

# Configure o embaixador do Lobby WLC 9800 com autenticação RADIUS e TACACS+

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Autenticar RADIUS](#)

[Configurar o ISE - RADIUS](#)

[Autenticar TACACS+](#)

[Configurar TACACS+ em WLC](#)

[Configurar o ISE - TACACS+](#)

[Verificar](#)

[Troubleshoot](#)

[Autenticar RADIUS](#)

[Autenticar TACACS+](#)

## Introduction

Este documento descreve como configurar os Controladores de LAN Sem Fio Catalyst 9800 para autenticação externa RADIUS e TACACS+ de usuários do Lobby Embaixador, com o uso do Identity Services Engine (ISE).

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modelo de configuração do Catalyst Wireless 9800
- Conceitos de AAA, RADIUS e TACACS+

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9800 Wireless Controller Series (Catalyst 9800-CL)
- Cisco IOS®-XE Gibraltar 16.12.1s
- ISE 2.3.0

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O usuário do Lobby Embaixador é criado pelo administrador da rede. Um usuário do Lobby Embaixador é capaz de criar um nome de usuário convidado, senha, descrição e vida útil. Também tem a capacidade de excluir o usuário convidado. O usuário convidado pode ser criado via GUI ou CLI.

## Configurar

### Diagrama de Rede



Neste exemplo, os Lobby Embaixadores "lobby" e "lobbyTac" estão configurados. O "lobby" do Embaixador do Lobby deve ser autenticado contra o servidor RADIUS e o Embaixador do Lobby "lobbyTac" é autenticado contra o TACACS+.

A configuração será feita em primeiro lugar para o Embaixador do Lobby RADIUS e, finalmente, para o Embaixador do Lobby TACACS+. A configuração do RADIUS e do TACACS+ ISE também é compartilhada.

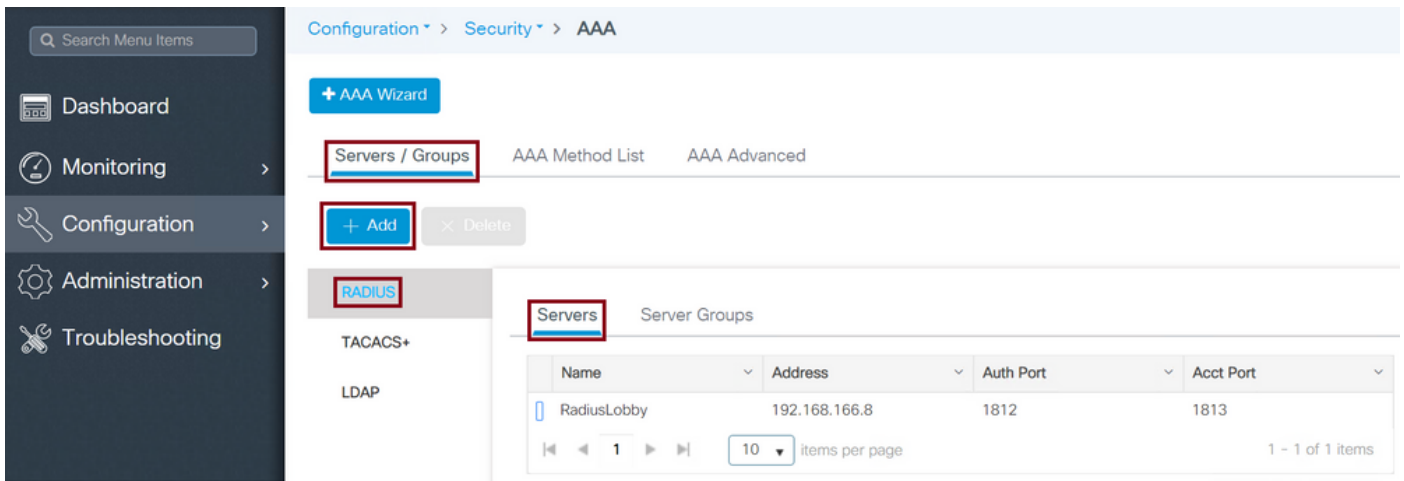
### Autenticar RADIUS

Configure o RADIUS no Wireless LAN Controller (WLC).

Etapa 1. Declarar o servidor RADIUS. Crie o ISE RADIUS Server na WLC.

GUI:

Navegue até **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add** conforme mostrado na imagem.



Quando a janela de configuração é aberta, os parâmetros de configuração obrigatórios são o nome do servidor RADIUS (não precisa corresponder ao nome do sistema ISE/AAA), o ENDEREÇO IP do servidor RADIUS e o segredo compartilhado. Qualquer outro parâmetro pode ser deixado como padrão ou pode ser configurado conforme desejado.

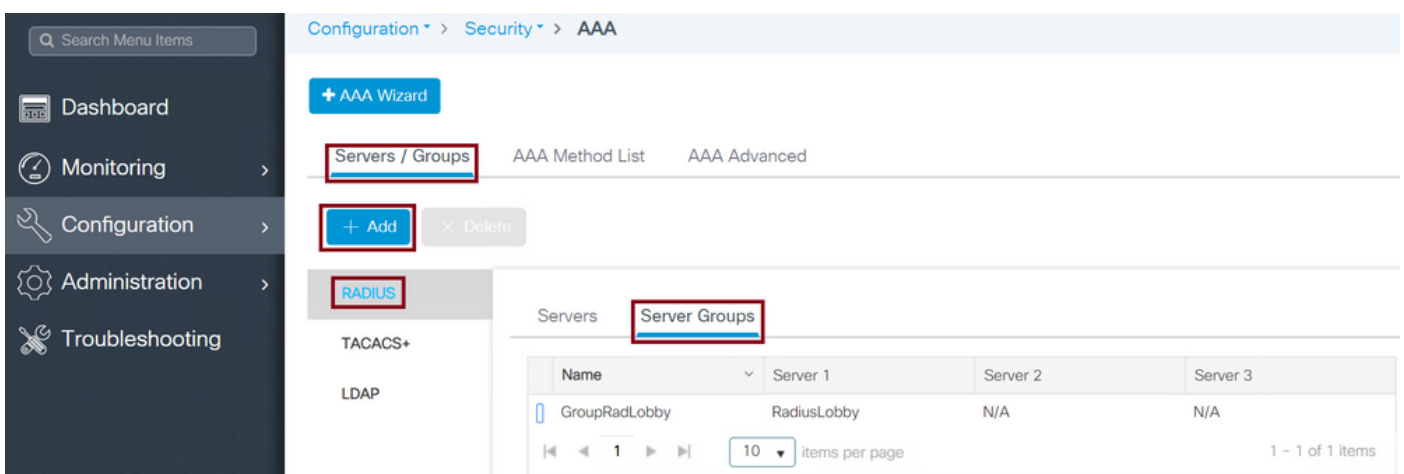
CLI:

```
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
```

Etapa 2. Adicione o servidor RADIUS a um grupo de servidores. Defina um grupo de servidores e adicione o servidor RADIUS configurado. Este será o servidor RADIUS usado para autenticação do usuário do Lobby Embaixador. Se houver vários servidores RADIUS configurados na WLC que podem ser usados para autenticação, a recomendação é adicionar todos os servidores RADIUS ao mesmo grupo de servidores. Se fizer isso, você permitirá que a WLC faça o balanceamento de carga das autenticações entre os servidores RADIUS no grupo de servidores.

