

# 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 WLConISE](#)

[Crea nuovo utente su 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

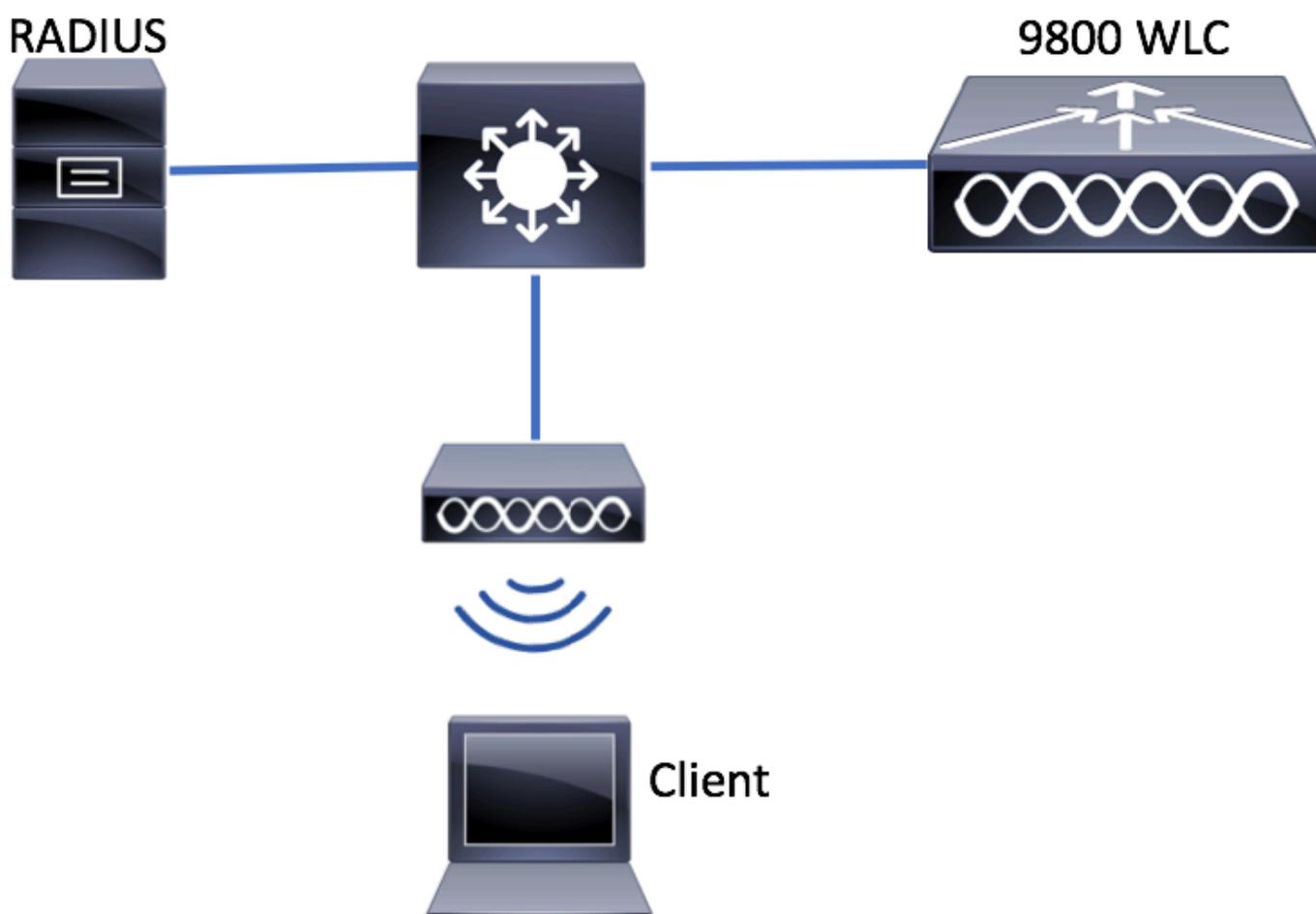
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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

