Configurar RADIUS & TACACS+ para GUI & CLI Auth en WLC 9800

Contenido

Introducción

Este documento describe cómo configurar un Catalyst 9800 para la autenticación externa RADIUS o TACACS+.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

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

- C9800-CL v17.9.2
- ISE 3.2.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cuando un usuario intenta acceder a la CLI o a la GUI del WLC, se le pide que ingrese un nombre de usuario y una contraseña. De forma predeterminada, estas credenciales se comparan con la base de datos local de usuarios, que está presente en el propio dispositivo. Alternativamente, el WLC se puede instruir para comparar las credenciales de entrada contra un servidor AAA remoto: el WLC puede hablar con el servidor con el uso de RADIUS o TACACS+.

Configurar

En este ejemplo, se configuran dos tipos de usuarios en el servidor AAA (ISE), respectivamente adminuser, yhelpdeskuser. Estos usuarios forman parte de admin-group y de los helpdesk-group grupos respectivamente. Se espera que el usuario adminuser, parte deladmin-group, tenga acceso completo al WLC. Por otro lado, el helpdeskuser, parte del helpdesk-group, está destinado a ser concedido solamente privilegios del monitor al WLC. Por lo tanto, no hay acceso a la configuración.

Este artículo primero configura el WLC e ISE para la autenticación RADIUS y luego realiza lo mismo para TACACS+.

Restricciones de usuario de sólo lectura

Cuando se utiliza TACACS+ o RADIUS para la autenticación 9800 WebUI, existen estas restricciones:

- Los usuarios con nivel de privilegio 0 existen pero no tienen acceso a la GUI
- Los usuarios con niveles de privilegio 1-14 sólo pueden ver la ficha Monitor (esto equivale al nivel de privilegio de un usuario autenticado localmente de sólo lectura)
- Los usuarios con el nivel de privilegio 15 tienen acceso completo
- No se admiten los usuarios con el nivel de privilegio 15 y un conjunto de comandos que sólo permite comandos específicos. El usuario todavía puede ejecutar los cambios de configuración a través de la interfaz de usuario Web

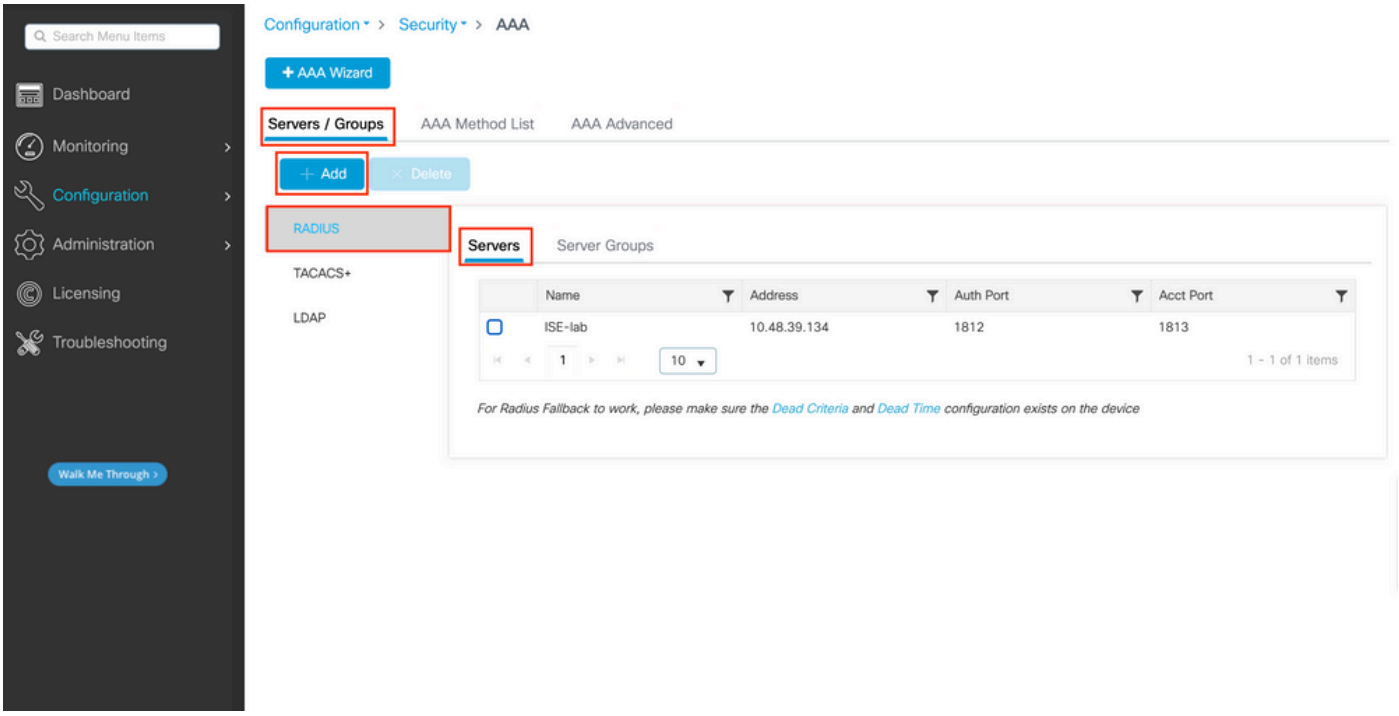
Estas consideraciones no se pueden cambiar ni modificar.

Configuración de la Autenticación RADIUS para el WLC

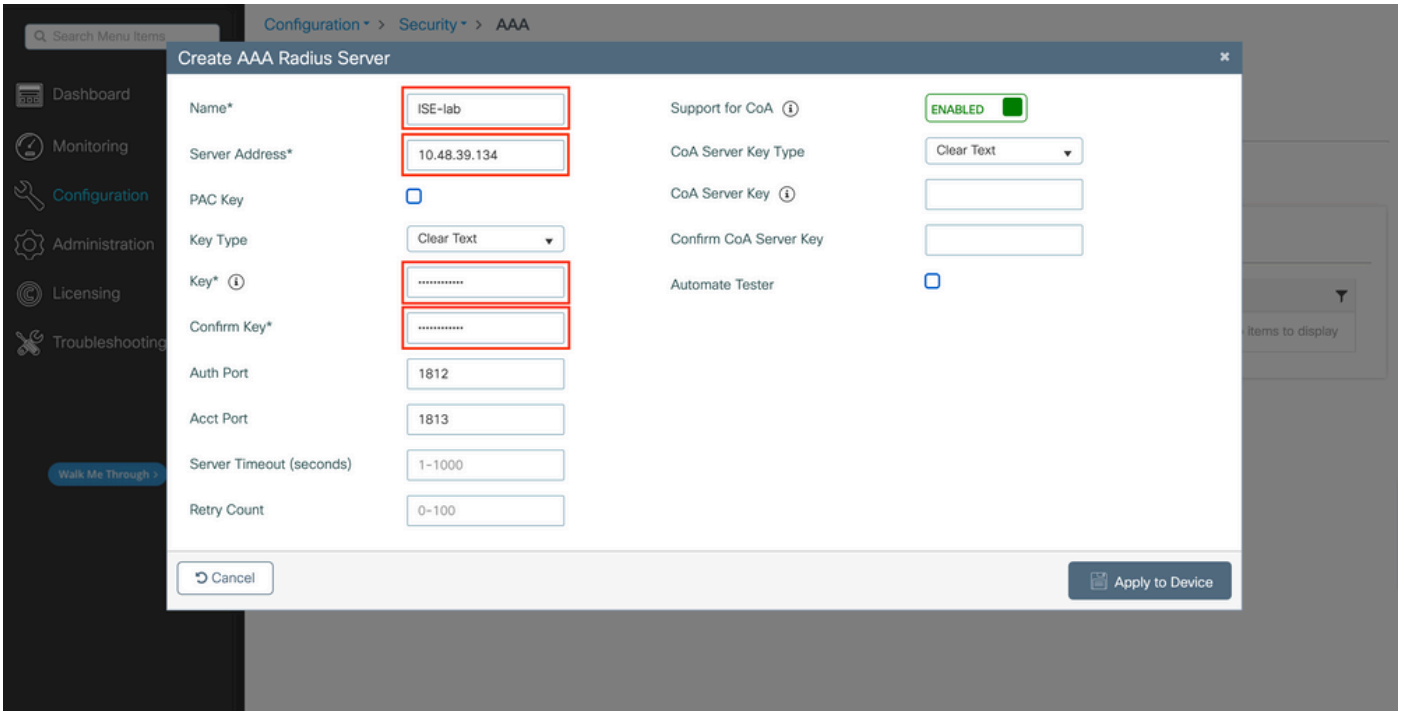
Paso 1. Declare el servidor RADIUS.

Desde la GUI:

En primer lugar, cree el servidor RADIUS de ISE en el WLC. Esto se puede hacer desde la pestaña Servers/Groups > RADIUS > Servers de la página GUI WLC accesible en https://<WLC-IP>/webui/#/aaa, o si navega a Configuration > Security > AAA , como se muestra en esta imagen.



Para agregar un servidor RADIUS en el WLC, haga clic en el botón Add enmarcado en rojo en la imagen. Se abrirá la ventana emergente que se muestra en la captura de pantalla.



En esta ventana emergente, debe proporcionar:

- El nombre del servidor (tenga en cuenta que no tiene que coincidir con el nombre del sistema de ISE)
- La dirección IP del servidor
- El secreto compartido entre el WLC y el servidor RADIUS

Se pueden configurar otros parámetros, como los puertos utilizados para la autenticación y la administración de cuentas, pero no son obligatorios y se dejan como predeterminados para esta documentación.

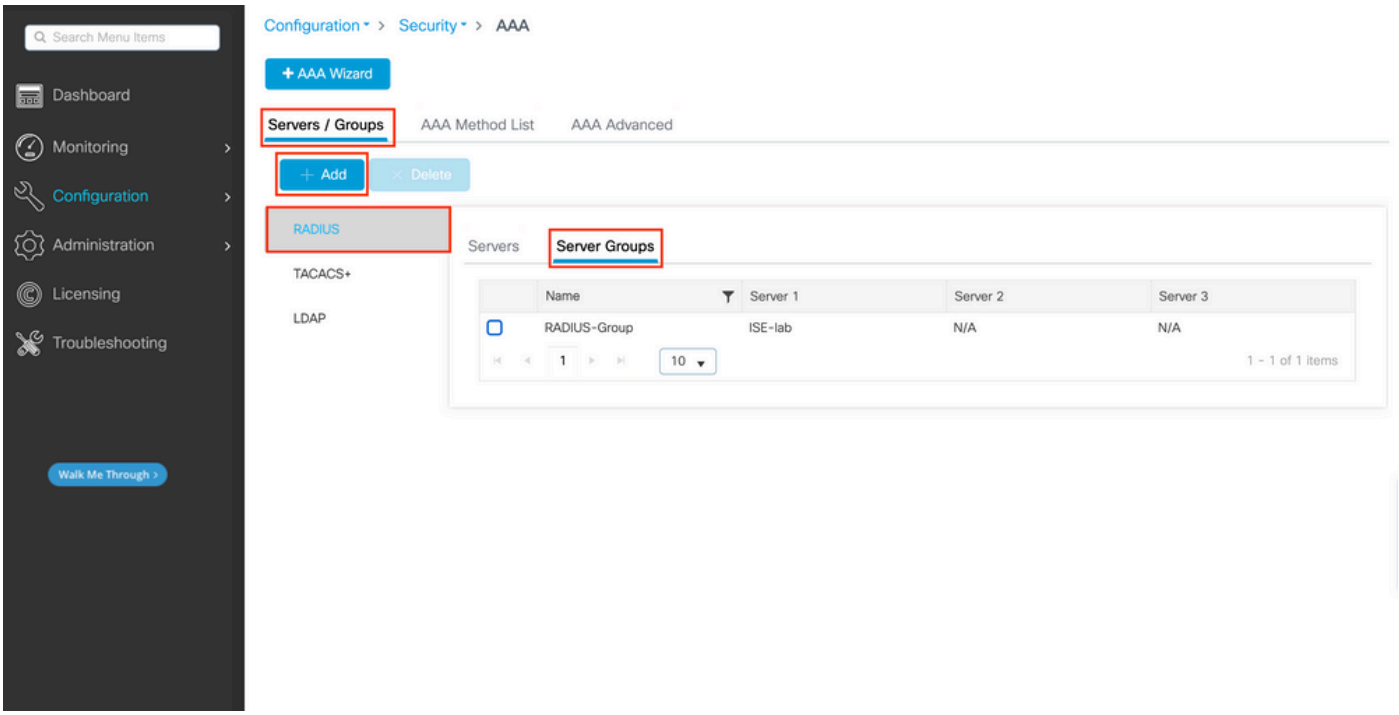
Desde CLI:

```
<#root>

WLC-9800(config)#radius server

ISE-lab

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

10.48.39.134

auth-port 1812 acct-port 1813
WLC-9800(config-radius-server)#key

Cisco123
```

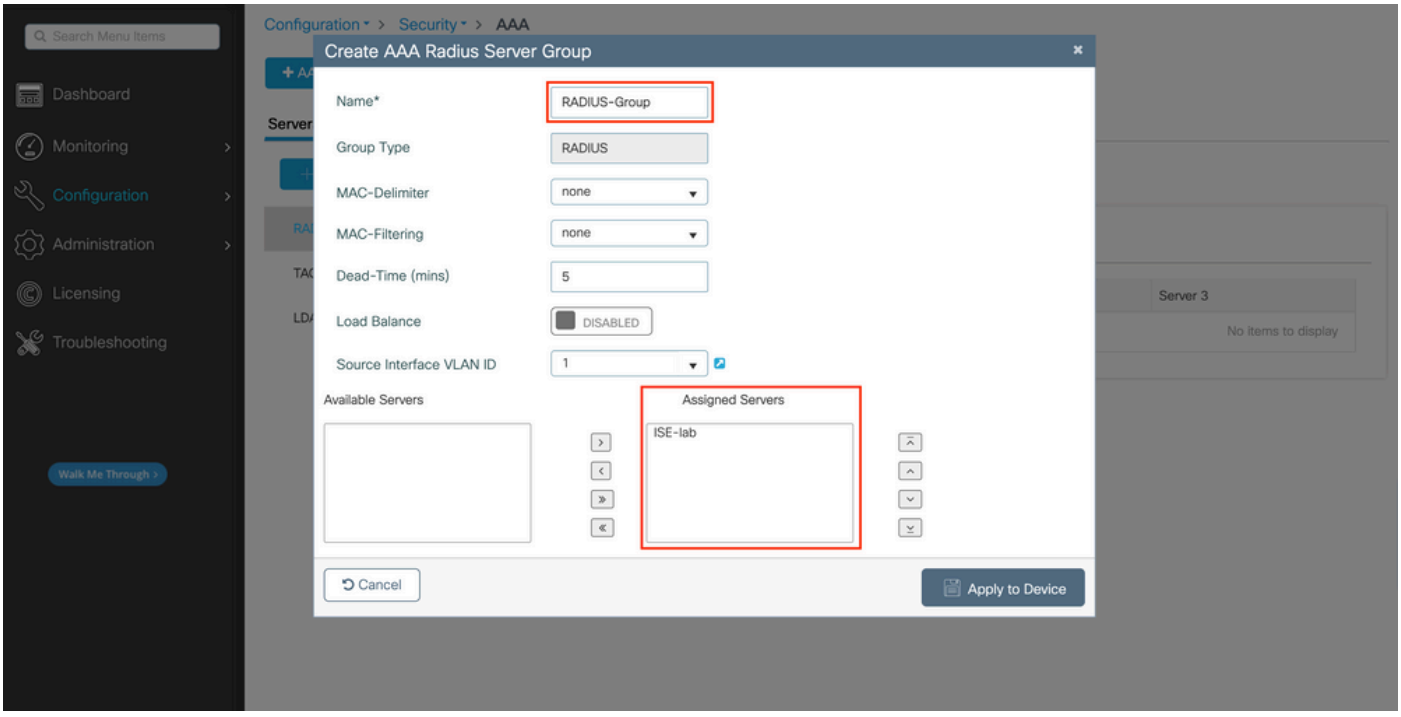
Paso 2. Asigne el servidor RADIUS a un grupo de servidores.

Desde la GUI:

En caso de que tenga varios servidores RADIUS que se puedan utilizar para la autenticación, se recomienda asignar todos estos servidores al mismo grupo de servidores. El WLC se ocupa del balanceo de carga de las diferentes autenticaciones entre los servidores en el grupo de servidores. Los grupos de servidores RADIUS se configuran desde la Servers/Groups > RADIUS > Server Groups pestaña desde la misma página GUI que la mencionada en el Paso 1, como se muestra en la imagen.



En cuanto a la creación del servidor, aparece una ventana emergente al hacer clic en el botón Agregar (enmarcado en la imagen anterior), que se muestra aquí.



En la ventana emergente, proporcione un nombre al grupo y mueva los servidores deseados a la lista Servidores asignados.

