

# Configure 9800 WLC Lobby Ambassador con RADIUS y autenticación TACACS+

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Autenticar RADIUS](#)

[Configuración de ISE - RADIUS](#)

[Autenticar TACACS+](#)

[Configuración de TACACS+ en WLC](#)

[Configuración de ISE - TACACS+](#)

[Verificación](#)

[Troubleshoot](#)

[Autenticar RADIUS](#)

[Autenticar TACACS+](#)

## Introducción

Este documento describe cómo configurar los controladores de LAN inalámbrica Catalyst 9800 para la autenticación externa RADIUS y TACACS+ de los usuarios embajadores de vestíbulo, con el uso de Identity Services Engine (ISE).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modelo de configuración de Catalyst Wireless 9800
- Conceptos de AAA, RADIUS y TACACS+

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Serie de controladores inalámbricos Catalyst 9800 (Catalyst 9800-CL)
- Cisco IOS®-XE Gibraltar 16.12.1s

- ISE 2.3.0

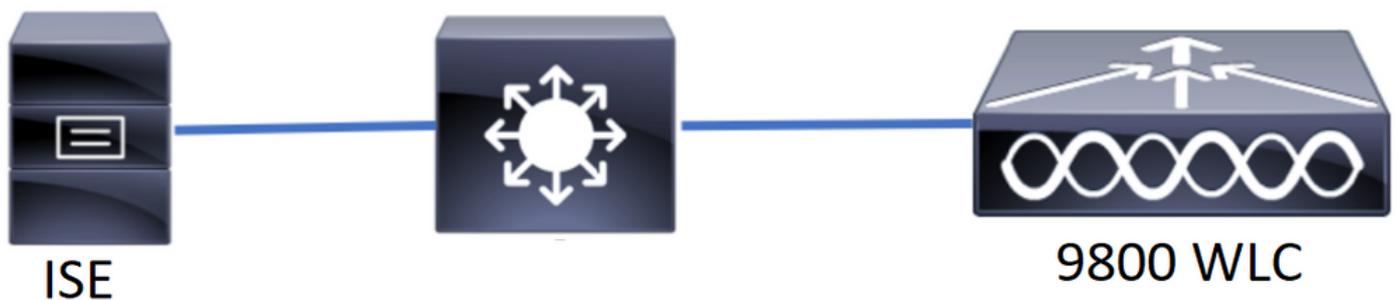
La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

El usuario Embajador del vestíbulo es creado por el administrador de la red. Un usuario Embajador del vestíbulo es capaz de crear el nombre de usuario, la contraseña, la descripción y la duración de un usuario invitado. También puede eliminar el usuario invitado. El usuario invitado se puede crear a través de GUI o CLI.

## Configurar

### Diagrama de la red



En este ejemplo, se configuran los Embajadores del vestíbulo "vestíbulo" y "vestíbuloTac". El "vestíbulo" del Embajador del vestíbulo debe autenticarse contra el servidor RADIUS y el Embajador del vestíbulo "vestíbuloTac" se autentica contra TACACS+.

La configuración se realizará primero para el embajador del vestíbulo RADIUS y finalmente para el embajador del vestíbulo TACACS+. También se comparten la configuración RADIUS y TACACS+ ISE.

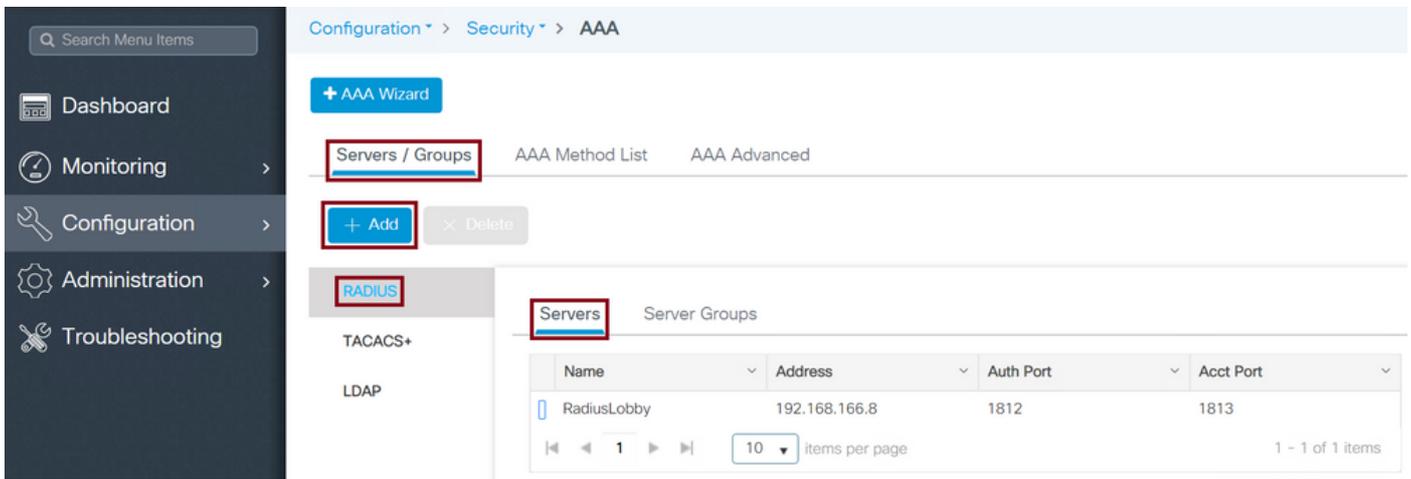
### Autenticar RADIUS

Configure RADIUS en Wireless LAN Controller (WLC).

Paso 1. Declare el servidor RADIUS. Cree el servidor RADIUS ISE en el WLC.

GUI:

Vaya a **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add** como se muestra en la imagen.



Cuando se abre la ventana de configuración, los parámetros de configuración obligatorios son el nombre del servidor RADIUS (no tiene que coincidir con el nombre del sistema ISE/AAA), la dirección IP del servidor RADIUS y el secreto compartido. Cualquier otro parámetro se puede dejar predeterminado o se puede configurar como se desee.

