

# Configurazione di 9800 WLC Lobby Ambassador con autenticazione RADIUS e TACACS+

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Autentica RADIUS](#)

[Configurare ISE - RADIUS](#)

[Autenticazione TACACS+](#)

[Configurazione di TACACS+ su WLC](#)

[Configurare ISE - TACACS+](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Autentica RADIUS](#)

[Autenticazione TACACS+](#)

## Introduzione

Questo documento descrive come configurare Catalyst 9800 Wireless LAN Controller per l'autenticazione esterna RADIUS e TACACS+ degli utenti di Lobby Ambassador, con l'uso di Identity Services Engine (ISE).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst Wireless 9800 modello di configurazione
- Concetti AAA, RADIUS e TACACS+

### 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 16.12.1s

- ISE 2.3.0

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.

## Premesse

L'utente Lobby Ambassador è creato dall'amministratore della rete. Un utente Lobby Ambassador è in grado di creare il nome utente, la password, la descrizione e la durata di un utente ospite. Consente inoltre di eliminare l'utente guest. L'utente guest può essere creato tramite GUI o CLI.

## Configurazione

### Esempio di rete



In questo esempio, sono configurati gli ambasciatori della sala d'attesa "lobby" e "lobbyTac". La "lobby" dell'ambasciatore della sala d'attesa deve essere autenticata dal server RADIUS e l'ambasciatore della sala d'attesa "lobbyTac" deve essere autenticato da TACACS+.

La configurazione verrà effettuata prima per l'ambasciatore della sala d'attesa RADIUS e infine per l'ambasciatore della sala d'attesa TACACS+. Viene condivisa anche la configurazione RADIUS e TACACS+ ISE.

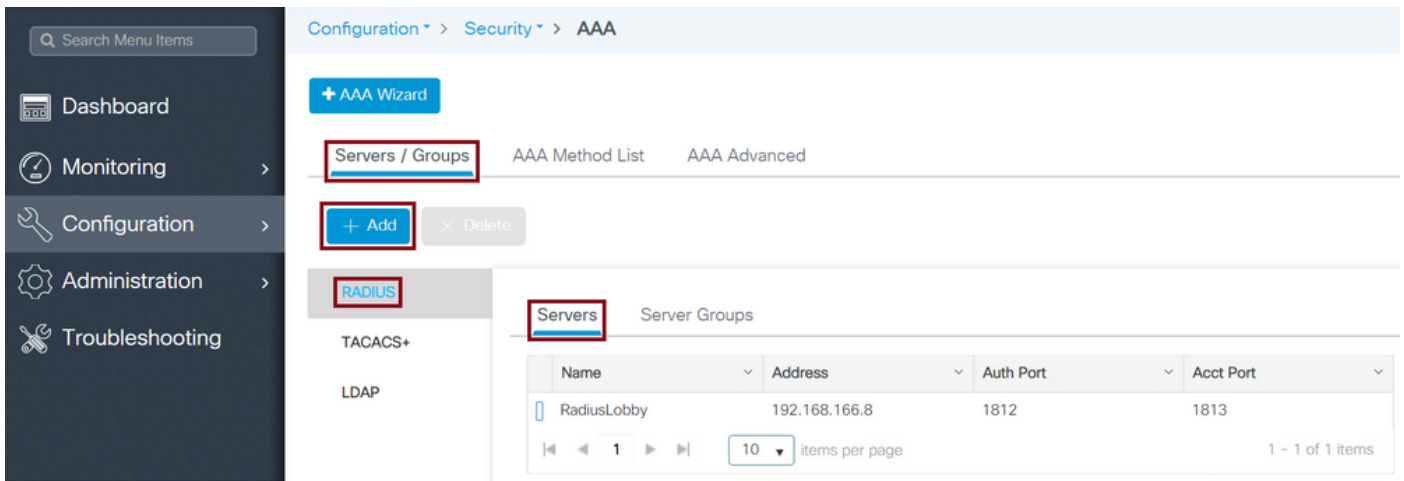
### Autentica RADIUS

Configurare RADIUS sul controller WLC.

Passaggio 1. Dichiarare il server RADIUS. Creare il server ISE RADIUS sul WLC.

GUI:

Selezionare **Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Server > + Aggiungi** come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione, i parametri di configurazione obbligatori sono il nome del server RADIUS (non deve necessariamente corrispondere al nome di sistema ISE/AAA), l'INDIRIZZO IP del server RADIUS e il segreto condiviso. Qualsiasi altro parametro può essere lasciato predefinito o configurato come desiderato.

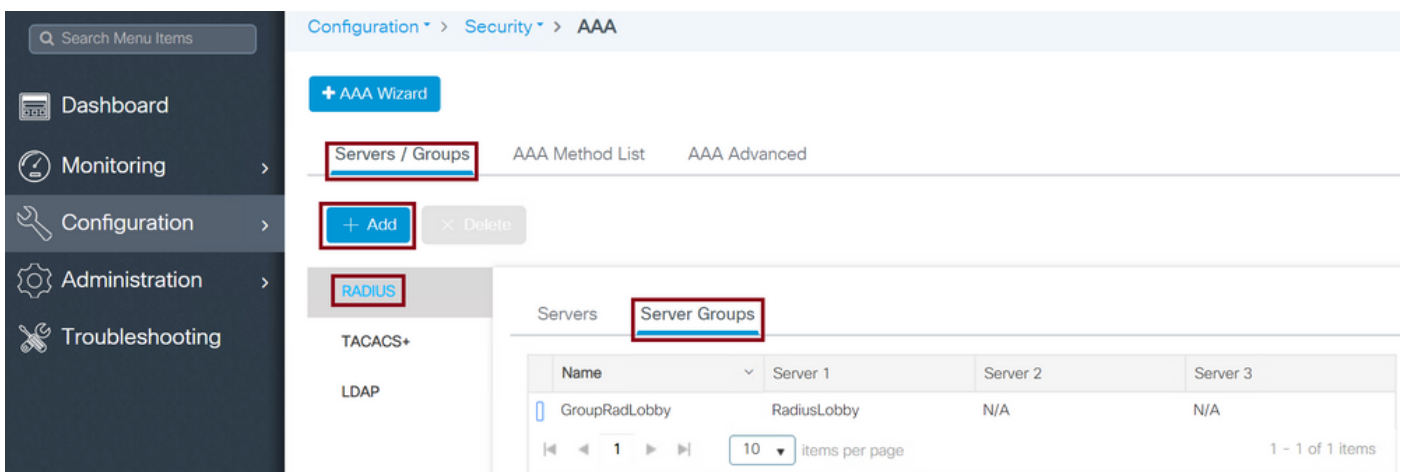
CLI:

```
Tim-eWLC1(config)#radius server RadiusLobby
Tim-eWLC1(config-radius-server)#address ipv4 192.168.166.8 auth-port 1812 acct-port 1813
Tim-eWLC1(config-radius-server)#key 0 Cisco1234
Tim-eWLC1(config)#end
```