Desde CLI:

<#root>

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

```
RADIUS-Group
```

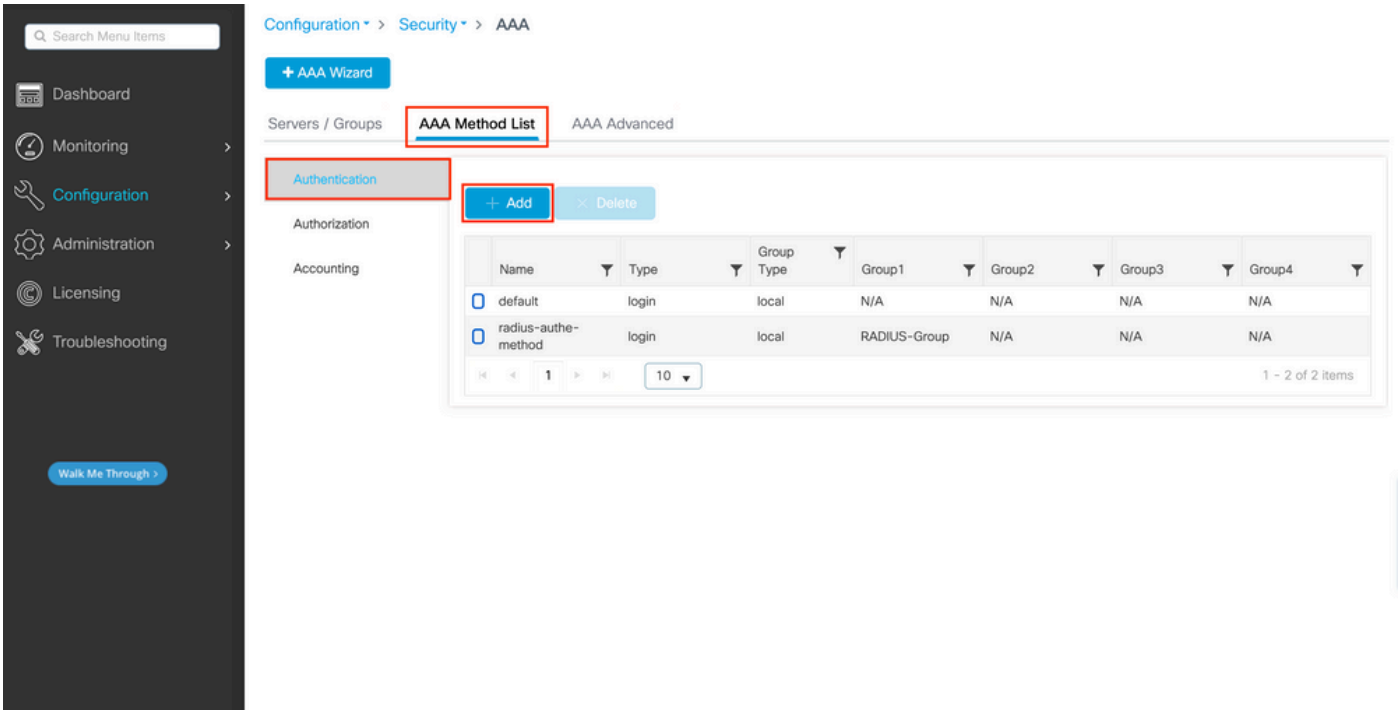
```
WLC-9800(config-sg-radius)# server name
```

```
ISE-lab
```

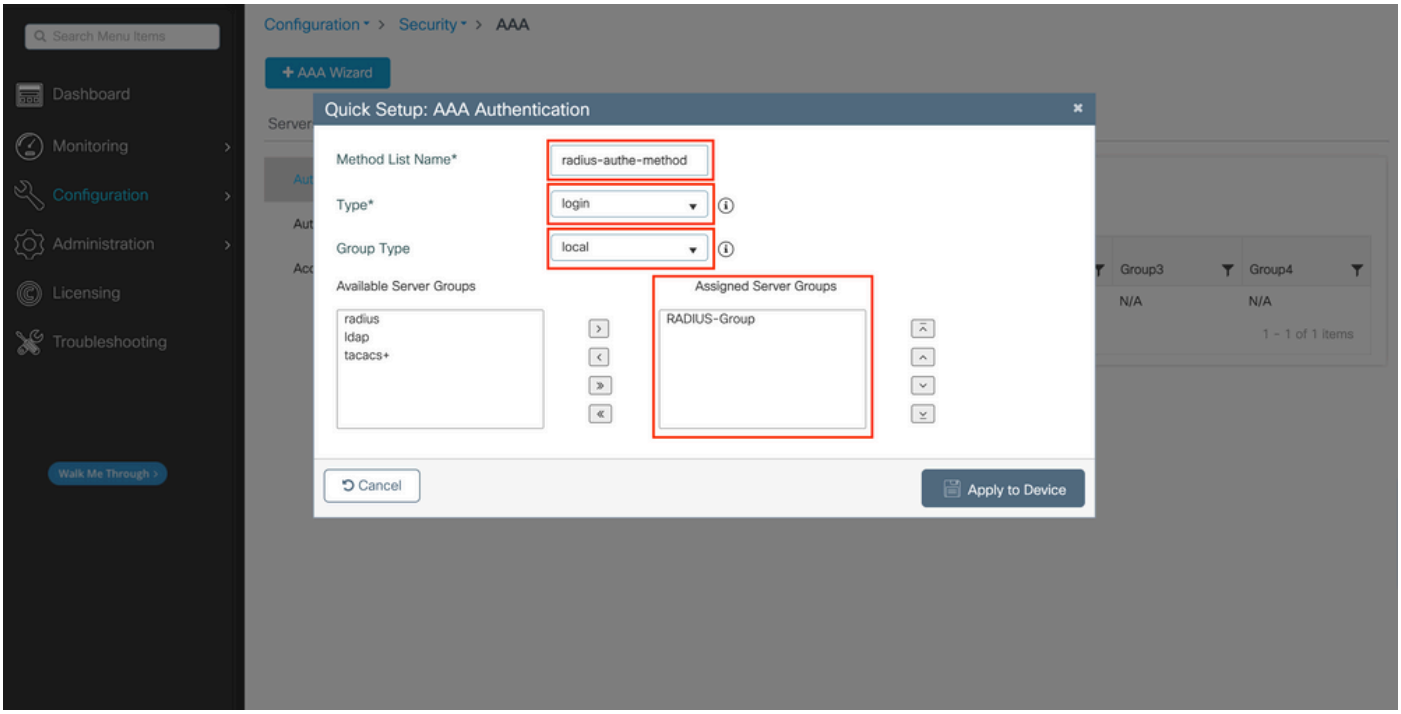
Paso 3. Cree un método de inicio de sesión de autenticación AAA que apunte al grupo de servidores RADIUS.

Desde la GUI:

Desde la página GUIhttps://<WLC-IP>/webui/#/aaa, navegue hasta la AAA Method List > Authentication pestaña y cree un método de autenticación como se muestra en esta imagen.



Como es habitual, cuando utiliza el botón Add (Agregar) para crear un método de autenticación, aparece una ventana emergente de configuración, similar a la que se muestra en esta imagen.



En esta ventana emergente, proporcione un nombre para el método. Elija Type como conexión y agregue el servidor de grupos creado en el paso anterior a la Assigned Server Groups lista. Con respecto al campo Tipo de grupo, son posibles varias configuraciones.

- Si elige el tipo de grupo como local, el WLC primero verifica si las credenciales del usuario existen localmente y después vuelve al grupo del servidor.
- Si elige el tipo de grupo como grupo y no marca la opción Volver a local, el WLC verifica solamente las credenciales del usuario contra el grupo del servidor.
- Si elige Group Type como grupo y marca la opción Fallback to local, el WLC verifica las credenciales del usuario contra el grupo del servidor y consulta la base de datos local solamente si el servidor no responde. Si el servidor envía un rechazo, el usuario se autenticará, aunque pueda existir en la base de datos local.

Desde CLI:

Si desea que las credenciales de usuario se comprueben con un grupo de servidores sólo si no se encuentran primero localmente, utilice:

```
<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method
```

```
 local group
```

RADIUS-Group

Si desea que las credenciales de usuario se comprueben sólo con un grupo de servidores, utilice:

```
    <#root>

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

radius-authe-method

```
 group
```

RADIUS-Group

Si desea que las credenciales de usuario se comprueben con un grupo de servidores y si esta última no responde con una entrada local, utilice:

```
    <#root>

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

radius-authe-method

group

RADIUS-Group

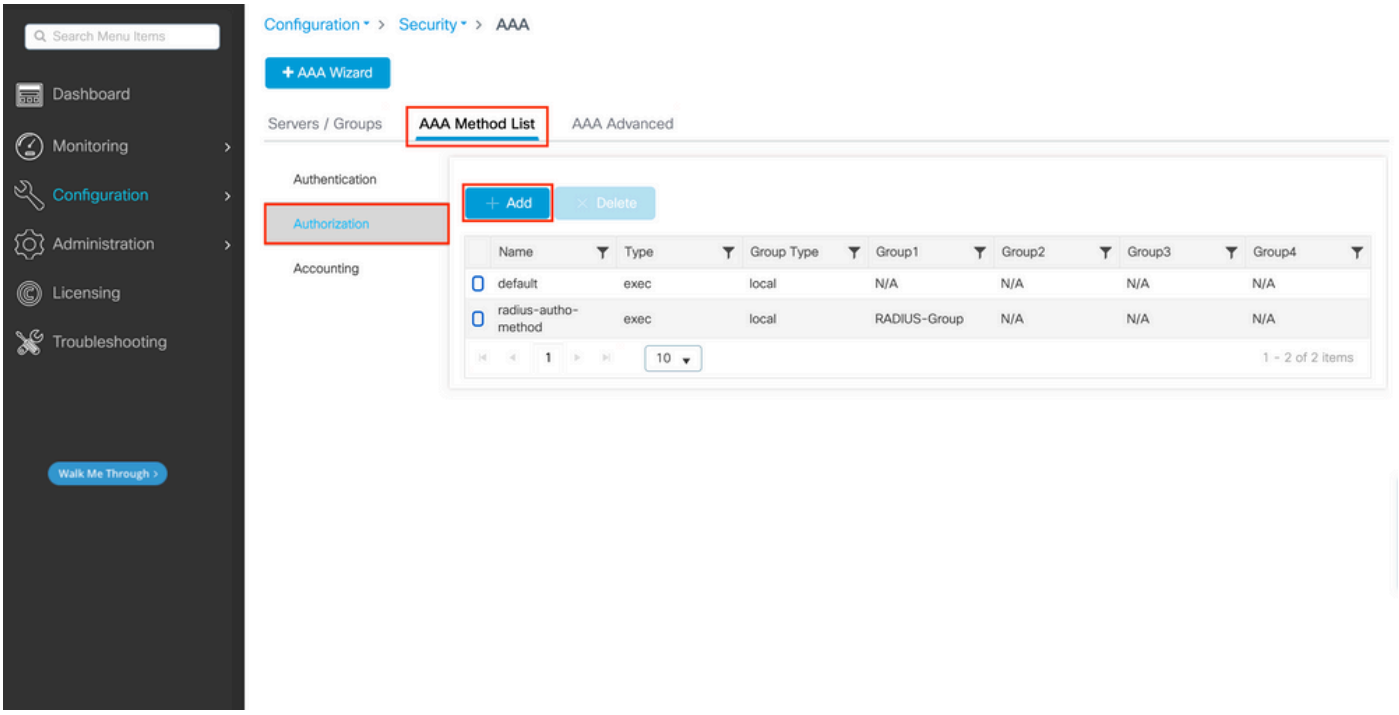
local

En este ejemplo de configuración, hay algunos usuarios que solo se crean localmente y algunos usuarios solo en el servidor ISE, por lo tanto, hacen uso de la primera opción.

Paso 4. Cree un método de ejecución de autorización AAA que apunte al grupo de servidores RADIUS.

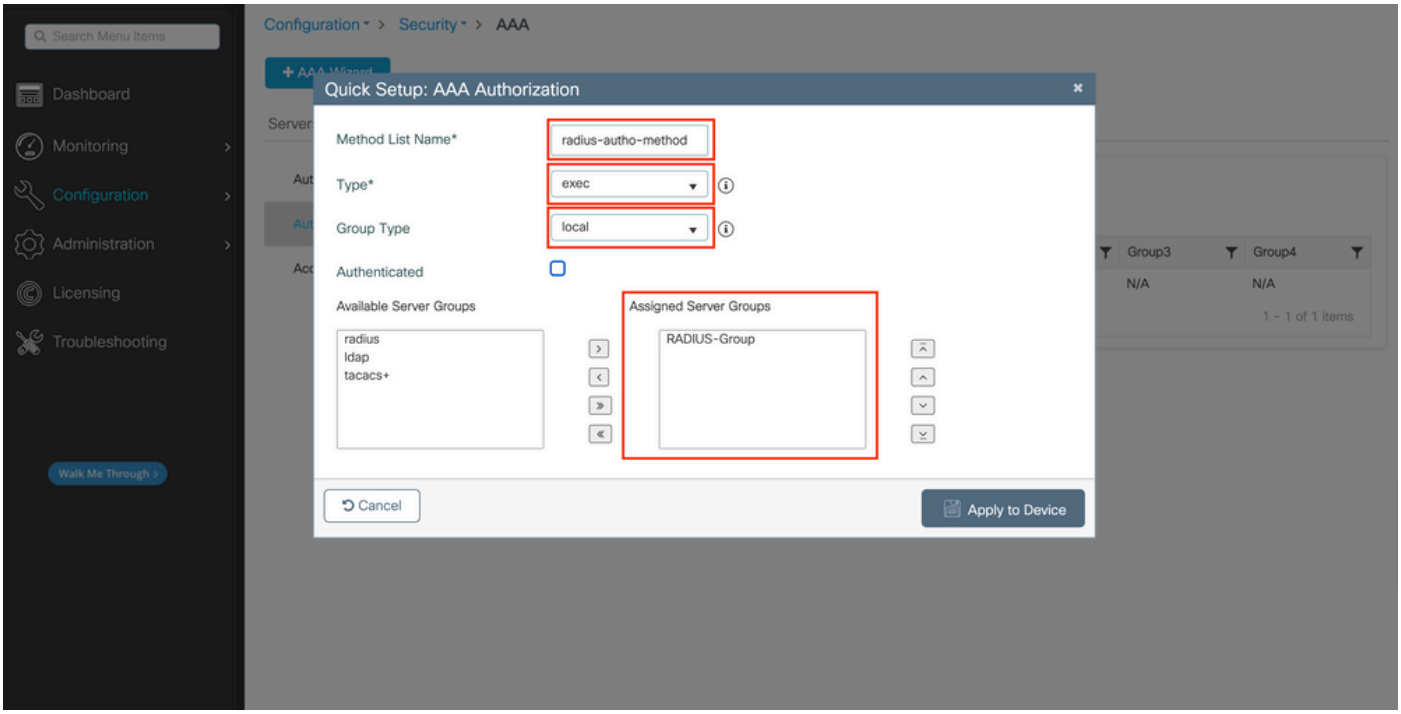
Desde la GUI:

El usuario también debe estar autorizado para que se le conceda acceso. En la GUI Page Configuration > Security > AAA, vaya a la AAA Method List > Authorization ficha y cree un método de autorización como se muestra en esta imagen.



Creación del método de autorización

Una ventana emergente de configuración de método de autorización similar a la representada aparece cuando se agrega una nueva con el botón Add (Agregar).



En esta ventana emergente de configuración, proporcione un nombre para el método de autorización, elija el Tipo como exec y utilice el mismo orden de Tipo de grupo que el utilizado para el método de autenticación en el Paso 3.

Desde CLI:

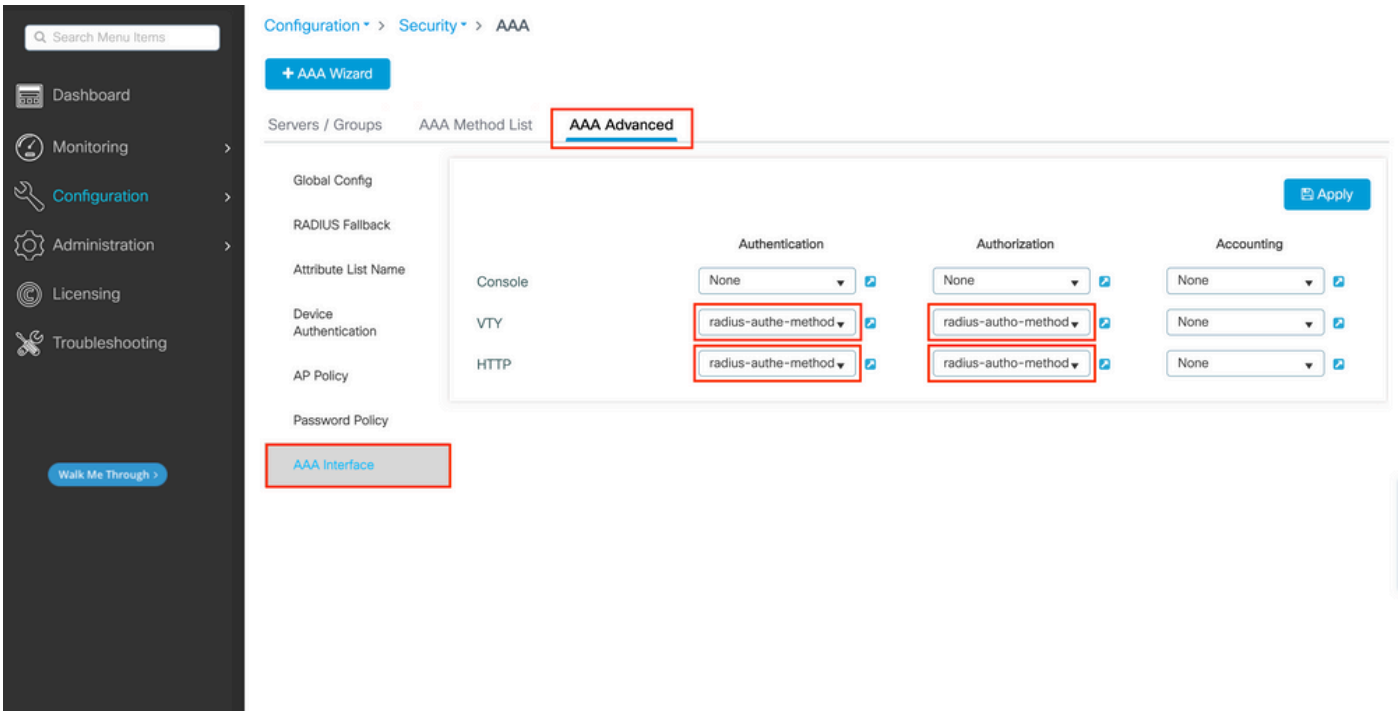
En cuanto al método de autenticación, la autorización se asigna primero para comprobar los usuarios con las entradas locales y, a continuación, con las entradas de un grupo de servidores.

```
<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

 local group

RADIUS-Group
```

Paso 5. Asigne los métodos a las configuraciones HTTP y a las líneas VTY utilizadas para Telnet/SSH.

