

# Configurazione di RADIUS & TACACS+ per GUI & CLI Auth su 9800 WLC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Restrizioni utente di sola lettura](#)

[Configurazione dell'autenticazione RADIUS per WLC](#)

[Configurare ISE per RADIUS](#)

[Configurazione di TACACS+ WLC](#)

[Configurazione TACACS+ ISE](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi di accesso WLC GUI o CLI RADIUS/TACACS+ tramite la CLI del WLC](#)

[Risoluzione dei problemi di accesso tramite GUI WLC o CLITACACS+ tramite l'interfaccia utente di ISE](#)

---

## Introduzione

In questo documento viene descritto come configurare un Catalyst 9800 per l'autenticazione esterna RADIUS o TACACS+.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst Wireless 9800 modello di configurazione
- Nozioni base su AAA, RADIUS e TACACS+

### Componenti usati

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

- C9800-CL v17.9.2

- ISE 3.2.0

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.

## Premesse

Quando un utente tenta di accedere alla CLI o alla GUI del WLC, gli viene richiesto di immettere un nome utente e una password. Per impostazione predefinita, queste credenziali vengono confrontate con il database locale degli utenti, presente nel dispositivo stesso. In alternativa, il WLC può essere istruito per confrontare le credenziali di input con un server AAA remoto: il WLC può comunicare con il server usando RADIUS o TACACS+.

## Configurazione

Nell'esempio, sono configurati due tipi di utenti sul server AAA (ISE), rispettivamente `adminuser`, `ehelpdeskuser`. Questi utenti fanno parte rispettivamente del `admin-group` gruppo e del `helpdesk-group` gruppo. L'utente `adminuser`, parte del `admin-group` WLC, deve avere accesso completo al WLC. D'altro canto, la `helpdeskuser` parte del `helpdesk-group` è intesa unicamente ad ottenere privilegi di controllo del WLC. Non è quindi possibile accedere alla configurazione.

In questo articolo viene prima configurato il WLC e l'ISE per l'autenticazione RADIUS, quindi si ottiene lo stesso risultato con TACACS+.

Restrizioni utente di sola lettura

Se si usa TACACS+ o RADIUS per l'autenticazione WebUI 9800, esistono le seguenti restrizioni:

- Gli utenti con livello di privilegio 0 esistono ma non hanno accesso alla GUI

- 

Gli utenti con i livelli di privilegio 1-14 possono solo visualizzare la scheda Monitor (equivalente al livello di privilegio di un utente autenticato localmente di sola lettura)

- 

Accesso completo per gli utenti con livello di privilegio 15

- 

Gli utenti con il livello di privilegio 15 e un set di comandi che consente solo comandi specifici non sono supportati. L'utente può comunque eseguire modifiche alla configurazione tramite WebUI

Queste considerazioni non possono essere modificate.

## Configurazione dell'autenticazione RADIUS per WLC

Passaggio 1. Dichiarare il server RADIUS.

### Dalla GUI:

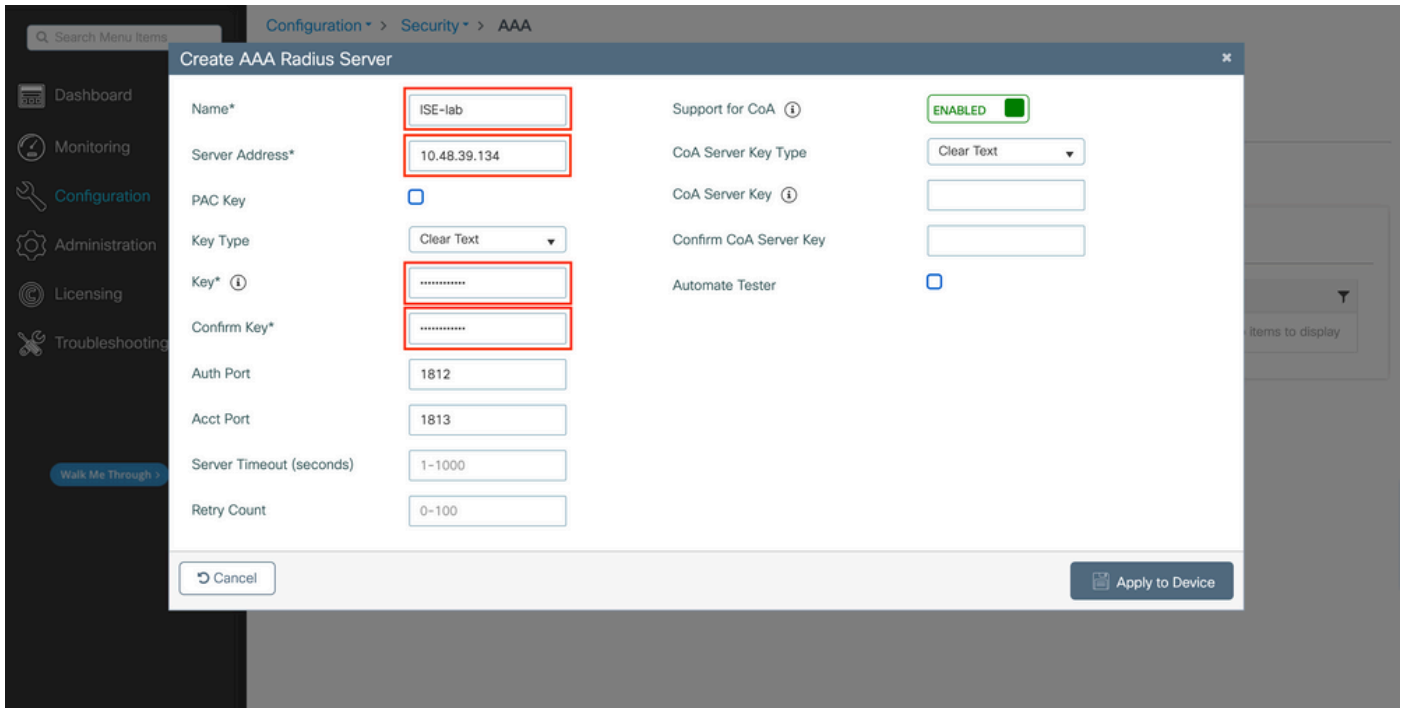
Innanzitutto, creare il server ISE RADIUS sul WLC. A tale scopo, è possibile selezionare la scheda Servers/Groups > RADIUS > Servers dalla pagina WLC della GUI accessibile in <https://<WLC-IP>/webui/#/aaa> o passare a Configuration > Security > AAA , come mostrato nell'immagine.

The screenshot shows the Cisco WLC GUI configuration page for AAA. The breadcrumb trail is Configuration > Security > AAA. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the 'Servers / Groups' configuration page. The 'RADIUS' tab is selected, and the 'Servers' sub-tab is active. A table lists the configured RADIUS servers. The 'Add' button is highlighted with a red box.

Name	Address	Auth Port	Acct Port
ISE-lab	10.48.39.134	1812	1813

For Radius Fallback to work, please make sure the [Dead Criteria](#) and [Dead Time](#) configuration exists on the device

Per aggiungere un server RADIUS al WLC, fare clic sul pulsante Add (Aggiungi) visualizzato in rosso nell'immagine. In questo modo viene aperta la finestra popup illustrata nello screenshot.



In questa finestra popup è necessario specificare:

- Il nome del server (non è necessario che corrisponda al nome del sistema ISE)
- Indirizzo IP del server
- Il segreto condiviso tra il WLC e il server RADIUS

È possibile configurare altri parametri, ad esempio le porte utilizzate per l'autenticazione e l'accounting, ma questi non sono obbligatori e vengono lasciati come predefiniti per questa documentazione.

Dalla CLI:

```
<#root>
```

```
WLC-9800(config)#radius server
```

```
ISE-lab
```

```
WLC-9800(config-radius-server)#address ipv4
```

```
10.48.39.134
```

```
auth-port 1812 acct-port 1813
```

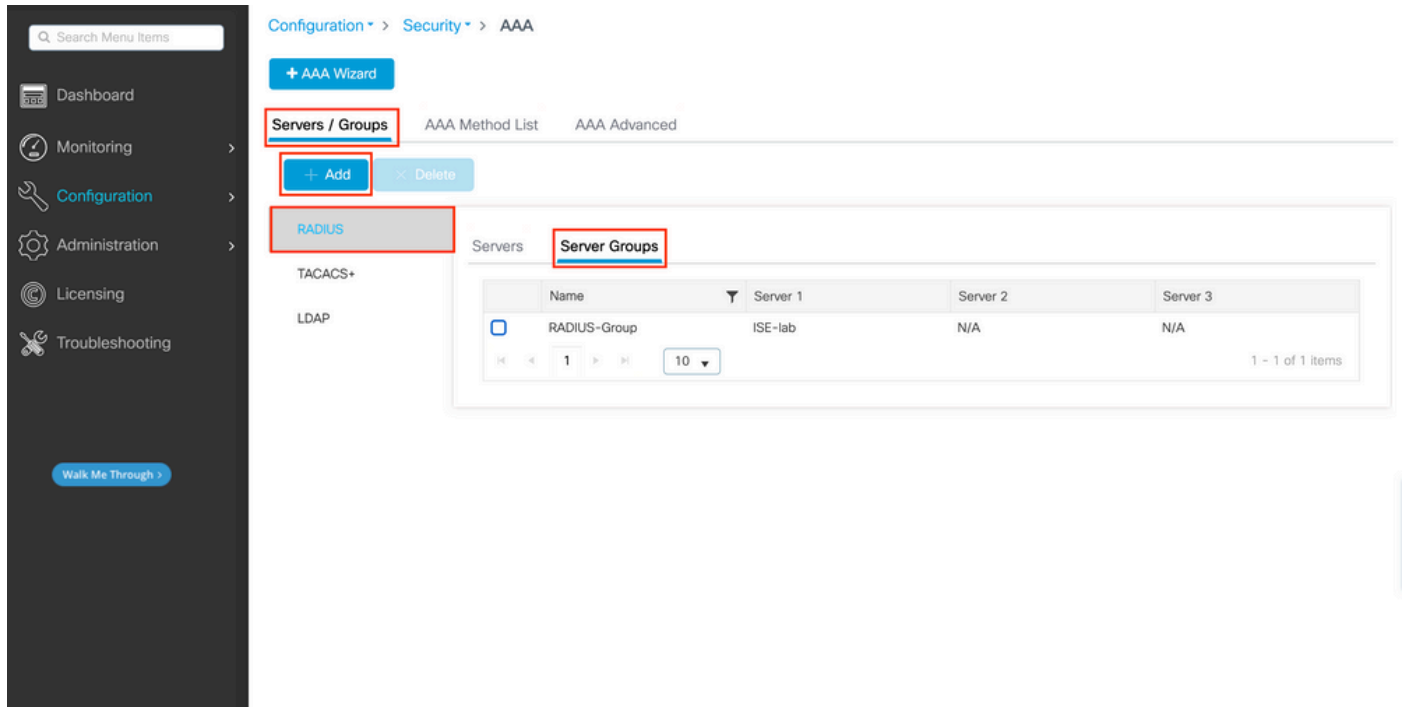
```
WLC-9800(config-radius-server)#key
```

```
Cisco123
```