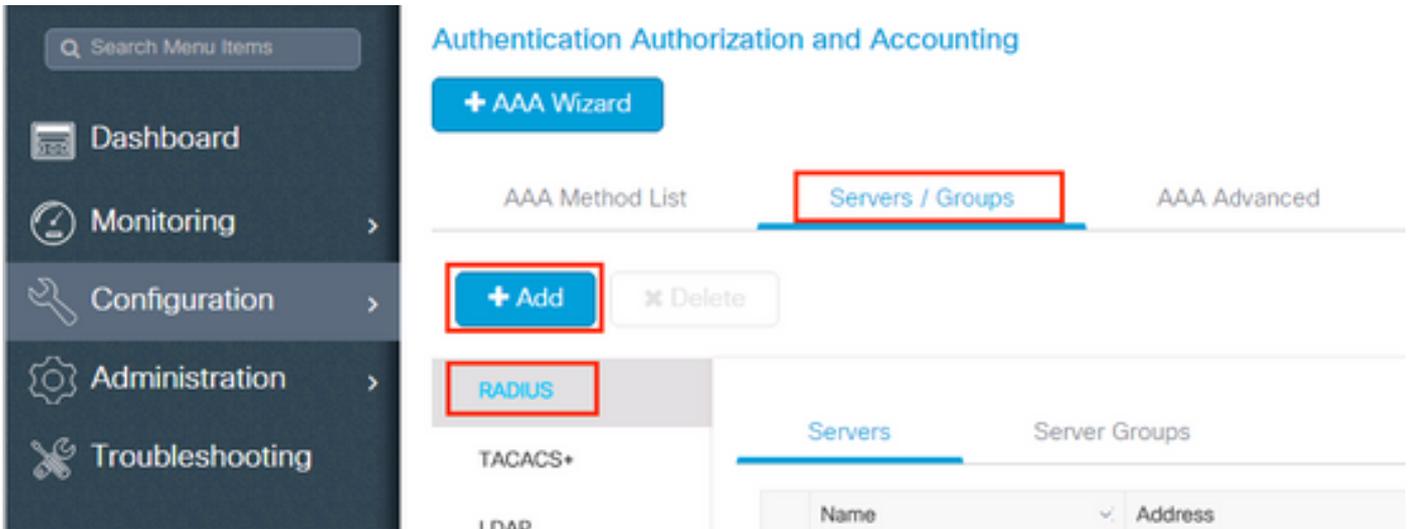


Configurazione WLC

Configurazione AAA su 9800 WLC

GUI:

Passaggio 1. Dichiarare il server RADIUS. 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.

The screenshot shows the "Create AAA Radius Server" form. The form has a dark header bar with the title "Create AAA Radius Server" and a close button (X). The form contains the following fields and options:

- Name\*: ISE-kcg
- IPV4/IPV6 Server Address\*: 172.16.0.11
- Shared Secret\*: .....
- Confirm Shared Secret\*: .....
- Auth Port: 1812
- Acct Port: 1813
- Server Timeout (seconds): 1-1000
- Retry Count: 0-100
- Support for CoA: ENABLED (checkbox checked)
- Clear PAC Key:
- Set New PAC Key:

At the bottom of the form, there are two buttons: "Cancel" and "Save & Apply to Device" (highlighted with a red box).

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**.

### Create AAA Radius Server Group

Name\*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

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

The screenshot shows the network configuration interface. On the left is a dark sidebar with menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), and Administration. The main content area is titled "Authentication Authorization and Accounting" and contains a "+ AAA Wizard" button. Below it, "AAA Method List" is highlighted with a red box. Under "AAA Method List", there are sections for "General" and "Authentication". The "Authentication" section is highlighted with a red box, and a "+ Add" button is also highlighted with a red box. To the right of the "AAA Method List" section, there is a "Servers / Groups" section with a table containing a "Name" column.

Immettere le informazioni:

Quick Setup: AAA Authentication

Method List Name\*

Type\*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

**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 5
# 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 WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC (2) : current
```

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
```

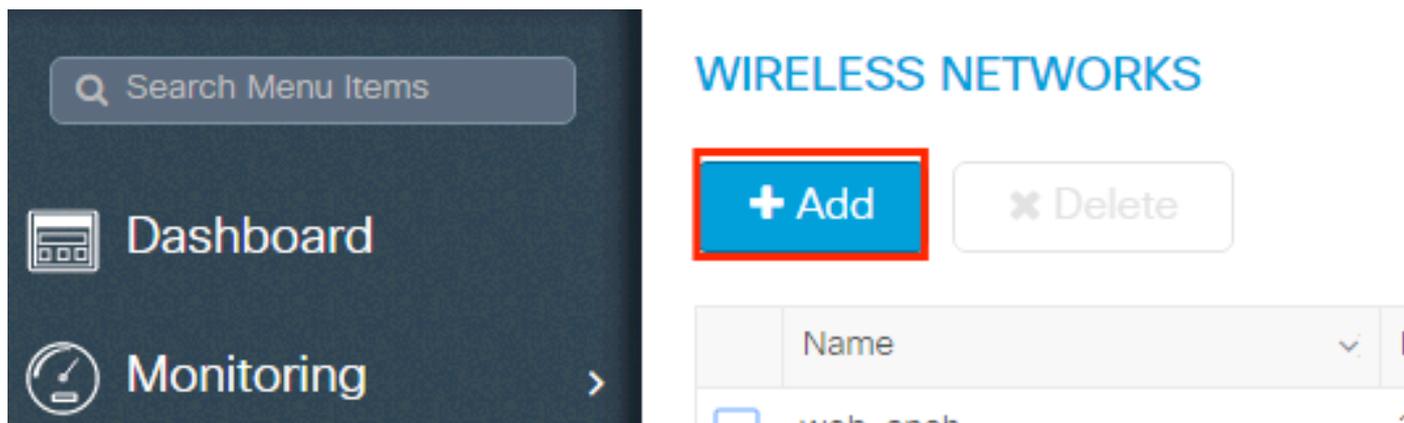
 **Nota: dead criteria** è il criterio utilizzato per contrassegnare un server RADIUS come inattivo. Si compone di: 1. Un timeout (in secondi) che rappresenta il periodo di tempo che deve trascorrere tra il momento in cui il controller ha ricevuto per ultimo un pacchetto valido dal server RADIUS e il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

### Add WLAN ✕

General	Security	Advanced
Profile Name*	<input type="text" value="prof-name"/>	Radio Policy <input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID <input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="1"/>	
Status	<input checked="" type="checkbox"/> ENABLED	

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

**Add WLAN** [Close]

General      **Security**      Advanced

Layer2      Layer3      AAA

Layer 2 Security Mode      WPA + WPA2 ▼

MAC Filtering     

Protected Management Frame

Fast Transition      Adaptive Enab... ▼

Over the DS     

Reassociation Timeout      20

PMF      Disabled ▼

WPA Parameters

WPA Policy     

[Cancel]      [Save & Apply to Device]