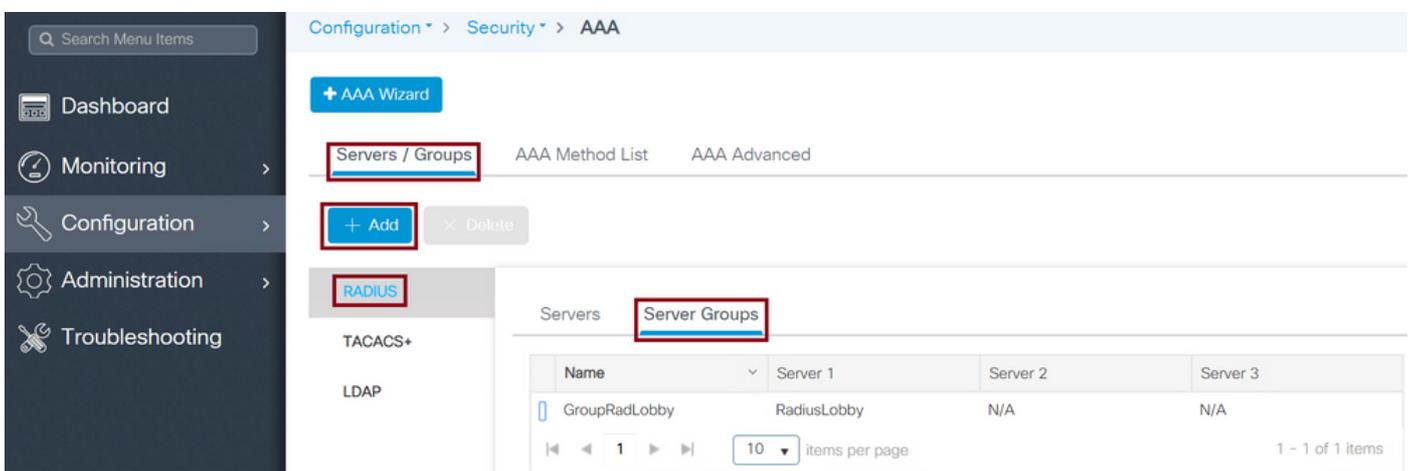
CLI:

```
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
```

Paso 2. Agregue el servidor RADIUS a un grupo de servidores. Defina un grupo de servidores y agregue el servidor RADIUS configurado. Este será el servidor RADIUS utilizado para la autenticación del usuario Embajador del vestíbulo. Si hay varios servidores RADIUS configurados en el WLC que se pueden utilizar para la autenticación, la recomendación es agregar todos los servidores Radius al mismo grupo de servidores. Si lo hace, deja que el WLC balancee las autenticaciones entre los servidores RADIUS en el grupo de servidores.

GUI:

Vaya a **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** como se muestra en la imagen.



Cuando se abra la ventana de configuración para dar un nombre al grupo, mueva los servidores RADIUS configurados de la lista Servidores disponibles a la lista Servidores asignados.

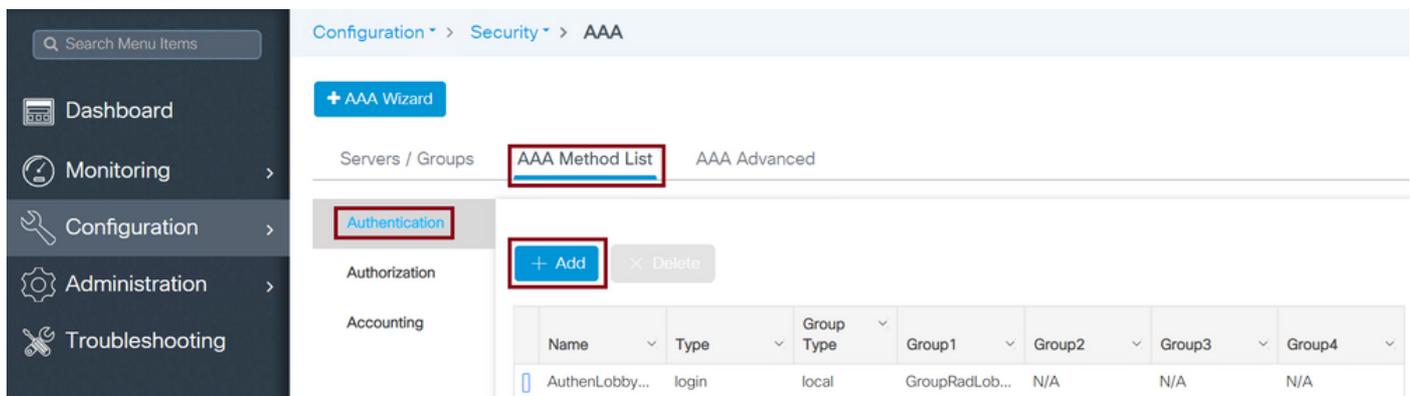
CLI:

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

Paso 3. Cree una lista de métodos de autenticación. La lista de métodos de autenticación define el tipo de autenticación que busca y también asociará el mismo tipo al grupo de servidores que define. Usted sabrá si la autenticación se hará localmente en el WLC o externa a un servidor RADIUS.

GUI:

Vaya a **Configuration > Security > AAA > AAA Method List > Authentication > + Add** como se muestra en la imagen.



Cuando se abra la ventana de configuración, proporcione un nombre, seleccione la opción de tipo como **Login** y asigne el grupo de servidores creado anteriormente.

Tipo de grupo como local.

GUI:

Si selecciona Tipo de grupo como 'local', el WLC primero verificará si el usuario existe en la base de datos local y luego se devolverá al Grupo de servidores solamente si el usuario Embajador de vestíbulo no se encuentra en la base de datos local.

CLI:

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

**Nota:** Tenga en cuenta el error [CSCvs87163](#) cuando utilice primero local. Esto se fija en 17.3.

Tipo de grupo como grupo.

GUI:

Si selecciona Tipo de grupo como 'grupo' y no hay reserva para la opción local marcada, el WLC

solamente verificará al usuario con el Grupo de servidores y no protegerá su base de datos local.

CLI:

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

Group Type (Tipo de grupo) como grupo y la opción de reserva a local está activada.

GUI:

Si selecciona Tipo de grupo como 'grupo' y se marca la opción de reserva a local, el WLC verificará al usuario con el Grupo de servidores y consultará la base de datos local solamente si el servidor RADIUS agota el tiempo de espera en la respuesta. Si el servidor responde, el WLC no activará una autenticación local.