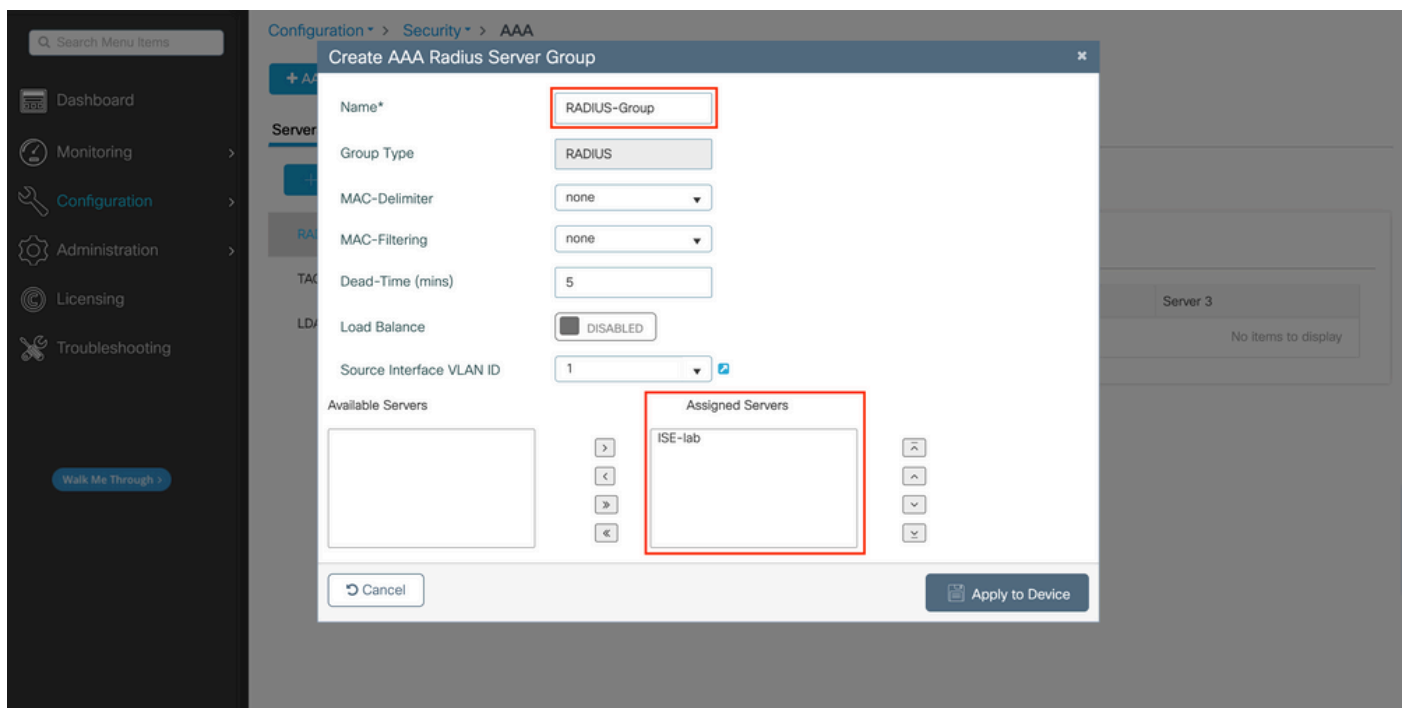
Passaggio 2. Mappare il server RADIUS a un gruppo di server.

## Dalla GUI:

Se si dispone di più server RADIUS utilizzabili per l'autenticazione, è consigliabile mappare tutti questi server allo stesso gruppo di server. Il WLC si occupa del bilanciamento del carico delle diverse autenticazioni tra i server del gruppo di server. I gruppi di server RADIUS vengono configurati dalla Servers/Groups > RADIUS > Server Groups scheda dalla stessa pagina GUI di quella indicata nel passaggio 1., come mostrato nell'immagine.



Per quanto riguarda la creazione del server, quando si fa clic sul pulsante Aggiungi (visualizzato nell'immagine precedente), qui illustrato, viene visualizzata una finestra popup.



Nel popup, fornire un nome al gruppo e spostare i server desiderati nell'elenco Server assegnati.

Dalla CLI:

\_\_\_\_\_  
<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

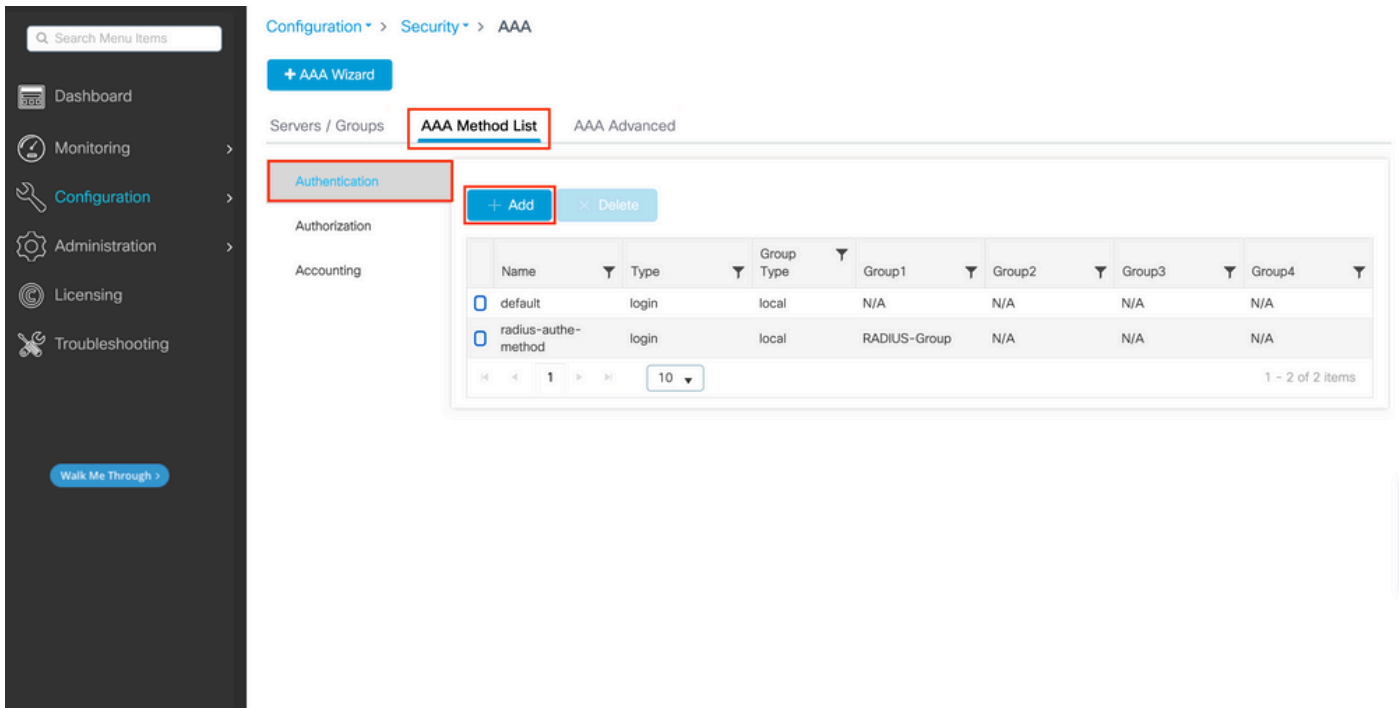
WLC-9800(config-sg-radius)# server name

ISE-lab

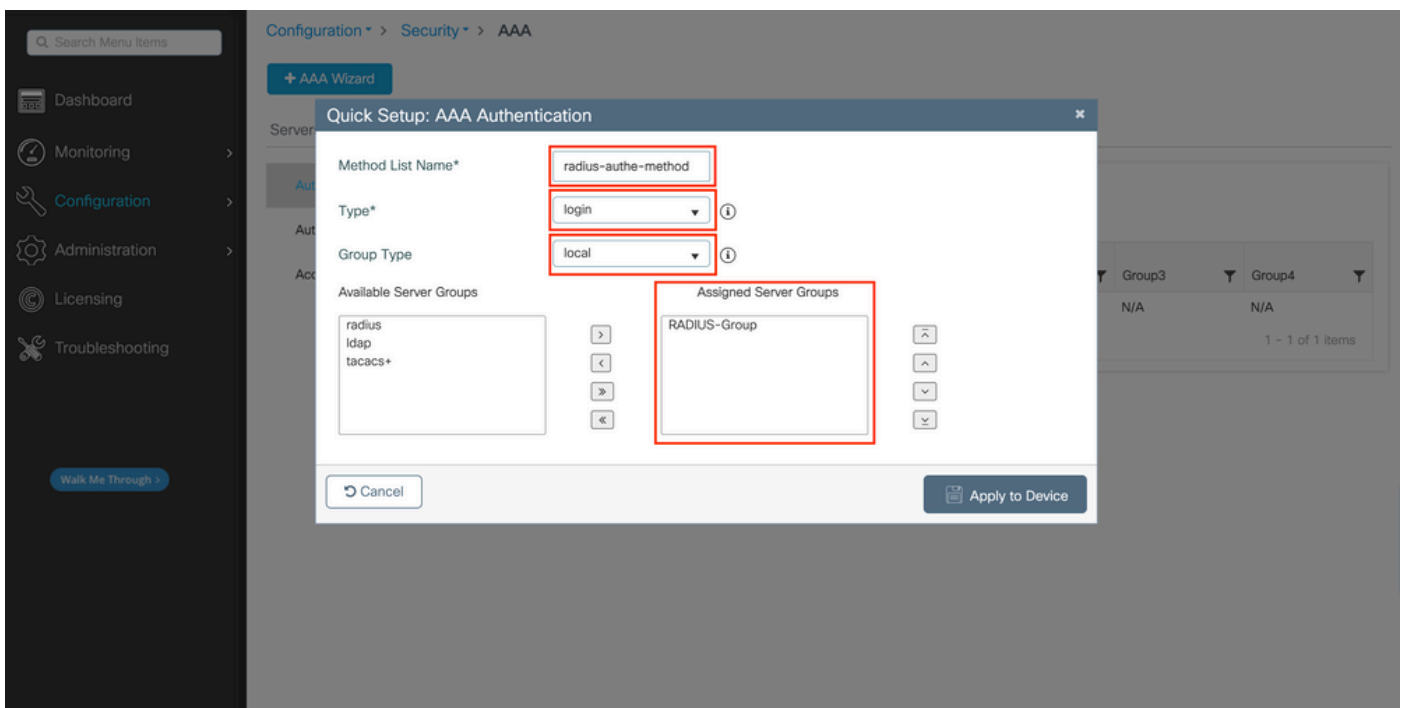
Passaggio 3. Creare un metodo di accesso con autenticazione AAA che punti al gruppo di server RADIUS.

Dalla GUI:

Sempre dalla pagina GUI <https://<WLC-IP>/webui/#/aaa>, passare alla AAA Method List > Authentication scheda e creare un metodo di autenticazione, come mostrato in questa immagine.



Come al solito, quando si utilizza il pulsante Aggiungi per creare un metodo di autenticazione, viene visualizzata una finestra popup di configurazione simile a quella illustrata in questa immagine.



In questa finestra popup, fornire un nome per il metodo. Scegliere Type come login e aggiungere all'elenco il server del gruppo creato nel passaggio precedente Assigned Server Groups. Per quanto riguarda il campo Tipo di gruppo, sono possibili diverse configurazioni.

- Se si sceglie Tipo di gruppo come locale, il WLC verifica innanzitutto se le credenziali dell'utente esistono localmente e quindi esegue il fallback al gruppo di server.
- Se si sceglie Tipo di gruppo come gruppo e non si seleziona l'opzione Ripristina locale, il WLC controlla semplicemente le credenziali dell'utente rispetto al gruppo di server.

- Se si sceglie Tipo di gruppo come gruppo e si seleziona l'opzione Fallback a locale, il WLC controlla le credenziali dell'utente rispetto al gruppo di server ed esegue una query sul database locale solo se il server non risponde. Se il server invia un rifiuto, l'utente deve essere autenticato, anche se può esistere nel database locale.