**Add WLAN** [Close]

PMF      Disabled ▼

WPA Parameters

WPA Policy     

WPA2 Policy     

WPA2 Encryption

AES(CCMP128)     

CCMP256     

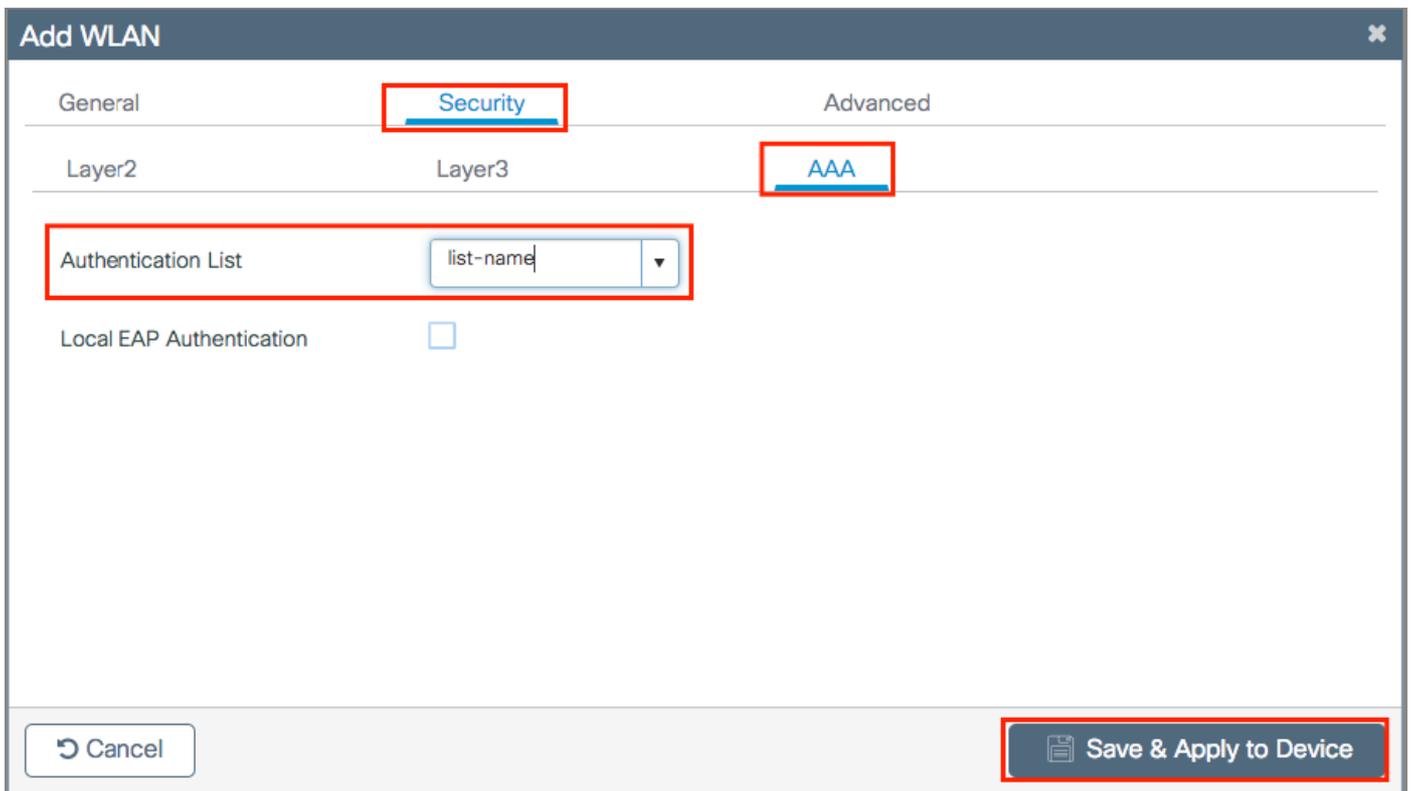
GCMP128     

GCMP256     

Auth Key Mgmt      802.1x ▼

[Cancel]      [Save & Apply to Device]