Passaggio 2. Aggiungere il server RADIUS a un gruppo di server. Definire un gruppo di server e aggiungere il server RADIUS configurato. Si tratta del server RADIUS utilizzato per l'autenticazione dell'utente Lobby Ambassador. Se nel WLC sono configurati più server RADIUS che possono essere utilizzati per l'autenticazione, si consiglia di aggiungere tutti i server RADIUS allo stesso gruppo di server. In questo caso, si consente al WLC di bilanciare il carico delle autenticazioni tra i server RADIUS nel gruppo di server.

GUI:

Selezionare **Configurazione > Sicurezza > AAA > Server / Gruppi > RADIUS > Gruppi di server > + Aggiungi** come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione per assegnare un nome al gruppo, spostare i server RADIUS configurati dall'elenco Server disponibili all'elenco Server assegnati.

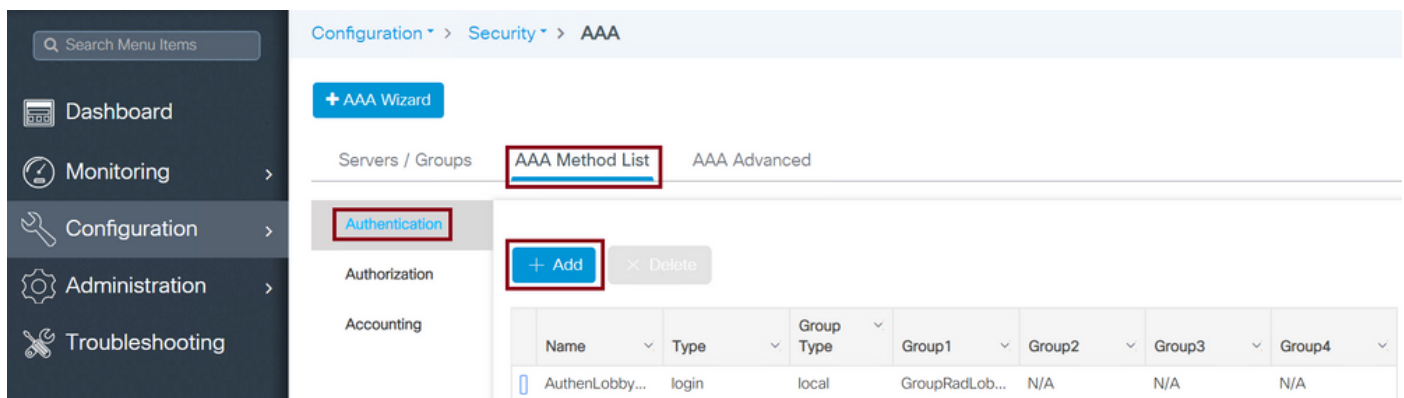
CLI:

```
Tim-eWLC1(config)#aaa group server radius GroupRadLobby  
Tim-eWLC1(config-sg-radius)#server name RadiusLobby  
Tim-eWLC1(config-sg-radius)#end
```

Passaggio 3. Creare un elenco di metodi di autenticazione. L'elenco dei metodi di autenticazione definisce il tipo di autenticazione da ricercare e lo stesso tipo verrà associato al gruppo di server definito. È possibile sapere se l'autenticazione verrà eseguita localmente sul WLC o esternamente a un server RADIUS.

GUI:

Passare a **Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > + Aggiungi** come mostrato nell'immagine.



The screenshot shows the Cisco GUI configuration page for AAA Method List. The breadcrumb navigation is Configuration > Security > AAA. The page title is AAA Method List. There are tabs for Servers / Groups, AAA Method List (selected), and AAA Advanced. On the left, there is a sidebar with navigation options: Dashboard, Monitoring, Configuration (selected), Administration, and Troubleshooting. In the main content area, there is a '+ AAA Wizard' button. Below it, there are tabs for Authentication (selected), Authorization, and Accounting. An '+ Add' button is highlighted. Below the buttons is a table with columns: Name, Type, Group Type, Group1, Group2, Group3, and Group4. The table contains one row: AuthenLobby..., login, local, GroupRadLob..., N/A, N/A, N/A.

Name	Type	Group Type	Group1	Group2	Group3	Group4
AuthenLobby...	login	local	GroupRadLob...	N/A	N/A	N/A

Quando viene visualizzata la finestra di configurazione, specificate un nome, selezionate l'opzione Tipo (Type) come **Accesso (Login)** e assegnate il gruppo di server creato in precedenza.

Tipo di gruppo locale.

GUI:

Se si seleziona il tipo di gruppo come 'locale', il WLC verifica innanzitutto se l'utente esiste nel database locale e quindi esegue il fallback al gruppo di server solo se l'utente di Lobby Ambassador non viene trovato nel database locale.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod local group GroupRadLobby  
Tim-eWLC1(config)#end
```

**Nota:** Tenere presente il bug [CSCvs87163](#) quando si utilizza prima local. Questo è fissato nella versione 17.3.

Tipo di gruppo come gruppo.

GUI:

Se si seleziona Tipo gruppo come 'gruppo' e non è selezionata l'opzione di fallback a locale, il

WLC confronterà l'utente con il gruppo di server e non archiverà il relativo database locale.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

Tipo di gruppo come gruppo e l'opzione fallback a locale è selezionata.

GUI:

Se si seleziona Group Type come 'group' e l'opzione fallback to local è selezionata, il WLC confronterà l'utente con il gruppo di server ed eseguirà una query sul database locale solo se il server RADIUS scade nella risposta. Se il server risponde, il WLC non attiva un'autenticazione locale.

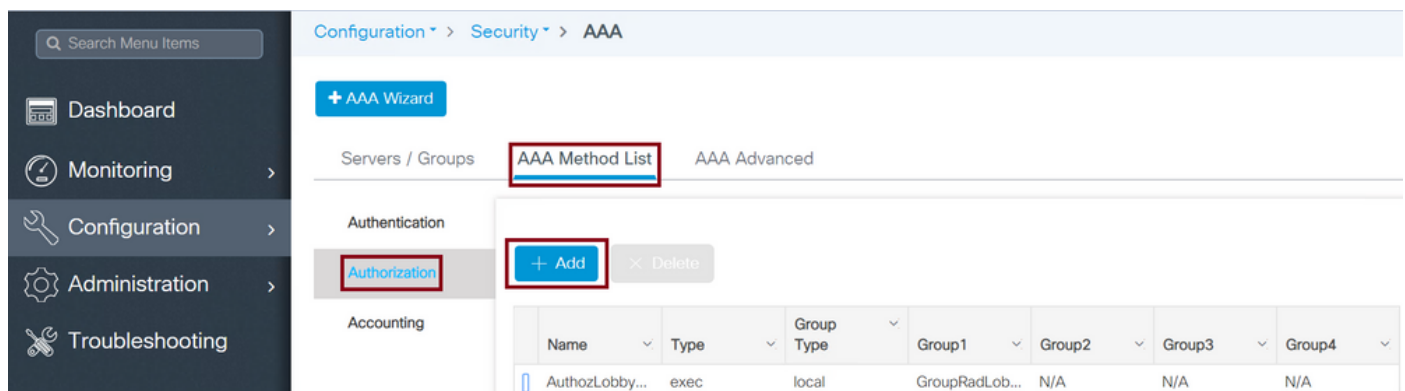
CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby local
Tim-eWLC1(config)#end
```

Passaggio 4. Creare un elenco dei metodi di autorizzazione. L'elenco dei metodi di autorizzazione definisce il tipo di autorizzazione necessario per l'ambasciatore della sala d'attesa, che in questo caso sarà 'exec'. Verrà inoltre collegato allo stesso gruppo di server definito. Consente inoltre di selezionare se l'autenticazione verrà eseguita localmente sul WLC o esternamente a un server RADIUS.

GUI:

Selezionare Configuration > Security > AAA > AAA Method List > Authorization > + Add (Configurazione > Sicurezza > AAA > Elenco dei metodi AAA > Autorizzazione > +Aggiungi) come mostrato nell'immagine.



The screenshot shows the WLC GUI configuration page for AAA Method List. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is selected. Under the 'Authorization' section, the '+ Add' button is highlighted. Below this, a table displays the configuration for a method named 'AuthozLobby...'. The table has columns for Name, Type, Group Type, and four Group options (Group1, Group2, Group3, Group4).

Name	Type	Group Type	Group1	Group2	Group3	Group4
AuthozLobby...	exec	local	GroupRadLob...	N/A	N/A	N/A

Quando viene visualizzata la finestra di configurazione in cui immettere un nome, selezionare l'opzione type come 'exec' e assegnare il gruppo di server creato in precedenza.

Tenere presente che il tipo di gruppo viene applicato nello stesso modo in cui è stato spiegato nella sezione Elenco metodi di autenticazione.

CLI:

Tipo di gruppo locale.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod local group GroupRadLobby
Tim-eWLC1(config)#end
```

Tipo di gruppo come gruppo.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

Tipo di gruppo come gruppo. Viene selezionata l'opzione di fallback a locale.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby local
Tim-eWLC1(config)#end
```

**Passaggio 5. Assegnare i metodi.** Una volta configurati, i metodi devono essere assegnati alle opzioni per accedere al WLC e creare l'utente guest, ad esempio la linea VTY (SSH/Telnet) o HTTP (GUI).

Questi passaggi non possono essere eseguiti dalla GUI, quindi devono essere eseguiti dalla CLI.

**Autenticazione HTTP/GUI:**

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AuthenLobbyMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozLobbyMethod
Tim-eWLC1(config)#end
```

Quando si apportano modifiche alle configurazioni HTTP, è consigliabile riavviare i servizi HTTP e HTTPS:

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

**Line VTY**

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AuthenLobbyMethod
Tim-eWLC1(config-line)#authorization exec AuthozLobbyMethod
Tim-eWLC1(config-line)#end
```

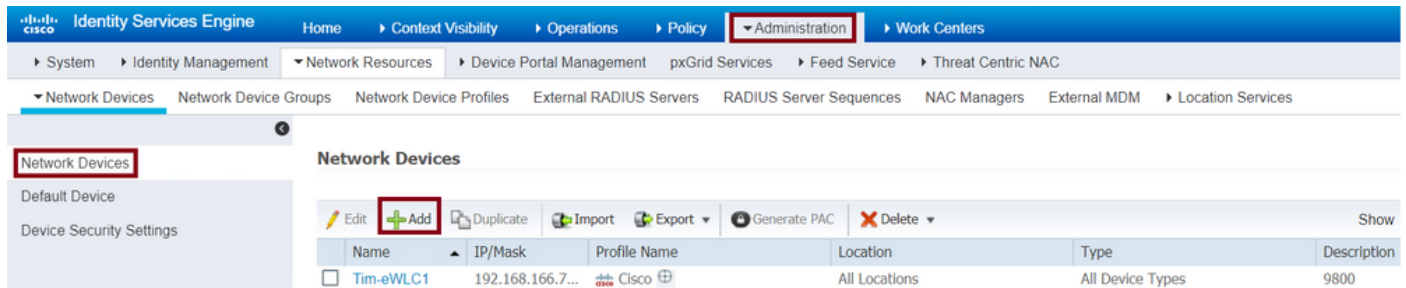
**Passaggio 6.** Questo passaggio è richiesto solo nelle versioni software precedenti alla 17.5.1 o alla 17.3.3 e non è richiesto dopo le versioni in cui [CSCvu29748](#) è stato implementato. Definire l'utente remoto. Il nome utente creato all'ISE per l'Ambasciatore di sala d'attesa deve essere definito come nome utente remoto sul WLC. Se il nome utente remoto non è definito nel WLC, l'autenticazione verrà eseguita correttamente; tuttavia, all'utente verrà concesso l'accesso completo al WLC invece di accedere solo ai privilegi di Ambasciatore della sala di attesa. Questa configurazione può essere eseguita solo dalla CLI.