Dalla CLI:

Se si desidera che le credenziali utente vengano controllate con un gruppo di server solo se non vengono trovate prima localmente, utilizzare:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```

```
local group
```

```
RADIUS-Group
```

Se si desidera che le credenziali utente vengano controllate solo con un gruppo di server, utilizzare:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```



group

**RADIUS-Group**

Se si desidera che le credenziali utente vengano controllate con un gruppo di server e se l'ultimo non risponde con una voce locale, utilizzare:

<#root>

WLC-9800(config)#aaa authentication login

**radius-auth-method**

group

**RADIUS-Group**

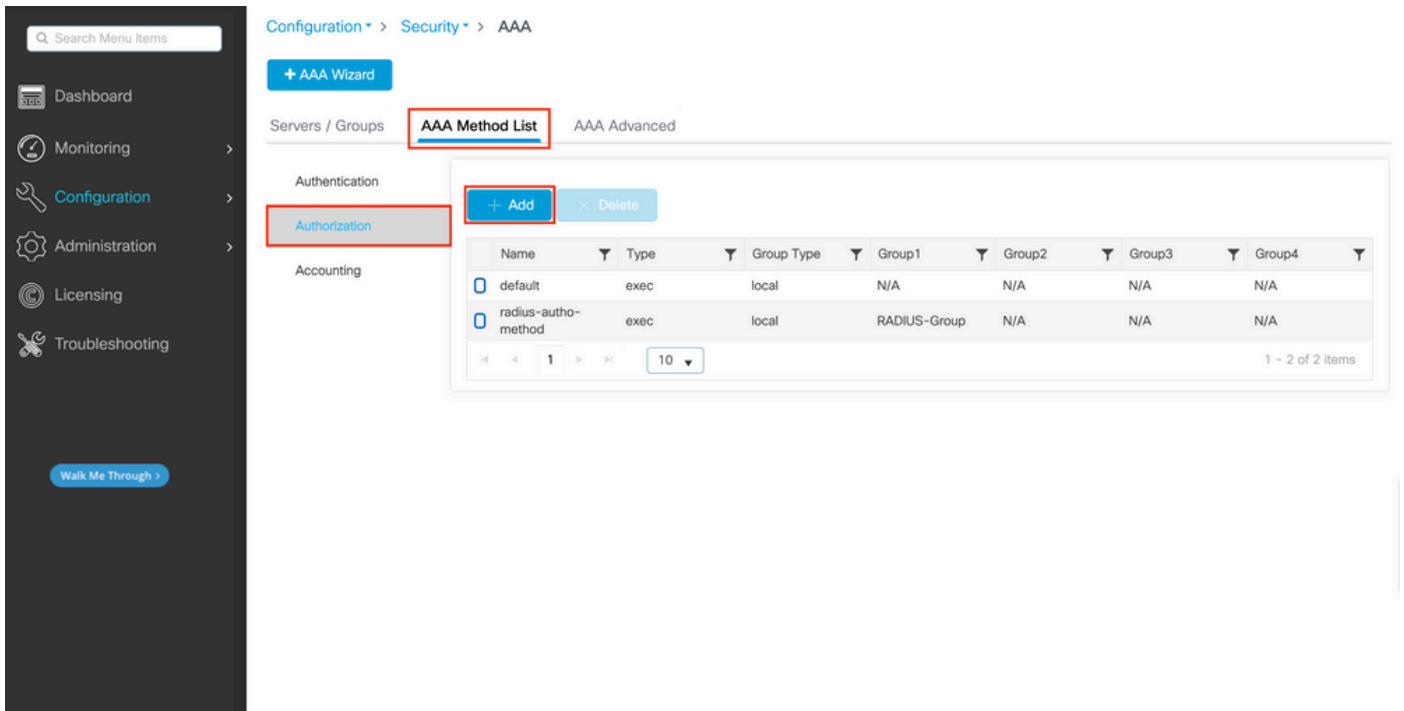
local

Nell'esempio di installazione, ci sono alcuni utenti che vengono creati solo localmente, e alcuni utenti solo sul server ISE, quindi, fare uso della prima opzione.

Passaggio 4. Creare un metodo di esecuzione dell'autorizzazione AAA che punti al gruppo di server RADIUS.

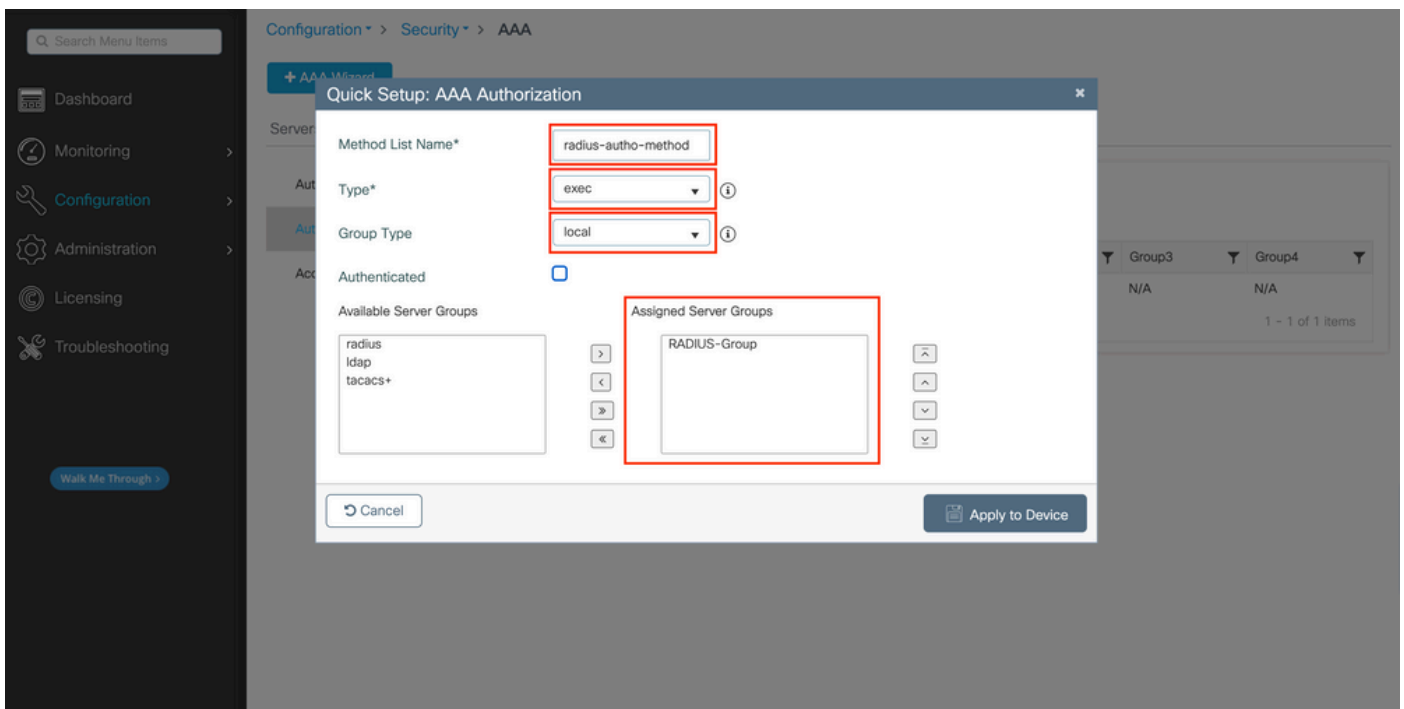
Dalla GUI:

L'utente deve anche essere autorizzato per poter accedere. Sempre da, GUI Page Configuration > Security > AAA passare alla AAA Method List > Authorization scheda e creare un metodo di autorizzazione come mostrato in questa immagine.



### Creazione metodo di autorizzazione

Quando si aggiunge un nuovo metodo di autorizzazione con il pulsante Aggiungi, viene visualizzato un menu popup di configurazione del metodo di autorizzazione simile a quello illustrato.



In questo popup di configurazione, fornire un nome per il metodo di autorizzazione, scegliere il Tipo come exec e utilizzare lo stesso ordine di Tipo di gruppo utilizzato per il metodo di autenticazione al passo 3.

### Dalla CLI:

Per quanto riguarda il metodo di autenticazione, l'autorizzazione viene assegnata innanzitutto per verificare gli utenti rispetto alle voci locali e quindi rispetto alle voci di un gruppo di server.

WLC-9800(config)#aaa authorization exec

radius-autho-method

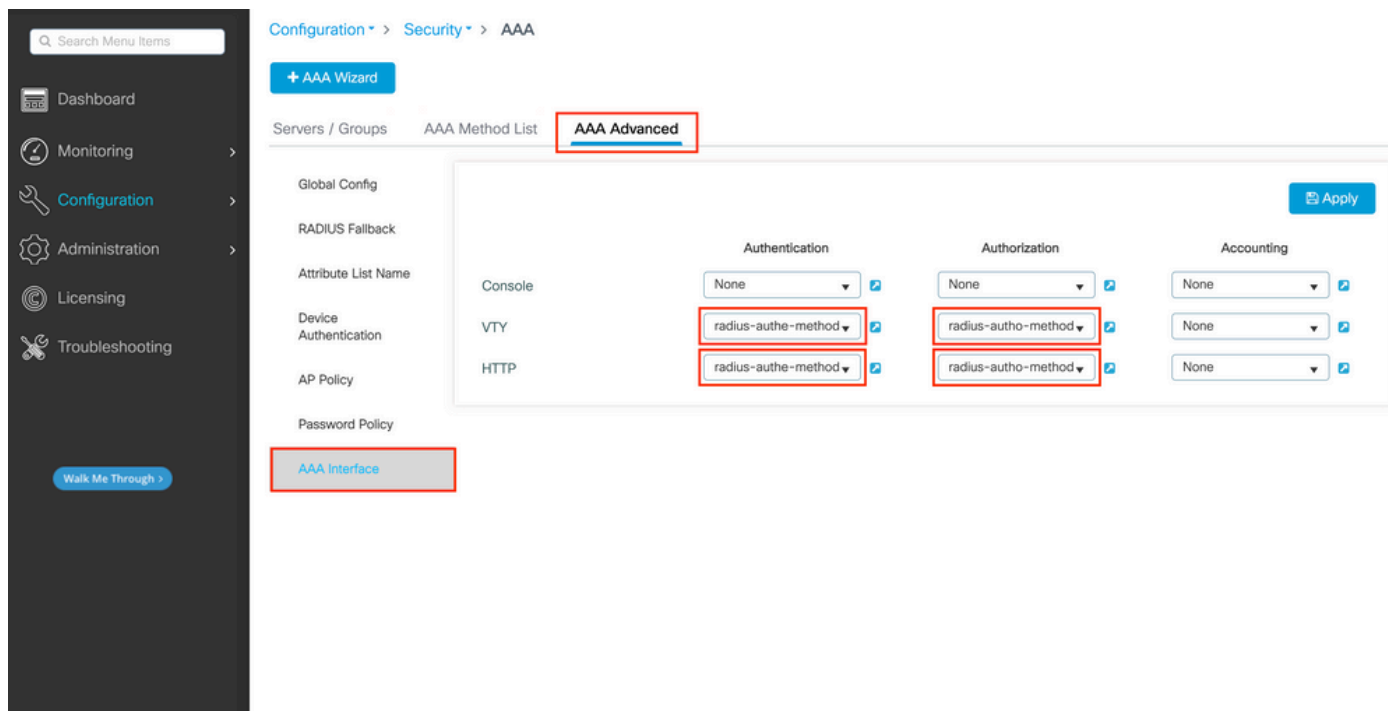
local group

RADIUS-Group

Passaggio 5. Assegnare i metodi alle configurazioni HTTP e alle linee VTY utilizzate per Telnet/SSH.

Dalla GUI:

I metodi di autenticazione e autorizzazione creati possono essere utilizzati per le connessioni utente HTTP e/o Telnet/SSH, configurabili dalla AAA Advanced > AAA Interface scheda ancora dalla pagina WLC della GUI accessibile in <https://<WLC-IP>/webui/#/aaa>, come mostrato nell'immagine:



CLI per autenticazione GUI:

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

**radius-authe-method**

WLC-9800(config)#ip http authentication aaa exec-authorization

**radius-autho-method**

CLI per autenticazione Telnet/SSH:

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

**radius-authe-method**

WLC-9800(config-line)#authorization exec

**radius-autho-method**

Quando si apportano modifiche alle configurazioni HTTP, è consigliabile riavviare i servizi HTTP e HTTPS. A tale scopo, è possibile utilizzare i seguenti comandi:

```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server
```

## Configurare ISE per RADIUS

Passaggio 1. Configurare il WLC come dispositivo di rete per RADIUS.

### Dalla GUI:

Per dichiarare il WLC usato nella sezione precedente come dispositivo di rete per RADIUS in ISE, selezionare Administration > Network Resources > Network Devices e aprire la scheda Network devices (Dispositivi di rete), come mostrato nell'immagine seguente.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is 'Administration > Network Resources > Network Devices'. The left sidebar has 'Network Devices' selected. The main content area is titled 'Network Devices' and shows a toolbar with buttons for Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete. Below the toolbar is a table with the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
WLC-9800	10.48.39.133/32	Cisco	All Locations	All Device Types	

Per aggiungere un dispositivo di rete, utilizzare il pulsante Aggiungi, che apre il modulo di configurazione del nuovo dispositivo di rete.