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
```

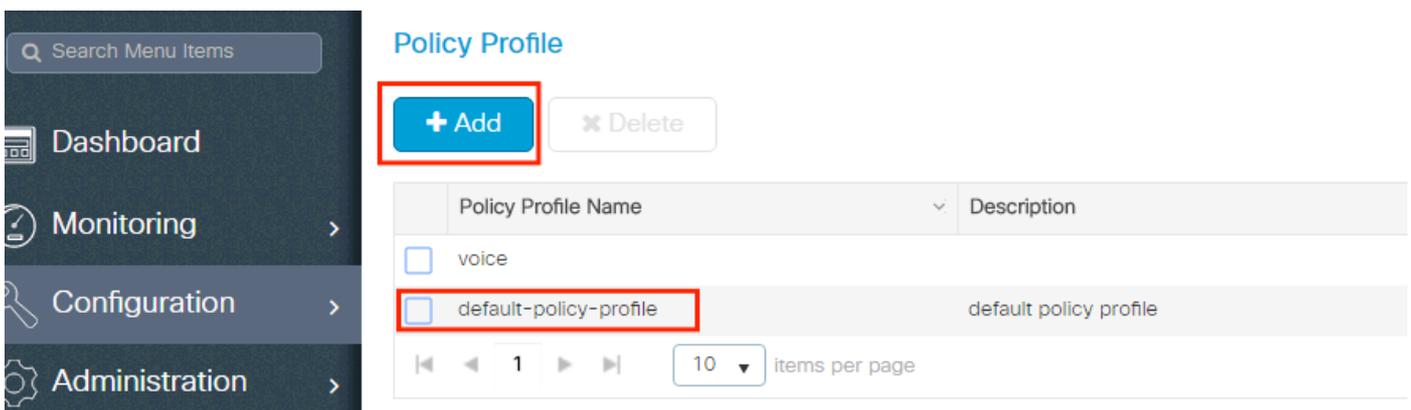
Configurazione del profilo di policy

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**.

### Edit Policy Profile

**General** | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	default-policy-profile
Description	default policy profile
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED

#### CTS Policy

Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

#### WLAN Switching Policy

Central Switching	<input checked="" type="checkbox"/>
Central Authentication	<input checked="" type="checkbox"/>
Central DHCP	<input checked="" type="checkbox"/>
Central Association Enable	<input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/>

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

## 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

### VLAN

VLAN/VLAN Group

Multicast VLAN

### WLAN ACL

IPv4 ACL

IPv6 ACL

### URL Filters

Pre Auth

Post Auth

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

✕
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)

**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

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

↶ Cancel

🔄 Update & Apply to Device

**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 **Configuration > Tags & Profiles > Tags > Policy** e aggiungere un nuovo elemento.

The screenshot shows the 'Manage Tags' interface. On the left is a navigation sidebar with 'Configuration' selected. The main area has tabs for 'Policy', 'Site', 'RF', and 'AP', with 'Policy' highlighted. Below the tabs are '+ Add' and 'x Delete' buttons, with '+ Add' highlighted. A table lists existing tags: 'central-anchor' and 'default-policy-tag' (with description 'default policy-tag'). The table has columns for 'Policy Tag Name' and 'Description'. At the bottom, there are pagination controls showing '1' items per page and a '10 items per page' dropdown.