GUI:

Navegue até **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** conforme mostrado na imagem.



Quando a janela de configuração abrir para dar um nome ao grupo, mova os servidores RADIUS configurados da lista Servidores disponíveis para a lista Servidores atribuídos.

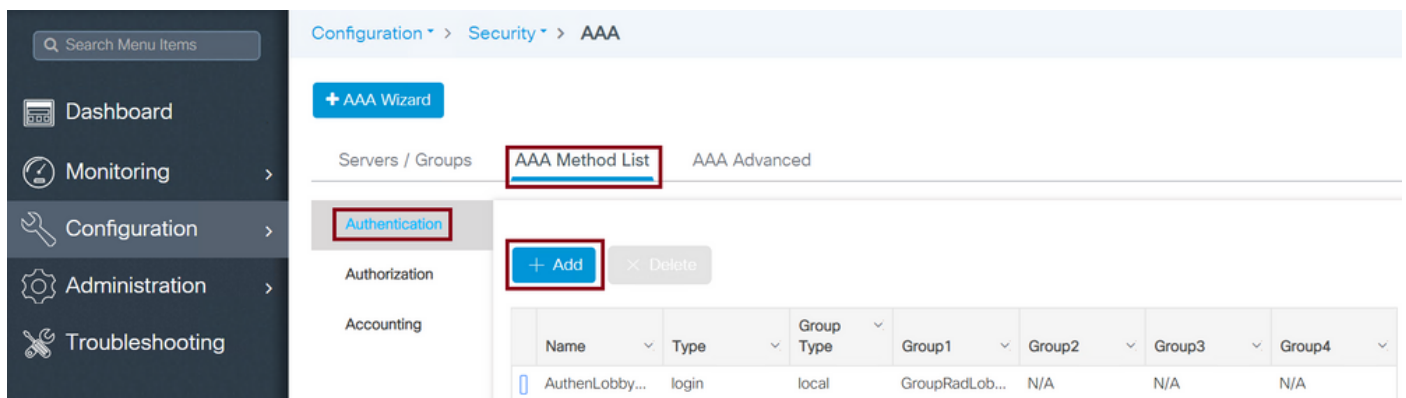
CLI:

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

Etapa 3. Criar uma lista de métodos de autenticação. A lista de métodos de autenticação define o tipo de autenticação que você procura e também anexará o mesmo ao grupo de servidores que você define. Você saberá se a autenticação será feita localmente na WLC ou em um servidor RADIUS externo.

GUI:

Navegue até **Configuration > Security > AAA > AAA Method List > Authentication > + Add** conforme mostrado na imagem.



Quando a janela de configuração abrir, forneça um nome, selecione a opção de tipo como **Login** e atribua o Grupo de servidores criado anteriormente.

Tipo de grupo como local.

GUI:

Se você selecionar Tipo de grupo como 'local', a WLC verificará primeiro se o usuário existe no banco de dados local e retornará para o Grupo de servidores somente se o usuário do Lobby Embaixador não for encontrado no banco de dados local.

CLI:

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

**Note:** Esteja ciente do bug [CSCvs87163](#) quando usar local primeiro. Isso é corrigido em 17.3.

Tipo de grupo como grupo.

GUI:

Se você selecionar Tipo de grupo como 'grupo' e não houver fallback para a opção local marcada,

a WLC irá apenas verificar o usuário em relação ao Grupo de servidores e não verificará em seu banco de dados local.

CLI:

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

Tipo de grupo como um grupo e a opção de retorno para local está marcada.

GUI:

Se você selecionar Tipo de grupo como 'grupo' e a opção de fallback para local estiver marcada, a WLC verificará o usuário em relação ao Grupo de servidores e consultará o banco de dados local somente se o servidor RADIUS expirar na resposta. Se o servidor responder, a WLC não acionará uma autenticação local.

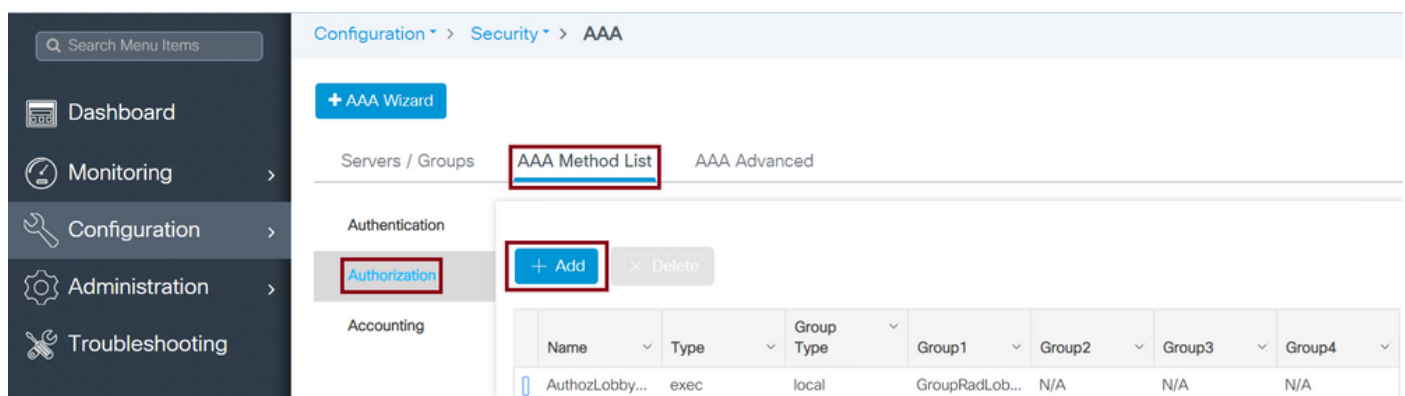
CLI:

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

Etapa 4. Criar uma lista de métodos de autorização. A lista de métodos de autorização define o tipo de autorização de que você precisa para o Embaixador do Lobby, que neste caso será 'exec'. Ele também será anexado ao mesmo grupo de servidores definido. Também permitirá selecionar se a autenticação será feita localmente na WLC ou em um servidor RADIUS externo.

GUI:

Navegue até **Configuration > Security > AAA > AAA Method List > Authorization > + Add** conforme mostrado na imagem.



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

Quando a janela de configuração abrir para fornecer um nome, selecione a opção de tipo como 'exec' e atribua o grupo de servidores criado anteriormente.