Network Devices List > New Network Device

### Network Devices

Name **WLC-9800**

Description

IP Address \* IP: **10.48.39.133 / 32**

Device Profile **Cisco**

Model Name

Software Version

Network Device Group

Location **All Locations** [Set To Default](#)

IPSEC **Is IPSEC Device** [Set To Default](#)

Device Type **All Device Types** [Set To Default](#)

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol **RADIUS**

Shared Secret **.....** [Show](#)

Use Second Shared Secret [?](#)

Second Shared Secret [Show](#)

CoA Port **1700** [Set To Default](#)

**RADIUS DTLS Settings** [?](#)

DTLS Required [?](#)

Shared Secret **radius/dtls** [?](#)

Nella nuova finestra, fornire un nome per il dispositivo di rete e aggiungere il relativo indirizzo IP. Scegliere le impostazioni di autenticazione RADIUS e configurare lo stesso segreto condiviso RADIUS usato sul WLC.

Passaggio 2. Creare un risultato di autorizzazione per restituire il privilegio.

#### Dalla GUI:

Per disporre dei diritti di accesso di amministratore, è necessario che l'amministratore disponga di un livello di privilegi pari a 15, che consente di accedere alla shell del prompt di esecuzione. D'altra parte, non è necessario che l'helpdeskuser necessario l'accesso immediato alla shell di esecuzione e può quindi essere assegnato con un livello di privilegio inferiore a 15. Per assegnare agli utenti il livello di privilegio appropriato, è possibile utilizzare i profili di autorizzazione. È possibile configurarli dall'ISE GUI Page Policy > Policy Elements > Results, nella scheda Authorization > Authorization Profiles mostrata nella figura seguente.

- Authentication
- Authorization
- Authorization Profiles**
- Downloadable ACLs
- Profiling
- Posture
- Client Provisioning

## Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 11

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

All

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	9800-admin-priv	Cisco	
<input type="checkbox"/>	9800-helpdesk-priv	Cisco	
<input type="checkbox"/>	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure ti
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	UDN	Cisco	Default profile used for UDN.
<input type="checkbox"/>	DenyAccess	Cisco	Default Profile with access type as Access-Reject

Per configurare un nuovo profilo di autorizzazione, utilizzare il pulsante Aggiungi che consente di aprire il modulo di configurazione del nuovo profilo di autorizzazione. Questo modulo deve essere particolarmente simile a questo per configurare il profilo assegnato al adminusermodulo.

Dictionary Conditions **Results**

Authentication > Authorization Profiles > New Authorization Profile

Authorization Profile

\* Name 9800-admin-priv

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement  ⓘ

Agentless Posture  ⓘ

Passive Identity Tracking  ⓘ

> Common Tasks

Advanced Attributes Settings

⋮ Cisco:cisco-av-pair = shell:priv-lvl=15

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = shell:priv-lvl=15

Submit Cancel

La configurazione mostrata concede il livello di privilegio 15 a qualsiasi utente a cui è associato. Come accennato in precedenza, questo è il comportamento previsto per il `adminuser` file creato nel passaggio successivo. Tuttavia, deve avere `helpdeskuser` un livello di privilegi inferiore e pertanto deve essere creato un secondo elemento di criterio.

L'elemento di criterio per l'oggetto `helpdeskuser` è simile a quello creato sopra, con la differenza che la stringa `shell:priv-lvl=15` deve essere modificata in `shell:priv-lvl=X` e sostituire X con il livello di privilegio desiderato. Nell'esempio viene utilizzato 1.

Passaggio 3. Creare gruppi di utenti su ISE.

Dall'interfaccia grafica:

I gruppi di utenti ISE vengono creati dalla scheda User Identity Groups di Administration > Identity Management > Groups GUI Page, mostrata nell'acquisizione schermo.



Cisco ISE Administration · Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

**User Identity Groups**

### User Identity Groups

Selected 0 Total 10

Edit **Add** Delete Import Export

Name	Description
<input type="checkbox"/> helpdesk-group	This is the group containing all users with read-only privileges.
<input type="checkbox"/> admin-group	This is the group containing all users with administrator privileges.
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Weeklyly (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group

Per creare un nuovo utente, utilizzare il pulsante Aggiungi che consente di aprire il modulo di configurazione del nuovo gruppo di identità utente, come illustrato.

Cisco ISE Administration · Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

User Identity Groups > New User Identity Group

### Identity Group

\* Name **admin-group**

Description This is the group containing all users with administrator privileges.

Submit Cancel

Specificare il nome del gruppo creato. Creare i due gruppi di utenti descritti in precedenza, ovvero admin-group e helpdesk-group.

Passaggio 4. Creare utenti su ISE.

Dall'interfaccia grafica:

Gli utenti ISE vengono creati dalla scheda Users of Administration > Identity Management > Identities GUI Page, visualizzata nell'acquisizione schermo.

Users

Latest Manual Network Scan Res...

# Network Access Users

Selected 0 Total 2

Edit **+ Add** Change Status Import Export Delete Duplicate

All

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled	adminuser				admin-group	
<input type="checkbox"/>	Enabled	helpdeskus...				helpdesk-group	

Per creare un nuovo utente, utilizzare il pulsante Aggiungi per aprire il nuovo modulo di configurazione utente di accesso alla rete, come illustrato.

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

\* Username **adminuser**

Status  Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration  
Password will expire in 60 days

Never Expires

Password Re-Enter Password

\* Login Password ..... Generate Password

Enable Password ..... Generate Password

> User Information

> Account Options

> Account Disable Policy

User Groups

admin-group

Fornire le credenziali agli utenti, ossia il nome utente e la password, usati per autenticare il WLC. Verificare inoltre che lo stato dell'utente sia Enabled. Infine, aggiungere l'utente al relativo gruppo correlato, creato nel passaggio 4., con il menu a discesa Gruppi di utenti alla fine del modulo.

Creare i due utenti descritti in precedenza, ovvero adminuser e helpdeskuser.

Passaggio 5. Autenticare gli utenti.

#### Dalla GUI:

In questo scenario, il criterio di autenticazione dei Set di criteri predefiniti di ISE, già preconfigurato, consente l'accesso alla rete predefinito. Questo set di criteri può essere visto dalla pagina Policy > Policy Sets dell'interfaccia grafica di ISE, come mostrato nella figura. Non c'è quindi bisogno di cambiarlo.

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores > Options	0	⚙️

Passaggio 6. Autorizzare gli utenti.

#### Dalla GUI:

Dopo che il tentativo di accesso ha superato la policy di autenticazione, è necessario che venga autorizzato e che ISE restituisca il profilo di autorizzazione creato in precedenza (accettazione autorizzazione, insieme al livello di privilegio).

In questo esempio, i tentativi di accesso vengono filtrati in base all'indirizzo IP del dispositivo (che è l'indirizzo IP del WLC) e distinguono il livello di privilegio da concedere in base al gruppo a cui appartiene un utente. Un altro approccio valido consiste nel filtrare gli utenti in base ai relativi nomi utente, poiché in questo esempio ogni gruppo contiene un solo utente.

Policy Sets → Default

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	152

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (2)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	9800 Helpdesk Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	9800-helpdesk-priv	Select from list	1	⚙️
✓	9800 Admin Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	9800-admin-priv	Select from list	2	⚙️

> Authorization Policy (12)

Reset Save

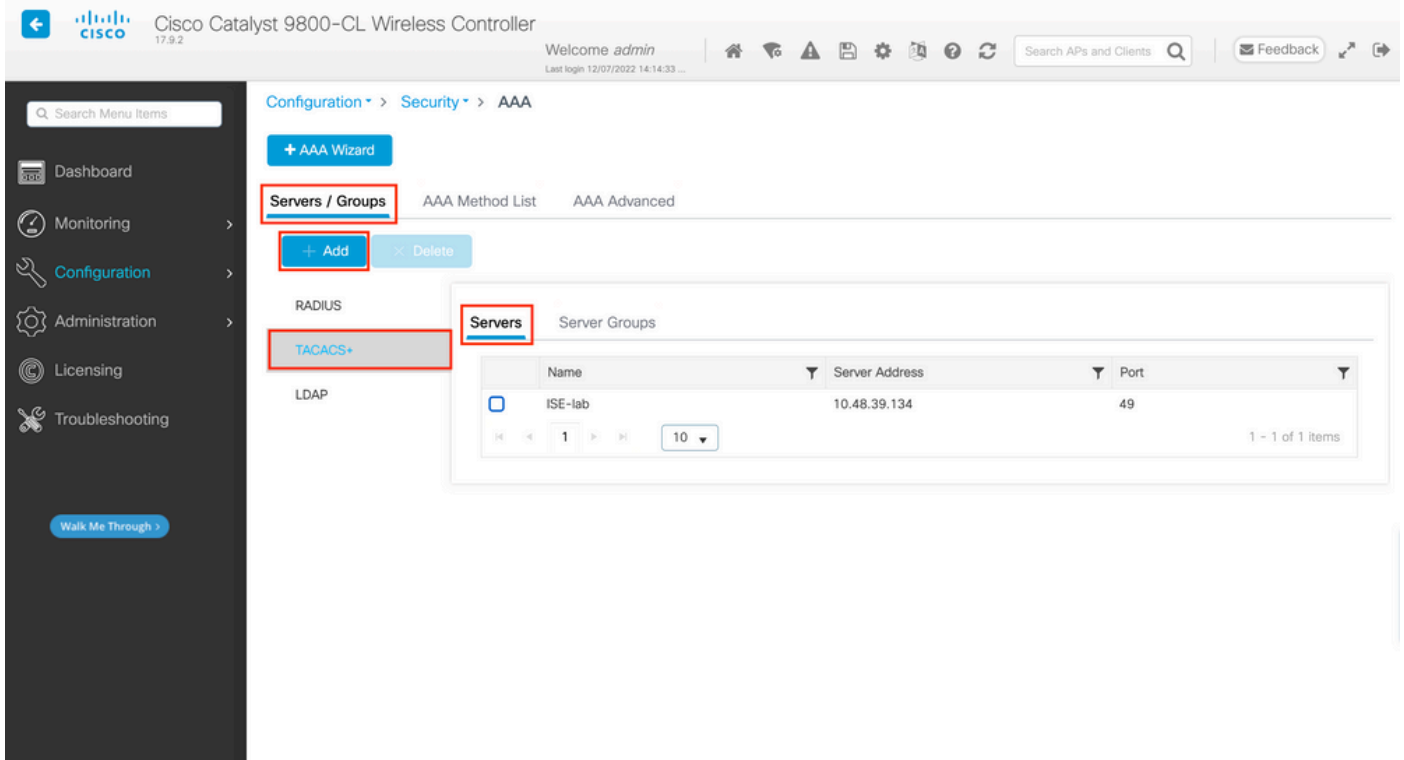
Al termine, le credenziali configurate per adminuser helpdesk e per l'utente possono essere usate per autenticarsi nel WLC tramite la GUI o Telnet/SSH.