**CLI:**

```
Tim-eWLC1(config)#aaa remote username lobby
```

**Configurare ISE - RADIUS**

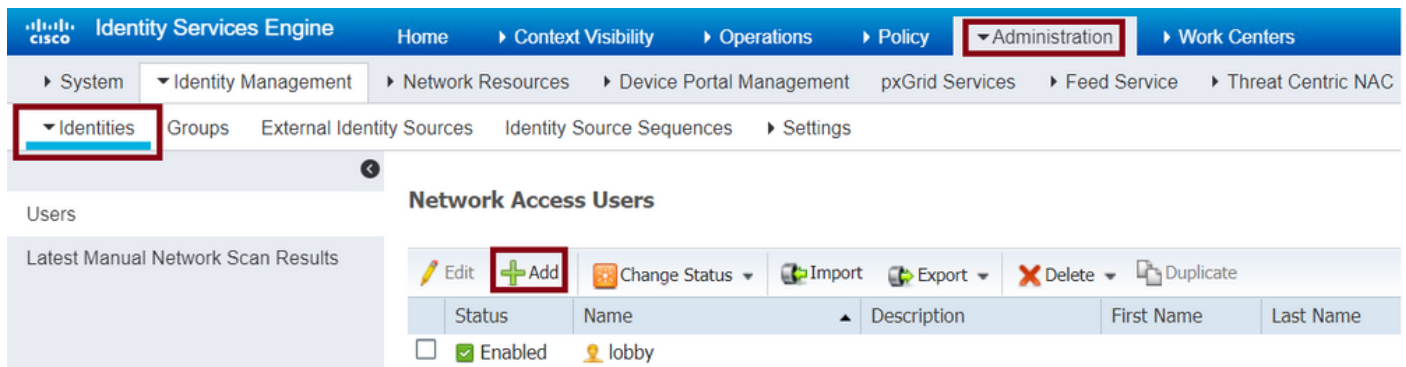
Passaggio 1. Aggiungere il WLC ad ISE. Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi**. Il WLC deve essere aggiunto all'ISE. Quando si aggiunge il WLC a ISE, abilitare le impostazioni di autenticazione RADIUS e configurare i parametri necessari, come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione, specificare un nome, IP ADD, abilitare le impostazioni di autenticazione RADIUS e in Raggio protocollo immettere il segreto condiviso necessario.

Passaggio 2. Creare l'utente Lobby Ambassador su ISE. Passare a **Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi**.

Aggiungi ad ISE il nome utente e la password assegnati all'Ambasciatore della sala d'attesa che crea gli utenti ospiti. Nome utente che l'amministratore assegnerà all'ambasciatore della sala d'attesa.



Quando viene visualizzata la finestra di configurazione, fornire il nome e la password per l'utente Lobby Ambassador. Verificare inoltre che lo stato sia Abilitato.

Passaggio 3. Creare un profilo di autorizzazione dei risultati. Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili autorizzazione > Aggiungi**. Creare un profilo di autorizzazione dei risultati per restituire al WLC un Access-Accept con gli attributi necessari, come mostrato nell'immagine.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaryes Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

### Standard Authorization Profiles

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

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	9800RadiusLobby	Cisco

Verificare che il profilo sia configurato per l'invio di un messaggio di autorizzazione di accesso, come mostrato nell'immagine.

Identity Services Engine Home Context Visibility Operations Policy

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaryes Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

### Authorization Profiles > 9800RadiusLobby

#### Authorization Profile

\* Name

Description

\* Access Type

È necessario aggiungere gli attributi manualmente in Impostazioni avanzate attributi. Gli attributi sono necessari per definire l'utente come Ambasciatore di lobby e per fornire il privilegio al fine di consentire all'Ambasciatore di lobby di apportare le modifiche necessarie.



## Advanced Attributes Settings

The screenshot shows two attribute entries in a list. Each entry consists of a dropdown menu on the left, an equals sign, and a text input field on the right. The first entry has 'Cisco:cisco-av-pair' in the dropdown and 'user-type=lobby-admin' in the text field. The second entry has 'Cisco:cisco-av-pair' in the dropdown and 'shell:priv-lvl=15' in the text field. A green plus icon is visible to the right of the second entry. Below each entry is a small orange downward arrow.

## Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = user-type=lobby-admin
cisco-av-pair = shell:priv-lvl=15
```

Passaggio 4. Creare un criterio per elaborare l'autenticazione. Selezionare **Criterio > Set di criteri > Aggiungi**. Le condizioni per configurare il criterio dipendono dalla decisione dell'amministratore. In questo caso vengono utilizzati la condizione Network Access-Username e il protocollo Default Network Access.

In base ai criteri di autorizzazione, è obbligatorio verificare che il profilo configurato in Autorizzazione risultati sia selezionato in modo da poter restituire gli attributi necessari al WLC, come mostrato nell'immagine.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is highlighted. Below the navigation bar, the 'Policy Sets' section is visible. A table lists the policy sets, with a '+' icon in the first column. The table has columns for 'Status', 'Policy Set Name', 'Description', 'Conditions', and 'Allowed Protocols / Server Sequence'. A search bar is located below the table. The first entry in the table is '9800LobbyRadius' with a green checkmark in the status column. The conditions for this entry are 'Network Access UserName EQUALS lobby'. The 'Allowed Protocols / Server Sequence' column shows 'Default Network Access' with a dropdown arrow and a '+' icon.

Quando viene visualizzata la finestra di configurazione, configurare il criterio di autorizzazione. È possibile lasciare il criterio di autenticazione predefinito.

## Autenticazione TACACS+

### Configurazione di TACACS+ su WLC

Passaggio 1. Dichiarare il server TACACS+. Creare l'ISE TACACS Server nel WLC.

GUI:

Passare a **Configurazione > Sicurezza > AAA > Server/Gruppi > TACACS+ > Server > + Aggiungi** come mostrato nell'immagine.

Quando si apre la finestra di configurazione, i parametri di configurazione obbligatori sono il nome del server TACACS+ (non deve corrispondere al nome del sistema ISE/AAA), l'INDIRIZZO IP del server TACACS e il segreto condiviso. Qualsiasi altro parametro può essere lasciato predefinito o configurato in base alle necessità.

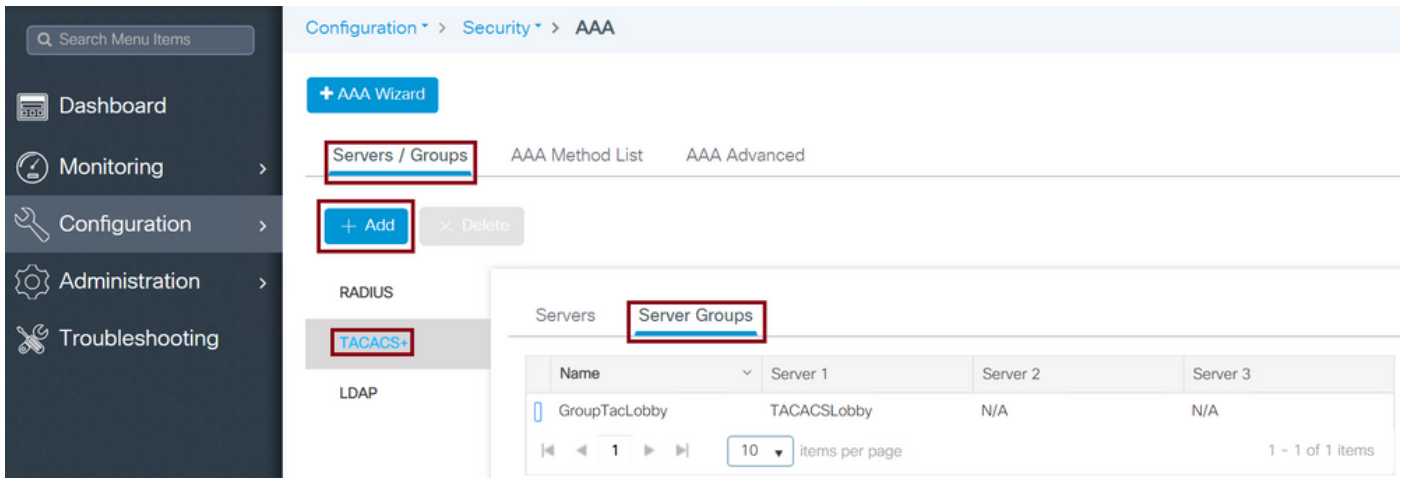
CLI:

```
Tim-eWLC1(config)#tacacs server TACACSLobby
Tim-eWLC1(config-server-tacacs)#address ipv4 192.168.166.8
Tim-eWLC1(config-server-tacacs)#key 0 Cisco123
Tim-eWLC1(config-server-tacacs)#end
```

Passaggio 2. Aggiungere il server TACACS+ a un gruppo di server. Definire un gruppo di server e aggiungere il server TACACS+ desiderato configurato. Verranno utilizzati i server TACACS+ per l'autenticazione.

GUI:

Selezionare **Configurazione > Sicurezza > AAA > Server / Gruppi > TACACS > Gruppi di server > + Aggiungi** come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione, assegnare un nome al gruppo e spostare i server TACACS+ desiderati dall'elenco Server disponibili all'elenco Server assegnati.

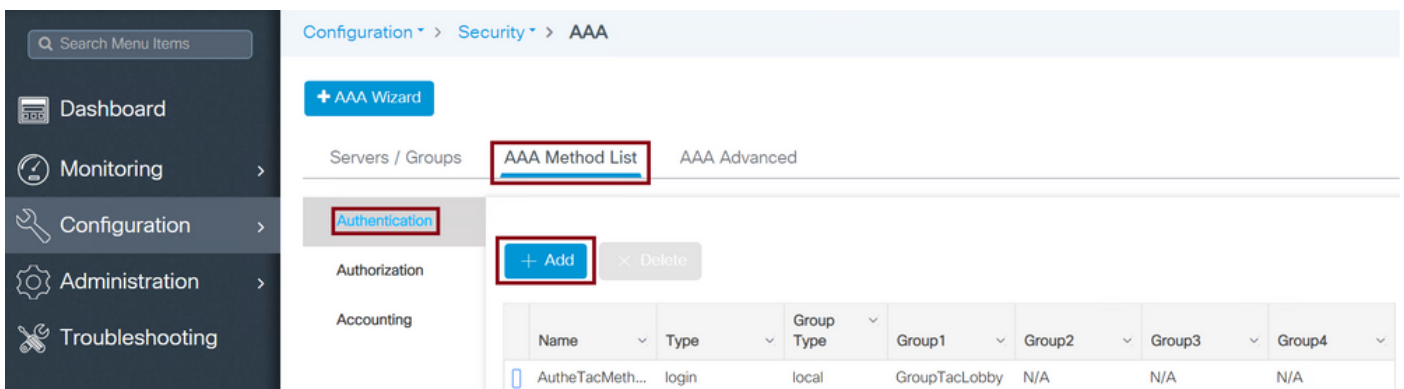
CLI:

```
Tim-eWLC1(config)#aaa group server tacacs+ GroupTacLobby
Tim-eWLC1(config-sg-tacacs+)#server name TACACSLobby
Tim-eWLC1(config-sg-tacacs+)#end
```

Passaggio 3. Creare un elenco di metodi di autenticazione. L'elenco dei metodi di autenticazione definisce il tipo di autenticazione necessaria e lo stesso tipo verrà associato al gruppo di server configurato. Permette anche di selezionare se l'autenticazione può essere effettuata localmente sul WLC o esternamente a un server TACACS+.

GUI:

Passare a **Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > + Aggiungi** come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione, specificate un nome, selezionate l'opzione Tipo (Type) come **Accesso (Login)** e assegnate il gruppo di server creato in precedenza.

Tipo di gruppo locale.

GUI:

Se si seleziona Tipo di gruppo come 'locale', il WLC controlla innanzitutto se l'utente esiste nel database locale e quindi esegue il fallback al gruppo di server solo se l'utente di Lobby Ambassador non viene trovato nel database locale.

**Nota:** Tenere presente questo bug [CSCvs87163](#) fissato al punto 17.3.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

Tipo di gruppo come gruppo.

GUI:

Se si seleziona Tipo di gruppo come gruppo e non si seleziona l'opzione di fallback a locale, il WLC confronterà l'utente con il gruppo di server e non archiverà il relativo database locale.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Tipo di gruppo come gruppo. Viene selezionata l'opzione di fallback a locale.

GUI:

Se si seleziona Group Type come 'group' e l'opzione Fallback to local è selezionata, il WLC confronterà l'utente con il Server Group ed eseguirà una query sul database locale solo se il server TACACS scade nella risposta. Se il server invia un rifiuto, l'utente non verrà autenticato, anche se esiste nel database locale.

CLI:

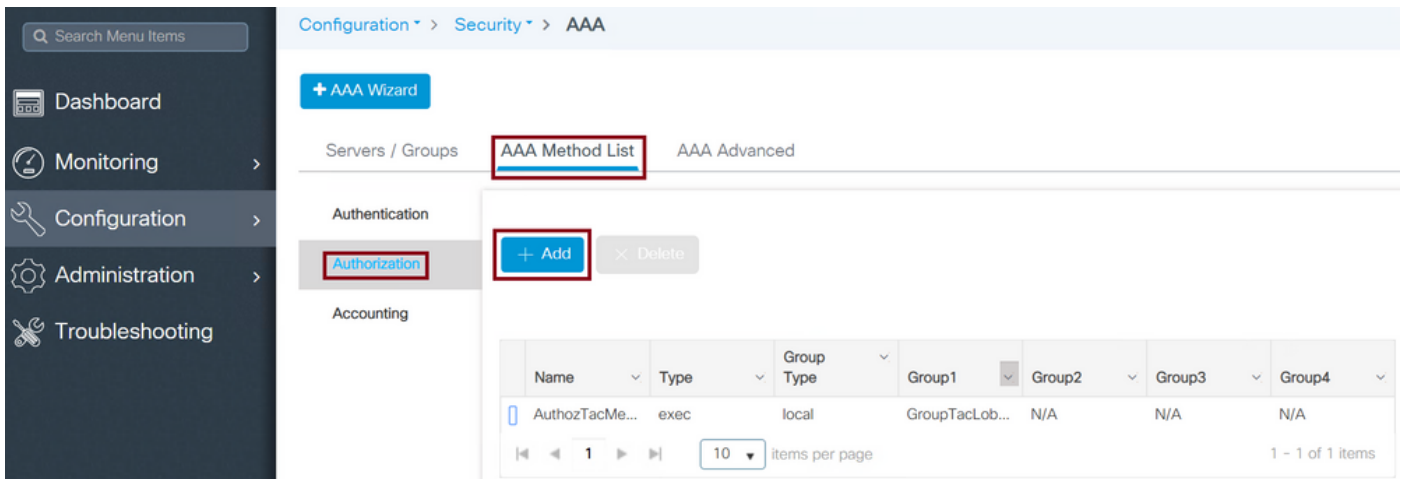
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Passaggio 4. Creare un elenco dei metodi di autorizzazione.

L'elenco dei metodi di autorizzazione definirà il tipo di autorizzazione necessario per l'ambasciatore della sala d'attesa, che in questo caso verrà eseguito. e allo stesso gruppo di server configurato. Inoltre, è possibile selezionare se l'autenticazione viene effettuata localmente sul WLC o esternamente a un server TACACS+.

GUI:

Selezionare Configuration > Security > AAA > AAA Method List > Authorization > + Add (Configurazione > Sicurezza > AAA > Elenco dei metodi AAA > Autorizzazione > +Aggiungi) come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione, specificate un nome, selezionate l'opzione di testo exec e assegnate il gruppo di server creato in precedenza.

Tenere presente che il tipo di gruppo viene applicato nello stesso modo in cui viene spiegato nella parte Authentication Method List.

CLI:

Tipo di gruppo locale.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

Tipo di gruppo come gruppo.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Tipo di gruppo come gruppo e l'opzione Fallback a locale è selezionata.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Passaggio 5. Assegnare i metodi. Una volta configurati, i metodi devono essere assegnati alle opzioni per accedere al WLC e creare l'utente guest, ad esempio la linea VTY o HTTP (GUI). Questi passaggi non possono essere eseguiti dalla GUI, quindi devono essere eseguiti dalla CLI.

Autenticazione HTTP/GUI:

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AutheTacMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozTacMethod
Tim-eWLC1(config)#end
```

Quando si apportano modifiche alle configurazioni HTTP, è consigliabile riavviare i servizi HTTP e HTTPS:

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

VTY linea:

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AutheTacMethod
Tim-eWLC1(config-line)#authorization exec AuthozTacMethod
Tim-eWLC1(config-line)#end
```

Passaggio 6. Definire l'utente remoto. Il nome utente creato all'ISE per l'Ambasciatore di sala d'attesa deve essere definito come nome utente remoto sul WLC. Se il nome utente remoto non è definito nel WLC, l'autenticazione verrà eseguita correttamente; tuttavia, all'utente verrà concesso l'accesso completo al WLC invece di accedere solo ai privilegi di Ambasciatore della sala di attesa. Questa configurazione può essere eseguita solo dalla CLI.

CLI:

```
Tim-eWLC1(config)#aaa remote username lobbyTac
```

## Configurare ISE - TACACS+

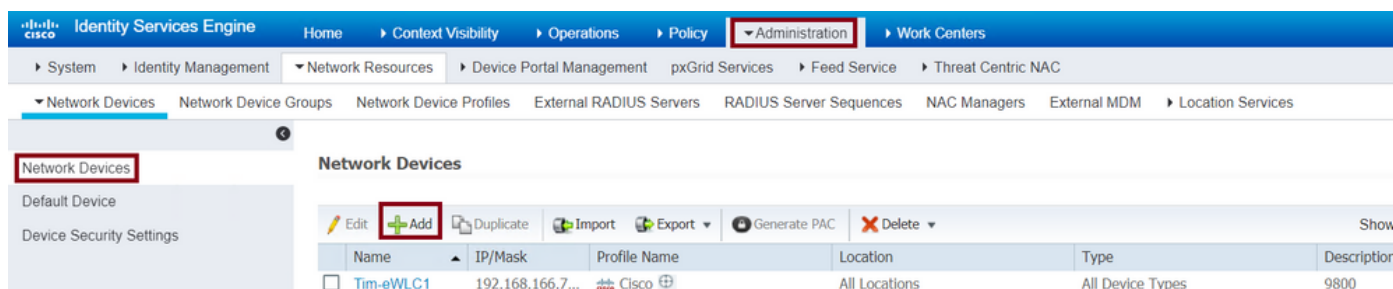
Passaggio 1. Abilitare l'amministratore del dispositivo. Selezionare **Amministrazione > Sistema > Distribuzione**. Prima di procedere, selezionare **Enable Device Admin Service** (Abilita servizio di amministrazione dispositivi) e accertarsi che ISE sia stato abilitato, come mostrato nell'immagine.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The navigation menu at the top includes 'Administration', which is highlighted with a red box. Below it, the 'Deployment' menu item is also highlighted with a red box. The main content area shows the 'Deployment Nodes List > timise23' page, with the 'Edit Node' button highlighted in red. The 'General Settings' tab is active, showing the following configuration details:

Hostname	timise23
FQDN	timise23.cisco.com
IP Address	192.168.166.8
Node Type	Identity Services Engine (ISE)

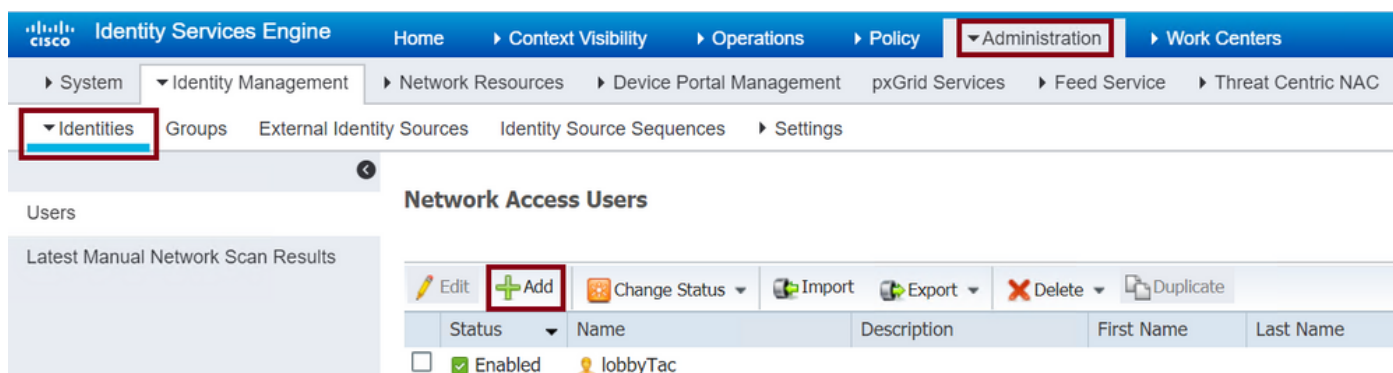
Below the configuration details, the 'Role' is set to 'STANDALONE' with a 'Make Primary' button. The 'Administration' checkbox is checked. Under 'Monitoring', the 'Role' is set to 'PRIMARY'. Under 'Policy Service', the 'Enable Device Admin Service' checkbox is checked and highlighted with a red box. Other services like 'Enable Session Services', 'Enable Profiling Service', 'Enable Threat Centric NAC Service', and 'Enable SXP Service' are also listed with their respective checkboxes and dropdown menus.

Passaggio 2. Aggiungere il WLC ad ISE. Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi**. Il WLC deve essere aggiunto all'ISE. Quando si aggiunge il WLC ad ISE, abilitare le impostazioni di autenticazione TACACS+ e configurare i parametri necessari, come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione con il nome IP ADD, abilitare le impostazioni di autenticazione TACACS+ e immettere il segreto condiviso richiesto.

Passaggio 3. Creare l'utente Lobby Ambassador su ISE. Passare a **Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi**. Ad ISE aggiungeremo il nome utente e la password assegnati all'ambasciatore della sala d'attesa che creerà gli utenti ospiti. Il nome utente assegnato dall'amministratore all'ambasciatore della sala d'attesa, come mostrato nell'immagine.



Quando viene visualizzata la finestra di configurazione, fornire il nome e la password per l'utente Lobby Ambassador. Verificare inoltre che lo stato sia Abilitato.

Passaggio 4. Creare un profilo TACACS+ dei risultati. Passare a **Work Center > Device Administration > Policy Elements > Results > TACACS Profiles** (Centri di lavoro > Amministrazione dispositivi > Elementi criteri > Risultati > Profili TACACS) come mostrato nell'immagine. Con questo profilo, restituire gli attributi necessari al WLC in modo da posizionare l'utente come Ambasciatore della lobby.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets

Conditions

Network Conditions

Results

- Allowed Protocols
- TACACS Command Sets
- TACACS Profiles**

### TACACS Profiles

0 Selected

Refresh **+ Add** Duplicate Trash Edit

<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"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

Quando viene visualizzata la finestra di configurazione, specificare un nome per il profilo, configurare anche un Privileged predefinito 15 e un Attributo personalizzato come Tipo obbligatorio, un nome come tipo utente e un valore lobby-admin. Inoltre, consente di selezionare **Common Task Type** come Shell, come mostrato nell'immagine.



Task Attribute View

Raw View

### Common Tasks

Common Task Type Shell

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege		(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

1 Selected

+ Add    🗑️ Trash    ✎ Edit

Type	Name	Value
MANDATORY	user-type	lobby-admin

Passaggio 5. Creare un set di criteri. Passare a **Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi** come mostrato nell'immagine. Le condizioni per configurare il criterio dipendono dalla decisione dell'amministratore. Per questo documento vengono utilizzati la condizione Network Access-Username e il protocollo Default Device Admin. In base ai criteri di autorizzazione, è obbligatorio verificare che il profilo configurato in Autorizzazione risultati sia selezionato in modo da poter restituire gli attributi necessari al WLC.

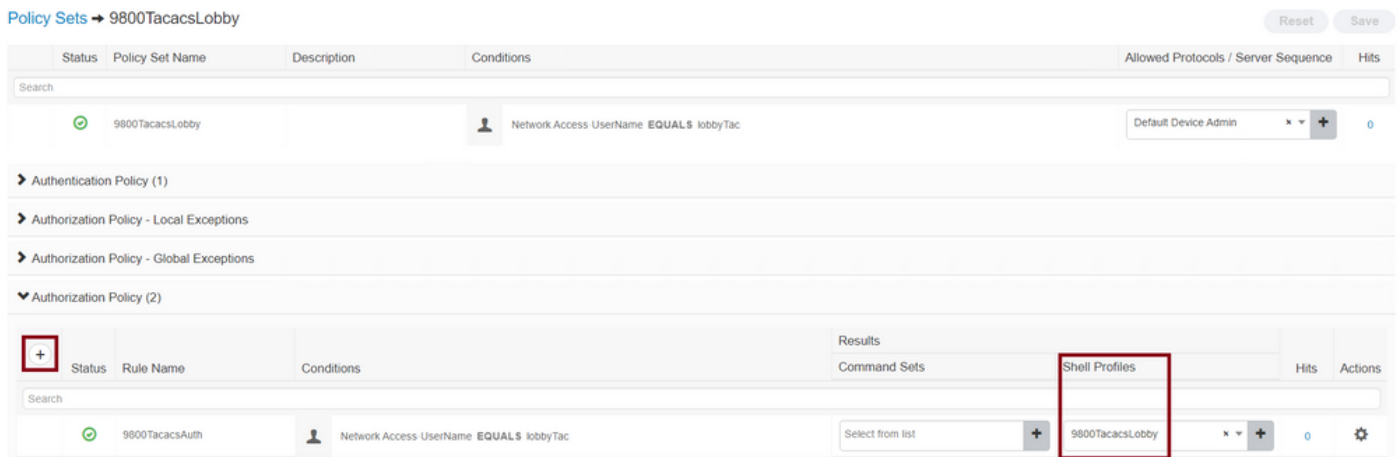
Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Device Admin Policy Sets

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
🟢	9800TacacsLobby		Network Access-UserName EQUALS lobbyTac	Default Device Admin	0		

Quando viene visualizzata la finestra di configurazione, configurare il criterio di autorizzazione. È possibile lasciare il criterio di autenticazione predefinito, come illustrato nell'immagine.

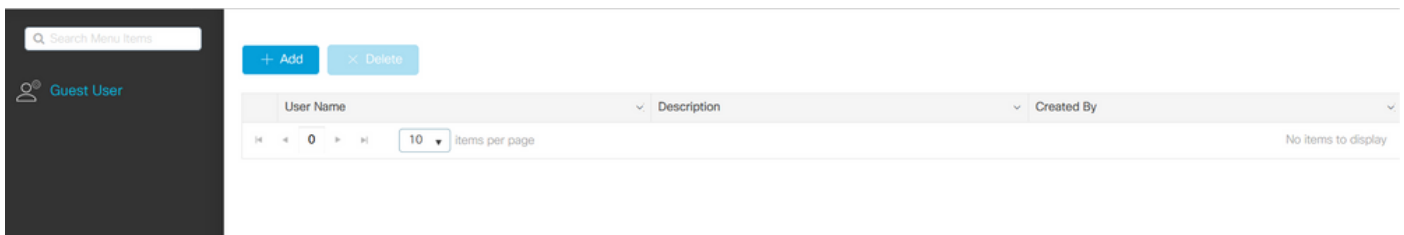


## Verifica

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