Desde la GUI:

Los métodos de autenticación y autorización creados se pueden utilizar para la conexión de usuario HTTP y/o Telnet/SSH, que se puede configurar desde la AAA Advanced > AAA Interface pestaña todavía desde la página WLC de GUI accesible en https://<WLC-IP>/webui/#/aaa, como se muestra en esta imagen:



CLI para autenticación GUI:

<#root>

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

radius-authe-method

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

radius-autho-method

CLI para autenticación Telnet/SSH:

<#root>

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

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-autho-method

Tenga en cuenta que cuando se realizan cambios en las configuraciones HTTP, es mejor reiniciar los servicios HTTP y HTTPS. Esto se puede lograr con estos comandos:

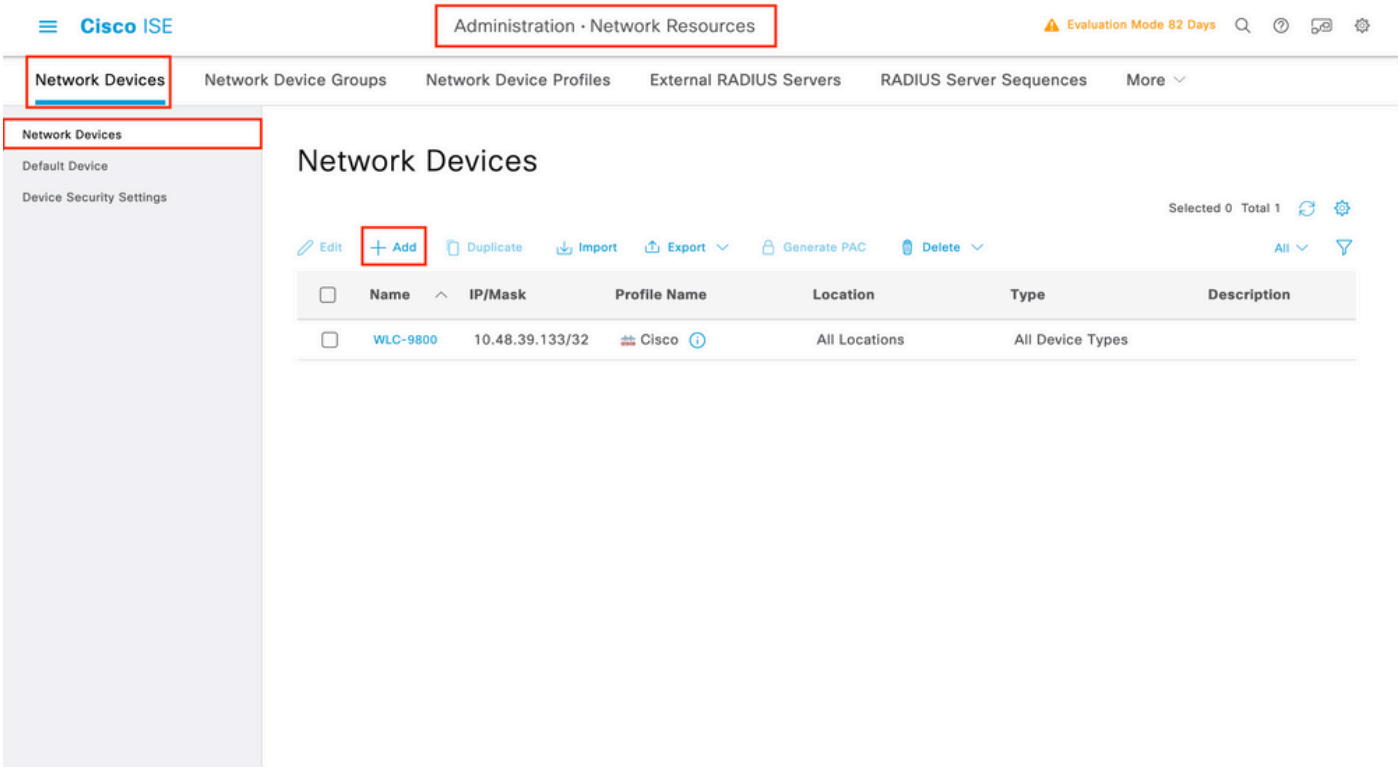
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-serv

Configuración de ISE para RADIUS

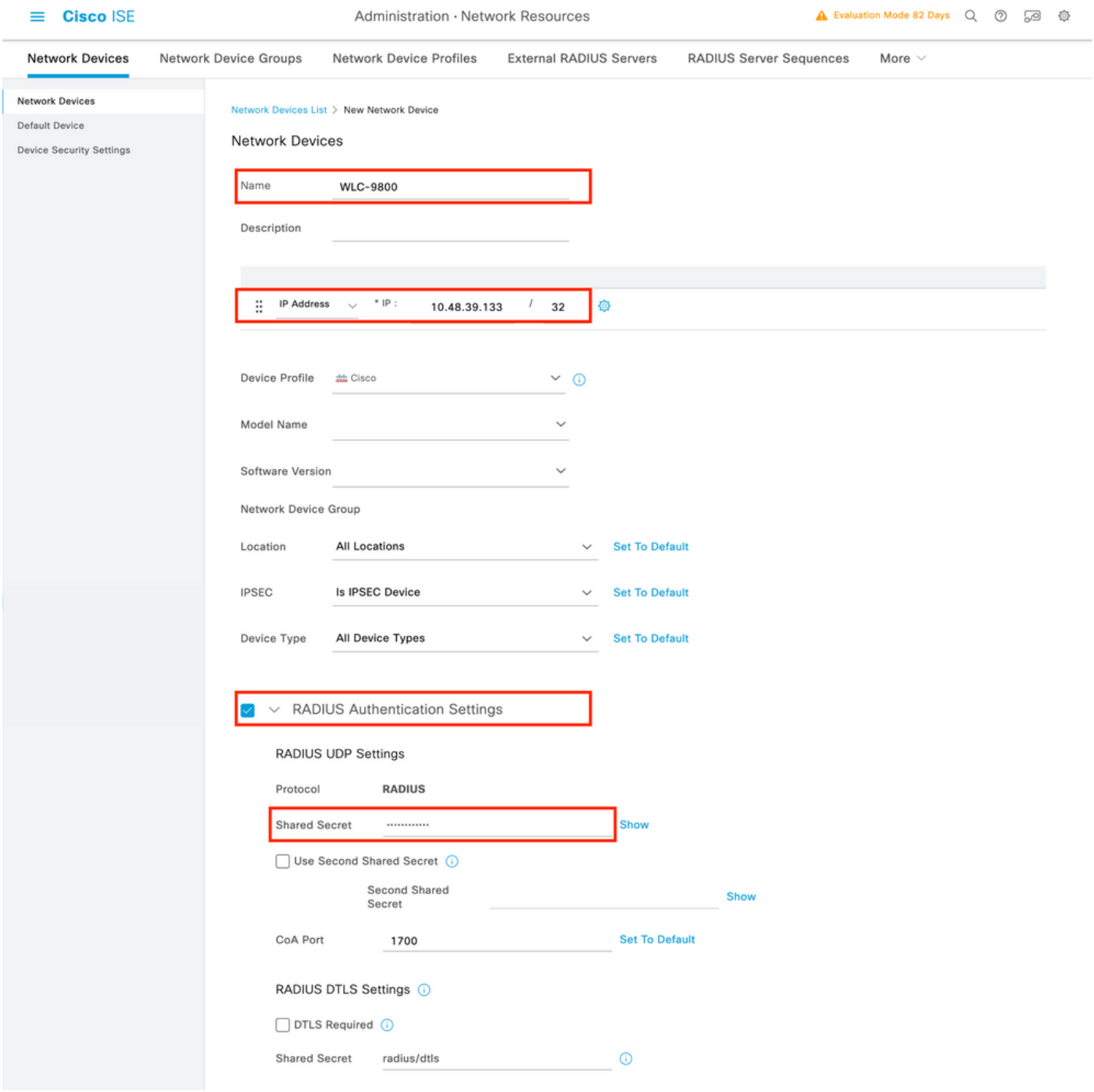
Paso 1. Configure el WLC como un dispositivo de red para RADIUS.

Desde la GUI:

Para declarar el WLC utilizado en la sección anterior como un dispositivo de red para RADIUS en ISE, navegue hasta Administration > Network Ressources > Network Devices y abra la ficha Network devices (Dispositivos de red), como se muestra en la siguiente imagen.



Para agregar un dispositivo de red, utilice el botón Add (Agregar), que abre el formulario de configuración del nuevo dispositivo de red.

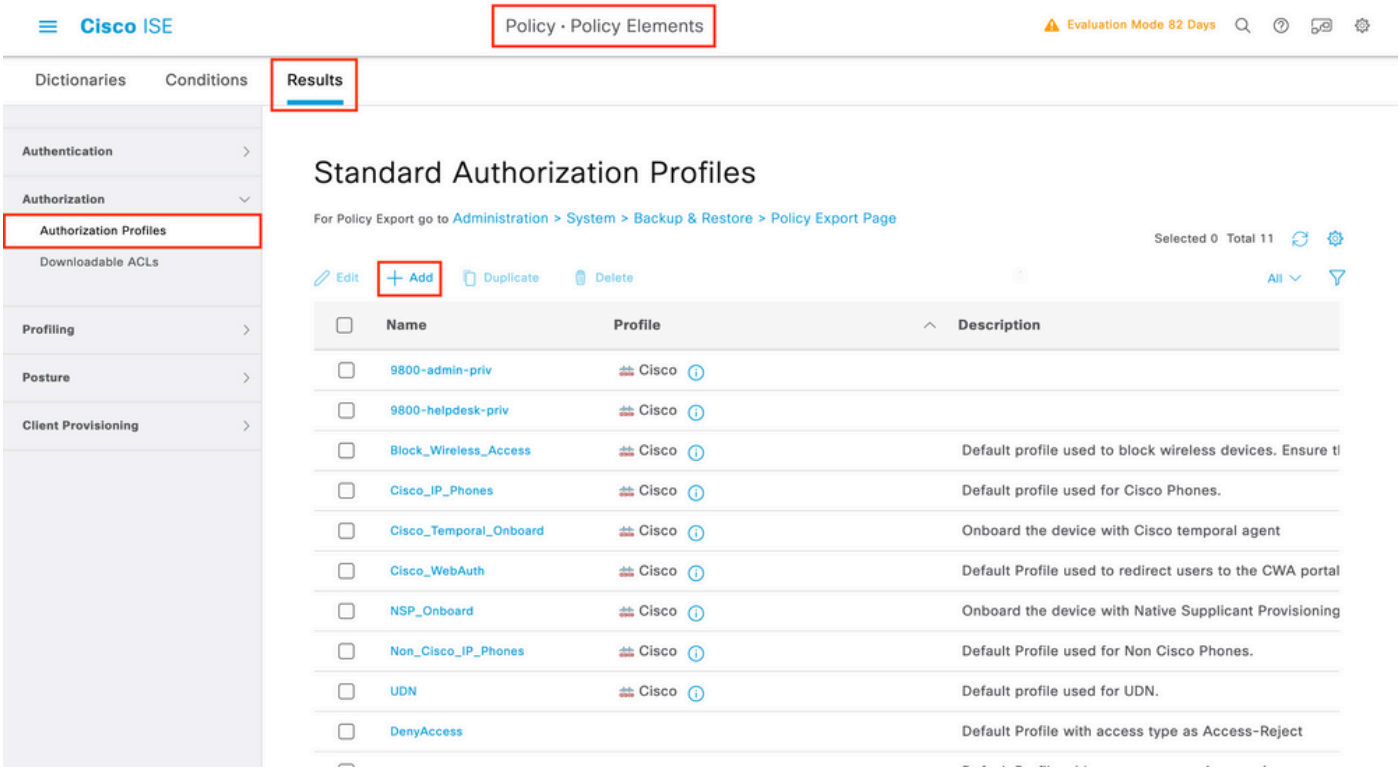


En la nueva ventana, proporcione un nombre para el dispositivo de red y agregue su dirección IP. Elija los ajustes de autenticación de RADIUS y configure el mismo secreto compartido de RADIUS que el que se utiliza en el WLC.

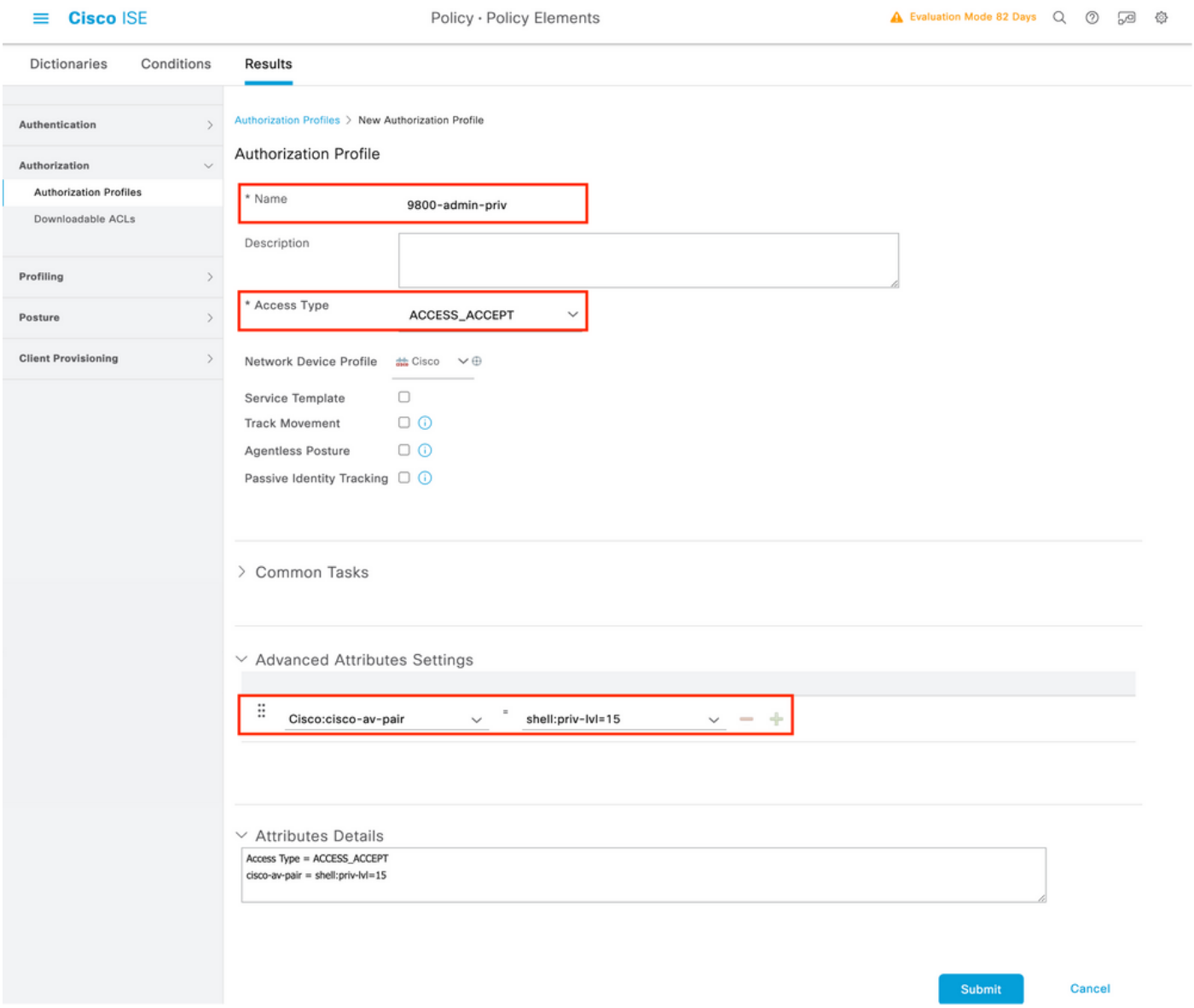
Paso 2. Cree un resultado de autorización para devolver el privilegio.

Desde la GUI:

Para tener derechos de acceso de administrador, el adminuser necesita tener un nivel de privilegio de 15, que permite acceder al intérprete de comandos exec. Por otro lado, el helpdeskuser no necesita acceso al shell exec prompt y, por lo tanto, se puede asignar con un nivel de privilegio inferior a 15. Para asignar el nivel de privilegio adecuado a los usuarios, se pueden utilizar perfiles de autorización. Estos se pueden configurar desde la ISE GUI Page Policy > Policy Elements > Results, en la pestaña Authorization > Authorization Profiles que se muestra en la siguiente imagen.



Para configurar un nuevo perfil de autorización, utilice el botón Agregar, que abre el formulario de configuración del nuevo perfil de autorización. Este formulario debe ser especialmente similar a este para configurar el perfil que se asigna a adminuser.