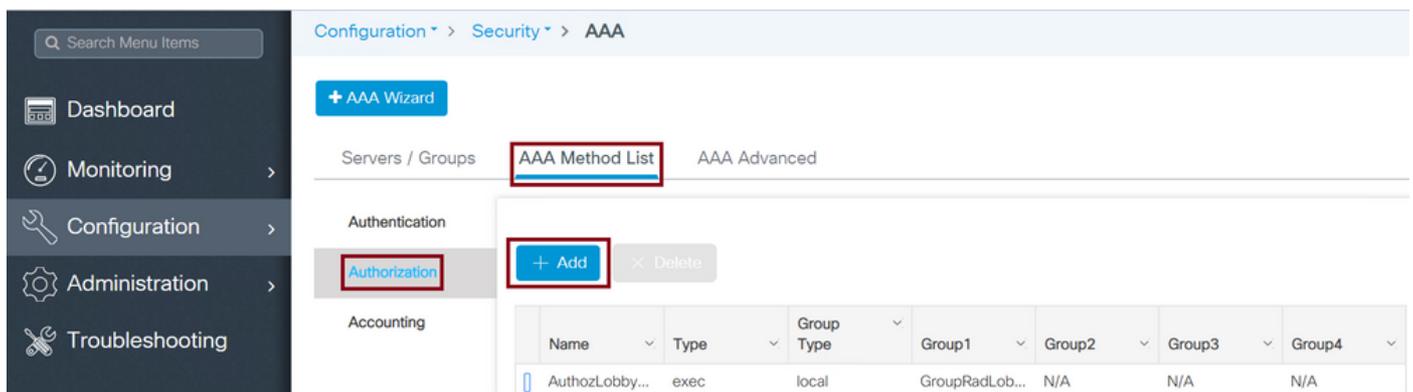
CLI:

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

Paso 4. Cree una lista de métodos de autorización. La lista de métodos de autorización define el tipo de autorización que necesita para el Embajador del vestíbulo, que en este caso será 'exec'. También se adjuntará al mismo grupo de servidores que se haya definido. También permitirá seleccionar si la autenticación se realizará localmente en el WLC o externa a un servidor RADIUS.

GUI:

Vaya a **Configuration > Security > AAA > AAA Method List > Authorization > + Add** como se muestra en la imagen.



The screenshot shows the Cisco WLC GUI configuration page for AAA Method List > Authorization. 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 the 'AuthozLobby...' method.

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

Cuando se abra la ventana de configuración para proporcionar un nombre, seleccione la opción de tipo como 'exec' y asigne el grupo de servidores creado anteriormente.

Tenga en cuenta que el tipo de grupo se aplica de la misma manera en que se explicó en la sección Lista de métodos de autenticación.

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
```

Group Type as group (Tipo de grupo) y la opción fallback to local (Volver a local) está activada.

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

**Paso 5. Asigne los métodos.** Una vez configurados los métodos, deben ser asignados a las opciones para iniciar sesión en el WLC para crear el usuario invitado como la línea VTY (SSH/Telnet) o HTTP (GUI).

Estos pasos no se pueden realizar desde la GUI, por lo que deben realizarse desde la CLI.

**Autenticación 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 realice cambios en las configuraciones HTTP, es mejor reiniciar los servicios HTTP y 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 (Línea 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
```

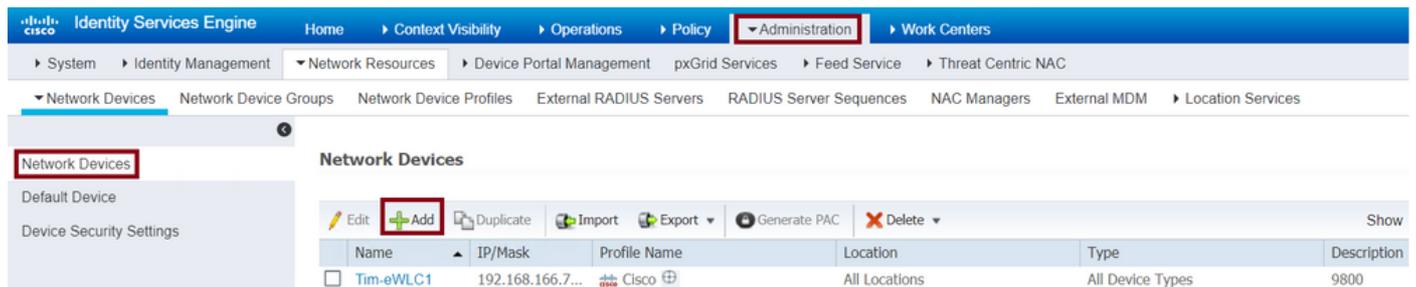
**Paso 6.** Este paso sólo se requiere en las versiones de software anteriores a 17.5.1 o 17.3.3 y no después de aquellas versiones donde [CSCvu29748](#) se implementó. Defina el usuario remoto. El nombre de usuario creado en ISE para el Embajador del vestíbulo debe definirse como un nombre de usuario remoto en el WLC. Si el nombre de usuario remoto no está definido en el WLC, la autenticación pasará correctamente, sin embargo, el usuario será otorgado con acceso completo al WLC en lugar de solamente acceso a los privilegios de Embajador del lobby. Esta configuración sólo se puede realizar a través de CLI.

CLI:

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

**Configuración de ISE - RADIUS**

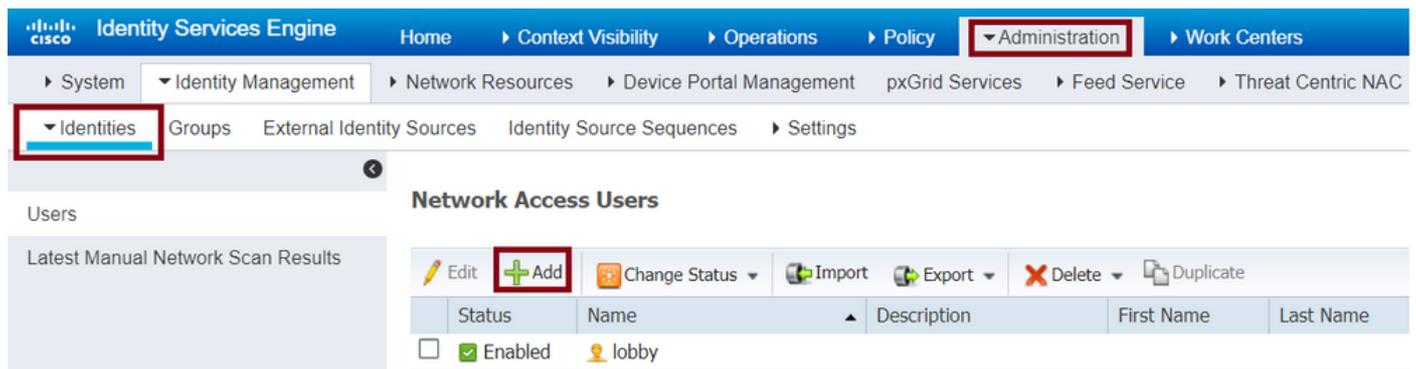
Paso 1. Agregue el WLC a ISE. Vaya a **Administration > Network Resources > Network Devices > Add**. El WLC debe agregarse a ISE. Cuando agrega el WLC a ISE, habilite RADIUS Authentication Settings y configure los parámetros necesarios como se muestra en la imagen.



Cuando se abra la ventana de configuración, proporcione un nombre, IP ADD, active RADIUS Authentication Settings y, en Protocol Radius, introduzca el secreto compartido necesario.