Lembre-se de que o Tipo de grupo se aplica da mesma maneira que foi explicado na seção Lista de métodos de autenticação.

CLI:

Tipo de grupo como local.

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

Tipo de grupo como grupo.

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

Tipo de grupo como grupo e a opção de retorno para local está marcada.

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

**Etapa 5. Atribua os métodos.** Quando os métodos são configurados, eles precisam ser atribuídos às opções para fazer login na WLC para criar o usuário convidado, como linha VTY (SSH/Telnet) ou HTTP (GUI).

Essas etapas não podem ser feitas na GUI, portanto, precisam ser feitas na CLI.

**Autenticação 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 você executa alterações nas configurações HTTP, é melhor reiniciar os serviços 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
```

**Linha 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
```

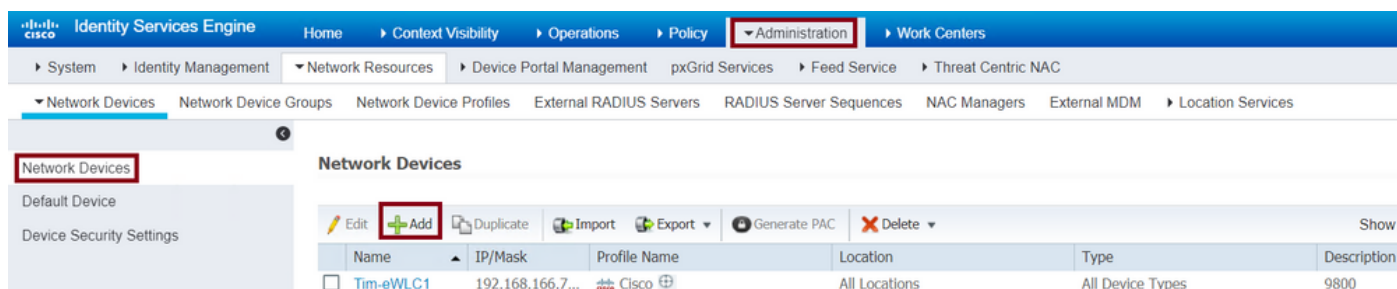
**Etapa 6.** Esta etapa é necessária somente em versões de software anteriores a 17.5.1 ou 17.3.3 e não é necessária após as versões em que [CSCvu29748](#) foi implementado. Defina o usuário remoto. O nome de usuário criado no ISE para o Embaixador do Lobby deve ser definido como um nome de usuário remoto na WLC. Se o nome de usuário remoto não estiver definido na WLC, a autenticação passará corretamente, no entanto, o usuário receberá acesso total à WLC em vez de apenas acesso aos privilégios do Embaixador de Lobby. Essa configuração pode ser feita somente via CLI.

**CLI:**

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

**Configurar o ISE - RADIUS**

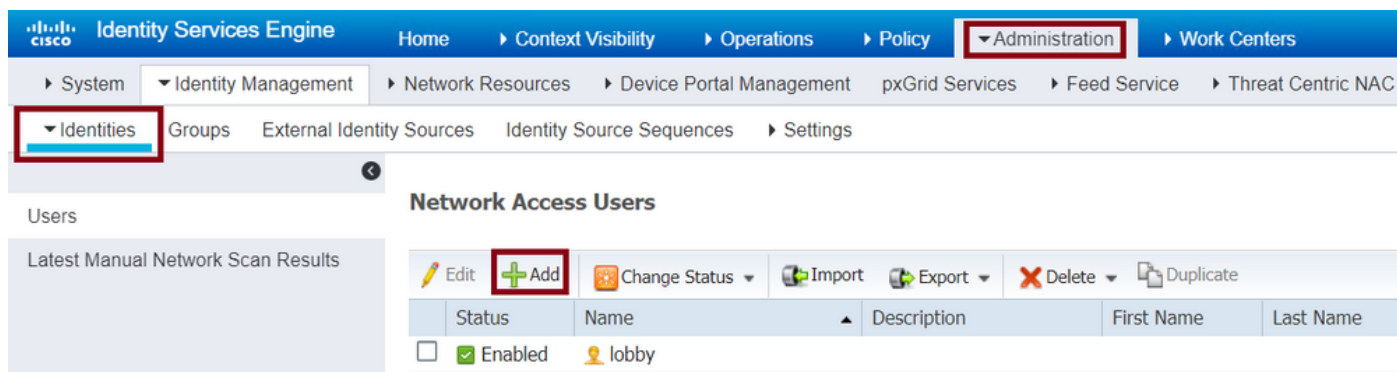
Etapa 1. Adicione a WLC ao ISE. Navegue até **Administration > Network Resources > Network Devices > Add**. A WLC precisa ser adicionada ao ISE. Quando você adicionar a WLC ao ISE, ative as Configurações de autenticação RADIUS e configure os parâmetros necessários conforme mostrado na imagem.



Quando a janela de configuração abrir, forneça um nome, ADD IP, ative Configurações de autenticação RADIUS e, em Raio de protocolo, insira o segredo compartilhado necessário.

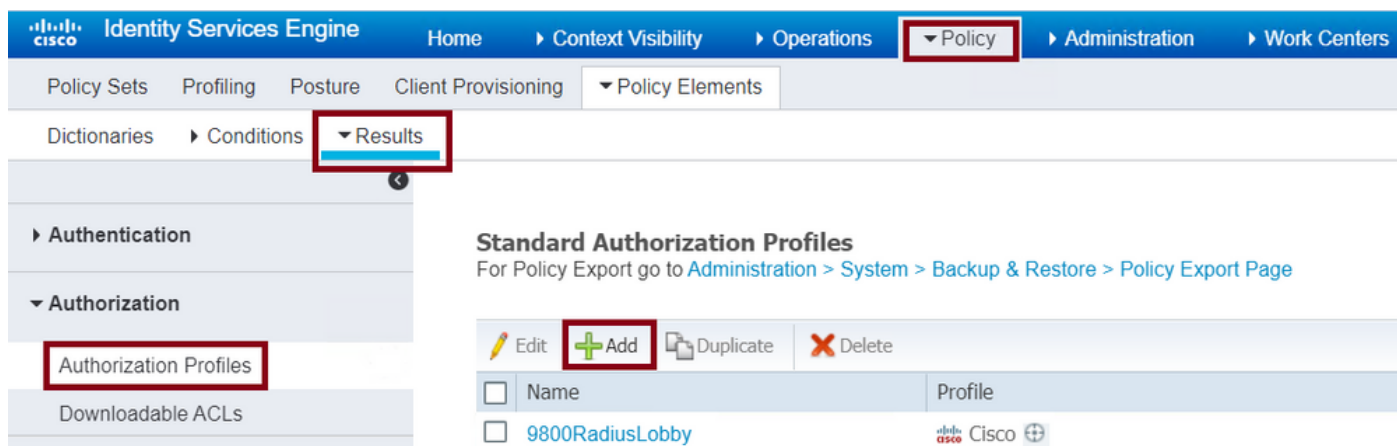
Etapa 2. Crie o usuário do Lobby Embaixador no ISE. Navegue até **Administração > Gerenciamento de identidades > Identidades > Usuários > Adicionar**.

