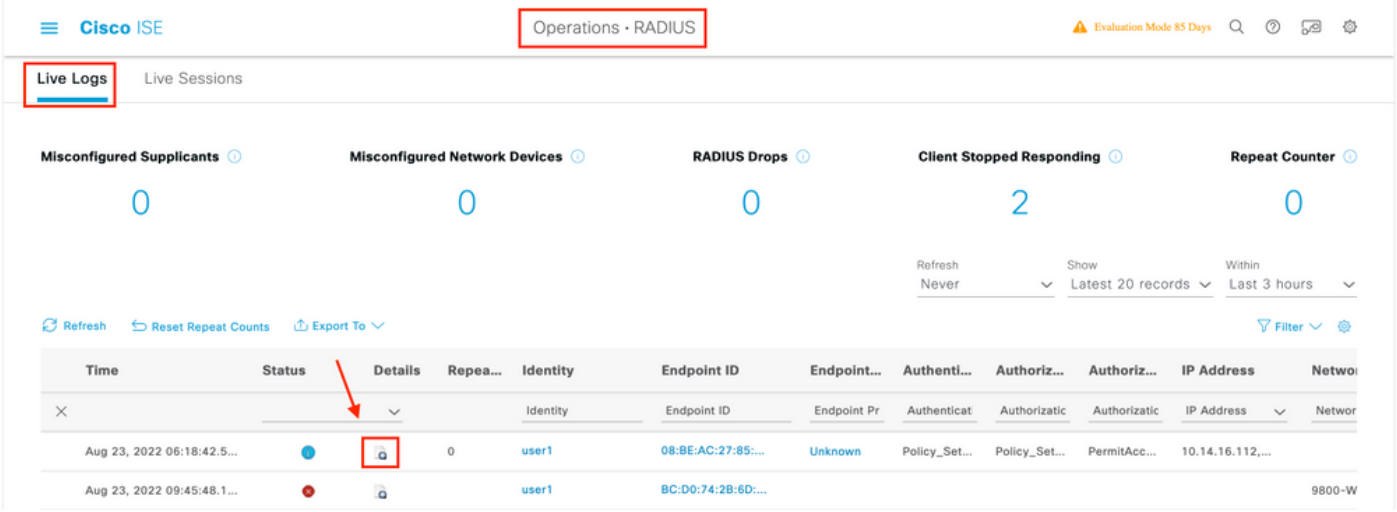


Passaggio 6. Scaricare la Traccia radioattiva sul computer, fare clic sul pulsante di download ed esaminarla.



Risoluzione dei problemi con ISE

In caso di problemi con l'autenticazione del client, è possibile verificare i log sul server ISE. Passare a **Operations > RADIUS > Live Logs** e visualizzare l'elenco delle richieste di autenticazione, il set di criteri corrispondente, il risultato di ogni richiesta e così via. È possibile ottenere maggiori dettagli facendo clic sulla lente di ingrandimento sotto la **Details** linguetta di ciascuna linea, come mostrato nell'immagine:


Cisco ISE
Operations · RADIUS
Evaluation Mode 85 Days
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
2
Repeat Counter
0
Refresh
Never
Show
Latest 20 records
Within
Last 3 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authenti...
Authoriz...
Authoriz...
IP Address
Networ
Identity
Endpoint ID
Endpoint Pr
Authenticat
Authorizatic
Authorizatic
IP Address
Networ
Aug 23, 2022 06:18:42.5...
0
user1
08:BE:AC:27:85:...
Unknown
Policy_Set...
Policy_Set...
PermitAcc...
10.14.16.112,...
Aug 23, 2022 09:45:48.1...
user1
BC:D0:74:2B:6D:...
9800-W

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).