### Configurazione di TACACS+ WLC

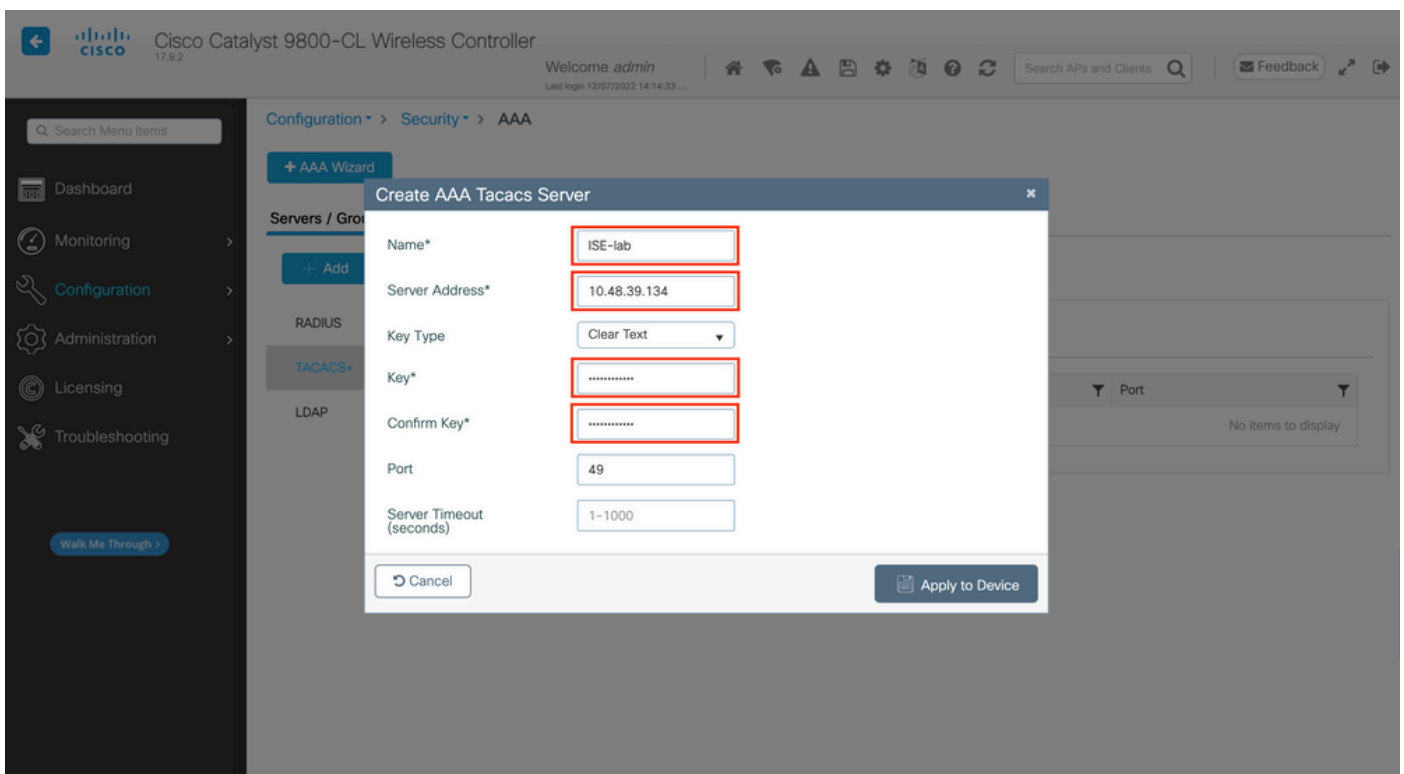
Passaggio 1. Dichiarare il server TACACS+.

#### Dalla GUI:

Innanzitutto, creare il server TACACS+ ISE sul WLC. A tale scopo, è possibile selezionare la scheda Servers/Groups > TACACS+ > Servers dalla pagina WLC della GUI accessibile nella pagina <https://<WLC-IP>/webui/#/aaa> o passare a Configuration > Security > AAA, come mostrato nell'immagine.



Per aggiungere un server TACACS al WLC, fare clic sul pulsante Add (Aggiungi) visualizzato in rosso nell'immagine precedente. Verrà visualizzata la finestra popup illustrata.



Quando si apre la finestra pop-up, fornire il nome del server (non deve corrispondere al nome del sistema ISE), il relativo indirizzo IP, la chiave condivisa, la porta utilizzata e il timeout.

In questa finestra popup è necessario specificare:

- Il nome del server (non è necessario che corrisponda al nome del sistema ISE)

- Indirizzo IP del server
- Il segreto condiviso tra il WLC e il server TACACS+

È possibile configurare altri parametri, ad esempio le porte utilizzate per l'autenticazione e l'accounting, ma questi non sono obbligatori e rimangono predefiniti per la presente documentazione.

Dalla CLI:

```
<#root>
```

```
WLC-9800(config)#tacacs server
```

```
ISE-lab
```

```
WLC-9800(config-server-tacacs)#address ipv4
```

```
10.48.39.134
```

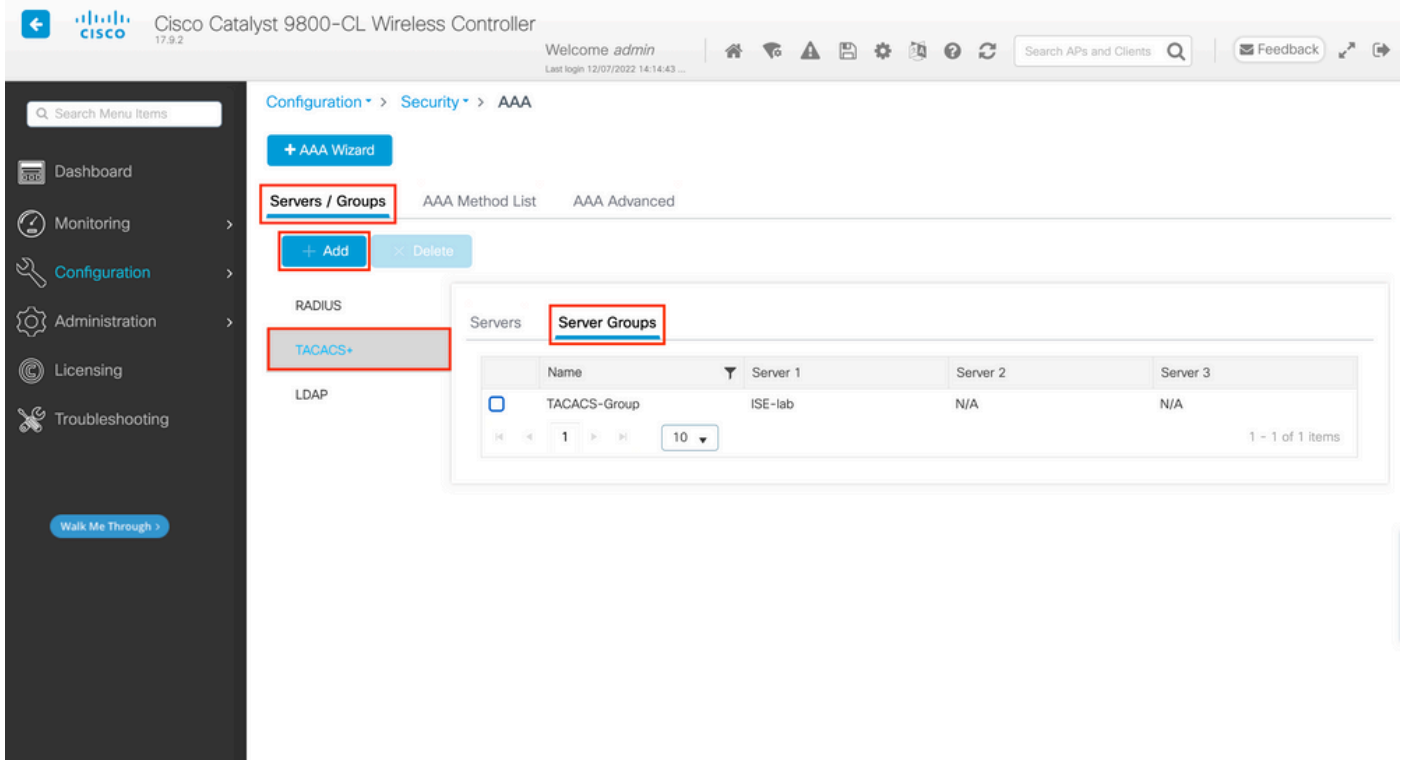
```
WLC-9800(config-server-tacacs)#key
```

```
Cisco123
```

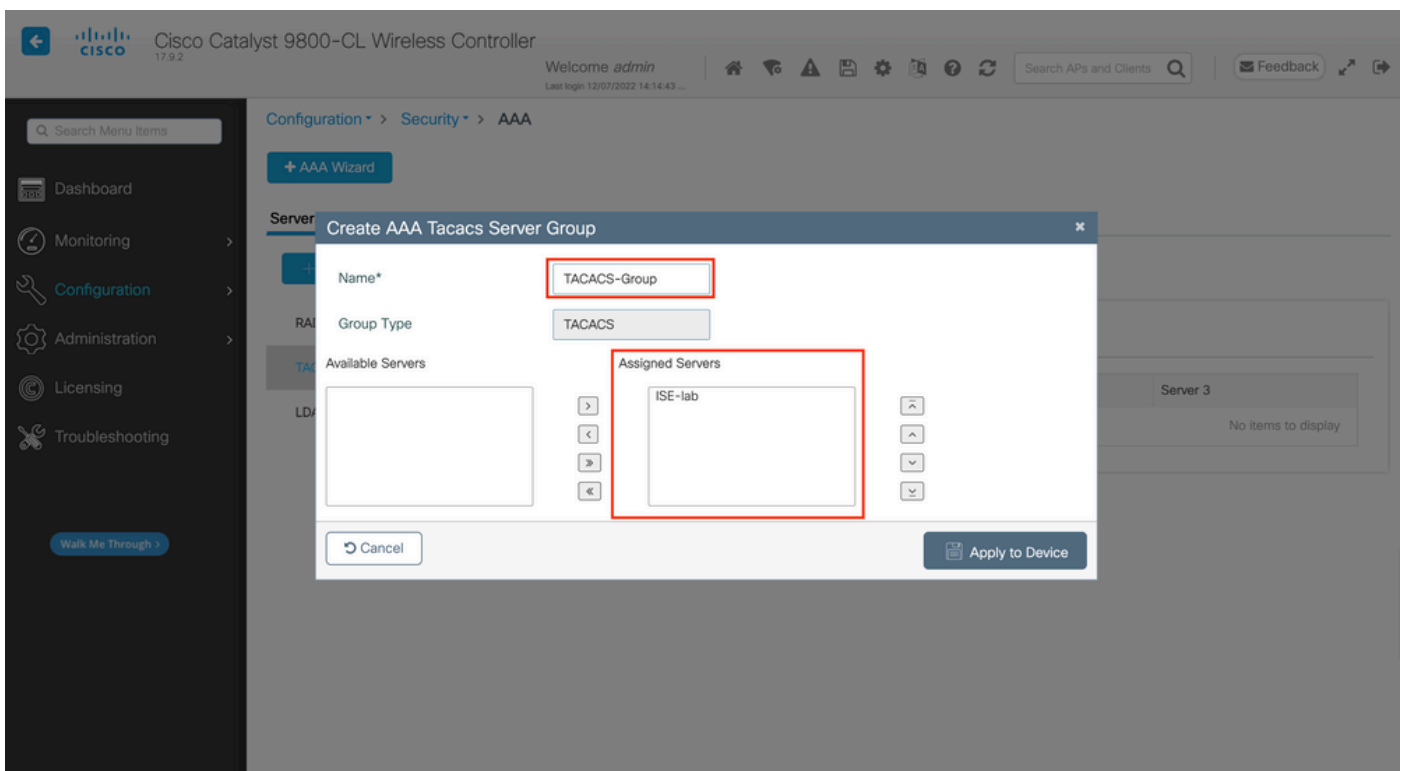
Passaggio 2. Mappare il server TACACS+ a un gruppo di server.

Dalla GUI:

Se si dispone di più server TACACS+ utilizzabili per l'autenticazione, si consiglia di mappare tutti questi server allo stesso gruppo di server. Il WLC si occupa quindi del bilanciamento del carico delle diverse autenticazioni tra i server del gruppo di server. I gruppi di server TACACS+ sono configurati dalla Servers/Groups > TACACS > Server Groups scheda dalla stessa pagina GUI di quella menzionata al punto 1., che è mostrata nell'immagine.



Per quanto riguarda la creazione del server, viene visualizzata una finestra popup quando si fa clic sul pulsante Aggiungi inquadrate nell'immagine precedente, rappresentata nell'immagine.



Nel popup, assegnare un nome al gruppo e spostare i server desiderati nell'elenco Server assegnati.