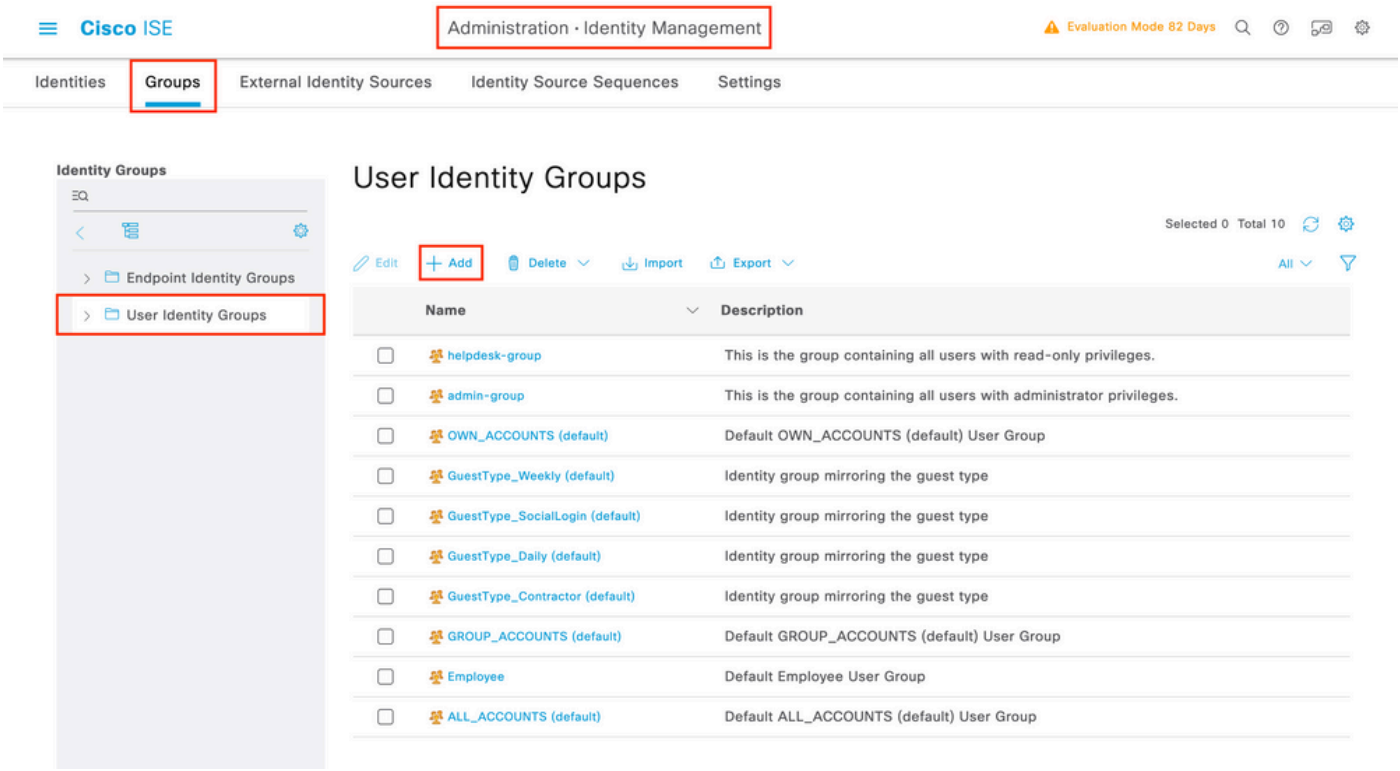
La configuración mostró el nivel de privilegio de concesiones 15 a cualquier usuario al que esté asociado. Como se ha mencionado anteriormente, este es el comportamiento esperado para el adminuser que se crea durante el paso siguiente. Sin embargo, el helpdeskuser debe tener un nivel de privilegio inferior y, por lo tanto, debe crearse un segundo elemento de política.

El elemento de directiva para el helpdeskuser es similar al creado justo encima, excepto que la cadena shell:priv-lvl=15 debe cambiarse a shell:priv-lvl=X y reemplazar X con el nivel de privilegio deseado. En este ejemplo, se utiliza 1.

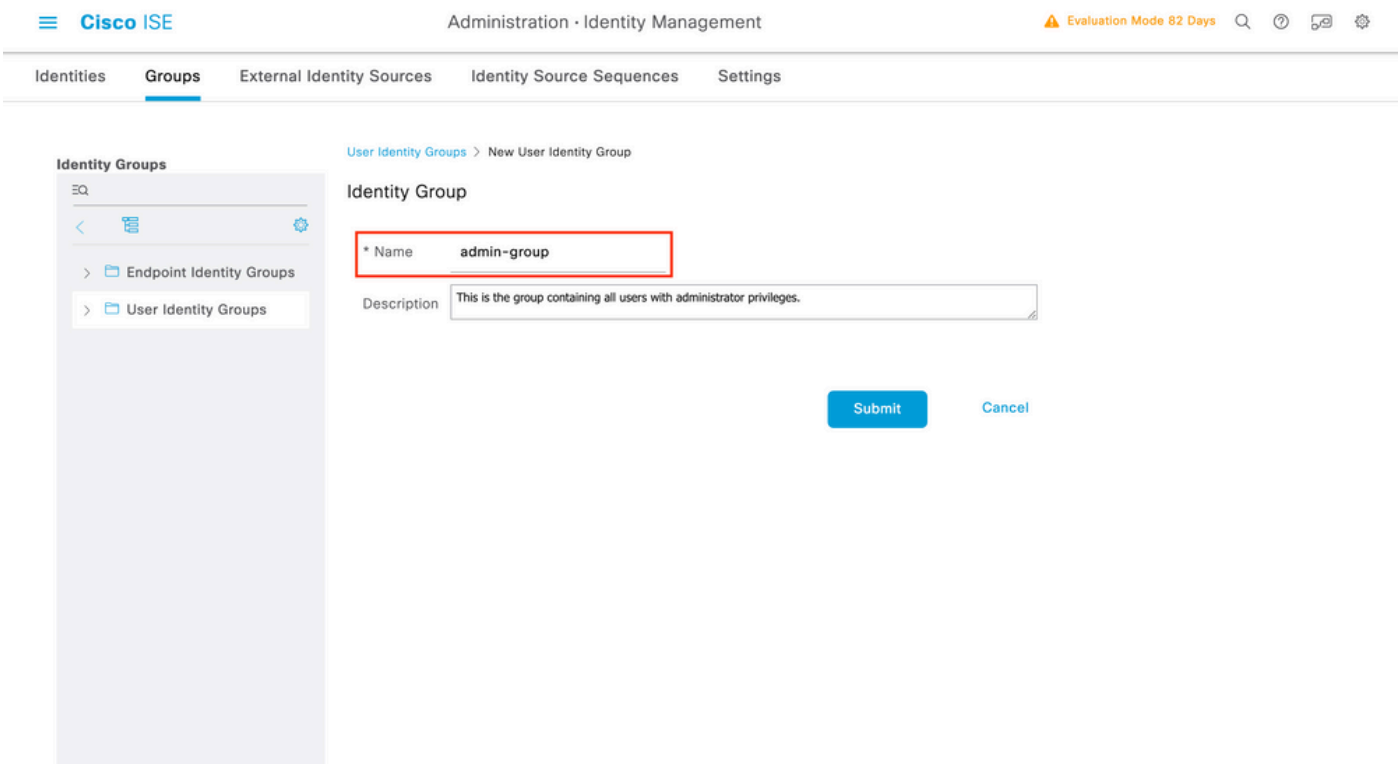
Paso 3. Cree grupos de usuarios en ISE.

Desde la GUI:

Los grupos de usuarios de ISE se crean en la ficha Grupos de identidades de usuario de Administration > Identity Management > Groups GUI Page, que se muestra en la captura de pantalla.



Para crear un nuevo usuario, utilice el botón Agregar, que abre el formulario de configuración del nuevo grupo de identidades de usuario como se muestra.

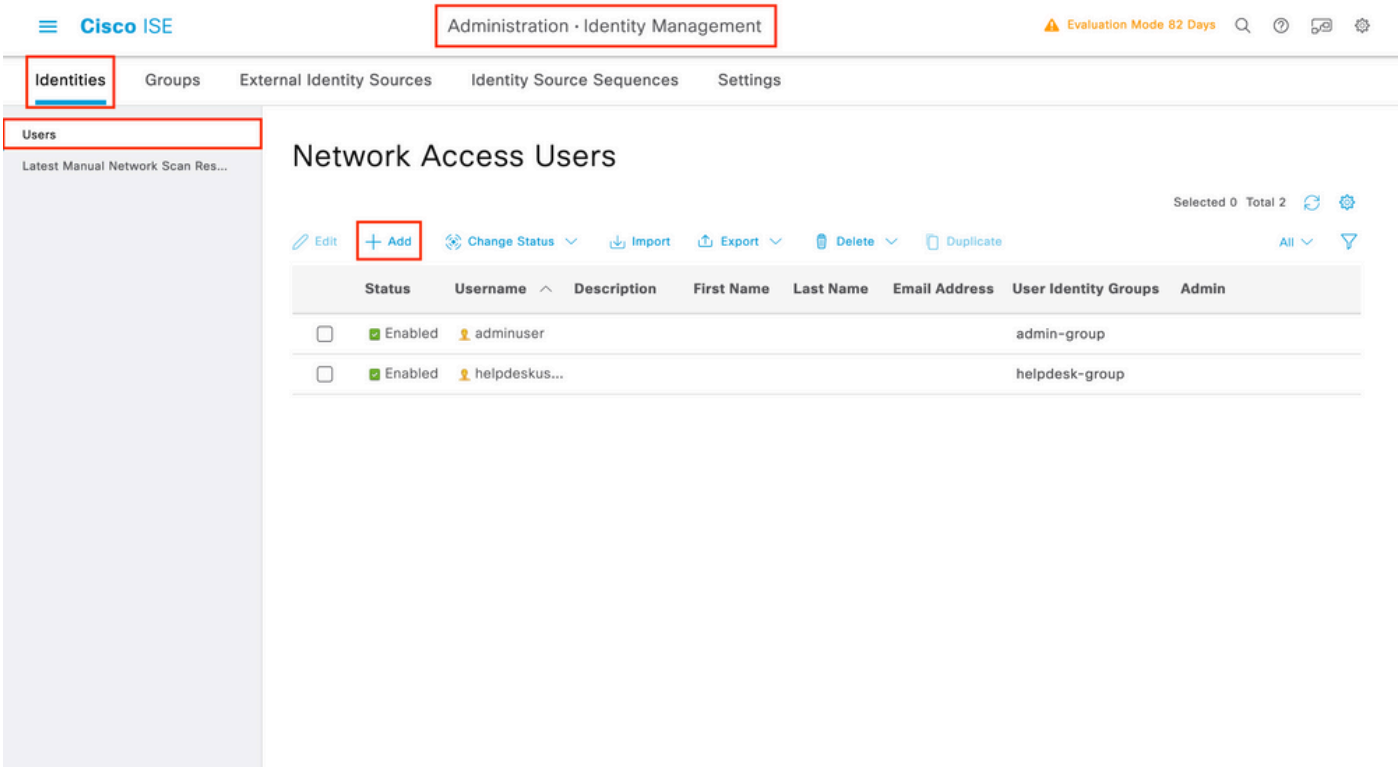


Proporcione el nombre del grupo que se ha creado. Cree los dos grupos de usuarios mencionados anteriormente, a saber, admin-group y helpdesk-group.

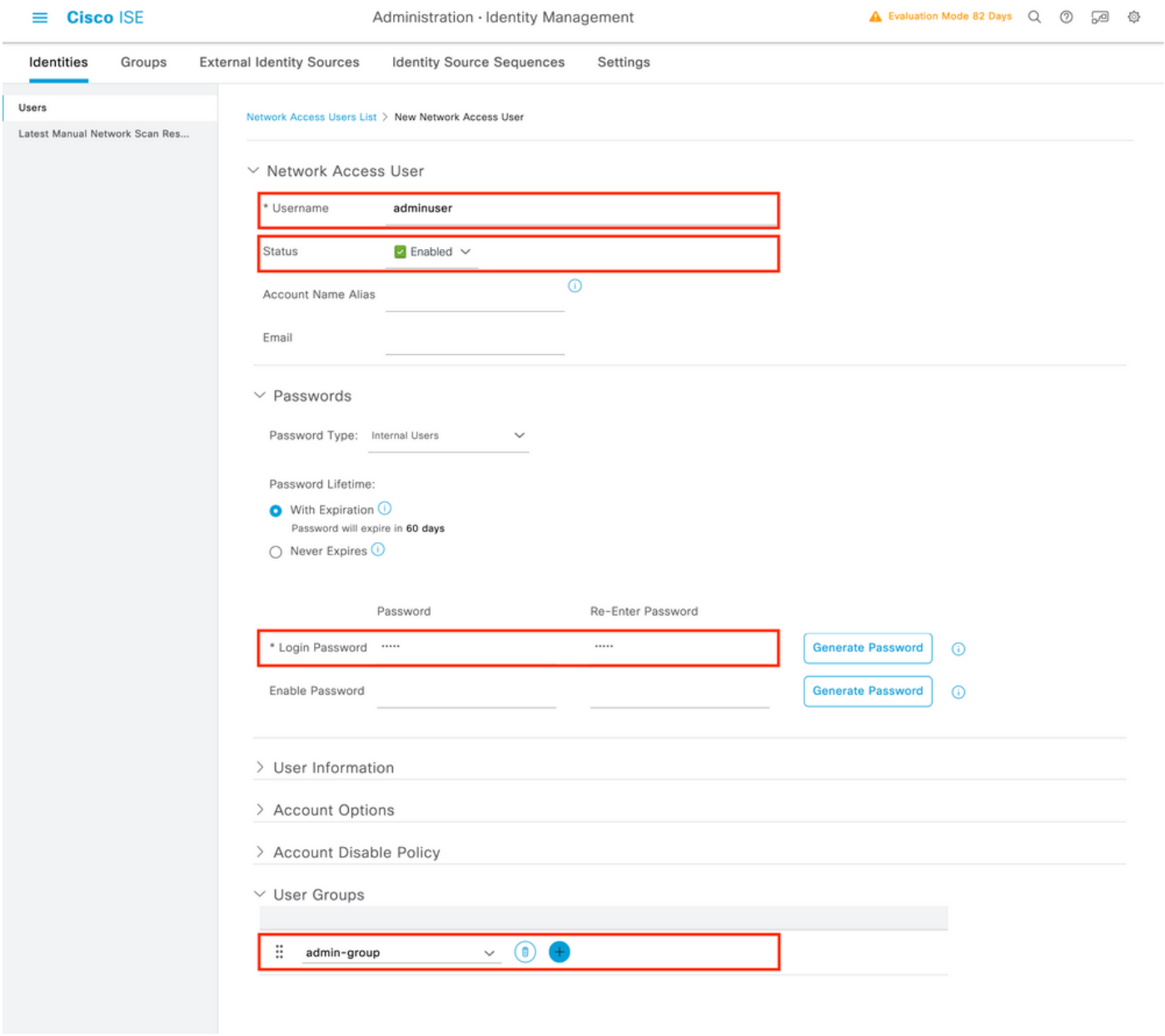
Paso 4. Cree usuarios en ISE.

Desde la GUI:

Los usuarios de ISE se crean en la ficha Users of the Administration > Identity Management > Identities GUI Page (Usuarios de), que se muestra en la captura de pantalla.



Para crear un nuevo usuario, utilice el botón Add (Agregar) para abrir el nuevo formulario de configuración de usuario de acceso a la red, como se muestra.



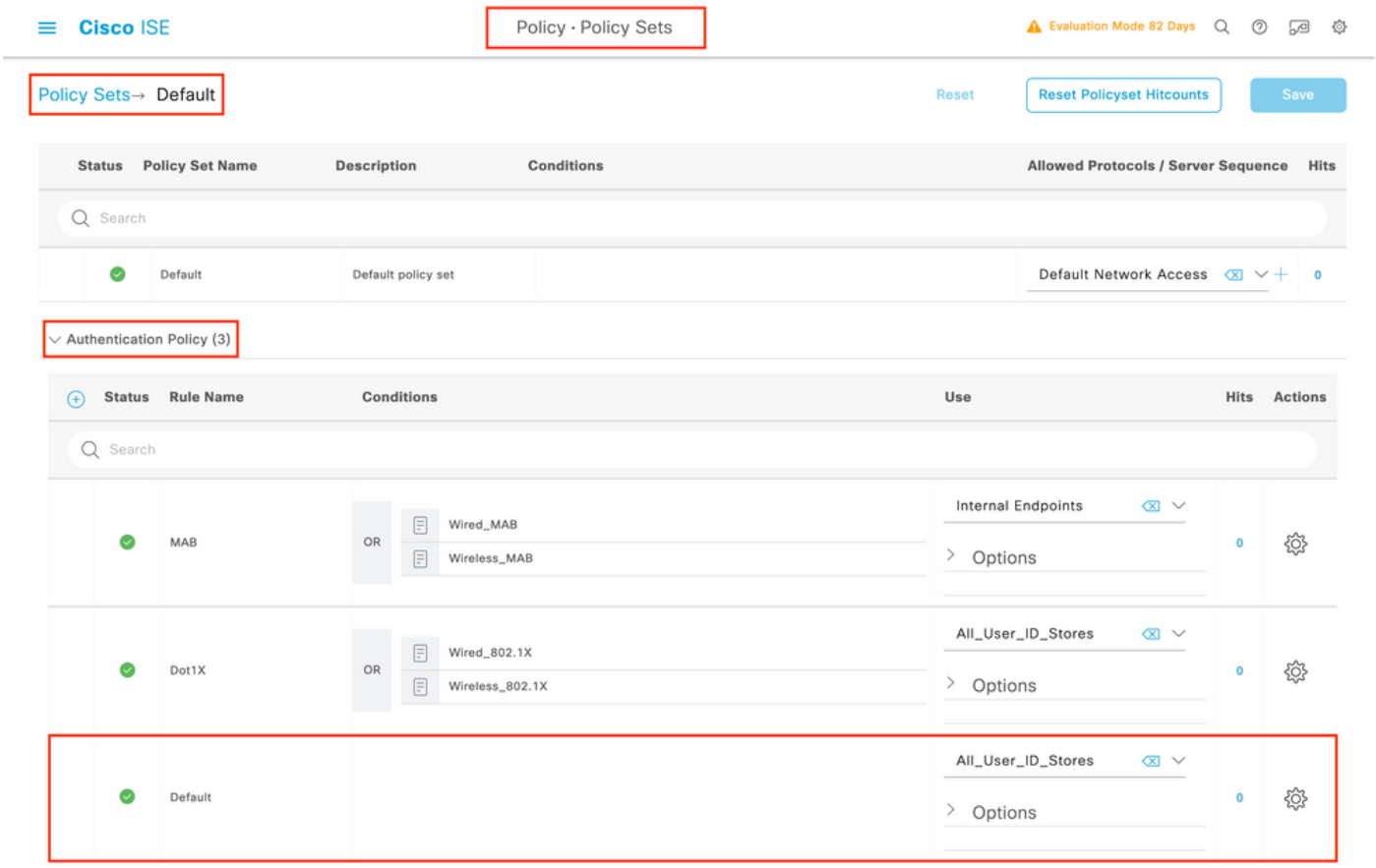
Proporcione las credenciales a los usuarios, a saber, su nombre de usuario y contraseña, que son los que se utilizan para autenticar en el WLC. Además, asegúrese de que el estado del usuario es Enabled. Por último, agregue el usuario a su grupo relacionado, que se ha creado en el paso 4, con el menú desplegable Grupos de usuarios al final del formulario.