Adicione ao ISE o nome de usuário e a senha atribuídos ao Embaixador do Lobby que cria os usuários convidados. Este é o nome de usuário que o Administrador atribuirá ao Embaixador do Lobby.



Quando a janela de configuração abrir, forneça o nome e a senha do usuário do Lobby Embaixador. Além disso, certifique-se de que o Status esteja Habilitado.

Etapa 3. Crie um perfil de autorização de resultados. Navegue até **Política > Elementos de política > Resultados > Autorização > Perfis de autorização > Adicionar**. Crie um perfil de autorização de resultado para retornar à WLC e Access-Accept com os atributos necessários, como mostrado na imagem.





Certifique-se de que o perfil esteja configurado para enviar um Access-Accept como mostrado na imagem.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. The 'Policy' menu is expanded, showing 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. Under 'Policy Elements', 'Results' is selected. The left sidebar shows a navigation tree with 'Authentication' and 'Authorization' expanded. The main content area displays the configuration for 'Authorization Profiles > 9800RadiusLobby'. The 'Authorization Profile' section has the following fields: '\* Name' (9800RadiusLobby), 'Description' (empty), and '\* Access Type' (ACCESS\_ACCEPT). The '\* Access Type' field is highlighted with a red box.

Você precisará adicionar os atributos manualmente em Advanced Attributes Settings (Configurações avançadas de atributos). Os atributos são necessários para definir o utilizador como Embaixador de Lobby e para dar o privilégio de permitir que o Embaixador de Lobby faça as alterações necessárias.

#### Advanced Attributes Settings

The screenshot shows the 'Advanced Attributes Settings' section. It contains two attribute entries, each highlighted with a red box. The first entry is 'Cisco:cisco-av-pair = user-type=lobby-admin'. The second entry is 'Cisco:cisco-av-pair = shell:priv-lvl=15'. Each entry has a dropdown arrow on the left and a plus sign on the right.

#### Attributes Details

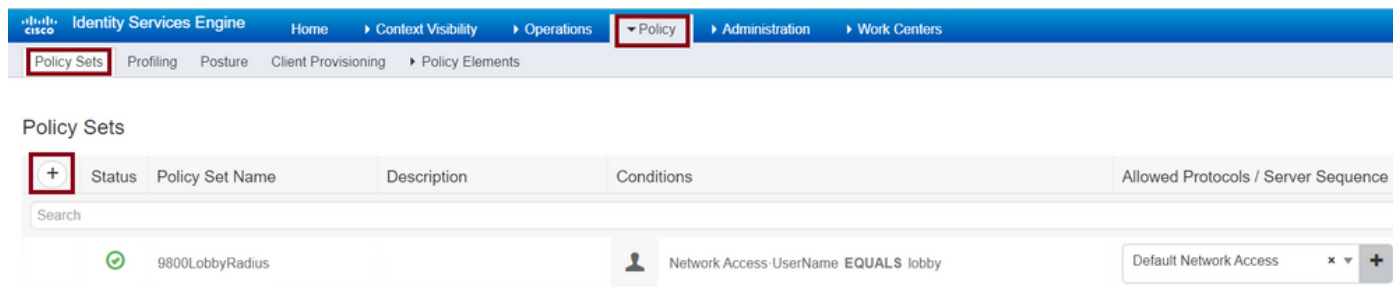
```
Access Type = ACCESS_ACCEPT
cisco-av-pair = user-type=lobby-admin
cisco-av-pair = shell:priv-lvl=15
```

Etapa 4. Crie uma política para processar a autenticação. Navegue até **Política > Conjuntos de políticas > Adicionar**. As condições para configurar a política dependem da decisão do administrador. A condição Network Access-Username e o protocolo Default Network Access são usados aqui.

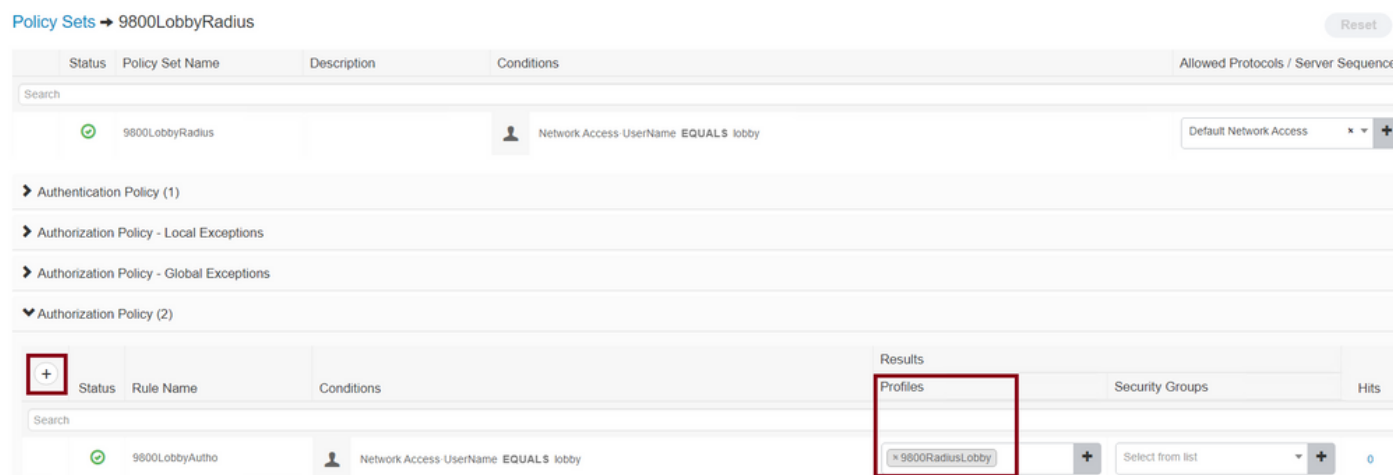
É obrigatório garantir que, na Política de autorização, o perfil configurado na Autorização de



resultados esteja selecionado, dessa forma você pode retornar os atributos necessários para a WLC, como mostrado na imagem.



Quando a janela de configuração abrir, configure a Política de autorização. A política de autenticação pode ser deixada como padrão.