Dalla CLI:

<#root>



WLC-9800(config)#aaa group server tacacs+

### TACACS-Group

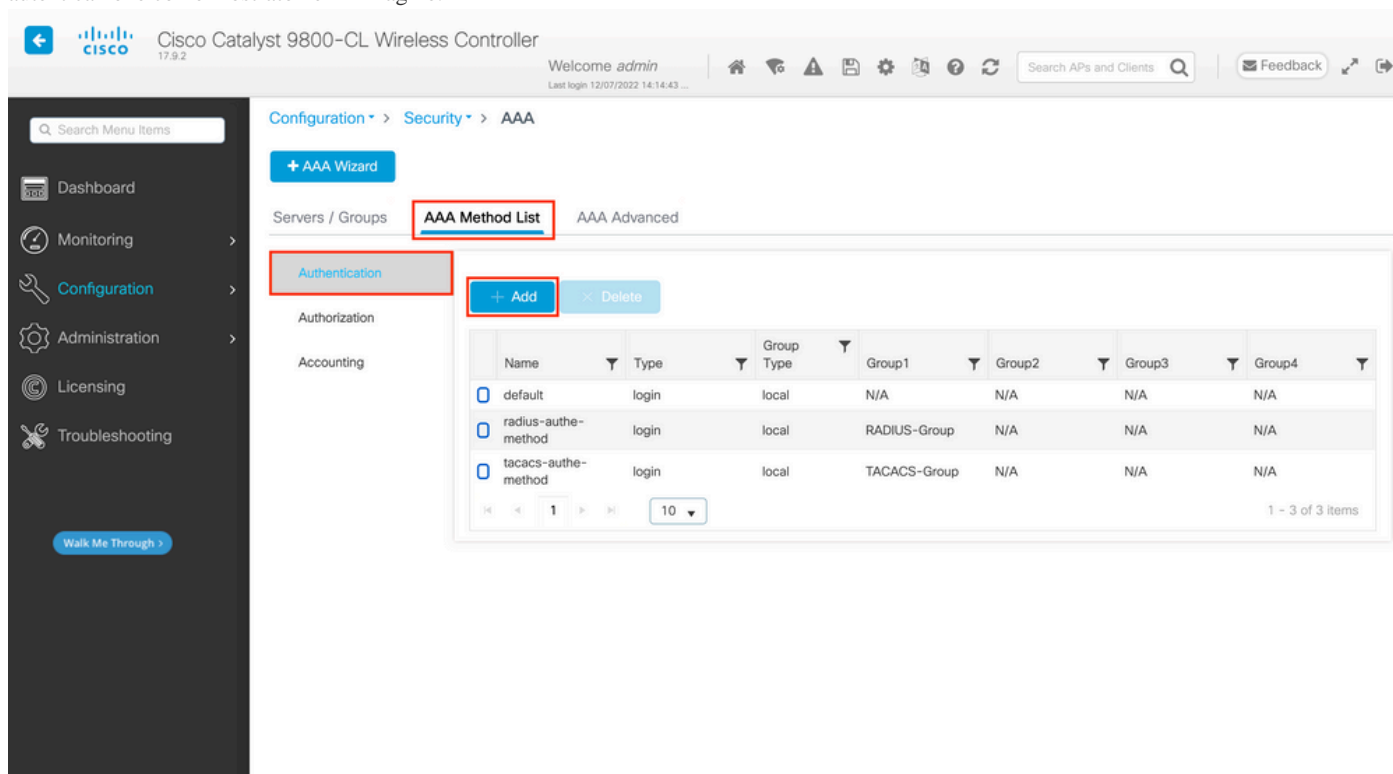
WLC-9800(config-sg-tacacs+)#server name

### ISE-lab

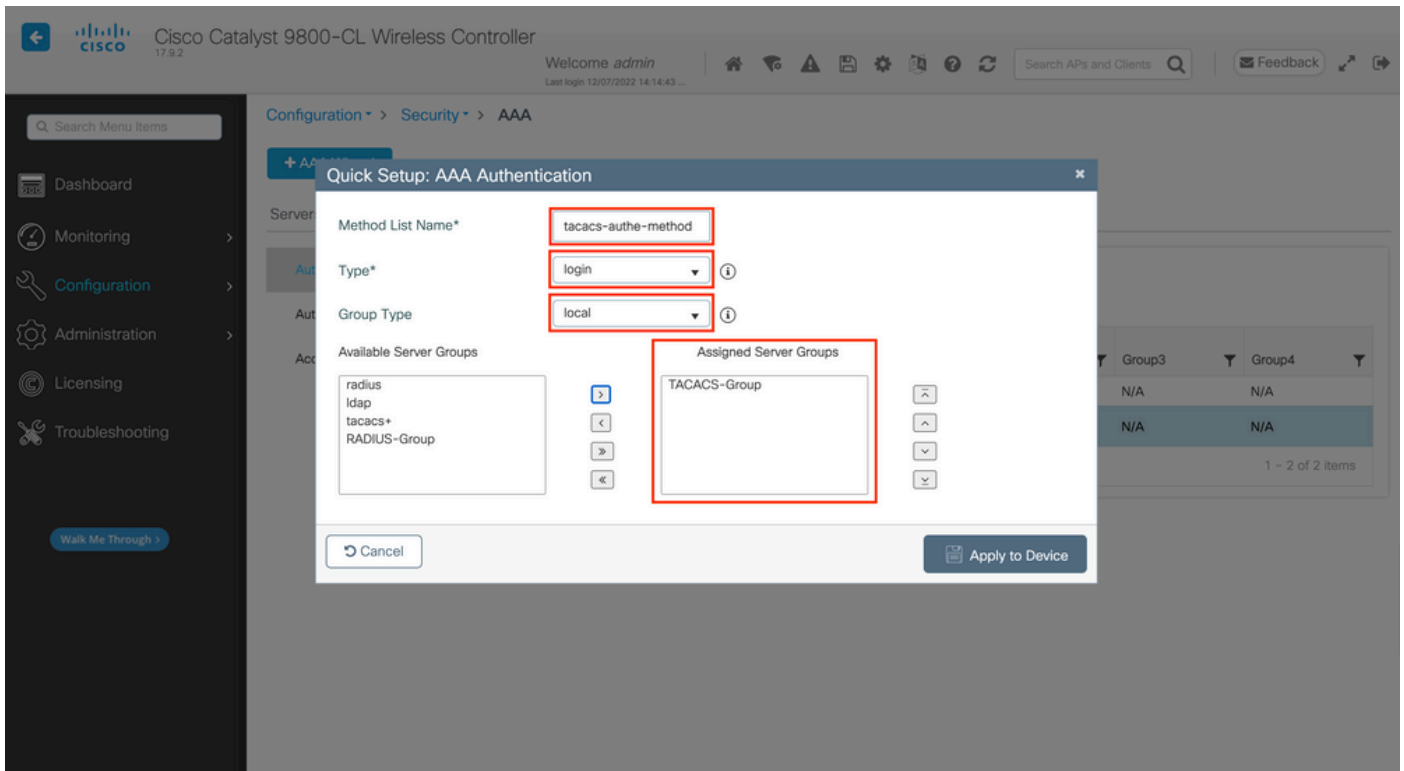
Passaggio 3. Creare un metodo di accesso con autenticazione AAA che punti al gruppo di server TACACS+.

Dalla GUI:

Sempre dalla pagina GUI <https://<WLC-IP>/webui/#/aaa>, passare alla AAA Method List > Authentication scheda e creare un metodo di autenticazione come mostrato nell'immagine.



Come al solito, quando si utilizza il pulsante Aggiungi per creare un metodo di autenticazione, viene visualizzata una finestra popup di configurazione simile a quella illustrata in questa immagine.



In questa finestra popup, fornire un nome per il metodo, scegliere Digitare come login, quindi aggiungere il server di gruppo creato nel passaggio precedente alla lista Gruppi di server assegnati. Per quanto riguarda il campo Tipo di gruppo, sono possibili diverse configurazioni.

- Se si sceglie Tipo di gruppo come locale, il WLC verifica innanzitutto se le credenziali dell'utente esistono localmente e quindi esegue il fallback al gruppo di server.
- Se si sceglie Tipo di gruppo come gruppo e non si seleziona l'opzione Ripristina locale, il WLC controlla semplicemente le credenziali dell'utente rispetto al gruppo di server.
- Se si sceglie Tipo di gruppo come gruppo e si seleziona l'opzione Fallback a locale, il WLC controlla le credenziali dell'utente rispetto al gruppo di server ed esegue una query sul database locale solo se il server non risponde. Se il server invia un rifiuto, l'utente deve essere autenticato, anche se può esistere nel database locale.

Dalla CLI:

Se si desidera che le credenziali utente vengano controllate con un gruppo di server solo se non vengono trovate prima localmente, utilizzare:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
tacacs-auth-method
```

local group

**TACACS-Group**

Se si desidera che le credenziali utente vengano controllate solo con un gruppo di server, utilizzare:

<#root>

WLC-9800(config)#aaa authentication login

**tacacs-auth-method**

group

**TACACS-Group**

Se si desidera che le credenziali dell'utente vengano controllate con un gruppo di server e se quest'ultimo non risponde con una voce locale, utilizzare:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

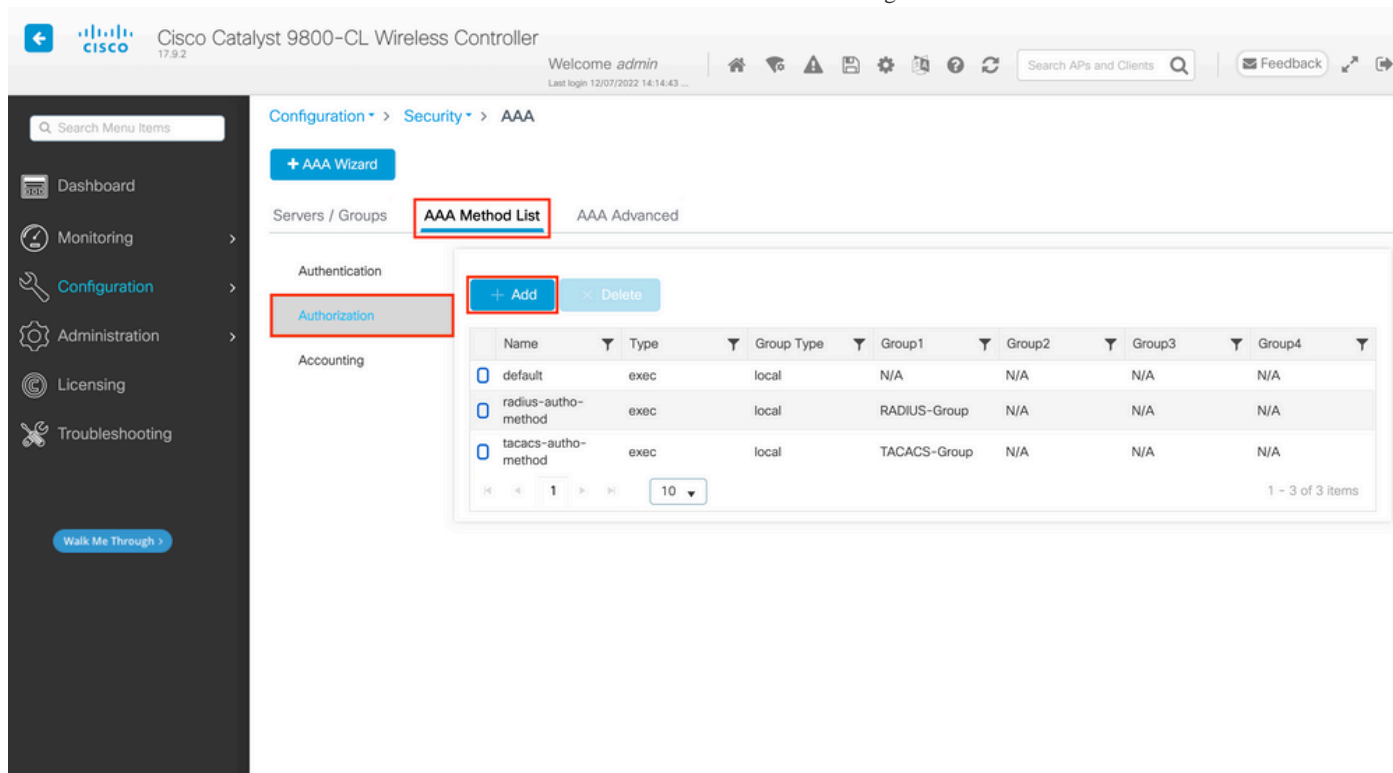
local

Nell'esempio di installazione, ci sono alcuni utenti che vengono creati solo localmente, e alcuni utenti solo sul server ISE, quindi fare uso della prima opzione.

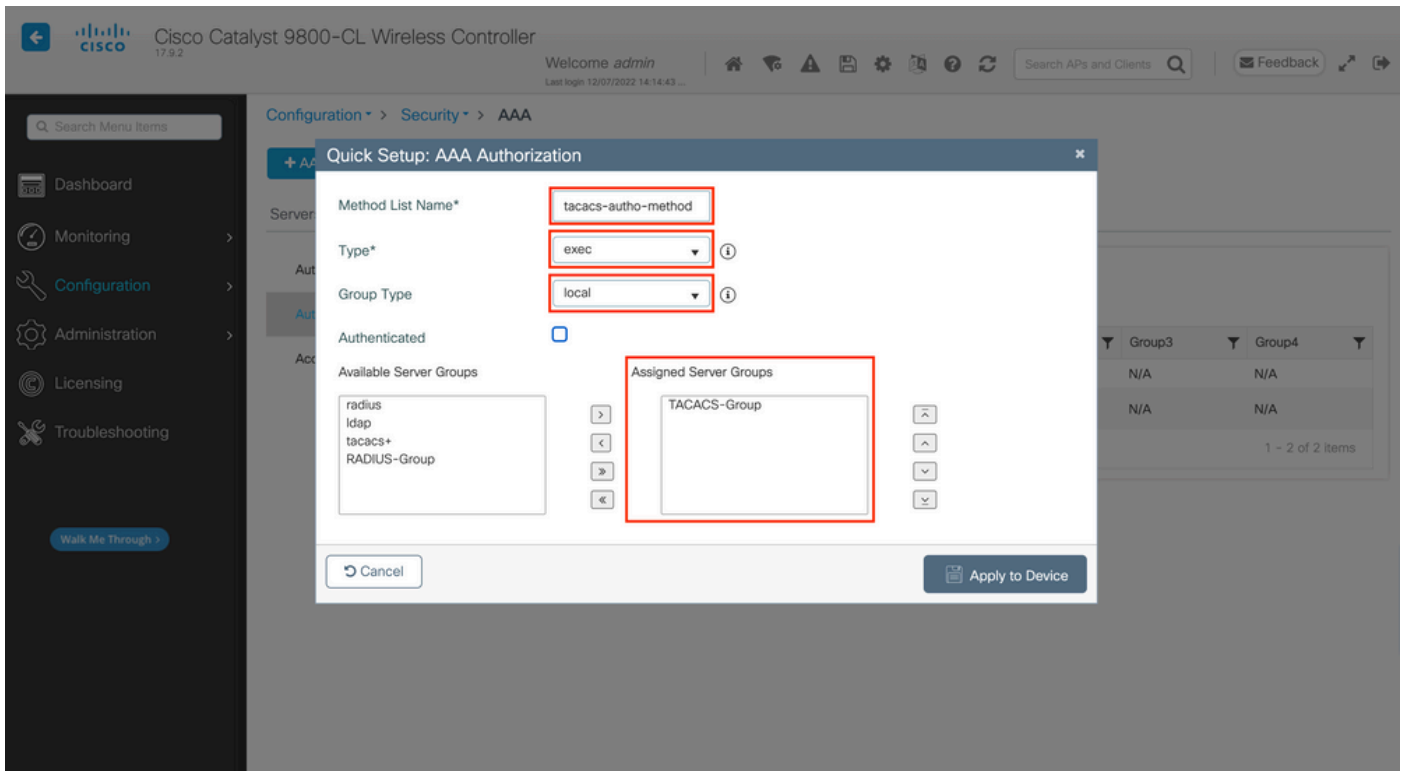
Passaggio 4. Creare un metodo di esecuzione dell'autorizzazione AAA che punti al gruppo di server TACACS+.

Dalla GUI:

L'utente deve anche essere autorizzato per poter accedere. Sempre dalla pagina GUI, Configuration > Security > AAA passare alla AAA Method List > Authorization scheda e creare un metodo di autorizzazione come mostrato nell'immagine.



Quando si aggiunge un nuovo metodo di autorizzazione con il pulsante Aggiungi, viene visualizzato un menu popup di configurazione del metodo di autorizzazione simile a quello illustrato.



In questo popup di configurazione, fornire un nome per il metodo di autorizzazione, scegliere Tipo come exec e utilizzare lo stesso ordine di Tipo di gruppo utilizzato per il metodo di autenticazione nel passaggio precedente.

Dalla CLI:

```
<#root>
```

```
WLC-9800(config)#aaa authorization exec
```

```
tacacs-autho-method
```

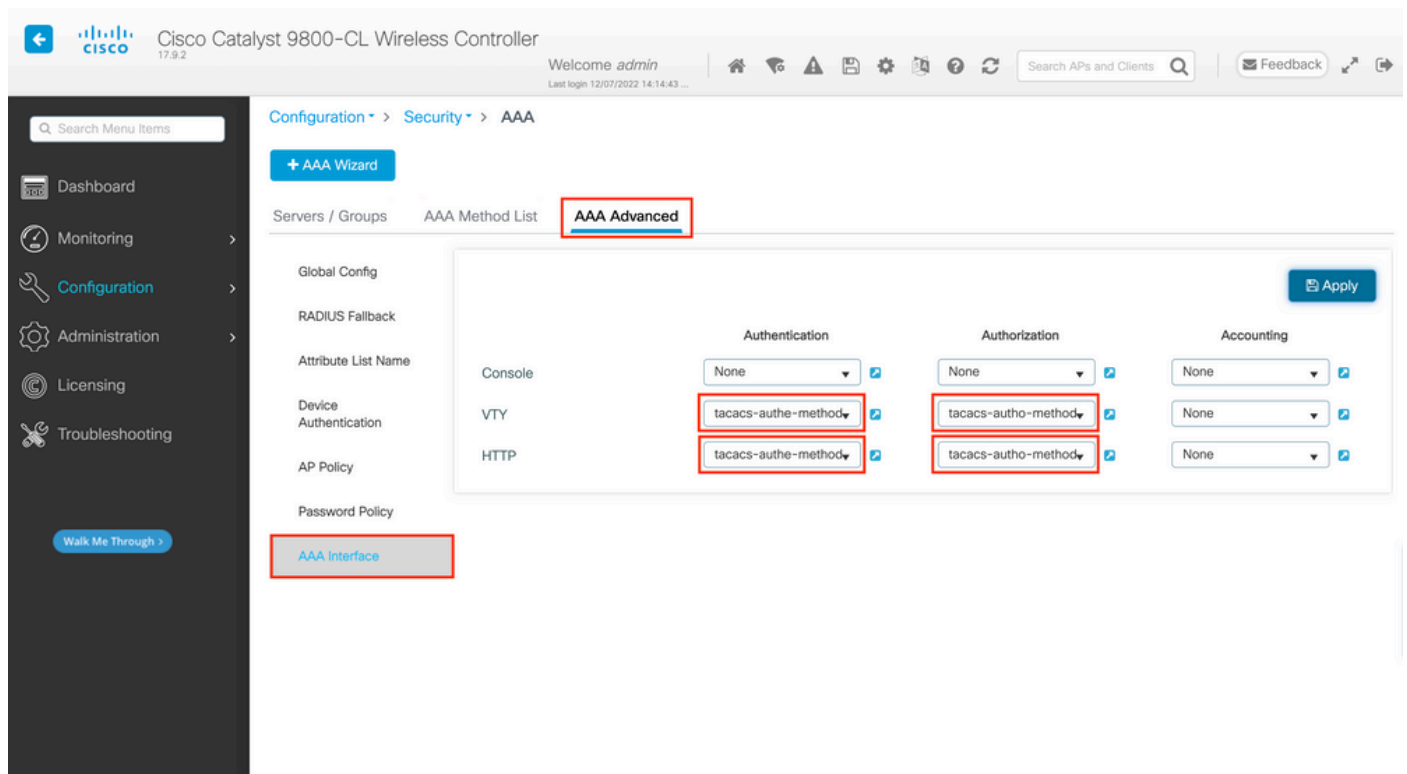
```
local group
```

```
TACACS-Group
```

Passaggio 5. Assegnare i metodi alle configurazioni HTTP e alle linee VTY utilizzate per Telnet/SSH.

## Dalla GUI:

I metodi di autenticazione e autorizzazione creati possono essere utilizzati per le connessioni utente HTTP e/o Telnet/SSH, configurabili dalla AAA Advanced > AAA Interface scheda ancora dalla pagina WLC della GUI accessibile in <https://<WLC-IP>/webui/#/aaa>, come mostrato nell'immagine.



## Dalla CLI:

Per l'autenticazione GUI:

```
<#root>
```

```
WLC-9800(config)#ip http authentication aaa login-authentication
```

```
tacacs-auth-method
```

```
WLC-9800(config)#ip http authentication aaa exec-authorization
```

```
tacacs-auth-method
```

Per l'autenticazione Telnet/SSH:

```
<#root>
```

```
WLC-9800(config)#line vty 0 15  
WLC-9800(config-line)#login authentication
```

```
tacacs-authe-method
```

```
WLC-9800(config-line)#authorization exec
```

```
tacacs-autho-method
```

Quando si apportano modifiche alle configurazioni HTTP, è consigliabile riavviare i servizi HTTP e HTTPS. A tale scopo, è possibile utilizzare i seguenti comandi.