Cree los dos usuarios mencionados anteriormente, a saber, el adminuser y helpdeskuser.

Paso 5. Autentique a los usuarios.

Desde la GUI:

En esta situación, la política de autenticación de los conjuntos de políticas predeterminados de ISE, que ya está preconfigurada, permite el acceso a la red predeterminado. Este conjunto de políticas se puede ver en la páginaPolicy > Policy Sets de la GUI de ISE, como se muestra en esta imagen. Por lo tanto, no hay necesidad de cambiarlo.

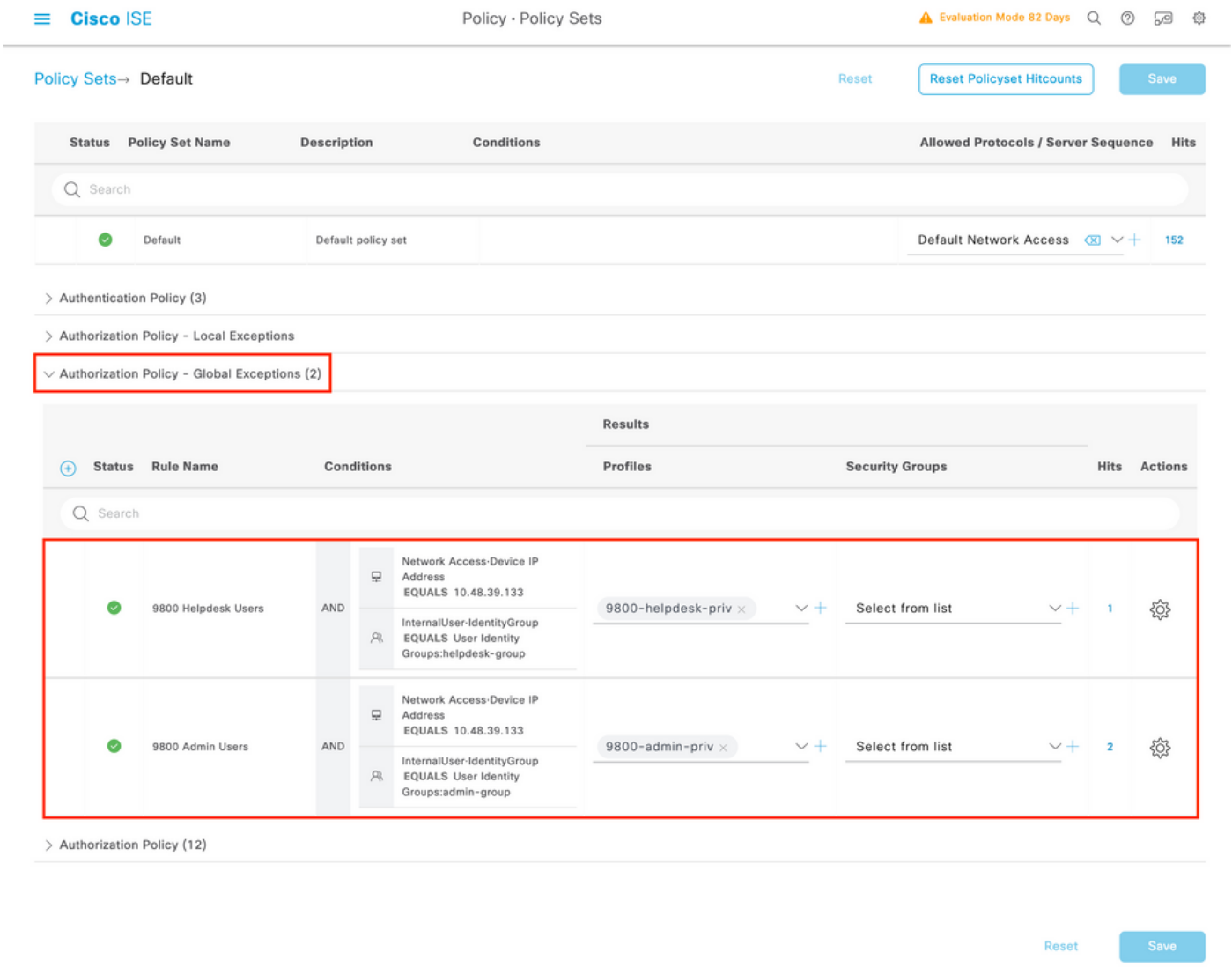


Paso 6. Autorizar a los usuarios.

Desde la GUI:

Una vez que el intento de inicio de sesión supera la política de autenticación, debe estar autorizado e ISE debe devolver el perfil de autorización creado anteriormente (aceptación de permiso, junto con el nivel de privilegio).

En este ejemplo, los intentos de inicio de sesión se filtran en función de la dirección IP del dispositivo (que es la dirección IP del WLC) y distinguen el nivel de privilegio que se otorgará en función del grupo al que pertenece un usuario. Otro enfoque válido es filtrar los usuarios en función de sus nombres de usuario, ya que cada grupo solo contiene un usuario en este ejemplo.



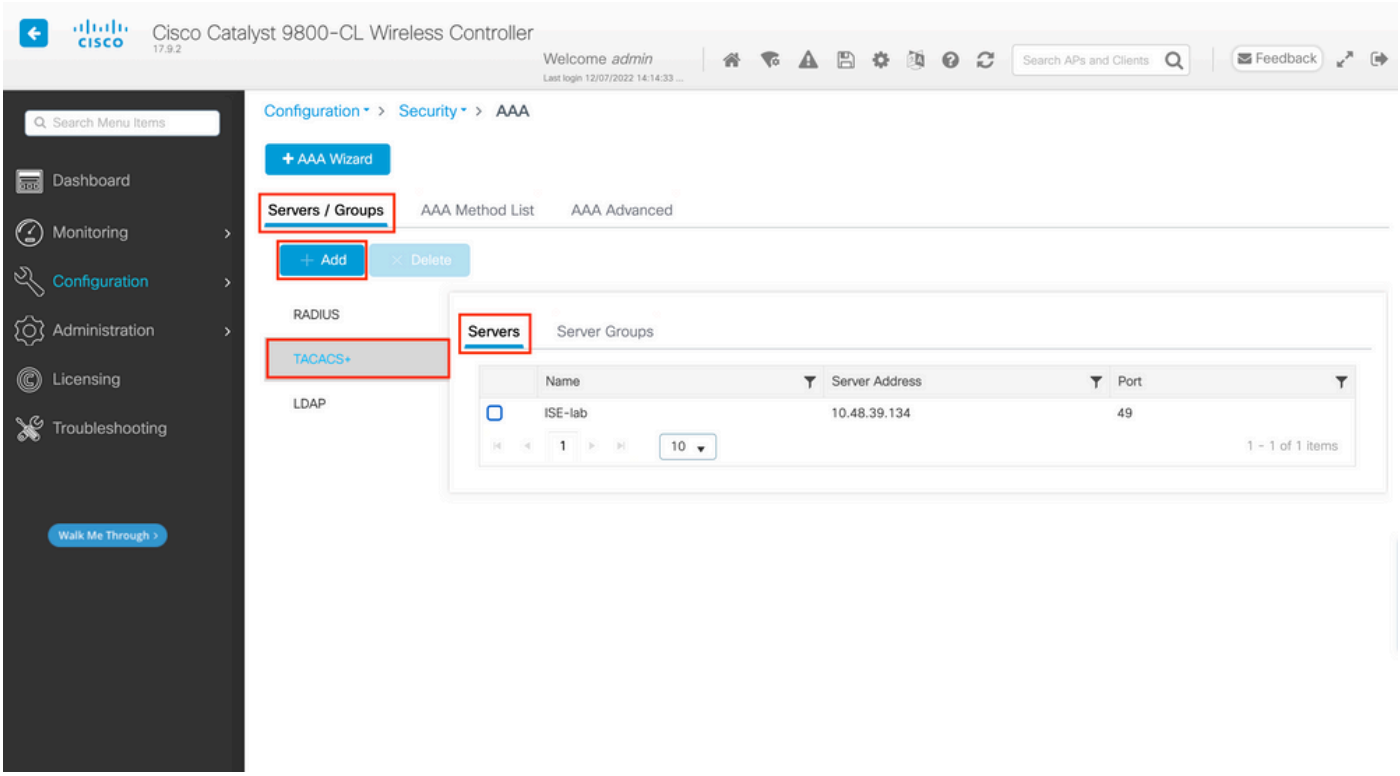
Después de que este paso se haya completado, las credenciales configuradas para adminuser y helpdesk usuario se pueden utilizar para autenticar en el WLC vía la GUI o a través de Telnet/SSH.

Configuración de TACACS+ WLC

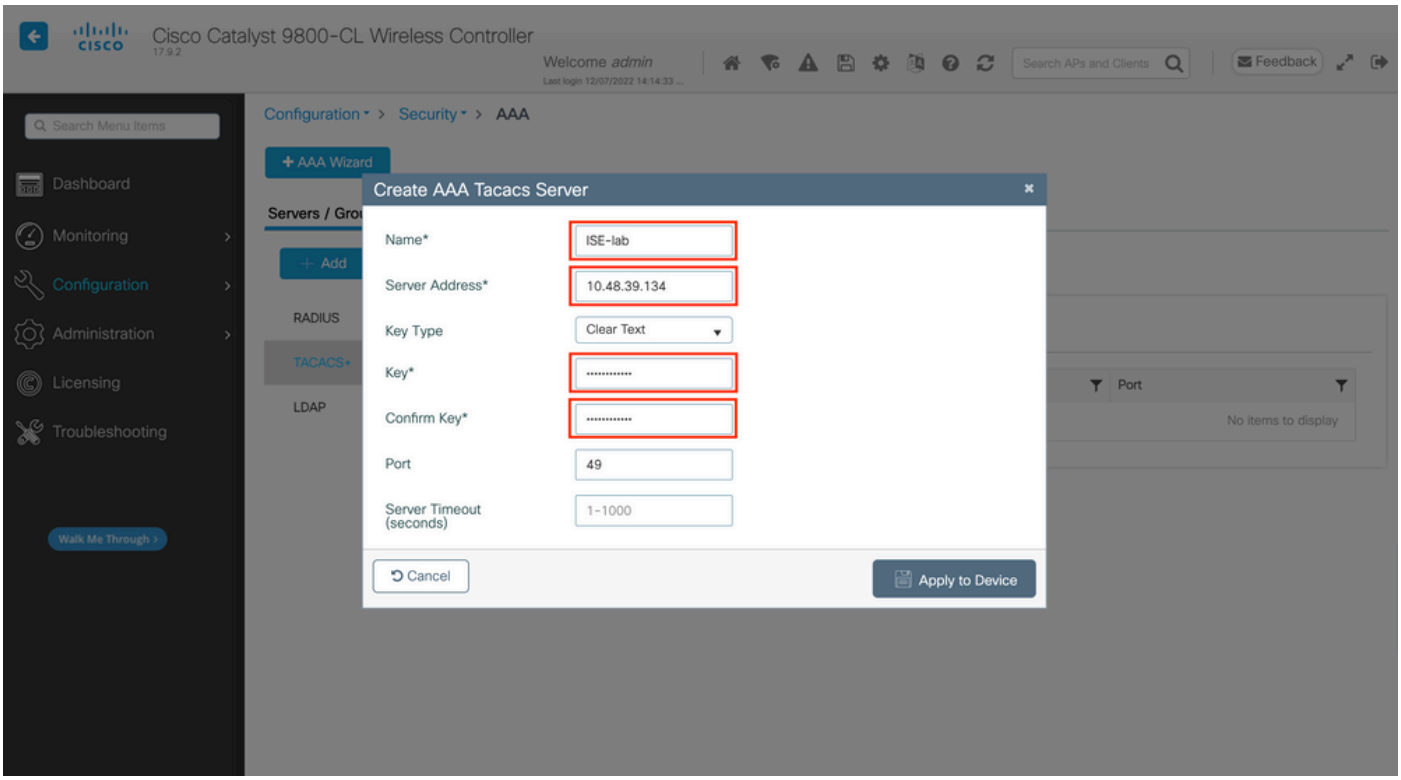
Paso 1. Declare el servidor TACACS+.

Desde la GUI:

En primer lugar, cree el ISE del servidor Tacacs+ en el WLC. Esto se puede hacer desde la pestaña Servers/Groups > TACACS+ > Servers de la página GUI WLC accesible en el https://<WLC-IP>/webui/#/aaa, o si navega a Configuration > Security > AAA, como se muestra en esta imagen.



Para agregar un servidor TACACS en el WLC, haga clic en el botón Add enmarcado en rojo en la imagen de arriba. Se abrirá la ventana emergente representada.



Cuando se abra la ventana emergente, proporcione el nombre del servidor (no tiene que coincidir con el nombre del sistema ISE), su dirección IP, la clave compartida, el puerto utilizado y el tiempo de espera.

En esta ventana emergente, debe proporcionar:

- El nombre del servidor (tenga en cuenta que no tiene que coincidir con el nombre del sistema de ISE)

- La dirección IP del servidor
- El secreto compartido entre el WLC y el servidor TACACS+

Se pueden configurar otros parámetros, como los puertos utilizados para la autenticación y la contabilidad, pero estos no son obligatorios y se dejan como predeterminados para esta documentación.

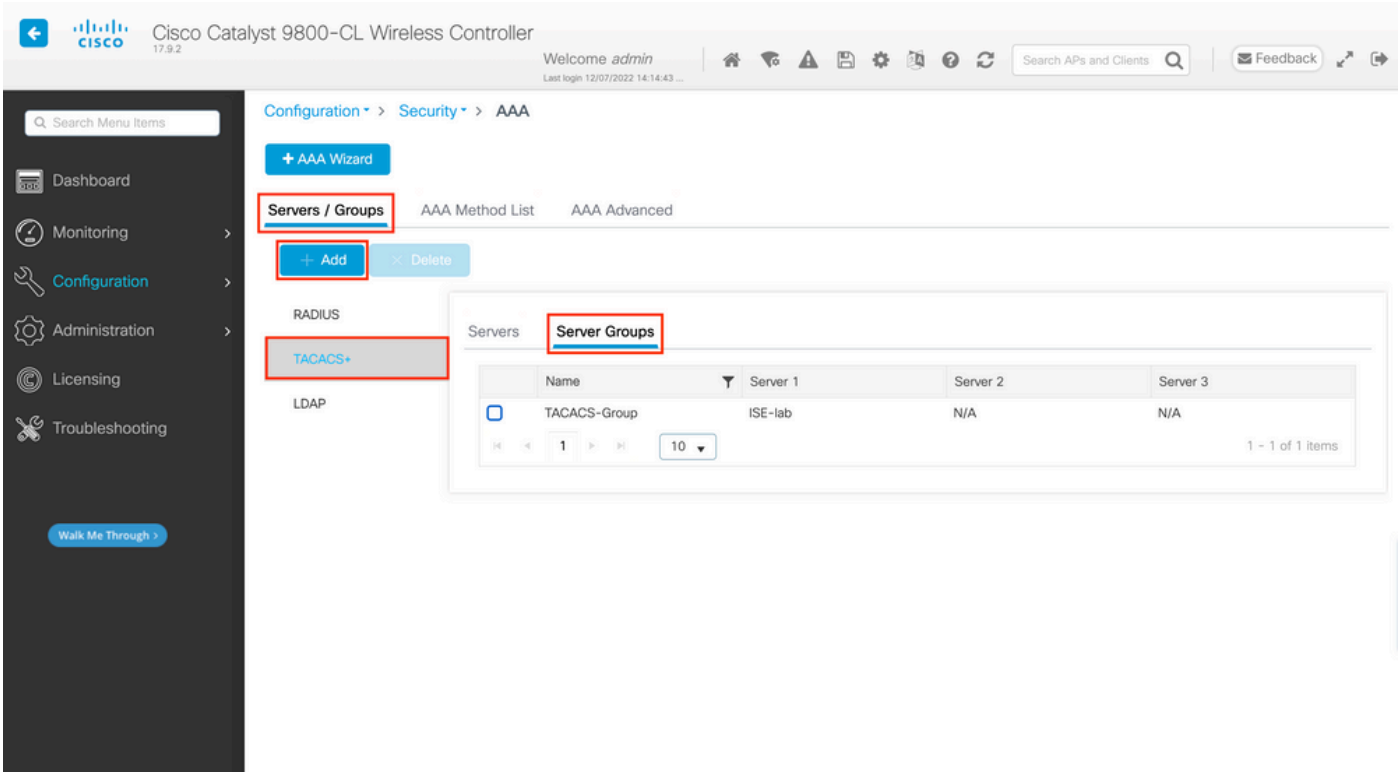
Desde CLI:

```
<#root>

WLC-9800(config)#tacacs server

ISE-lab

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

10.48.39.134

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

Cisco123
```

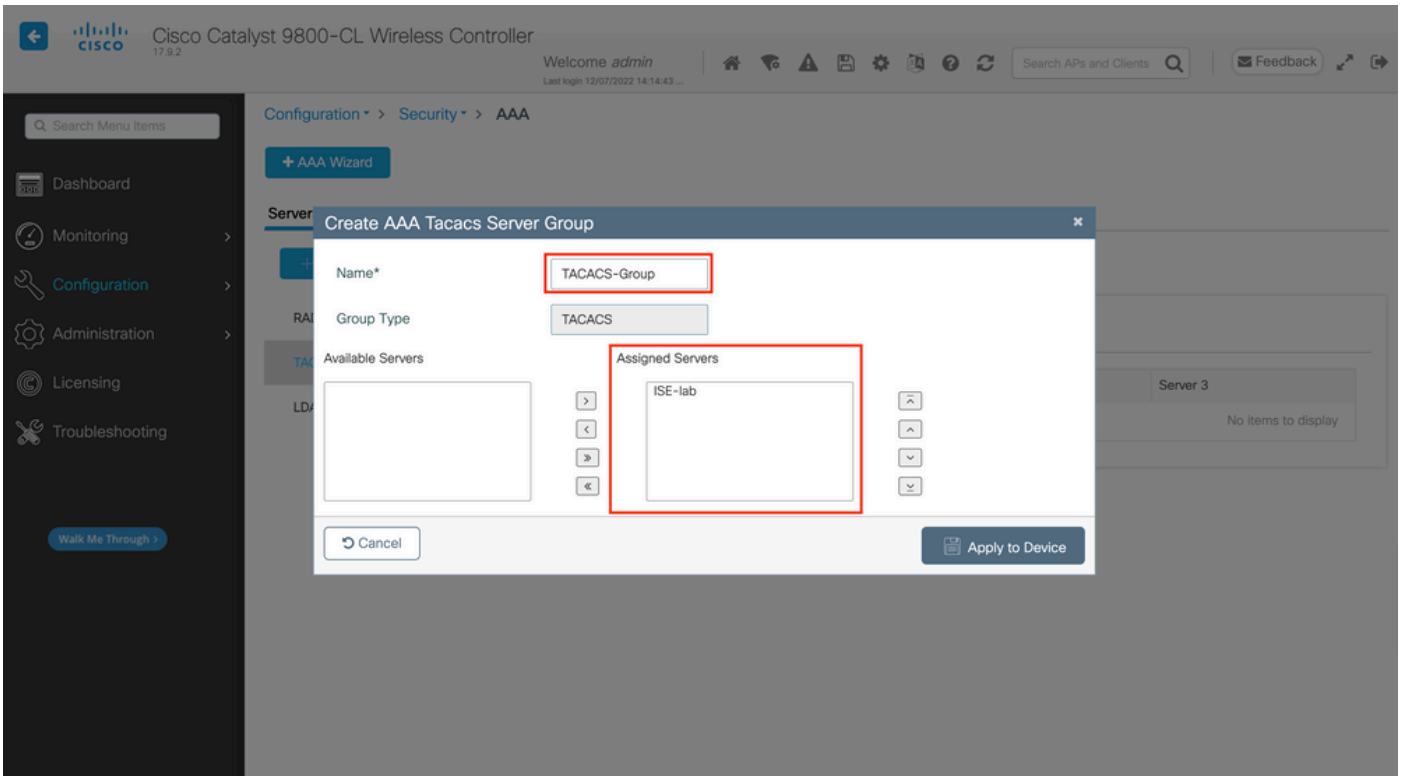
Paso 2. Asigne el servidor TACACS+ a un grupo de servidores.