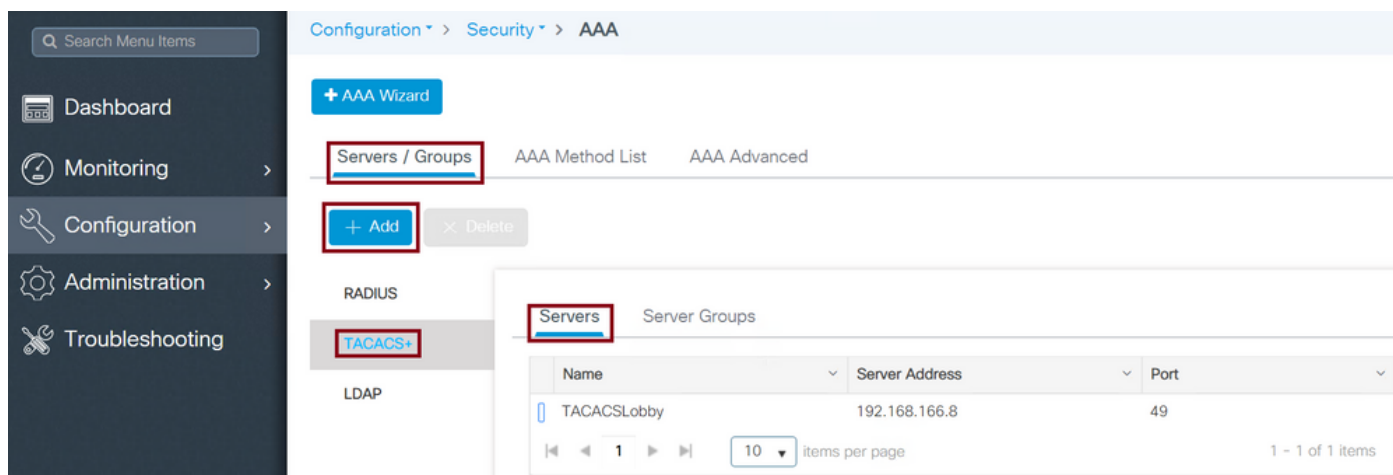
## Autenticar TACACS+

### Configurar TACACS+ em WLC

Etapa 1. Declarar o servidor TACACS+. Crie o servidor TACACS ISE na WLC.

GUI:

Navegue até **Configuration > Security > AAA > Servers/Groups > TACACS+ > Servers > + Add** conforme mostrado na imagem.



Quando a janela de configuração é aberta, os parâmetros de configuração obrigatórios são o

nome do Servidor TACACS+ (não precisa corresponder ao nome do sistema ISE/AAA), o ENDEREÇO IP do Servidor TACACS e o Segredo Compartilhado. Qualquer outro parâmetro pode ser deixado como padrão ou pode ser configurado conforme necessário.

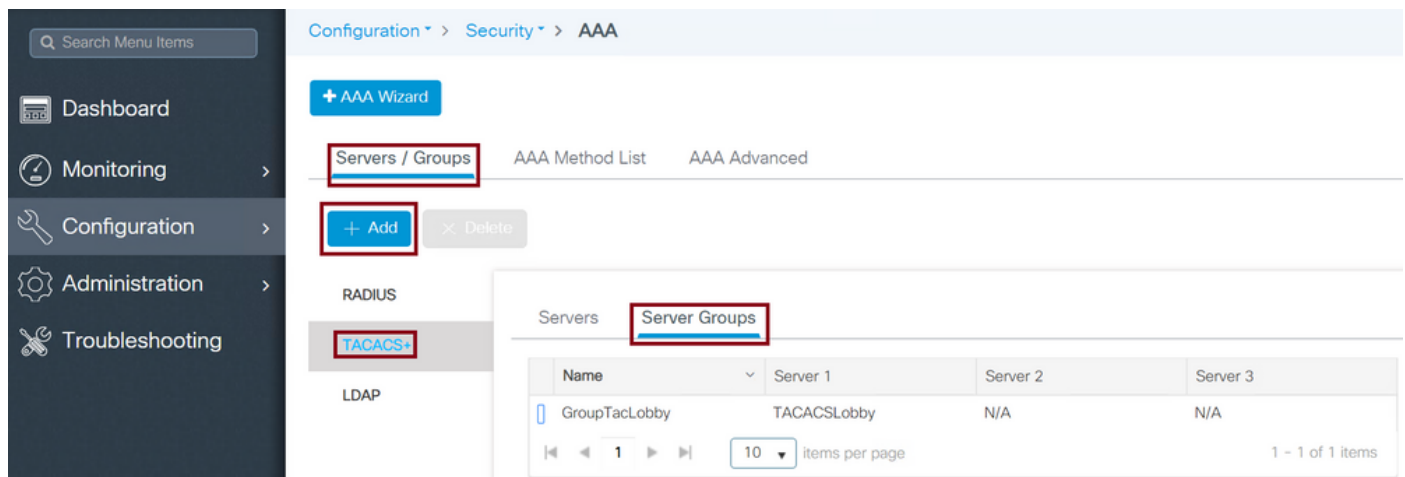
CLI:

```
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
```

Etapa 2. Adicione o servidor TACACS+ a um grupo de servidores. Defina um grupo de servidores e adicione o servidor TACACS+ desejado configurado. Esses serão os servidores TACACS+ usados para autenticação.

GUI:

Navegue até **Configuration > Security > AAA > Servers / Groups > TACACS > Server Groups > + Add** conforme mostrado na imagem.



Quando a janela de configuração abrir, atribua um nome ao grupo e mova os servidores TACACS+ desejados da lista Servidores disponíveis para a lista Servidores atribuídos.

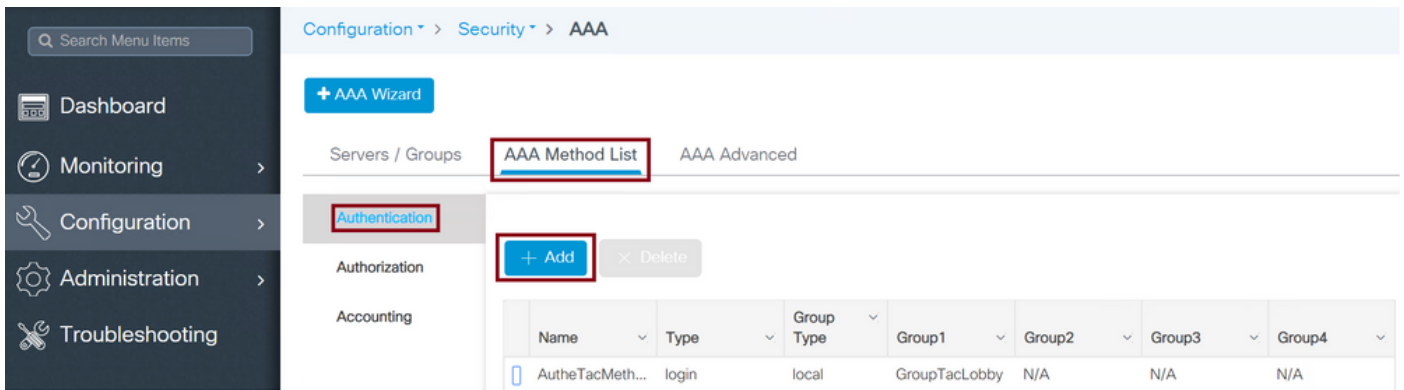
CLI:

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

Etapa 3. Criar uma lista de métodos de autenticação. A lista de métodos de autenticação define o tipo de autenticação necessária e também anexará o mesmo ao grupo de servidores configurado. Também permite selecionar se a autenticação pode ser feita localmente na WLC ou em um servidor TACACS+ externo.