```
WLC-9800(config)#no ip http server  
WLC-9800(config)#no ip http secure-server  
WLC-9800(config)#ip http server  
WLC-9800(config)#ip http secure-server
```

### **Configurazione TACACS+ ISE**

Passaggio 1. Configurare il WLC come dispositivo di rete per TACACS+.

#### Dalla GUI:

Per dichiarare il WLC usato nella sezione precedente come dispositivo di rete per RADIUS in ISE, selezionare Administration > Network Resources > Network Devices e aprire la scheda Network devices (Dispositivi di rete), come mostrato nell'immagine.

Administration · Network Resources

Network Devices

Network Devices

Default Device  
Device Security Settings

Network Devices

Selected 1 Total 1

Edit + Add Duplicate Import Export Generate PAC Delete

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input checked="" type="checkbox"/>	WLC-9800	10.48.39....	Cisco	All Locations	All Device Types	

Nell'esempio, il WLC è già stato aggiunto per l'autenticazione RADIUS (fare riferimento al passaggio 1. della sezione [Configurazione di RADIUS ISE](#)). Pertanto, la sua configurazione deve essere modificata semplicemente per configurare l'autenticazione TACACS, che può essere effettuata quando si sceglie il WLC nell'elenco dei dispositivi di rete e si fa clic sul pulsante Edit (Modifica). Verrà aperto il modulo di configurazione dei dispositivi di rete, come mostrato nell'immagine.

Administration · Network Resources

Network Devices

Network Devices

Default Device  
Device Security Settings

General Settings

Enable KeyWrap

Key Encryption Key  Show

Message Authenticator Code Key  Show

Key Input Format

ASCII  HEXADECIMAL

TACACS Authentication Settings

Shared Secret ..... Show

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

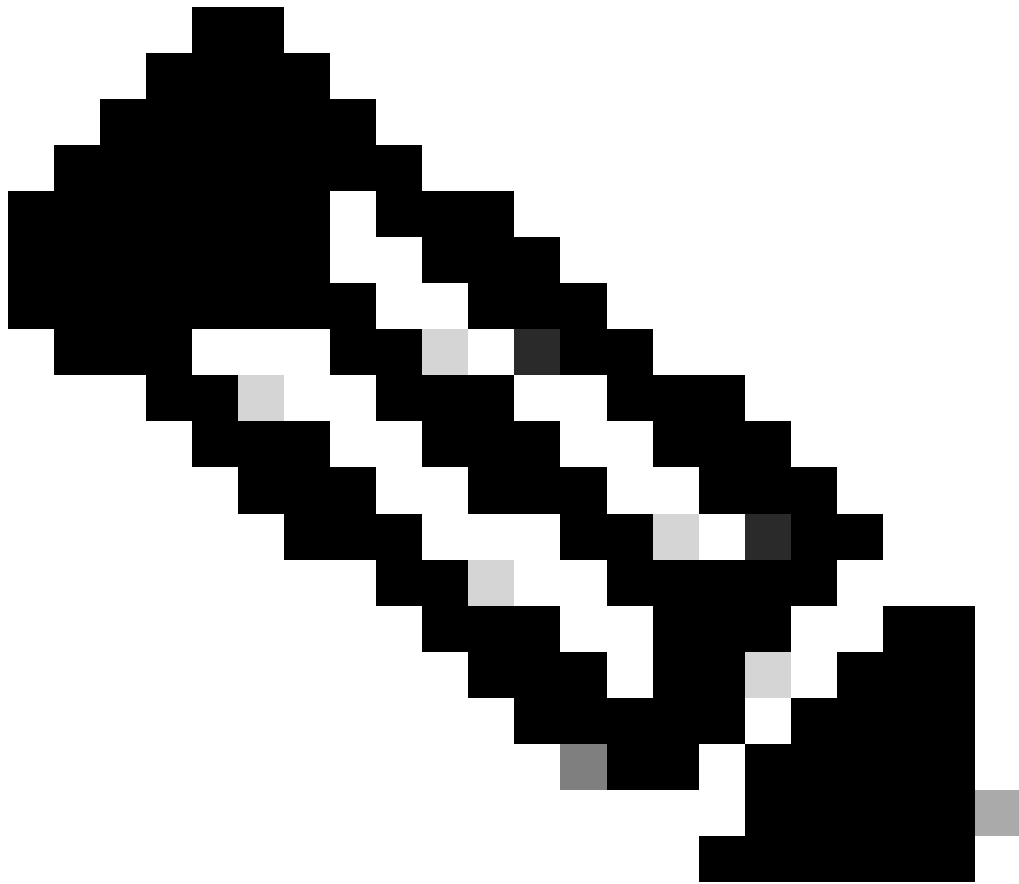
SNMP Settings

Advanced TrustSec Settings

Una volta aperta la nuova finestra, scorrere fino alla sezione TACACS Authentication Settings, abilitare queste impostazioni e aggiungere il segreto condiviso immesso nel Passaggio 1. della sezione [Configure TACACS+ WLC](#).

Passaggio 2. Attivare la funzione Device Admin per il nodo.





**Nota:** per utilizzare ISE come server TACACS+, è necessario disporre di un pacchetto di licenze Device Administration e di una licenza Base o Mobility.

---

Dalla GUI:

Una volta installate le licenze di Device Administration, è necessario abilitare la funzione Device Admin per il nodo in modo da poter utilizzare ISE come server TACACS+. A tale scopo, modificare la configurazione del nodo di distribuzione ISE utilizzato, disponibile in Administrator > Deployment, e fare clic sul relativo nome o farlo con l'aiuto del Edit pulsante.

Deployment

- Deployment
- PAN Failover

### Deployment Nodes

Selected 0 Total 1

Edit Register Syncup Deregister

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise	Administration, Monitoring, Policy Service	STANDALO...	SESSION,PROFILER	<input checked="" type="checkbox"/>

Una volta aperta la finestra di configurazione del nodo, selezionare l'opzione Enable Device Admin Service (Abilita servizio di amministrazione dispositivi) nella sezione Policy Service (Servizio criteri), come mostrato nell'immagine.

Deployment

Deployment Nodes List > ise

### Edit Node

**General Settings** Profiling Configuration

Hostname **ise**

FQDN **ise.cisco.com**

IP Address **10.48.39.134**

Node Type **Identity Services Engine (ISE)**

Role **STANDALONE** [Make Primary](#)

Administration

Monitoring

Role **PRIMARY**

Other Monitoring Node \_\_\_\_\_

Dedicated MnT ⓘ

Policy Service

Enable Session Services ⓘ

Include Node in Node Group **None**

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

**Enable Device Admin Service ⓘ**

Enable Passive Identity Service ⓘ

pxGrid ⓘ

[Reset](#) [Save](#)

Passaggio 3. Creare profili TACACS per restituire il privilegio.

#### Dalla GUI:

Per disporre dei diritti di accesso di amministratore, è necessario che `adminuser` l'amministratore disponga di un livello di privilegi pari a 15, che consente di accedere alla shell del prompt di esecuzione. D'altra parte, non è `helpdeskuser` necessario l'accesso immediato alla shell di esecuzione e può quindi essere assegnato con un livello di privilegio inferiore a 15. Per assegnare agli utenti il livello di privilegio appropriato, è possibile utilizzare i profili di autorizzazione. Questi possono essere configurati dalla pagina dell'interfaccia grafica di ISE Work Centers > Device Administration > Policy Elements, sotto la scheda Results > TACACS Profiles come mostrato nella figura seguente.

- Conditions
  - Library Conditions
  - Smart Conditions
- Network Conditions
- Results
  - Allowed Protocols
  - TACACS Command Sets
  - TACACS Profiles**

### TACACS Profiles

Rows/Page 6 << 1 >> Go 6 Total Rows

**Add** Duplicate Trash Edit

Filter

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	IOS Admin	Shell	Assigned to each user in the group admin-group
<input type="checkbox"/>	IOS Helpdesk	Shell	Assigned to each user in the group helpdesk-group
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

Per configurare un nuovo profilo TACACS, fare clic sul pulsante Add (Aggiungi) per aprire il modulo di configurazione del nuovo profilo, simile a quello mostrato nella figura. Questo modulo deve essere particolarmente simile a questo per configurare il profilo assegnato a adminuser (ovvero con privilegi di shell di livello 15).

TACACS Profiles > IOS Admin  
TACACS Profile

Name  
IOS Admin

Description  
Assigned to each user in the group  
admin-group

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input type="checkbox"/> Timeout		Minutes (0-9999)
<input type="checkbox"/> Idle Time		Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
No data found.		

Cancel Save

Ripetere l'operazione per il helpdesk profilo. Per quest'ultimo valore, sia Privilegio predefinito che Privilegio massimo sono impostati su 1.

Passaggio 4. Creare gruppi di utenti su ISE.

Questa procedura è simile a quella illustrata al passo 3. della sezione [Configurazione di RADIUS ISE](#) in questo documento.

Passaggio 5. Creare gli utenti su ISE.

Questa procedura è simile a quella illustrata al punto 4. della sezione [Configurazione di RADIUS ISE](#) in questo documento.



Passaggio 6. Creare un set di criteri di amministrazione del dispositivo.

#### Dalla GUI:

Per quanto riguarda l'accesso RADIUS, una volta creati gli utenti, le loro policy di autenticazione e autorizzazione devono ancora essere definite su ISE per poter concedere loro i diritti di accesso appropriati. A tal fine, l'autenticazione TACACS utilizza i Device Admin Policy Set, che possono essere configurati dal Work Centers > Device Administration > Device Admin Policy Sets GUI Page router come mostrato.

Policy Sets

Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
							
	Search						
	WLC TACACS Authentication		 Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin   	0		
	Default	Tacacs Default policy set		Default Device Admin   	0		

[Reset](#) [Save](#)

Per creare un set di criteri di amministrazione del dispositivo, utilizzare il pulsante di aggiunta visualizzato in rosso nell'immagine precedente per aggiungere un elemento all'elenco dei set di criteri. Fornire un nome per il set appena creato, una condizione in base alla quale deve essere applicato e la sequenza Protocolli/server consentiti (qui, i numeri Default Device Admin sufficienti). Utilizzare il pulsante per finalizzare l'aggiunta del set di criteri e utilizzare la freccia a destra per accedere alla pagina di configurazione corrispondente, come indicato in precedenza Save.

Policy Sets → **WLC TACACS Authentication**

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		All_User_ID_Stores > Options	0	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	Helpdesk users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	AllowAllCommands	IOS Helpdesk	0		
✓	Admin users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	AllowAllCommands	IOS Admin	0		
✓	Default		DenyAllCommands	Deny All Shell Profile	0		

Reset

Save

Il set di criteri specifico 'Autenticazione TACACS WLC' in questo esempio filtra le richieste con l'indirizzo IP uguale all'indirizzo IP del WLC di esempio C9800.

Come criterio di autenticazione, la regola predefinita è stata lasciata in quanto soddisfa le esigenze del caso di utilizzo. Sono state impostate due regole di autorizzazione:

- La prima viene attivata quando l'utente appartiene al gruppo definito admin-group. Consente tutti i comandi (tramite la regola predefinita Permit\_all) e assegna il privilegio 15 (tramite il profilo TACACS definito IOS\_Admin).
- La seconda viene attivata quando l'utente appartiene al gruppo definito helpdesk-group. Consente tutti i comandi (tramite la Permit\_all regola predefinita) e assegna il privilegio 1 (tramite il profilo TACACS definito IOS\_Helpdesk).

Al termine, le credenziali configurate per adminuser gli utenti ehelphdesk possono essere usate per autenticarsi nel WLC tramite la GUI o con

Telnet/SSH.

Risoluzione dei problemi

Se il server RADIUS prevede l'invio dell'attributo RADIUS del tipo di servizio, è possibile aggiungere sul WLC:

```
radius-server attribute 6 on-for-login-auth
```

Risoluzione dei problemi di accesso WLC GUI o CLI RADIUS/TACACS+ tramite la CLI del WLC

Per risolvere i problemi di accesso a TACACS+ alla GUI o alla CLI del WLC, usare il comando `showdebug tacacs` insieme al `terminal monitor` e visualizzare l'output dal vivo quando si tenta di eseguire l'accesso.

Ad esempio, un accesso riuscito seguito da una disconnessione dell'adminuser/utente genera questo output.

```
<#root>
```

```
WLC-9800#
```

```
terminal monitor
```

```
WLC-9800#
```

```
debug tacacs
```

```
TACACS access control debugging is on
```

```
WLC-9800#
```

```
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
```

```
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

Dai log si può verificare che il server TACACS+ restituisce il privilegio corretto (ovvero AV priv-lvl=15).

Quando si esegue l'autenticazione RADIUS, viene visualizzato un output di debug simile relativo al traffico RADIUS.

I comandi `debug aaa authentication` e `debug aaa authorization`, invece, mostrano quale elenco di metodi viene scelto dal WLC quando l'utente



tenta di eseguire l'accesso.

Risoluzione dei problemi di accesso WLC GUI o TACACS+ CLI tramite l'interfaccia utente di ISE

Da questa pagina Operations > TACACS > Live Logs, è possibile visualizzare ogni autenticazione utente eseguita con TACACS+ fino alle ultime 24 ore. Per espandere i dettagli di un'autorizzazione TACACS+ o di un'autenticazione, utilizzare il pulsante Dettagli relativo a questo evento.

The screenshot shows the Cisco ISE Live Logs interface. At the top, there is a navigation bar with 'Cisco ISE' on the left, 'Operations · TACACS' in the center, and 'Evaluation Mode 82 Days' on the right. Below the navigation bar, there is a 'Live Logs' tab highlighted with a red box. The main content area displays a table of logs with columns: Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, and N. The first row of the table is highlighted with a red box, and its 'Type' column contains the word 'Authorization'. The table also includes controls for Refresh (Never), Show (Latest 20 records), and Within (Last 3 hours). At the bottom, it shows 'Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time)' and 'Records Shown: 6'.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	N
Dec 08, 2022 06:51:46.1...	✓	🔒	helpdeskuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:51:46.0...	✓	🔒	helpdeskuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:38:38.2...	✓	🔒	adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:38:38.1...	✓	🔒	adminuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:34:54.0...	✓	🔒	adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:34:53.9...	✓	🔒	adminuser	Authentication	WLC TACACS Authentication >...		ise	W

Quando è espanso, un tentativo di autenticazione riuscito per l'oggetto helpdeskuser avrà il seguente aspetto:

## Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

## Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

## Steps

```

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Device IP Address
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
13045 TACACS+ will use the password prompt from global
TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (
🚧 Step latency=3149ms)
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - InternalUser.IdentityGroup
13015 Returned TACACS+ Authentication Reply

```

Da questa schermata è possibile verificare che l'utente helpdeskuser è stato autenticato correttamente nel dispositivo di rete WLC-9800 con l'aiuto del criterio di autenticazione WLC TACACS Authentication > Default. Inoltre, il profilo di autorizzazione IOS Helpdesk è stato assegnato a questo utente e gli è stato concesso il livello di privilegio 1.

## 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).