Desde la GUI:

En caso de que tenga varios servidores TACACS+ que se puedan utilizar para la autenticación, se recomienda asignar todos estos servidores al mismo grupo de servidores. El WLC entonces se ocupa del balanceo de carga de las diferentes autenticaciones entre los servidores en el grupo de servidores. Los grupos de servidores TACACS+ se configuran desde la Servers/Groups > TACACS > Server Groups pestaña desde la misma página de GUI que la mencionada en el Paso 1, que se muestra en la imagen.



En cuanto a la creación del servidor, aparece una ventana emergente al hacer clic en el botón Agregar enmarcado en la imagen anterior, que se representa en la imagen.



En la ventana emergente, asigne un nombre al grupo y mueva los servidores deseados a la lista Servidores asignados.

Desde CLI:

```
<#root>
```

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

TACACS-Group

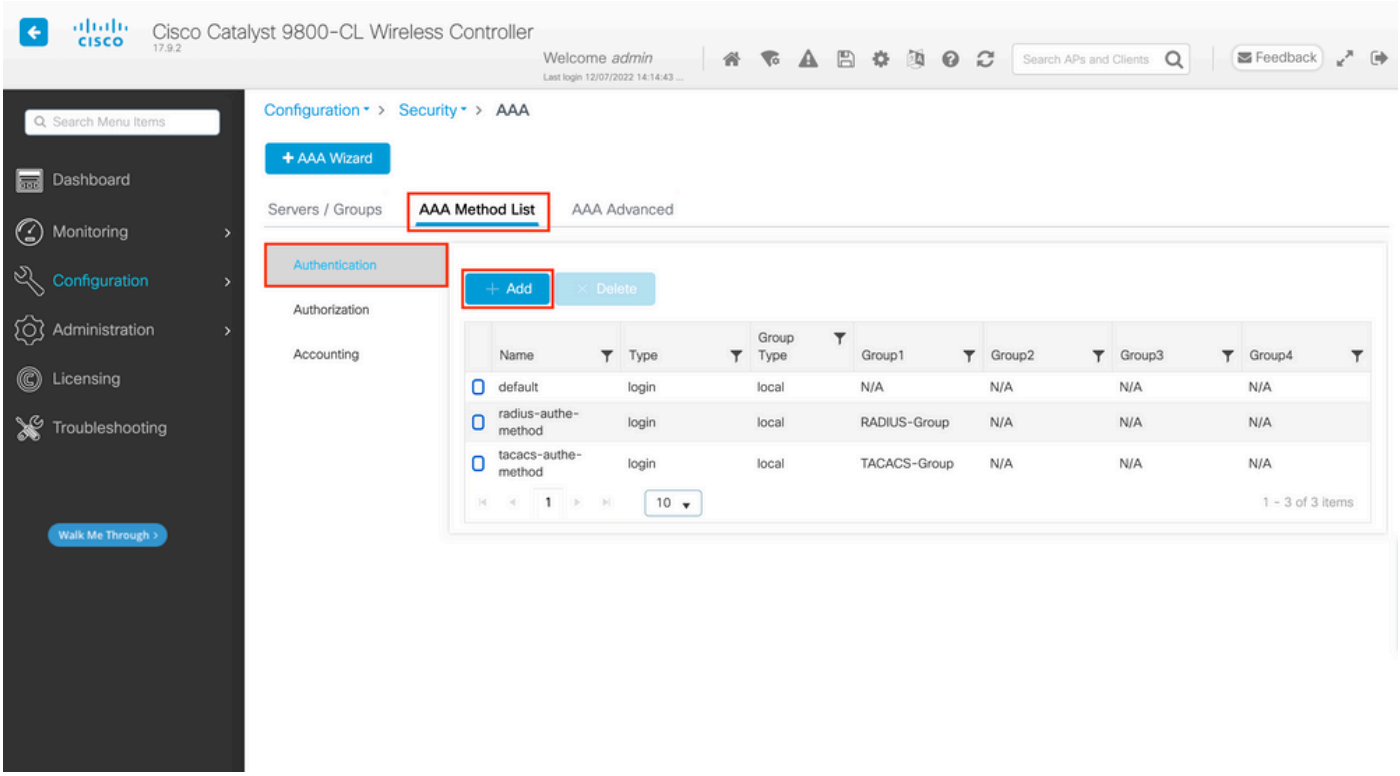
```
WLC-9800(config-sg-tacacs+)#server name
```

ISE-lab

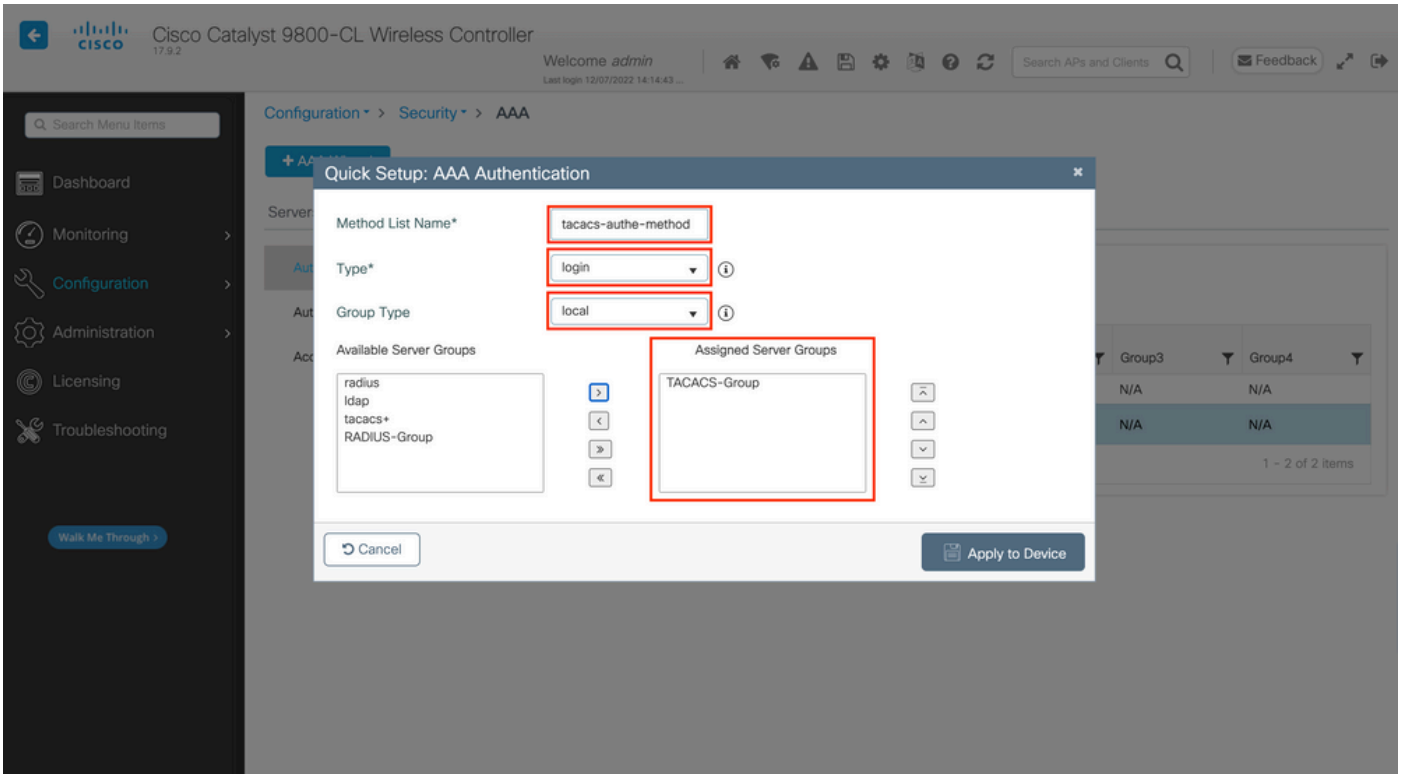
Paso 3. Cree un método de registro de autenticación AAA que apunte al grupo de servidores TACACS+.

Desde la GUI:

En la página GUIhttps://<WLC-IP>/webui/#/aaa, vaya a la AAA Method List > Authentication ficha y cree un método de autenticación como se muestra en la imagen.



Como es habitual, cuando utiliza el botón Add (Agregar) para crear un método de autenticación, aparece una ventana emergente de configuración, similar a la que se muestra en esta imagen.



En esta ventana emergente, proporcione un nombre para el método, elija Tipo como login y agregue el servidor de grupos creado en el paso anterior a la lista Grupos de servidores asignados. Con respecto al campo Tipo de grupo, son posibles varias configuraciones.

- Si elige el tipo de grupo como local, el WLC primero verifica si las credenciales del usuario existen localmente y después vuelve al grupo del servidor.
- Si elige el tipo de grupo como grupo y no marca la opción Volver a local, el WLC verifica solamente las credenciales del usuario contra el grupo del servidor.
- Si elige Group Type como grupo y marca la opción Fallback to local, el WLC verifica las credenciales del usuario contra el grupo del servidor y consulta la base de datos local solamente si el servidor no responde. Si el servidor envía un rechazo, el usuario se autenticará, aunque pueda existir en la base de datos local.

Desde CLI:

Si desea que las credenciales de usuario se comprueben con un grupo de servidores sólo si no se encuentran primero localmente, utilice:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

```
 local group
```

TACACS-Group

Si desea que las credenciales de usuario sólo se comprueben con un grupo de servidores, utilice:

```
<#root>

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

tacacs-authe-method

```
 group
```

TACACS-Group

Si desea que las credenciales de usuario se comprueben con un grupo de servidores y si esta última no responde con una entrada local, utilice:

```
<#root>
```

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

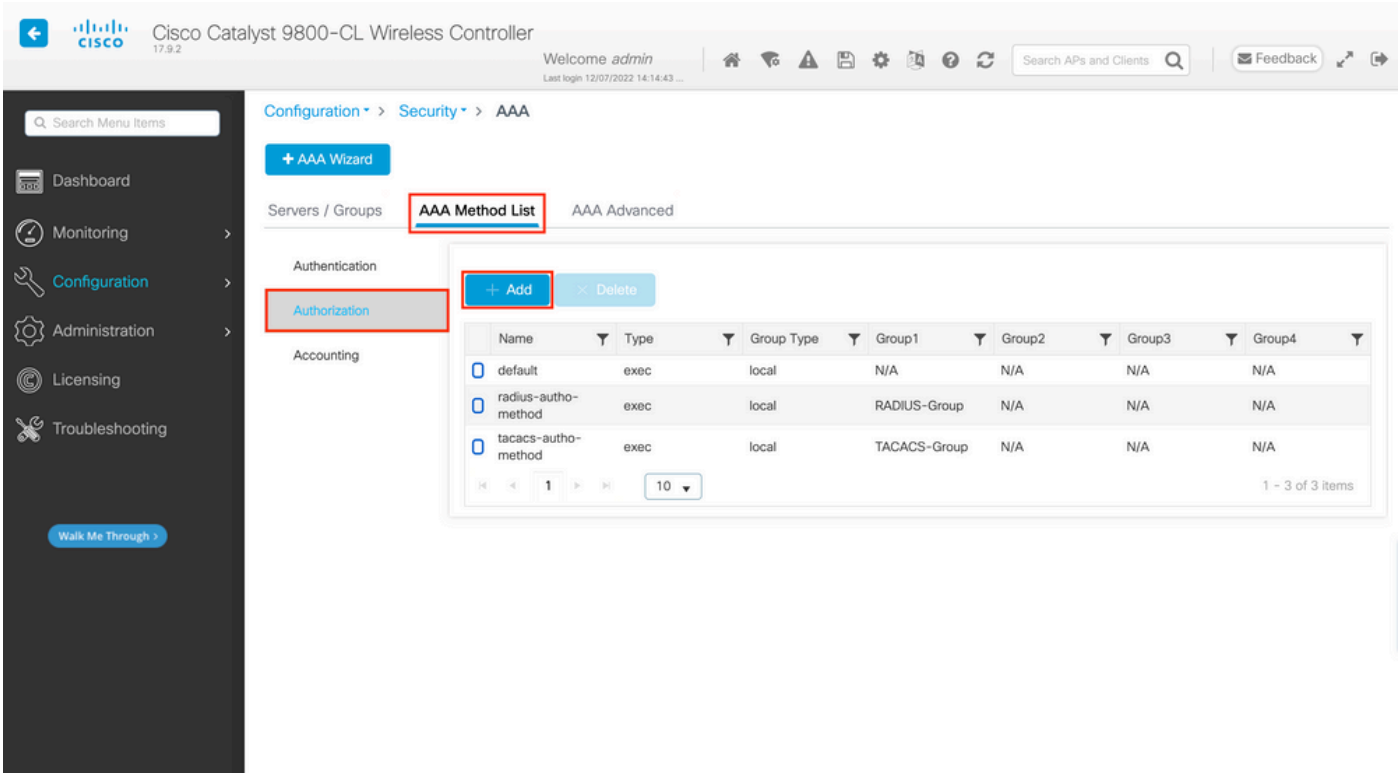
local

En esta configuración de ejemplo, hay algunos usuarios que solo se crean localmente y otros usuarios solo en el servidor ISE, por lo tanto, hacen uso de la primera opción.

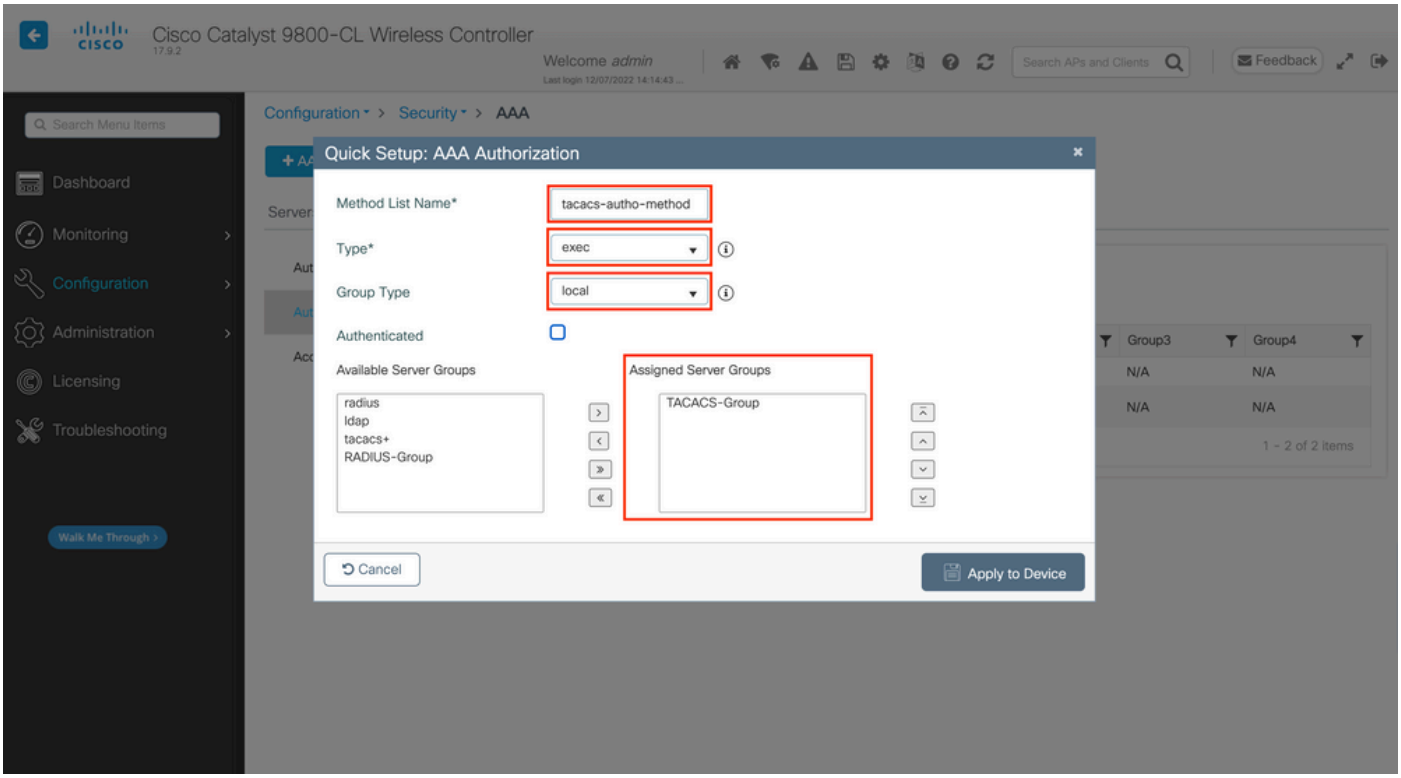
Paso 4. Cree un método exec de autorización AAA que apunte al grupo de servidores TACACS+.

Desde la GUI:

El usuario también tiene que estar autorizado para que se le conceda acceso. En la página GUIConfiguration > Security > AAA, vaya a la AAA Method List > Authorization ficha y cree un método de autorización como se muestra en la imagen.



Una ventana emergente de configuración de método de autorización similar a la representada aparece cuando se agrega una nueva con el botón Add (Agregar).



En esta ventana emergente de configuración, proporcione un nombre para el método de autorización, elija Type as exec y utilice el mismo orden de Group Type que el utilizado para el método de autenticación en el paso anterior.

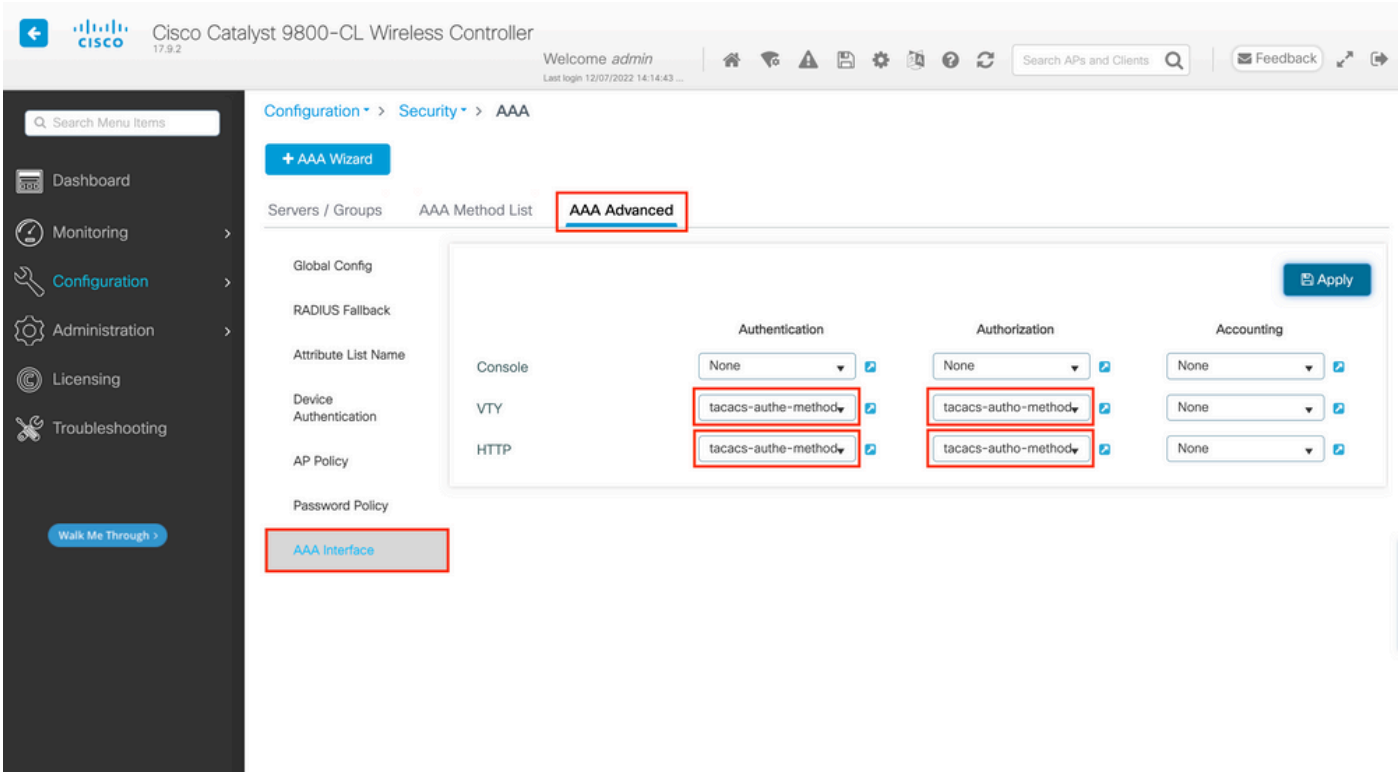
Desde CLI:

```
<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

 local group

TACACS-Group
```

Paso 5. Asigne los métodos a las configuraciones HTTP y a las líneas VTY utilizadas para Telnet/SSH.

Desde la GUI:

Los métodos de autenticación y autorización creados se pueden utilizar para la conexión de usuario HTTP y/o Telnet/SSH, que se puede configurar desde la AAA Advanced > AAA Interface ficha todavía desde la página WLC de GUI accesible en https://<WLC-IP>/webui/#/aaa, como se muestra en la imagen.



Desde CLI:

Para la autenticación GUI:

```
<#root>

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

tacacs-authe-method

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

tacacs-autho-method
```

Para autenticación Telnet/SSH:

<#root>

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

tacacs-authe-method

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

tacacs-autho-method

Tenga en cuenta que cuando se realizan cambios en las configuraciones HTTP, es mejor reiniciar los servicios HTTP y HTTPS. Esto se puede lograr con estos comandos.

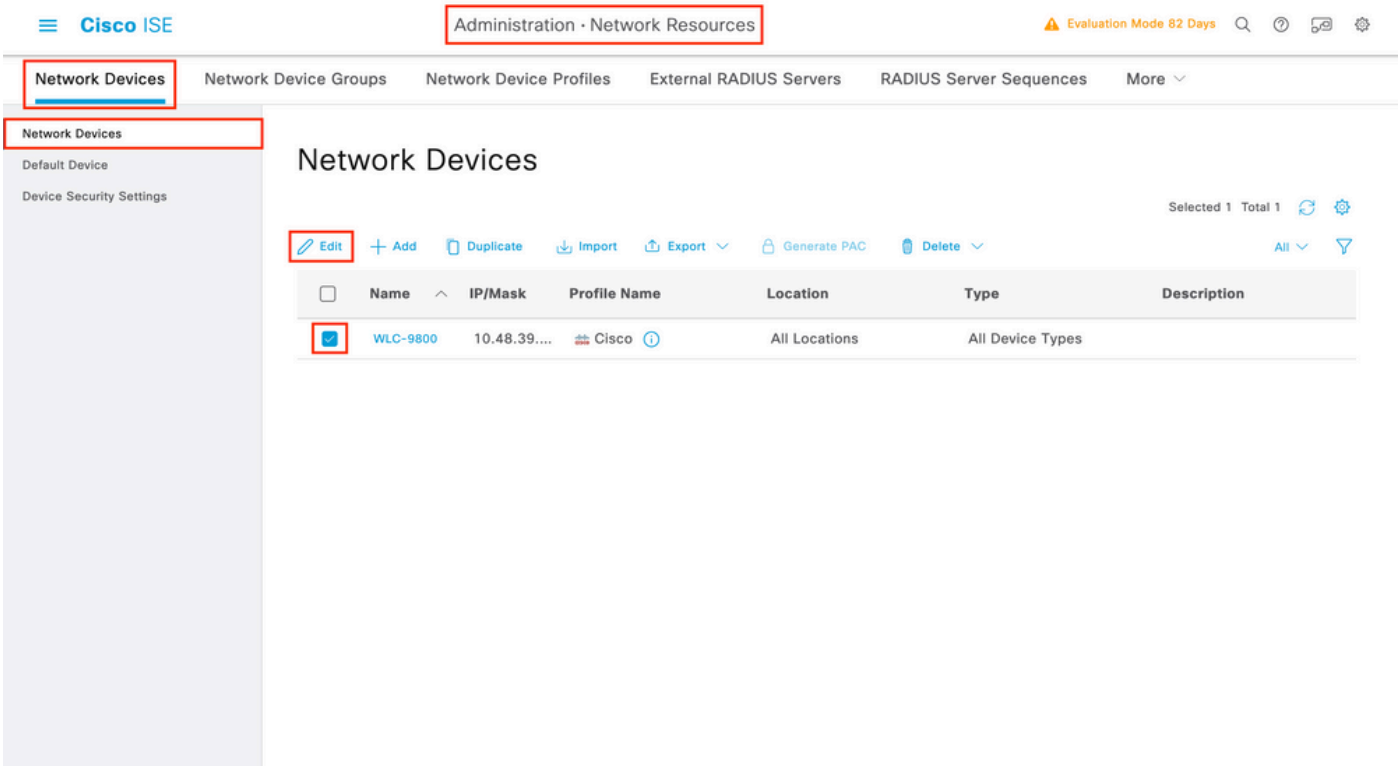
```
WLC-9800(config)#no ip http server
WLC-9800(config)#no ip http secure-server
WLC-9800(config)#ip http server
WLC-9800(config)#ip http secure-server
```

Configuración de ISE de TACACS+

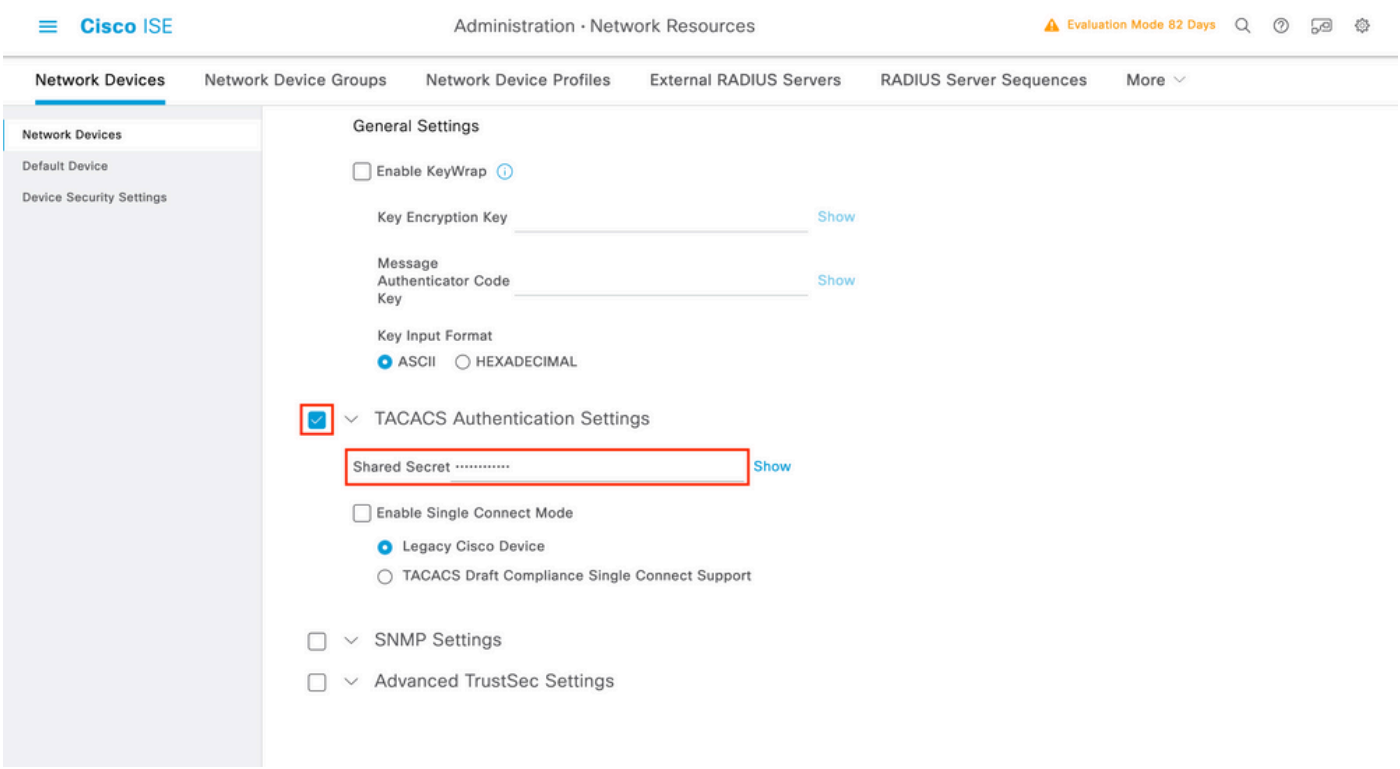
Paso 1. Configure el WLC como un dispositivo de red para TACACS+.

Desde la GUI:

Para declarar el WLC utilizado en la sección anterior como un dispositivo de red para RADIUS en ISE, navegue hasta Administration > Network Resources > Network Devices y abra la ficha Network devices (Dispositivos de red), como se muestra en esta imagen.

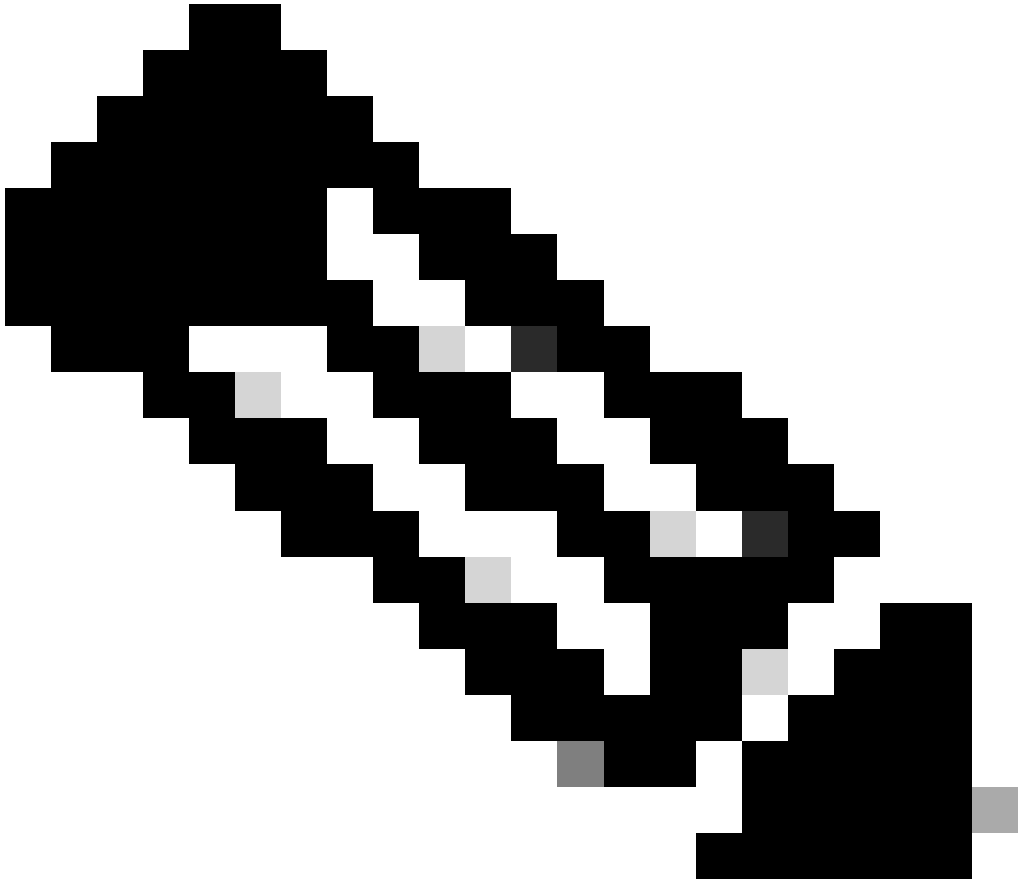


En este ejemplo, el WLC ya se ha agregado para la autenticación RADIUS (consulte el Paso 1 de la sección Configuración de RADIUS ISE). Por lo tanto, su configuración simplemente necesita ser modificada para configurar la autenticación TACACS, que se puede hacer cuando usted elige el WLC en la lista de dispositivos de red y hace clic en el botón Edit. Esto abre el formulario de configuración del dispositivo de red como se muestra en esta imagen.



Una vez que se haya abierto la nueva ventana, desplácese hacia abajo hasta la sección Configuración de autenticación TACACS, habilite estas configuraciones y agregue el secreto compartido ingresado durante el Paso 1 de la sección Configuración de TACACS+ WLC.