GUI:

Navegue até **Configuration > Security > AAA > AAA Method List > Authentication > + Add** conforme mostrado na imagem.



Quando a janela de configuração abrir, forneça um nome, selecione a opção de tipo como **Login** e atribua o Grupo de servidores criado anteriormente.

Tipo de grupo como local.

GUI:

Se você selecionar Tipo de grupo como 'local', a WLC verificará primeiro se o usuário existe no banco de dados local e retornará para o Grupo de servidores somente se o usuário do Lobby Embaixador não for encontrado no banco de dados local.

**Note:** Esteja ciente deste bug [CSCvs87163](#) que é fixada em 17.3.

CLI:

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

Tipo de grupo como grupo.

GUI:

Se você selecionar Tipo de grupo como grupo e não houver fallback para a opção local marcada, a WLC irá apenas verificar o usuário em relação ao Grupo de servidores e não verificará em seu banco de dados local.

CLI:

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

Tipo de grupo como grupo e a opção de retorno para local está marcada.

GUI:

Se você selecionar o tipo de grupo como 'grupo' e a opção Fallback to local estiver marcada, a WLC verificará o usuário em relação ao grupo de servidores e consultará o banco de dados local somente se o servidor TACACS expirar na resposta. Se o servidor enviar uma rejeição, o usuário não será autenticado, mesmo que exista no banco de dados local.

CLI:

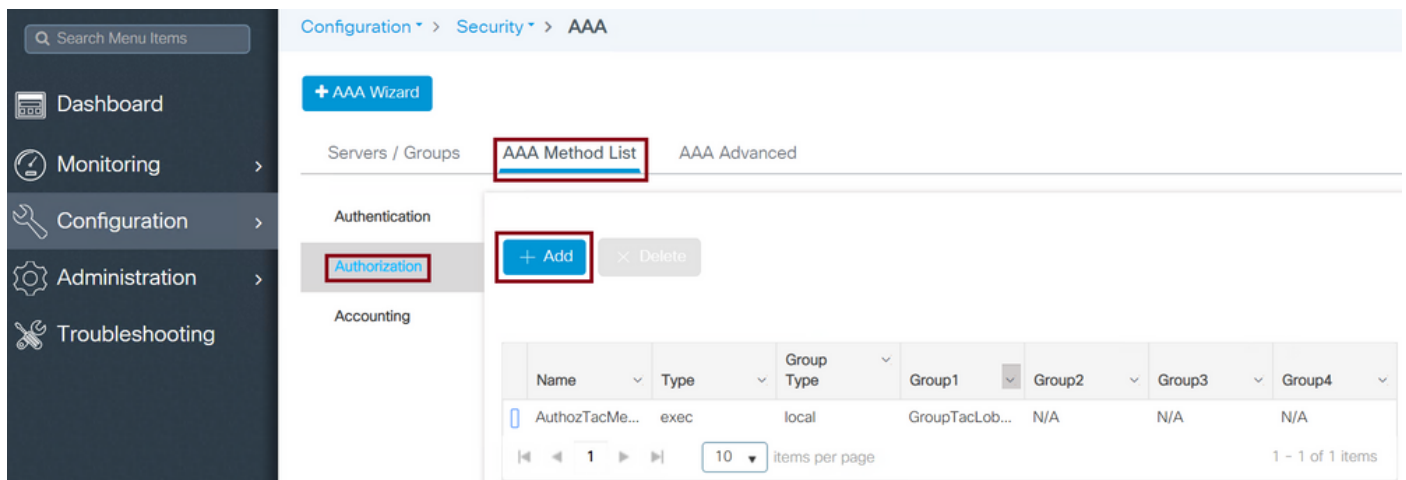
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Etapa 4. Criar uma lista de métodos de autorização.

A lista de métodos de autorização definirá o tipo de autorização necessário para o Embaixador do Lobby, que, neste caso, será executivo. Ele também está conectado ao mesmo grupo de servidores configurado. Também é permitido selecionar se a autenticação é feita localmente na WLC ou em um servidor TACACS+ externo.

GUI:

Navegue até **Configuration > Security > AAA > AAA Method List > Authorization > + Add** conforme mostrado na imagem.



Quando a janela de configuração abrir, forneça um nome, selecione a opção de tipo como exec e atribua o grupo de servidores criado anteriormente.

Lembre-se de que o Tipo de grupo se aplica da mesma forma que é explicado na parte Lista de métodos de autenticação.

CLI:

Tipo de grupo como local.

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

Tipo de grupo como grupo.

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

O tipo de grupo como grupo e a opção Fallback to local estão marcados.

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

Etapa 5. Atribua os métodos. Quando os métodos são configurados, eles precisam ser atribuídos às opções para fazer login na WLC para criar o usuário convidado, como linha VTY ou HTTP (GUI). Essas etapas não podem ser feitas na GUI, portanto, precisam ser feitas na CLI.

## Autenticação 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 você faz alterações nas configurações HTTP, é melhor reiniciar os serviços 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
```

## Linha VTY:

```
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
```

Etapa 6. Defina o usuário remoto. O nome de usuário criado no ISE para o Embaixador do Lobby deve ser definido como um nome de usuário remoto na WLC. Se o nome de usuário remoto não estiver definido na WLC, a autenticação passará corretamente, no entanto, o usuário receberá acesso total à WLC em vez de apenas acesso aos privilégios do Embaixador de Lobby. Essa configuração pode ser feita somente via CLI.

## CLI:

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

## Configurar o ISE - TACACS+

Etapa 1. Habilitar administrador de dispositivos. Navegue até **Administração > Sistema > Implantação**. Antes de prosseguir, selecione **Habilitar serviço de administração de dispositivo** e verifique se o ISE foi habilitado conforme mostrado na imagem.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > Deployment > Deployment Nodes List > timise23. The 'Edit Node' page is displayed, with the 'General Settings' tab selected. The configuration details are as follows:

- Hostname: timise23
- FQDN: timise23.cisco.com
- IP Address: 192.168.166.8
- Node Type: Identity Services Engine (ISE)
- Role: STANDALONE (with a 'Make Primary' button)
- Administration:
- Monitoring: 
  - Role: PRIMARY
  - Other Monitoring Node: [Empty field]
- 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:  (highlighted with a red box)

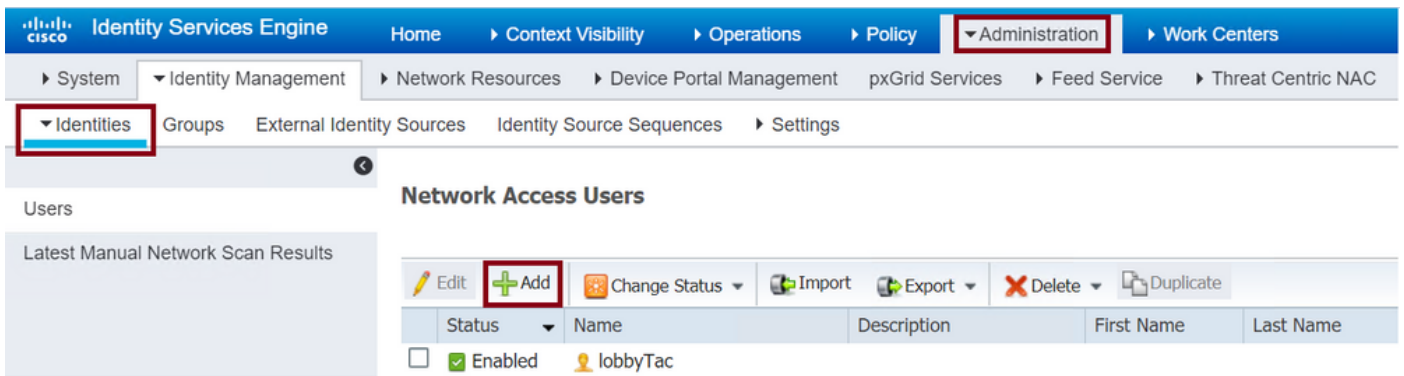
Etapa 2. Adicione a WLC ao ISE. Navegue até **Administration > Network Resources > Network Devices > Add**. A WLC precisa ser adicionada ao ISE. Quando você adicionar a WLC ao ISE, ative as Configurações de autenticação TACACS+ e configure os parâmetros necessários como mostrado na imagem.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > Network Resources > Network Devices. The 'Network Devices' page is displayed, showing a table of network devices. The 'Add' button is highlighted with a red box.

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> Tim-eWLC1	192.168.166.7...	Cisco	All Locations	All Device Types	9800

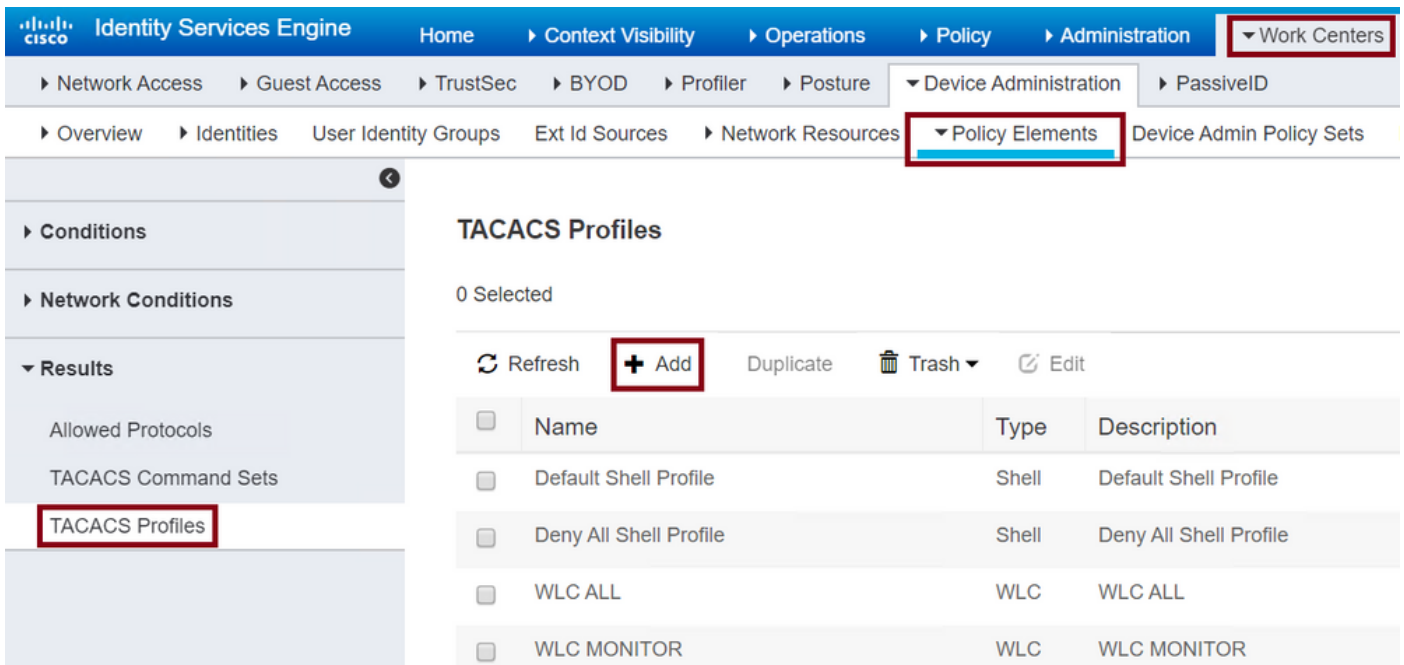
Quando a janela de configuração se abrir para fornecer um nome, ADD IP, ativar as Configurações de autenticação TACACS+ e inserir o segredo compartilhado necessário.

Etapa 3. Crie o usuário do Lobby Embaixador no ISE. Navegue até **Administração > Gerenciamento de identidades > Identidades > Usuários > Adicionar**. Adicione ao ISE o nome de usuário e a senha atribuídos ao Embaixador do Lobby que criará os usuários convidados. Este é o nome de usuário que o Administrador atribui ao Embaixador do Lobby, como mostrado na imagem.



Quando a janela de configuração abrir, forneça o nome e a senha do usuário do Lobby Embaixador. Além disso, certifique-se de que o Status esteja Habilitado.

Etapa 4. Crie um perfil TACACS+ de resultados. Navegue até **Centros de trabalho > Administração de dispositivos > Elementos de política > Resultados > Perfis TACACS** como mostrado na imagem. Com esse perfil, retorne os atributos necessários à WLC para colocar o usuário como Embaixador de Lobby.



Quando a janela de configuração for aberta, forneça um nome para o perfil, configure também um Padrão Privilegiado 15 e um Atributo Personalizado como Tipo Obrigatório, nomeie como usuário-type e value lobby-admin. Além disso, deixe o **Tipo de Tarefa Comum** ser selecionado como Shell, como mostrado na imagem.



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)

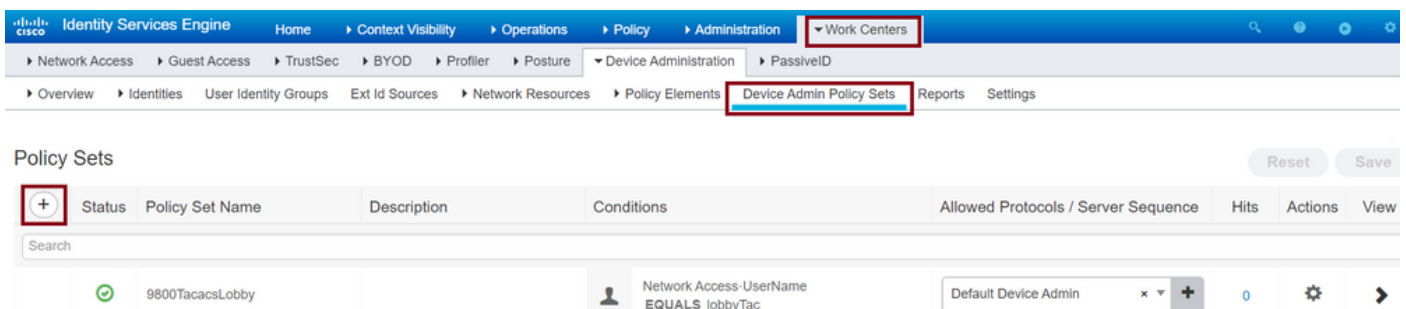
### Custom Attributes

1 Selected

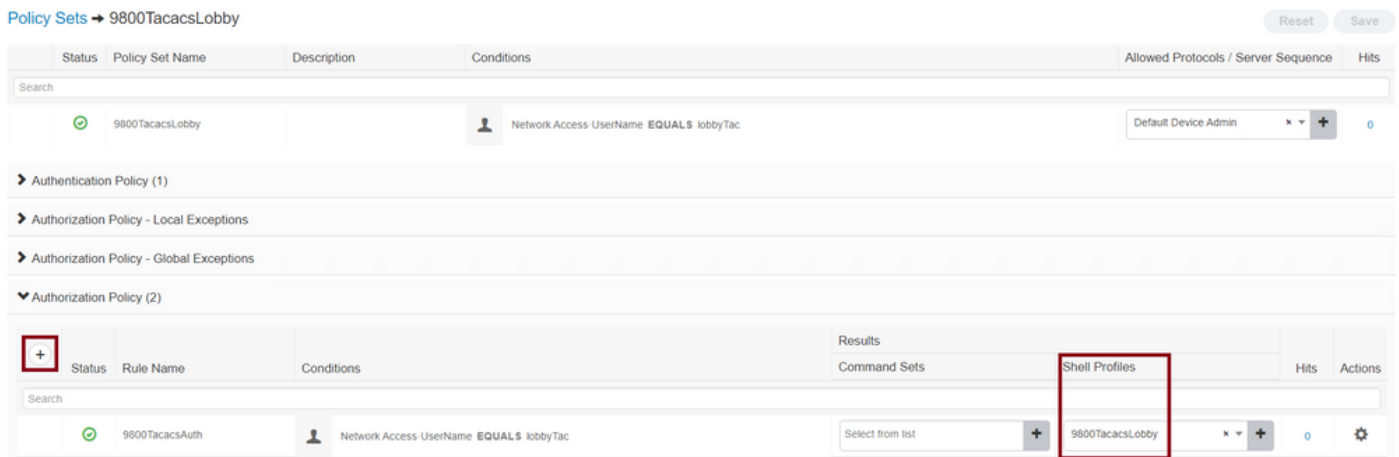
+ Add    🗑️ Trash    ✎ Edit

<input checked="" type="checkbox"/>	Type	Name	Value
<input checked="" type="checkbox"/>	MANDATORY	user-type	lobby-admin

Etapa 5. Criar um Conjunto de Políticas. Navegue até **Centros de trabalho > Administração do dispositivo > Conjuntos de políticas do administrador do dispositivo** conforme mostrado na imagem. As condições para configurar a política dependem da decisão do administrador. Para este documento, a condição Network Access-Username e o protocolo Default Device Admin são usados. É obrigatório garantir, de acordo com a Política de autorização, que o perfil configurado sob a Autorização de resultados esteja selecionado, dessa forma, você poderá devolver os atributos necessários à WLC.



Quando a janela de configuração abrir, configure a Diretiva de autorização. A política de autenticação pode ser deixada como padrão, como mostrado na imagem.

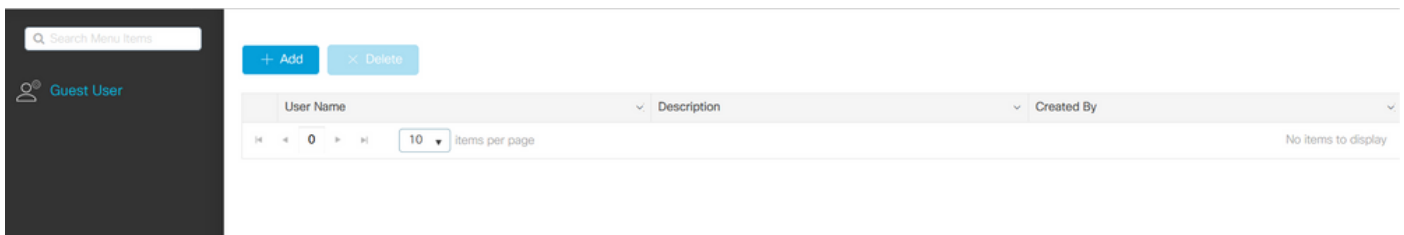


## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