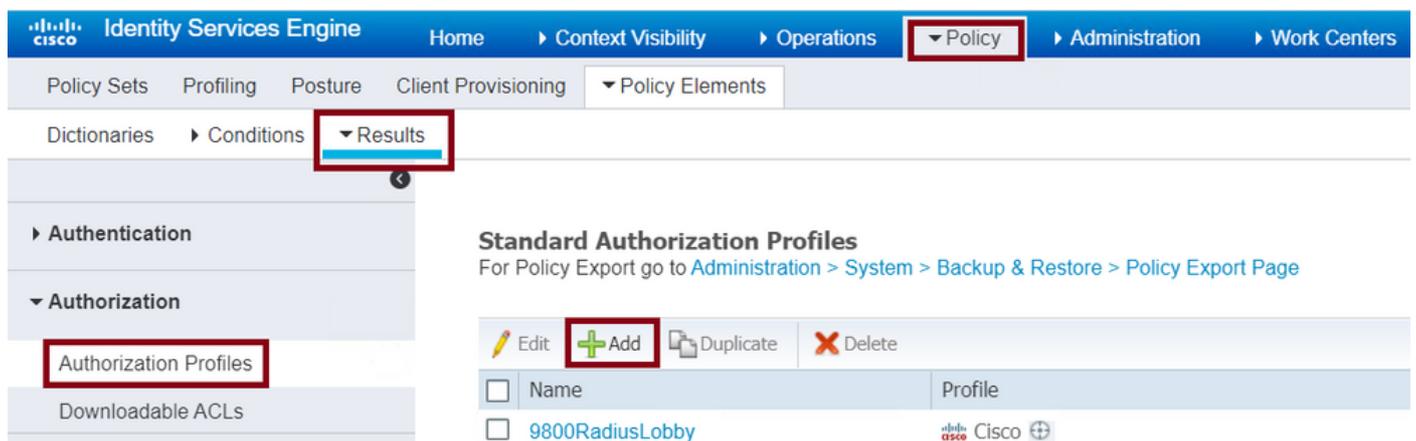
Paso 2. Cree el usuario Embajador del vestíbulo en ISE. Vaya a **Administration > Identity Management > Identities > Users > Add**.

Agregue a ISE el nombre de usuario y la contraseña asignados al Embajador del vestíbulo que crea los usuarios invitados. Este es el nombre de usuario que el Administrador asignará al Embajador del vestíbulo.



Cuando se abra la ventana de configuración, proporcione el nombre y la contraseña para el usuario Embajador del vestíbulo. Además, asegúrese de que el estado esté habilitado.

Paso 3. Cree un perfil de autorización de resultados. Vaya a **Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add**. Cree un perfil de autorización de resultado para regresar al WLC un Access-Accept con los atributos necesarios como se muestra en la imagen.



Asegúrese de que el perfil esté configurado para enviar un Access-Accept como se muestra en la

imagen.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. The left sidebar has 'Authentication' and 'Authorization' sections. The main content area is titled 'Authorization Profiles > 9800RadiusLobby' and 'Authorization Profile'. The 'Name' field is '9800RadiusLobby'. The 'Description' field is empty. The '\* Access Type' dropdown menu is set to 'ACCESS\_ACCEPT' and is highlighted with a red box.

Deberá agregar los atributos manualmente en Configuración de atributos avanzados. Los atributos son necesarios para definir al usuario como embajador de vestíbulo y para proporcionar el privilegio para que el embajador de vestíbulo pueda hacer los cambios necesarios.

#### Advanced Attributes Settings

The screenshot shows the 'Advanced Attributes Settings' section. Two attribute entries are visible, both highlighted with red boxes:

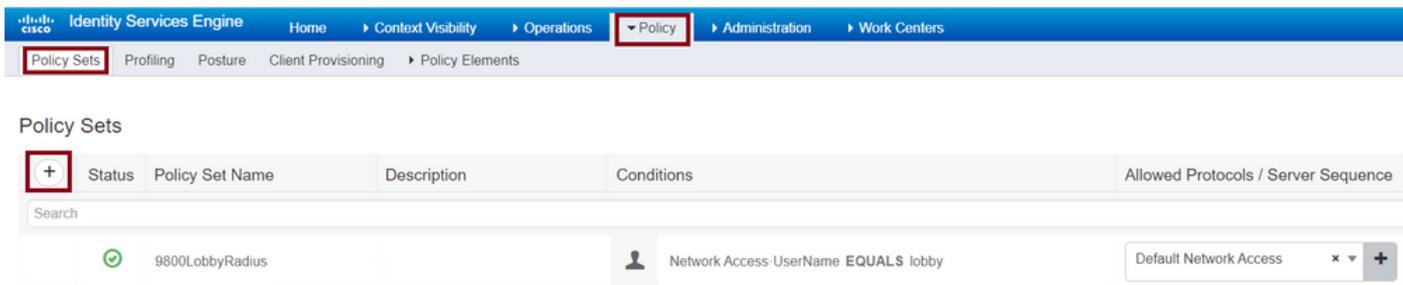
- Cisco:cisco-av-pair = user-type=lobby-admin
- Cisco:cisco-av-pair = shell:priv-lvl=15

#### Attributes Details

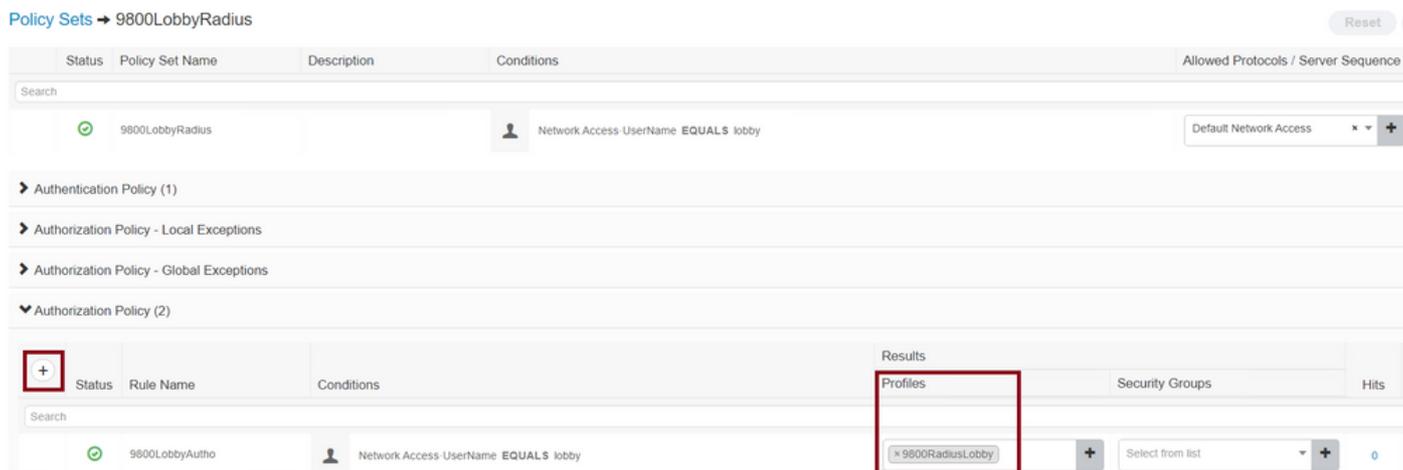
```
Access Type = ACCESS_ACCEPT
cisco-av-pair = user-type=lobby-admin
cisco-av-pair = shell:priv-lvl=15
```

Paso 4. Cree una política para procesar la autenticación. Navegue hasta **Política > Conjuntos de políticas > Agregar**. Las condiciones para configurar la política dependen de la decisión del administrador. Aquí se utilizan la condición Network Access-Username y el protocolo Default Network Access .