Associare il profilo WLAN al profilo di policy desiderato.

The screenshot shows the 'Add Policy Tag' dialog box. The 'Name\*' field is highlighted with a red box and contains the text 'PolicyTagName'. Below it is a 'Description' field with the placeholder 'Enter Description'. At the bottom left, the '+ Add' button is highlighted with a red box. The dialog also features dropdown menus for 'WLAN Profile' and 'Policy Profile', both currently empty. At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons. The dialog also shows pagination controls with '0' items per page and a '10 items per page' dropdown, and the text 'No items to display'.

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

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

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

✕
✓

↶ Cancel
📄 Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 1 ▷ ▶	10 items per page
<input type="checkbox"/> prof-name	default-policy-profile
1 - 1 of 1 items	

↶ Cancel
📄 Save & Apply to Device

**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**.

The screenshot shows the 'Edit AP' configuration window with the 'General' tab selected. The 'Policy' dropdown menu is highlighted with a red box, showing 'default-policy-tag' as the selected option. The 'Update & Apply to Device' button is also highlighted with a red box at the bottom right of the window.

Field	Value
AP Name*	AP3802-02-WS
Location*	default location
Base Radio MAC	00:42:68:c6:41:20
Ethernet MAC	00:42:68:a0:d0:22
Admin Status	Enabled
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