```
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
```

Esta é a aparência da GUI do Embaixador de Lobby após uma autenticação bem-sucedida.



## Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

## Autenticar RADIUS

Para autenticação RADIUS, essas depurações podem ser usadas:

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

Verifique se a lista de métodos correta está selecionada na depuração. Além disso, os atributos necessários são retornados pelo ISE Server com o nome de usuário, o tipo de usuário e o privilégio corretos.

```
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: %WEBSEVER-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'
```

## Autenticar TACACS+

Para autenticação TACACS+, essa depuração pode ser usada:

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

Assegure-se de que a autenticação seja processada com o nome de usuário correto e o ADD IP do ISE. Além disso, o status "PASS" deve ser visto. Na mesma depuração, logo após a fase de autenticação, o processo de autorização será apresentado. Nessa autorização, a fase garante que o nome de usuário correto seja usado junto com o ADD IP do ISE correto. Nessa fase, você deve ser capaz de ver os atributos configurados no ISE que indicam a WLC como um usuário embaixador de lobby com o privilégio certo.

Exemplo de fase de autenticação:

```
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)
```

Exemplo de fase de autorização:

```
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
```

Os exemplos de depuração mencionados anteriormente para RADIUS e TACACS+ têm as principais etapas para um login bem-sucedido. As depurações são mais detalhadas e a saída será maior. Para desativar as depurações, este comando pode ser usado:

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