Es obligatorio asegurar bajo la Política de Autorización que el perfil configurado bajo la Autorización de Resultados está seleccionado, de esa manera usted puede devolver los atributos necesarios al WLC como se muestra en la imagen.



Quando se abra la ventana de configuración, configure la política de autorización. La política de autenticación se puede dejar como predeterminada.



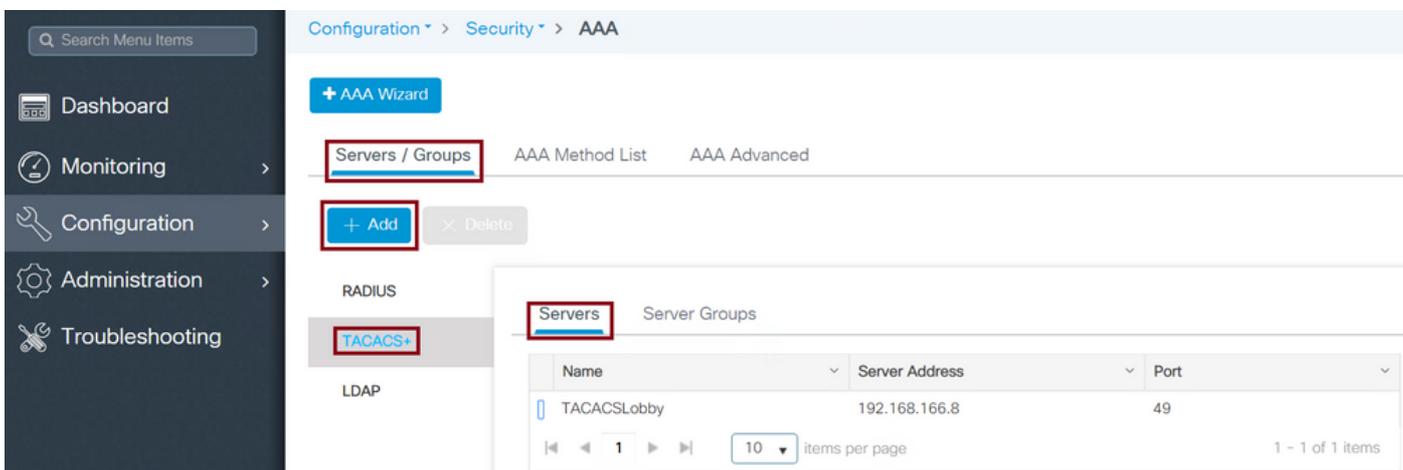
## Autenticar TACACS+

### Configuración de TACACS+ en WLC

Paso 1. Declare el servidor TACACS+. Cree el ISE TACACS Server en el WLC.

GUI:

Vaya a **Configuration > Security > AAA > Servers/Groups > TACACS+ > Servers > + Add** como se muestra en la imagen.



Quando se abre la ventana de configuración, los parámetros de configuración obligatorios son el nombre del servidor TACACS+ (no tiene que coincidir con el nombre del sistema ISE/AAA), la dirección IP del servidor TACACS y el secreto compartido. Cualquier otro parámetro se puede dejar predeterminado o se puede configurar según sea necesario.

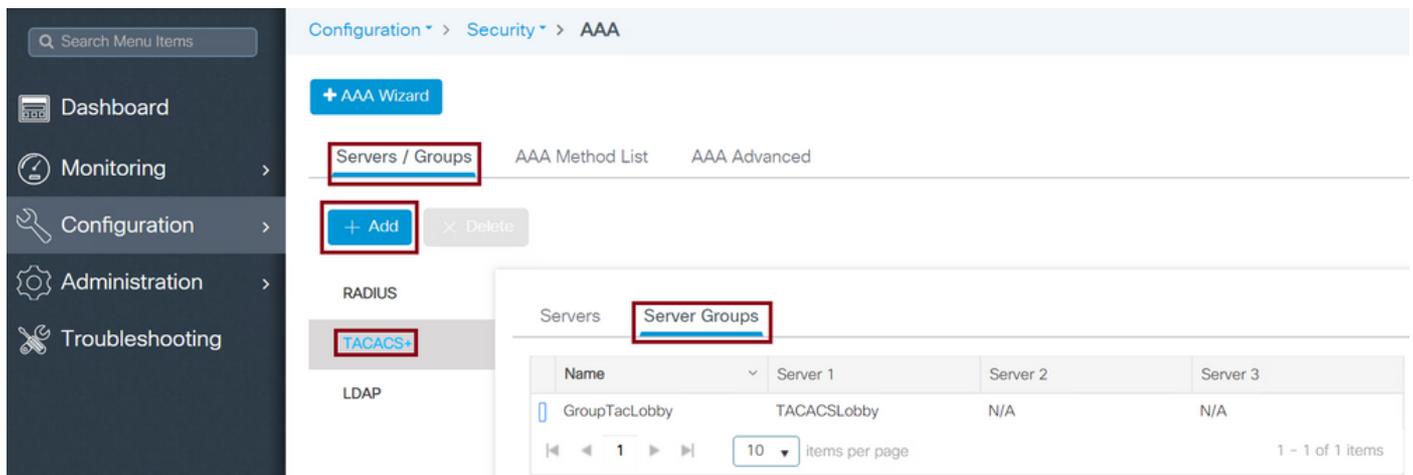
CLI:

```
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
```

Paso 2. Agregue el servidor TACACS+ a un grupo de servidores. Defina un grupo de servidores y agregue el servidor TACACS+ que desee configurado. Serán los servidores TACACS+ utilizados para la autenticación.

GUI:

Vaya a **Configuration > Security > AAA > Servers / Groups > TACACS > Server Groups > + Add** como se muestra en la imagen.



Cuando se abra la ventana de configuración, asigne un nombre al grupo y mueva los servidores TACACS+ deseados de la lista Servidores disponibles a la lista Servidores asignados.