Version	Primary Software Version: 10.0.200.50
	Predownloaded Status: N/A
	Predownloaded Version: N/A
	Next Retry Time: N/A
	Boot Version: 1.0.0
	IOS Version: 10.0.200.52
	Mini IOS Version: 0.0.0.0
IP Config	IP Address: 172.16.0.207
	Static IP: <input type="checkbox"/>
Time Statistics	Up Time: 9 days 1 hrs 17 mins 24 secs
	Controller Associated Time: 0 days 3 hrs 26 mins 41 secs
	Controller Association Latency: 8 days 21 hrs 50 mins 33 secs

 **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



Flex Profile



Site Tag



RF Profile



RF Tag



## Apply



Tag APs



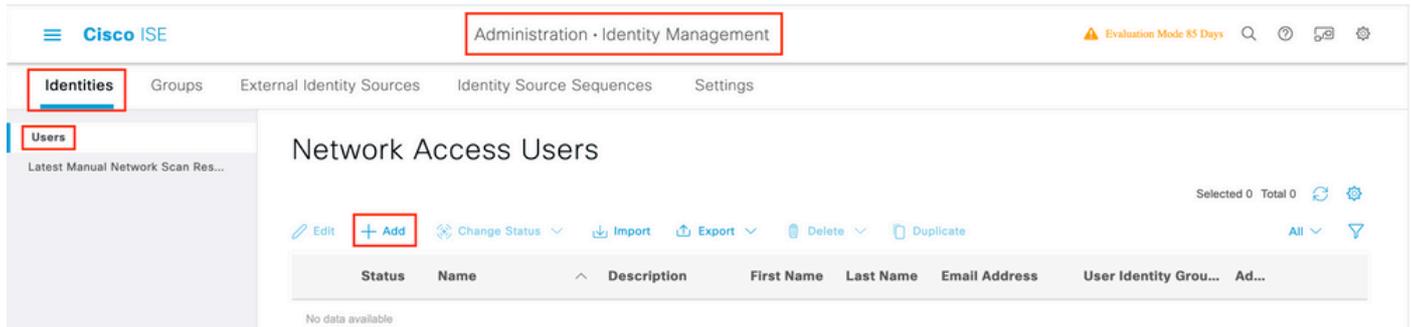
Done

Start Now →

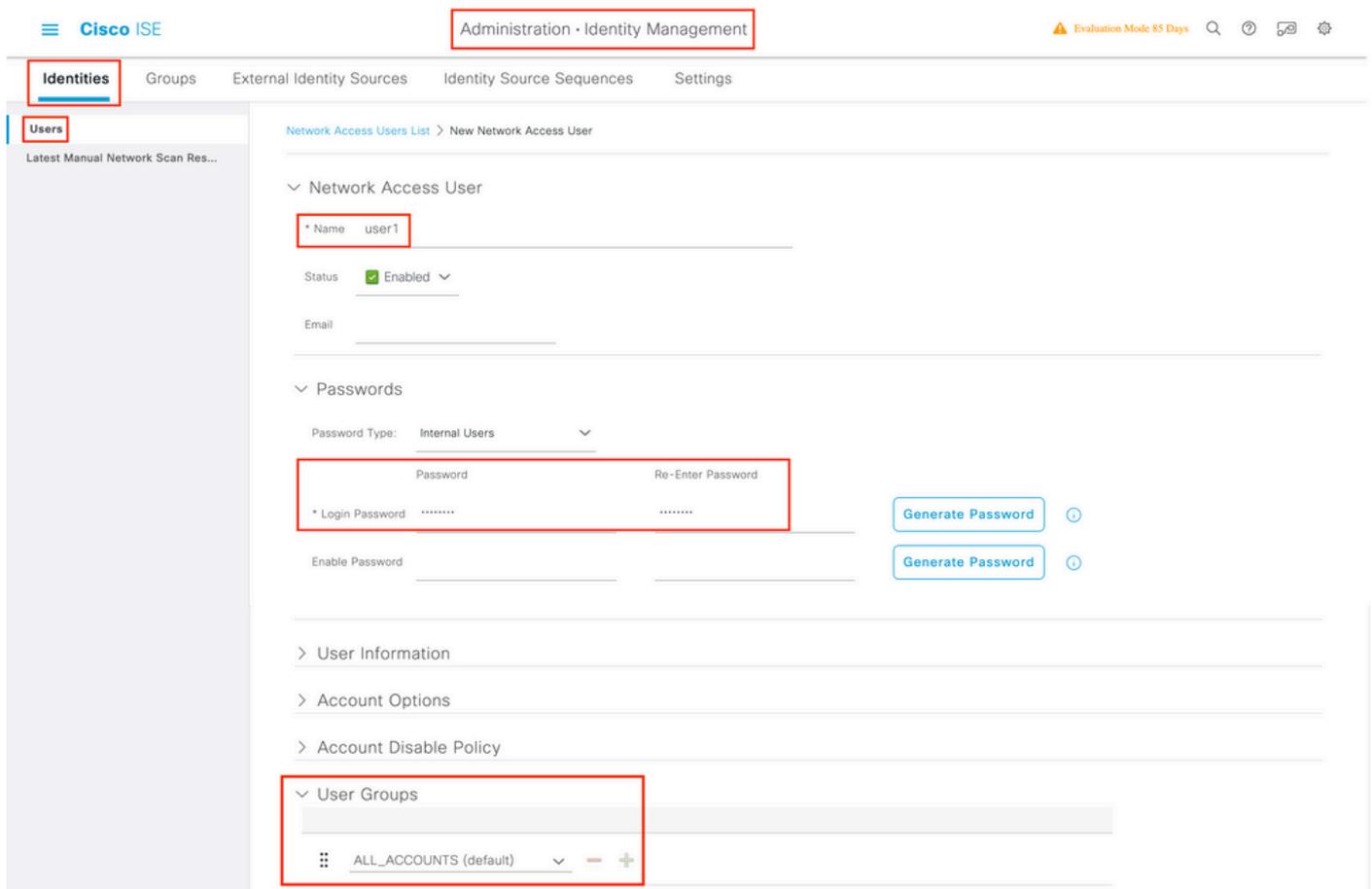
su questo argomento, vedere il capitolo relativo alla gestione dei dispositivi di rete nel manuale Cisco Identity Services Engine Administrator Guide, : [Network Device Groups](#)

## 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:

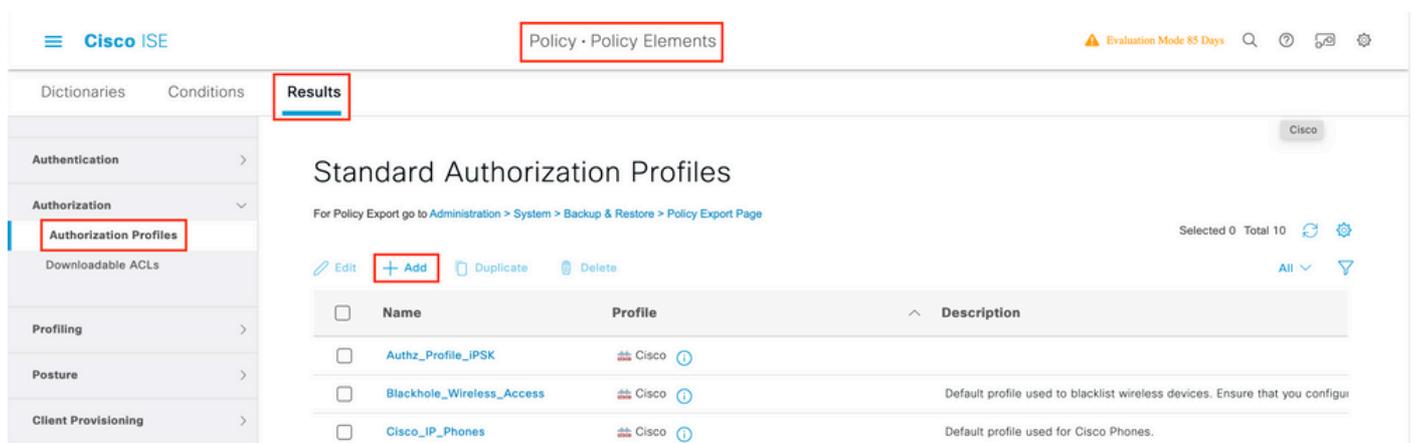


## Creazione del profilo di autorizzazione

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.



The screenshot displays the Cisco ISE web interface. The breadcrumb navigation path is **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. The 'Results' tab is selected in the top navigation bar. The left sidebar shows the 'Authorization' menu with 'Authorization Profiles' highlighted. The main content area is titled 'Standard Authorization Profiles' and includes a table of existing profiles. The '+ Add' button is highlighted with a red box.

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	Authz_Profile_IPSK	Cisco	
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configu
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.

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.