```
show run aaa
show run | sec remote
show run | sec http
show aaa method-lists authentication
show aaa method-lists authorization
show aaa servers
show tacacs
```

Ecco come appare la GUI di Lobby Ambassador dopo l'autenticazione riuscita.



## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

### Autentica RADIUS

Per l'autenticazione RADIUS, è possibile utilizzare i seguenti debug:

```
Tim-eWLc1#debug aaa authentication
Tim-eWLc1#debug aaa authorization
Tim-eWLc1#debug aaa attr
Tim-eWLc1#terminal monitor
```

Accertarsi che l'elenco dei metodi corretto sia selezionato dal comando debug. Inoltre, gli attributi richiesti vengono restituiti dal server ISE con il nome utente, il tipo di utente e il privilegio corretti.

```
Feb 5 02:35:27.659: AAA/AUTHEN/LOGIN (00000000): Pick method list 'AuthenLobbyMethod'
```

```
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(0):
7FBA5500C870 0 00000081 username(450) 5 lobby
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(1):
7FBA5500C8B0 0 00000001 user-type(1187) 4 lobby-admin
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(2):
7FBA5500C8F0 0 00000001 priv-lvl(335) 4 15(F)
Feb 5 02:35:27.683: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host
192.168.166.104 by user 'lobby' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
```

## Autenticazione TACACS+

Per l'autenticazione TACACS+, è possibile usare questo debug:

```
Tim-eWLC1#debug tacacs
Tim-eWLC1#terminal monitor
```

Verificare che l'autenticazione venga elaborata con il nome utente corretto e ISE IP ADD. Inoltre, deve essere visualizzato lo stato "PASS". Nello stesso debug, subito dopo la fase di autenticazione, viene presentato il processo di autorizzazione. In questa autorizzazione, fase assicura che venga utilizzato il nome utente corretto insieme all'ISE IP ADD corretto. Da questa fase, dovrebbe essere possibile visualizzare gli attributi configurati su ISE che dichiarano il WLC come utente Lobby Ambassador con il privilegio giusto.

Esempio di fase di autenticazione:

```
Feb 5 02:06:48.245: TPLUS: Queuing AAA Authentication request 0 for processing
Feb 5 02:06:48.245: TPLUS: Authentication start packet created for 0(lobbyTac)
Feb 5 02:06:48.245: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.250: TPLUS: Received authen response status GET_PASSWORD (8)
Feb 5 02:06:48.266: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.266: TPLUS: Received authen response status PASS (2)
```

Esempio di fase di autorizzazione:

```
Feb 5 02:06:48.267: TPLUS: Queuing AAA Authorization request 0 for processing
Feb 5 02:06:48.267: TPLUS: Authorization request created for 0(lobbyTac)
Feb 5 02:06:48.267: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.279: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.279: TPLUS: Processed AV priv-lvl=15
Feb 5 02:06:48.279: TPLUS: Processed AV user-type=lobby-admin
Feb 5 02:06:48.279: TPLUS: received authorization response for 0: PASS
```

Gli esempi di debug menzionati precedentemente per RADIUS e TACACS+ sono fondamentali per la riuscita del login. I debug sono più dettagliati e l'output sarà più grande. Per disabilitare i debug, è possibile usare questo comando:

```
Tim-eWLC1#undebug all
```