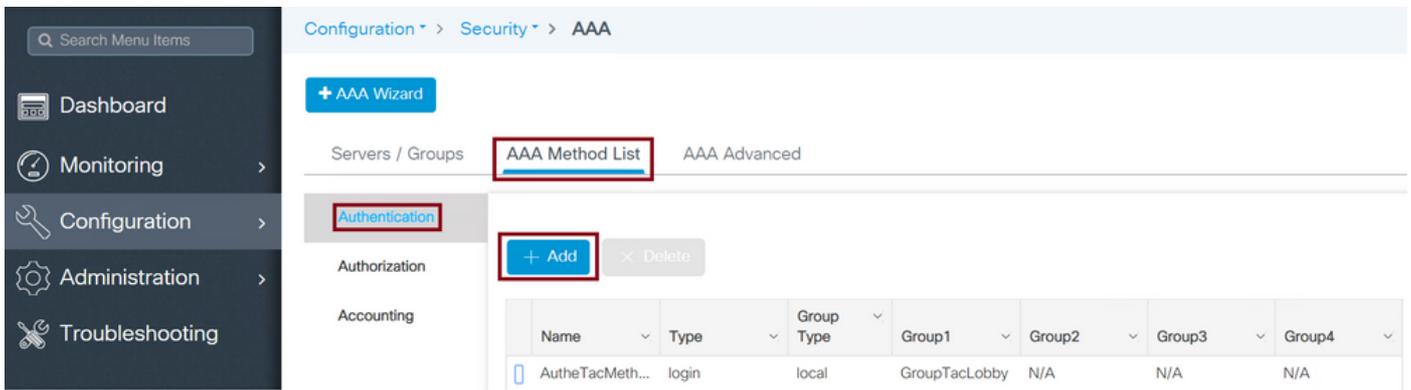
CLI:

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

Paso 3. Cree una lista de métodos de autenticación. La lista de métodos de autenticación define el tipo de autenticación necesaria y también asociará el mismo tipo al grupo de servidores configurado. También permite seleccionar si la autenticación se puede hacer localmente en el WLC o externa a un servidor TACACS+.

GUI:

Vaya a **Configuration > Security > AAA > AAA Method List > Authentication > + Add** como se muestra en la imagen.



Cuando se abra la ventana de configuración, proporcione un nombre, seleccione la opción de tipo como **Login** y asigne el grupo de servidores creado anteriormente.

Tipo de grupo como local.

GUI:

Si selecciona Tipo de grupo como 'local', el WLC primero verificará si el usuario existe en la base de datos local y luego devolverá al Grupo de servidores solamente si el usuario Embajador de vestíbulo no se encuentra en la base de datos local.

**Nota:** Tenga en cuenta este error de funcionamiento [CSCvs87163](#) fijado en 17.3.

CLI:

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

Tipo de grupo como grupo.

GUI:

Si selecciona Tipo de grupo como grupo y no hay reserva en la opción local marcada, el WLC solamente verificará al usuario con el Grupo de servidores y no protegerá su base de datos local.

CLI:

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

Group Type as group (Tipo de grupo) y la opción fallback to local (Volver a local) está activada.

GUI:

Si selecciona Tipo de Grupo como 'grupo' y la opción Reserva a local está marcada, el WLC verificará al usuario con el Grupo de Servidor y consultará la base de datos local solamente si el Servidor TACACS agota el tiempo de espera en la respuesta. Si el servidor envía un rechazo, el usuario no se autenticará, aunque exista en la base de datos local.

CLI:

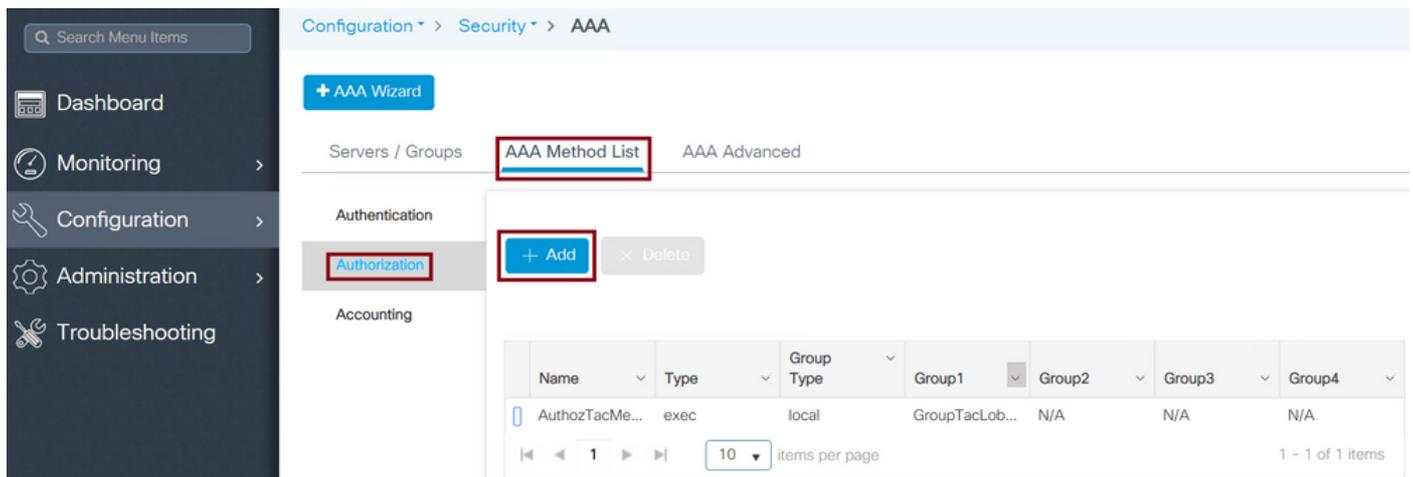
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Paso 4. Cree una lista de métodos de autorización.

La lista de métodos de autorización definirá el tipo de autorización que se necesita para el Embajador del vestíbulo que en este caso será ejecutivo. También se asocia al mismo grupo de servidores configurado. También se permite seleccionar si la autenticación se realiza localmente en el WLC o externa a un servidor TACACS+.

GUI:

Vaya a **Configuration > Security > AAA > AAA Method List > Authorization > + Add** como se muestra en la imagen.



Cuando se abra la ventana de configuración, proporcione un nombre, seleccione la opción type como exec y asigne el grupo de servidores creado anteriormente.

Tenga en cuenta que el tipo de grupo se aplica de la misma manera que se explica en la parte Lista de métodos de autenticación.