Cisco ISE Policy - Policy Elements Evaluation Mode 85 Days

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > PermitAccessVlan1416

Authorization Profile

\* Name PermitAccessVlan1416

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Security Group

VLAN Tag ID 1 Edit Tag ID/Name 1416

Voice Domain Permission

Advanced Attributes Settings

Select an item

Attributes Details

Access Type = ACCESS\_ACCEPT

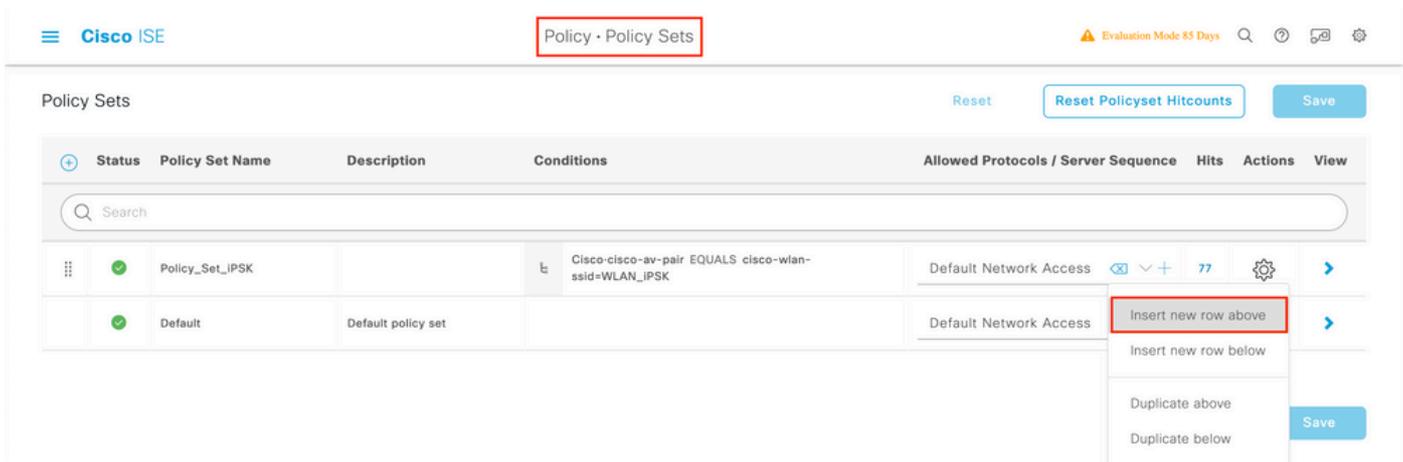
Tunnel-Private-Group-ID = 1:1416

Tunnel-Type = 1:13

Tunnel-Medium-Type = 1:6

## Crea set di criteri

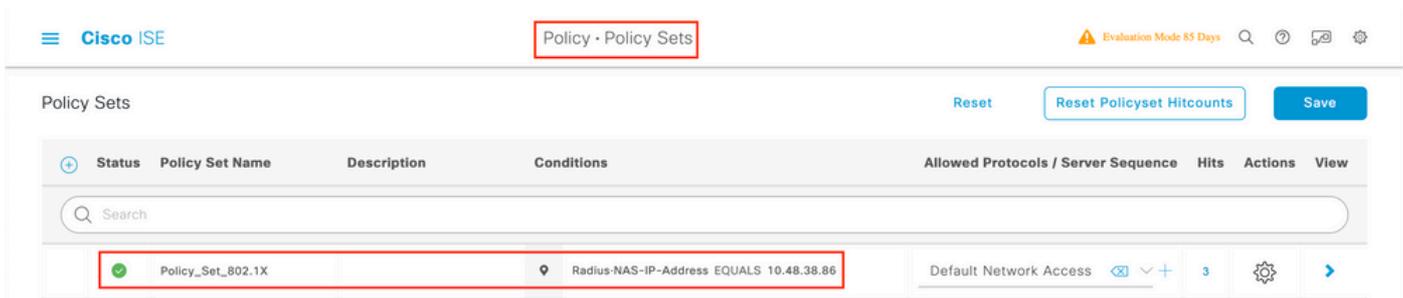
Un set di criteri definisce un insieme di regole di autenticazione e autorizzazione. Per crearne uno, andare a **Policy > Policy Sets**, fare clic sull'ingranaggio del primo set di criteri nell'elenco e selezionare **Insert new row above** come mostrato in questa immagine:



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.

Policy Sets → Policy\_Set\_802.1X

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Policy_Set_802.1X		Radius-NAS-IP-Address EQUALS 10.48.38.86	Default Network Access	3

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Auth_Policy_802.1X	Radius-Called-Station-ID ENDS_WITH Test-802.1X	Internal Users		

### 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.

Authorization Policy (2)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Authz_Policy_802.1X	Radius-Called-Station-ID ENDS_WITH Test-802.1X	PermitAccessVlan1416	Select from list	14	
✓	Default		DenyAccess	Select from list	0	

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](#)

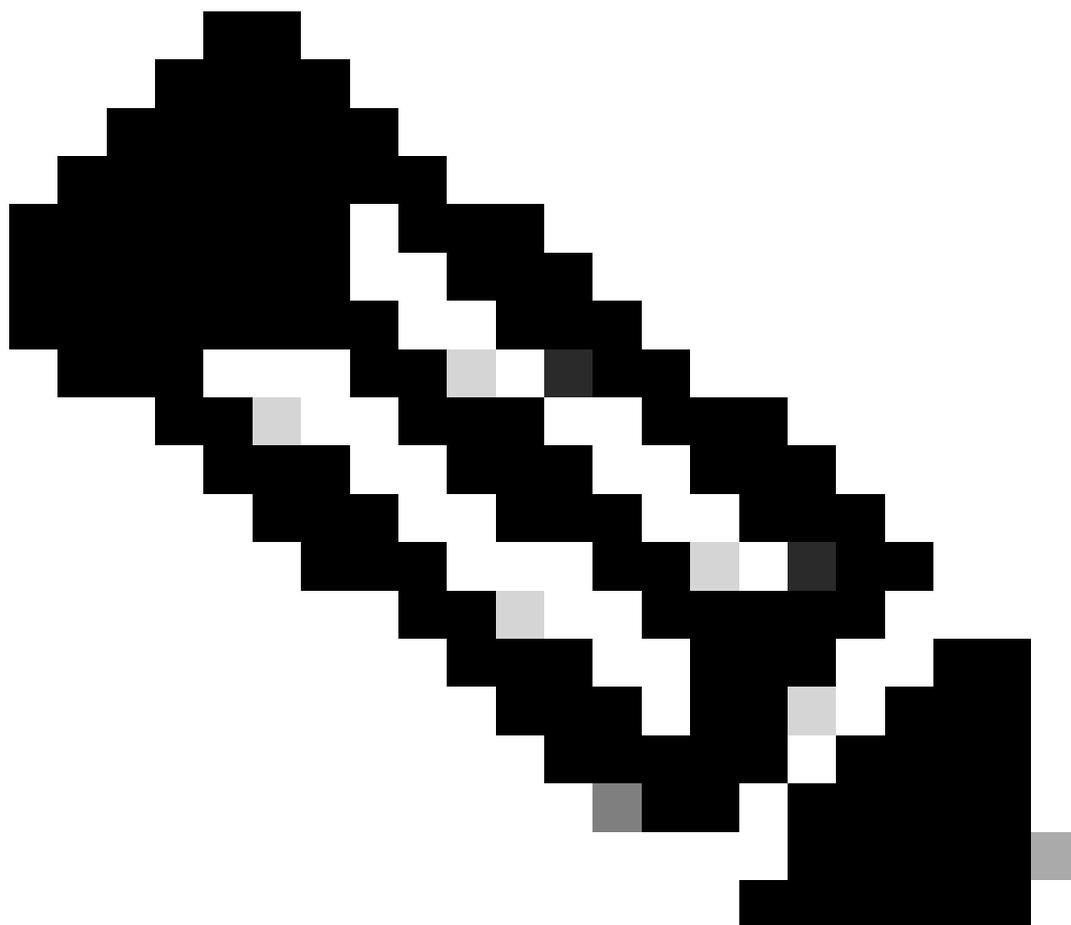
## Verifica

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 servers
# 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 Ad
```