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
```

Group Type como grupo y la opción Fallback to local está marcada.

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

Paso 5. Asigne los métodos. Una vez configurados los métodos, deben ser asignados a las opciones para iniciar sesión en el WLC para crear el usuario invitado como línea VTY o HTTP (GUI). Estos pasos no se pueden realizar desde la GUI, por lo que deben realizarse desde la CLI.

## Autenticación 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
```

Cuando realice cambios en las configuraciones HTTP, es mejor reiniciar los servicios HTTP y 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
```

## Línea 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
```

**Paso 6.** Defina el usuario remoto. El nombre de usuario creado en ISE para el Embajador del vestíbulo debe definirse como un nombre de usuario remoto en el WLC. Si el nombre de usuario remoto no está definido en el WLC, la autenticación pasará correctamente, sin embargo, el usuario será otorgado con acceso completo al WLC en lugar de solamente acceso a los privilegios de Embajador del lobby. Esta configuración sólo se puede realizar a través de CLI.

## CLI:

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

## Configuración de ISE - TACACS+

**Paso 1.** Habilitar administrador de dispositivos. Vaya a **Administration > System > Deployment**. Antes de continuar, seleccione **Enable Device Admin Service** y asegúrese de que ISE se haya habilitado como se muestra en la imagen.

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation path is Administration > Deployment > Deployment Nodes List > timise23 > Edit Node. The 'General Settings' tab is active, showing the following configuration:

- 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)

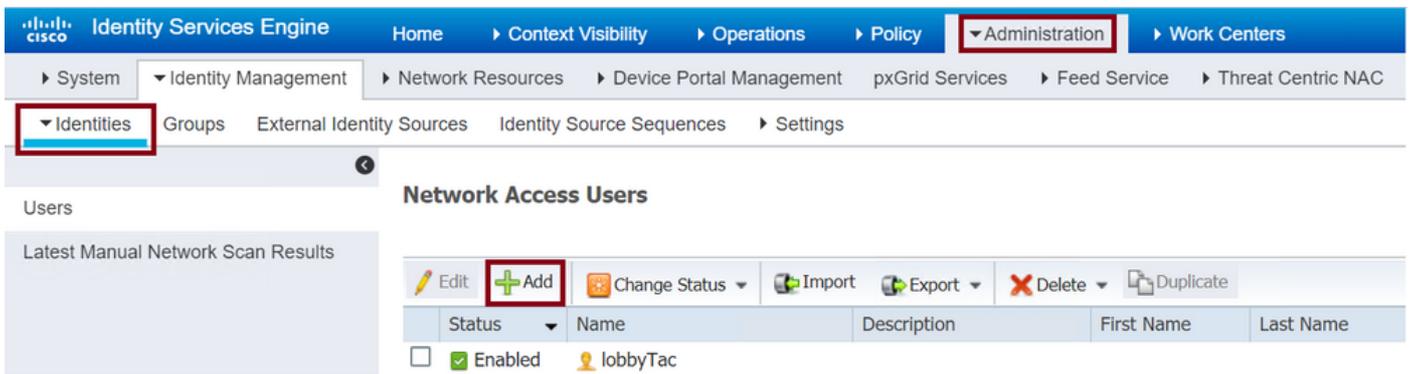
Paso 2. Agregue el WLC a ISE. Vaya a **Administration > Network Resources > Network Devices > Add**. El WLC debe agregarse a ISE. Cuando agrega el WLC a ISE, habilite la Configuración de Autenticación TACACS+ y configure los parámetros necesarios como se muestra en la imagen.

The screenshot shows the Cisco Identity Services Engine Administration interface for the 'Network Devices' configuration page. The navigation path is Administration > Network Resources > Network Devices > Add. The 'Add' button is highlighted with a red box. Below the table, the following network device is listed:

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

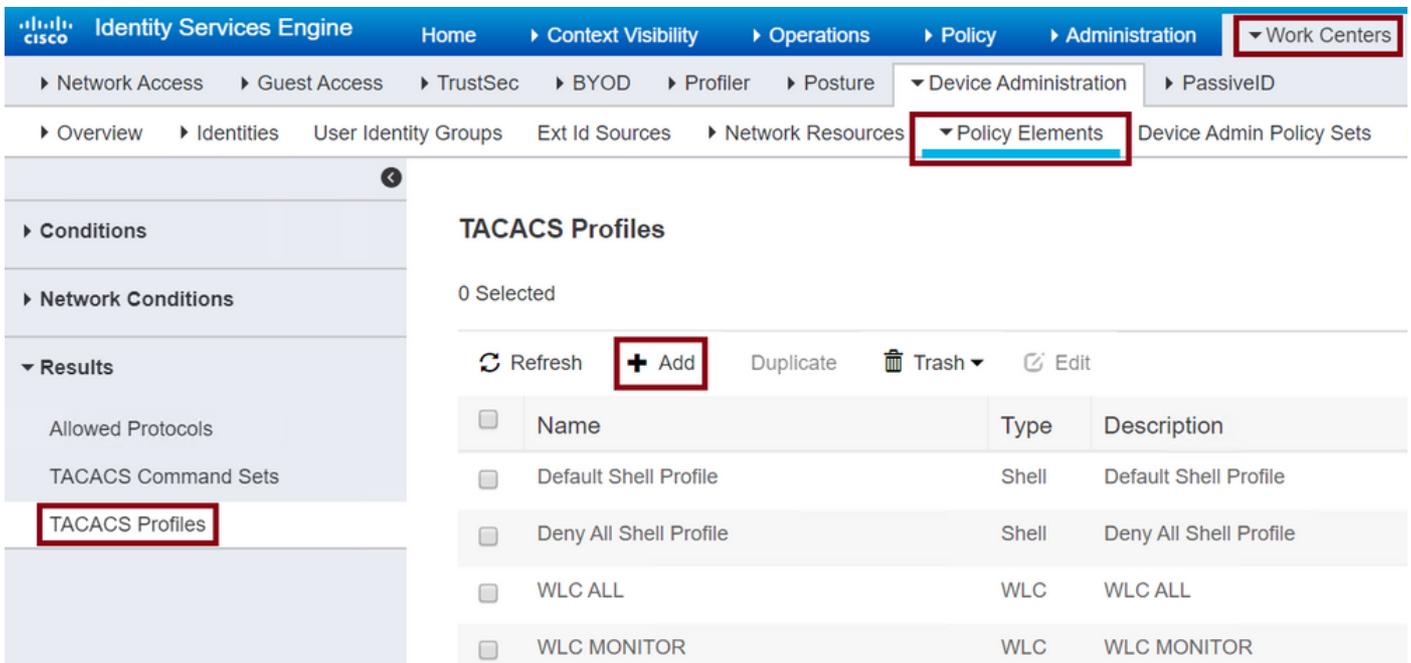
Cuando se abre la ventana de configuración para proporcionar un nombre, IP ADD, active TACACS+ Authentication Settings e introduzca el secreto compartido necesario.

Paso 3. Cree el usuario Embajador del vestíbulo en ISE. Vaya a **Administration > Identity Management > Identities > Users > Add**. Agregue a ISE el nombre de usuario y la contraseña asignados al Embajador del vestíbulo que creará los usuarios invitados. Este es el nombre de usuario que el administrador asigna al Embajador del vestíbulo como se muestra en la imagen.



Cuando se abra la ventana de configuración, proporcione el nombre y la contraseña para el usuario Embajador del vestíbulo. Además, asegúrese de que el estado esté habilitado.

Paso 4. Cree un perfil de resultados TACACS+. Vaya a **Centros de Trabajo > Administración de Dispositivos > Elementos de Política > Resultados > Perfiles TACACS** como se muestra en la imagen. Con este perfil, devuelva los atributos necesarios al WLC para colocar al usuario como embajador de lobby.



Cuando se abra la ventana de configuración, proporcione un nombre al perfil, también configure un Privilegio Predeterminado 15 y un Atributo Personalizado como Tipo Obligatorio, nombre como tipo de usuario y valor lobby-admin. Además, deje que el **Tipo de tarea común** se seleccione como Shell como se muestra en la imagen.

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

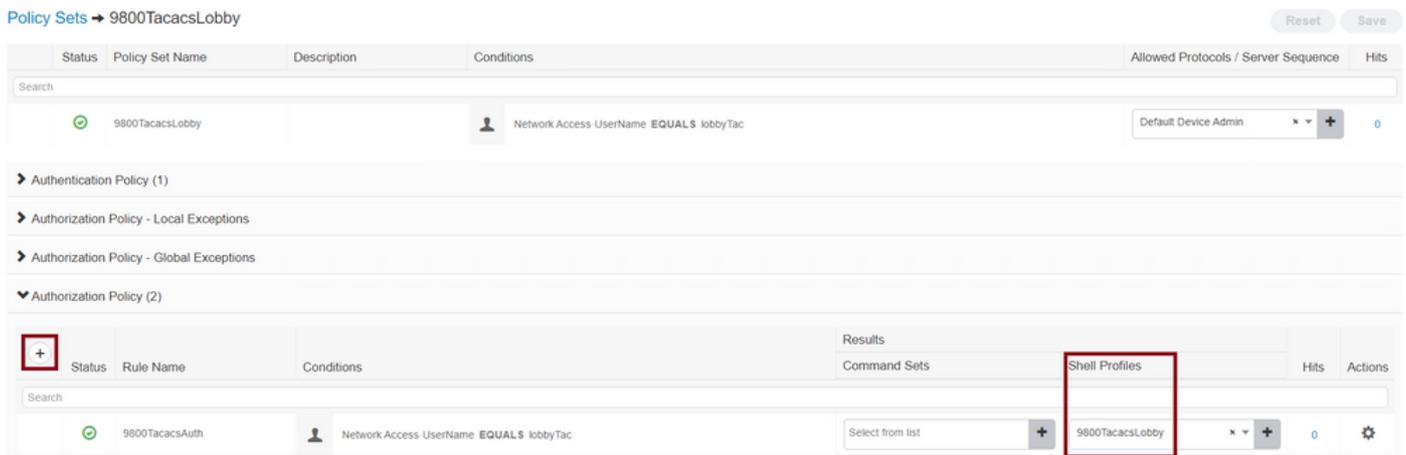
1 Selected

+ Add    🗑️ Trash    ✎ Edit

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

Paso 5. Cree un conjunto de políticas. Vaya a **Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos** como se muestra en la imagen. Las condiciones para configurar la política dependen de la decisión del administrador. Para este documento, se utilizan la condición Network Access-Username y el protocolo Default Device Admin . Es obligatorio asegurar bajo la Política de Autorización que el perfil configurado bajo la Autorización de Resultados está seleccionado, de esa manera usted puede devolver los atributos necesarios al WLC.

Cuando se abra la ventana de configuración, configure la política de autorización. La política de autenticación se puede dejar como predeterminada, como se muestra en la imagen.

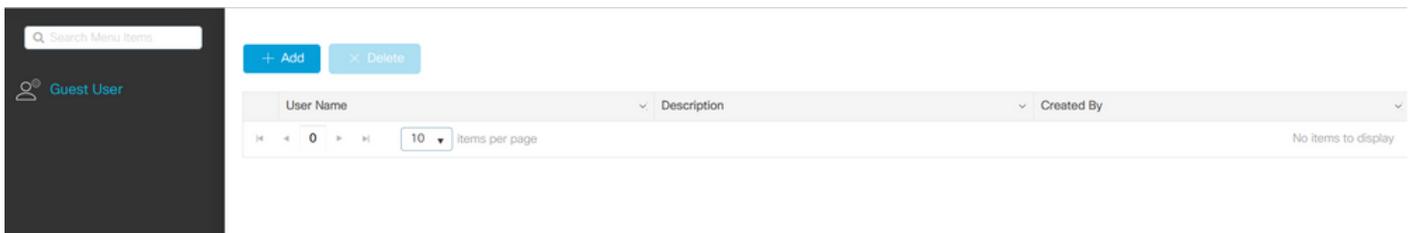


## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

```
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
```

Así es como se ve la GUI del Embajador del vestíbulo después de una autenticación exitosa.



## Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

### Autenticar RADIUS

Para la autenticación RADIUS, se pueden utilizar estos debugs:

```
Tim-eWLC1#debug aaa authentication
Tim-eWLC1#debug aaa authorization
Tim-eWLC1#debug aaa attr
Tim-eWLC1#terminal monitor
```

Asegúrese de que la lista de métodos correcta esté seleccionada en la depuración. Además, el servidor ISE devuelve los atributos necesarios con el nombre de usuario, el tipo de usuario y el privilegio adecuados.

```
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'
```

## Autenticar TACACS+

Para la autenticación TACACS+, se puede utilizar este debug:

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

Asegúrese de que la autenticación se procesa con el nombre de usuario y la IP ADD de ISE adecuados. Además, debe verse el estado "PASS". En la misma depuración, justo después de la fase de autenticación, se presentará el proceso de autorización. En esta autorización, la fase garantiza que se utilice el nombre de usuario correcto junto con la IP ADD correcta de ISE. A partir de esta fase, debería poder ver los atributos configurados en ISE que indican al WLC como usuario Embajador en el vestíbulo con el privilegio correcto.

Ejemplo de fase de autenticación:

```
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)
```

Ejemplo de fase de autorización:

```
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
```

Los ejemplos de depuración mencionados anteriormente para RADIUS y TACACS+ tienen los pasos clave para un inicio de sesión exitoso. Los debugs son más detallados y el resultado será mayor. Para inhabilitar los debugs, se puede utilizar este comando:

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