---

 **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
```

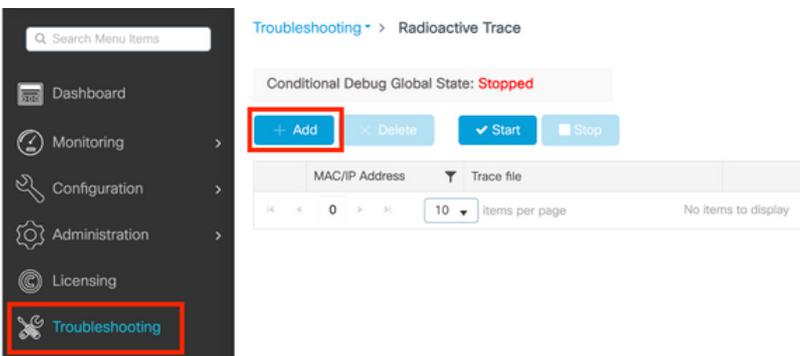
---

 **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.



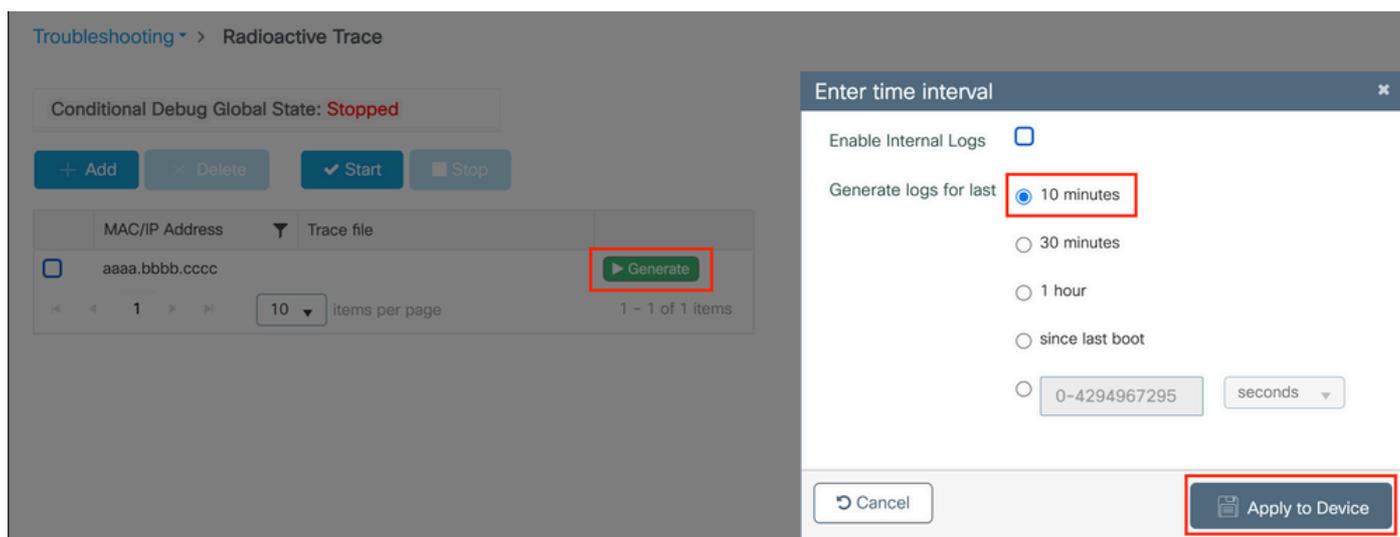
The screenshot displays the Cisco GUI interface for configuring Radioactive Trace. On the left, a navigation menu is visible with 'Troubleshooting' highlighted. The main content area shows the 'Radioactive Trace' configuration page. At the top, the 'Conditional Debug Global State' is set to 'Stopped'. Below this, there are four buttons: '+ Add', 'Delete', 'Start', and 'Stop'. The '+ Add' button is highlighted with a red box. Below the buttons is a table with two columns: 'MAC/IP Address' and 'Trace file'. The table is currently empty, and the text 'No items to display' is shown at the bottom right of the table area.

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

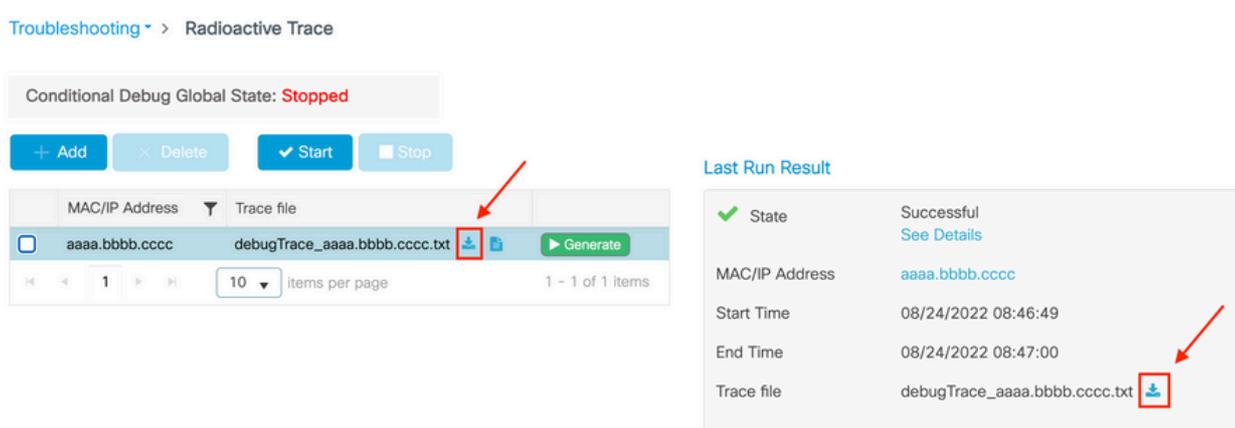
Passaggio 3. Riprodurre il problema.

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:

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	Netwo
Aug 23, 2022 06:18:42.5...	<span style="color: blue;">●</span>		0	user1	08:BE:AC:27:85:...	Unknown	Policy_Set...	Policy_Set...	PermitAcc...	10.14.16.112,...	
Aug 23, 2022 09:45:48.1...	<span style="color: red;">●</span>			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).