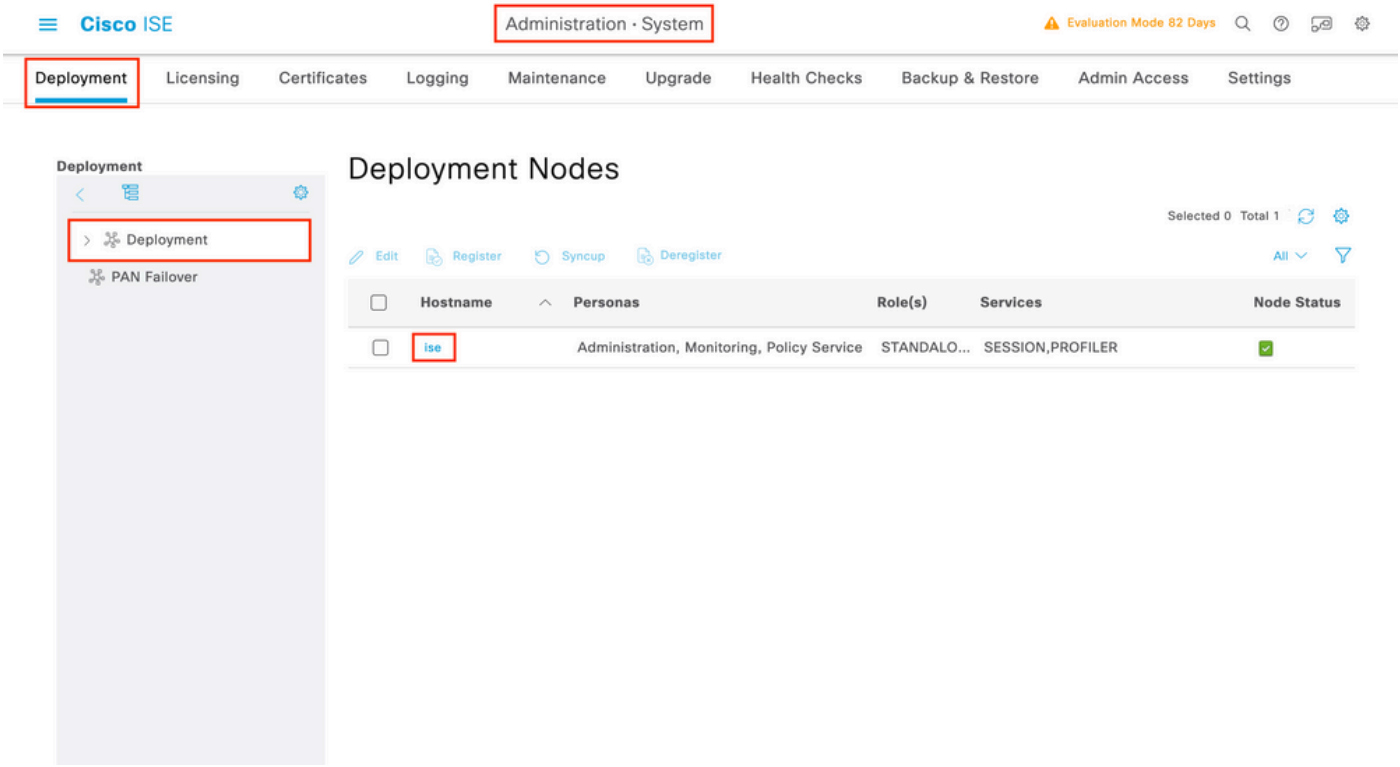
Paso 2. Active la función Device Admin para el nodo.



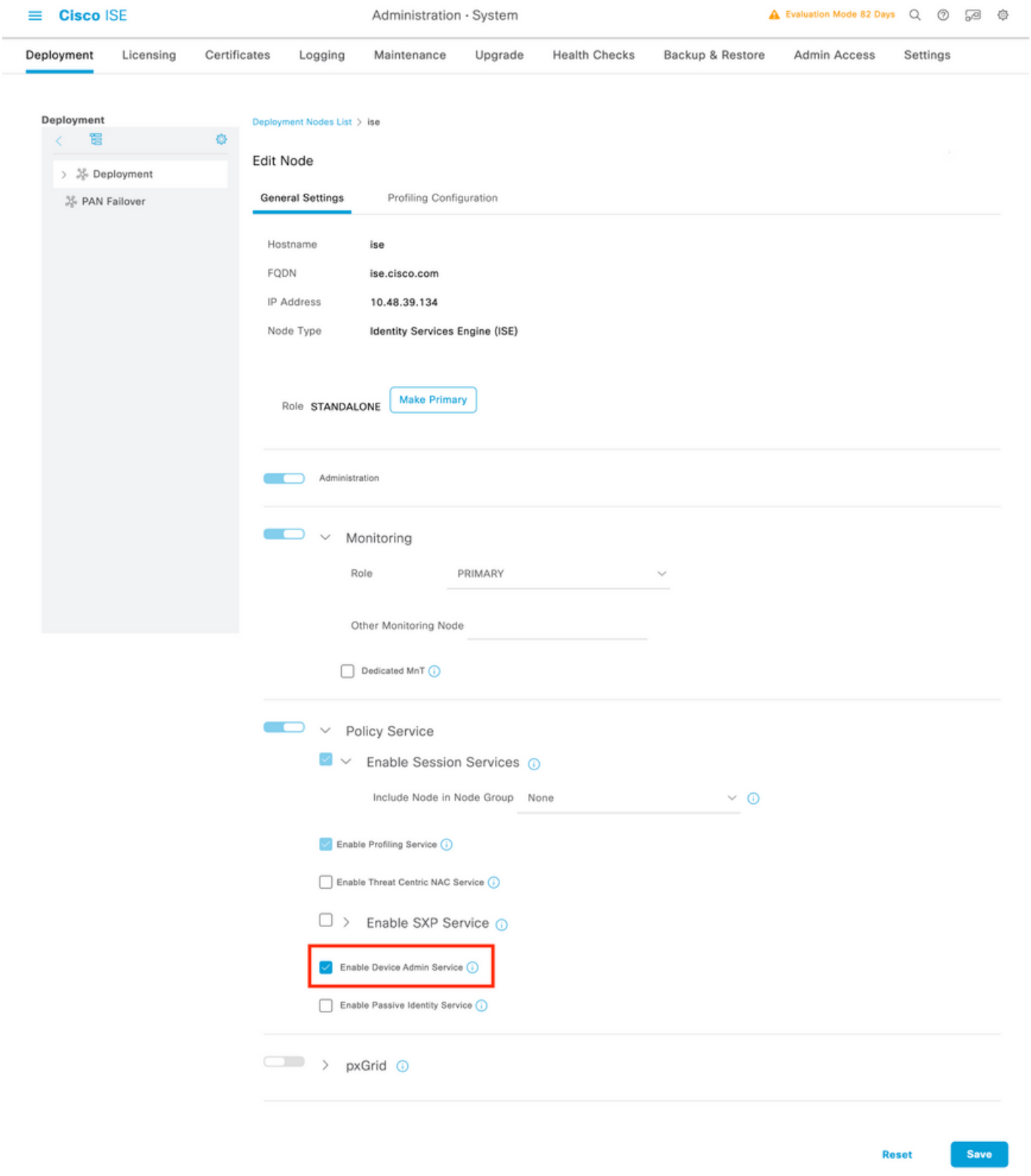
Nota: para utilizar ISE como servidor TACACS+, debe disponer de un paquete de licencias Device Administration y una licencia Base o Mobility.

Desde la GUI:

Una vez instaladas las licencias Device Administration, debe habilitar la función Device Admin para el nodo para poder utilizar ISE como servidor TACACS+. Para ello, edite la configuración del nodo de implementación de ISE utilizado, que se encuentra en Administrator > Deployment, y haga clic en su nombre o hágalo con la ayuda del Edit botón.



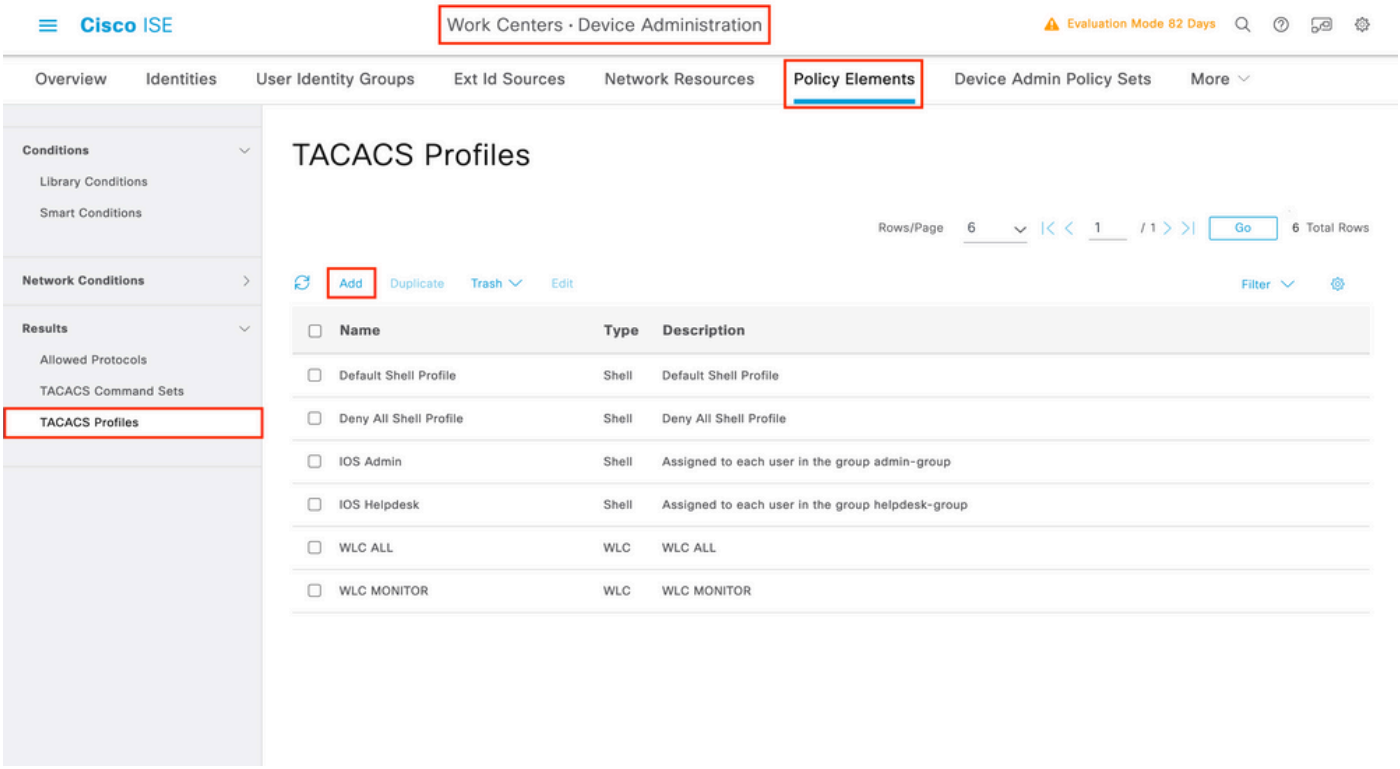
Una vez abierta la ventana de configuración del nodo, verifique la opción Enable Device Admin Service bajo la sección Policy Service, como se muestra en esta imagen.



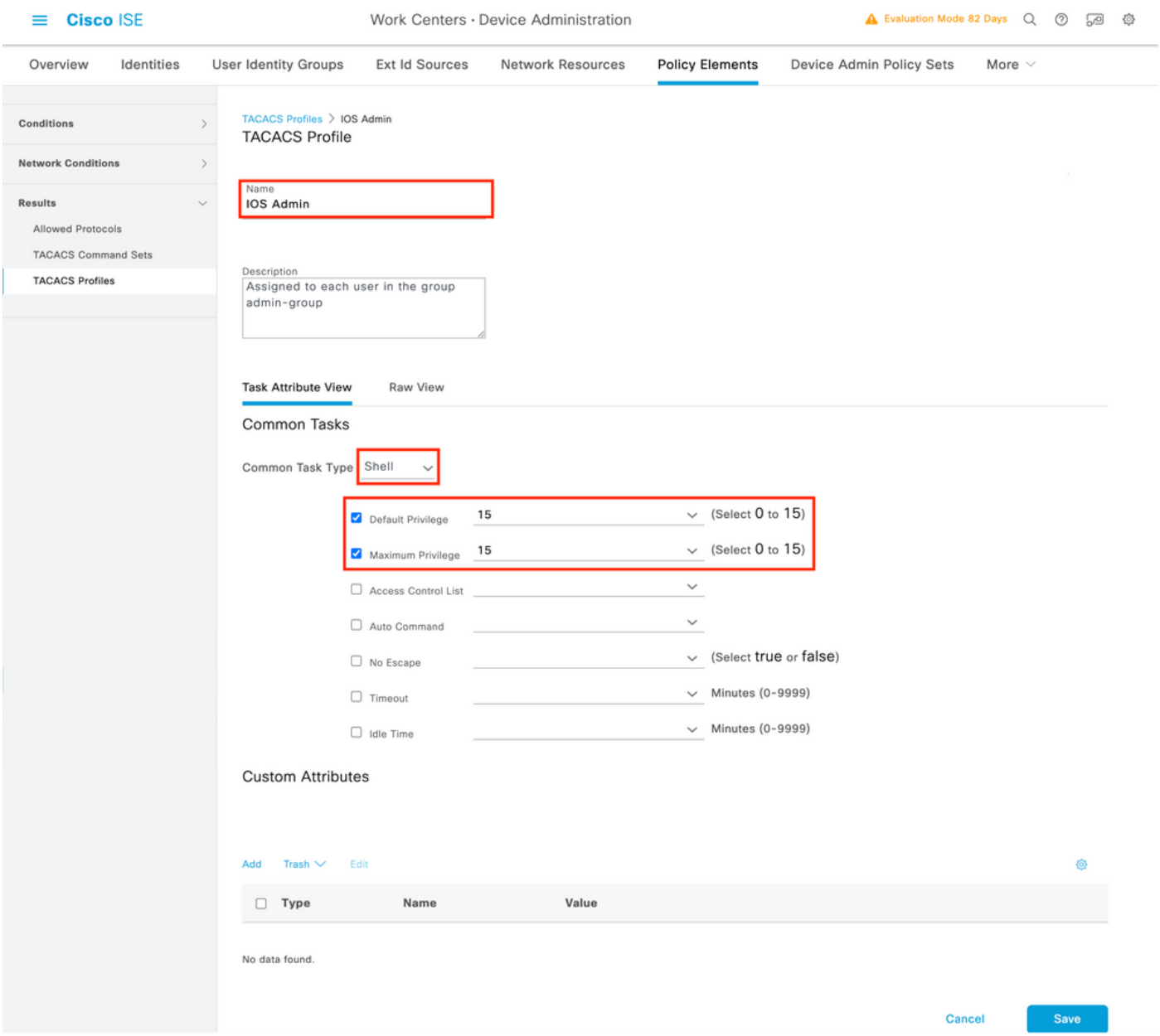
Paso 3. Cree perfiles TACACS para devolver el privilegio.

Desde la GUI:

Para tener derechos de acceso de administrador, el adminuser necesita tener un nivel de privilegio de 15, que permite acceder al intérprete de comandos exec. Por otro lado, el helpdeskuser no necesita acceso al shell exec prompt y, por lo tanto, se puede asignar con un nivel de privilegio inferior a 15. Para asignar el nivel de privilegio adecuado a los usuarios, se pueden utilizar perfiles de autorización. Se pueden configurar desde la página de la GUI de ISEWork Centers > Device Administration > Policy Elements, en la pestaña Results > TACACS Profiles que se muestra en la siguiente imagen.



Para configurar un nuevo perfil TACACS, utilice el botón Add (Agregar), que abre el nuevo formulario de configuración del perfil similar al que se muestra en la imagen. Este formulario debe tener un aspecto especial para configurar el perfil que se asigna al adminuser (es decir, con el nivel 15 de privilegios de shell).



Repita la operación para el helpdesk perfil. Para este último, el privilegio predeterminado, así como el privilegio máximo, se establecen en 1.

Paso 4. Cree grupos de usuarios en ISE.

Esto es lo mismo que se presentó en el paso 3 de la sección Configuración de RADIUS ISE de este documento.

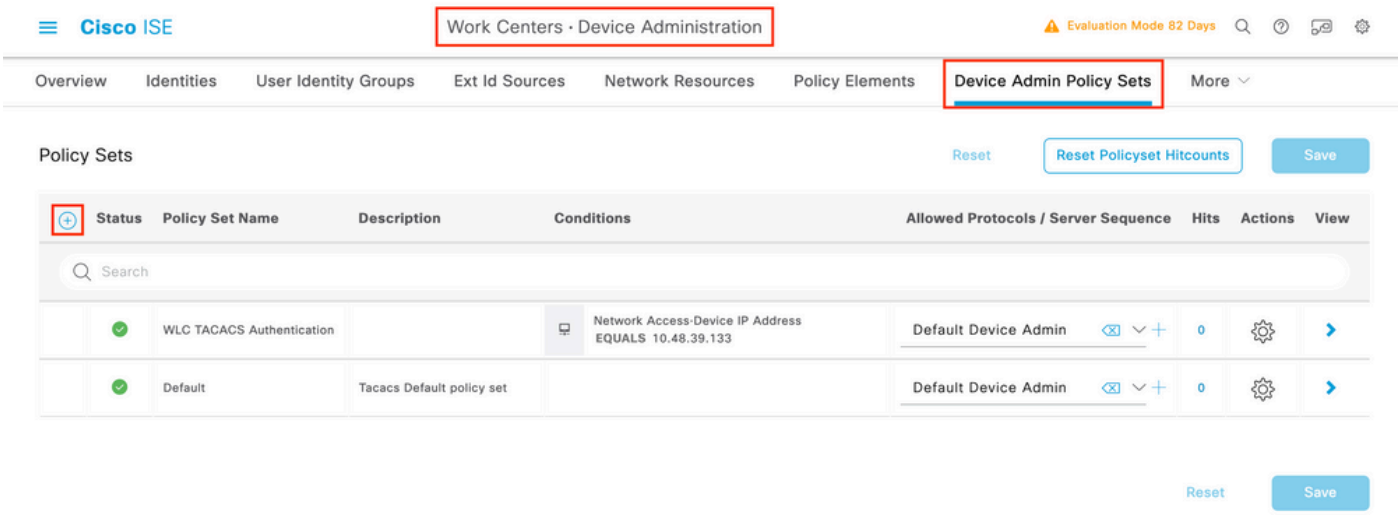
Paso 5. Cree los usuarios en ISE.

Esto es lo mismo que se presenta en el Paso 4 de la sección Configuración de RADIUS ISE de este documento.

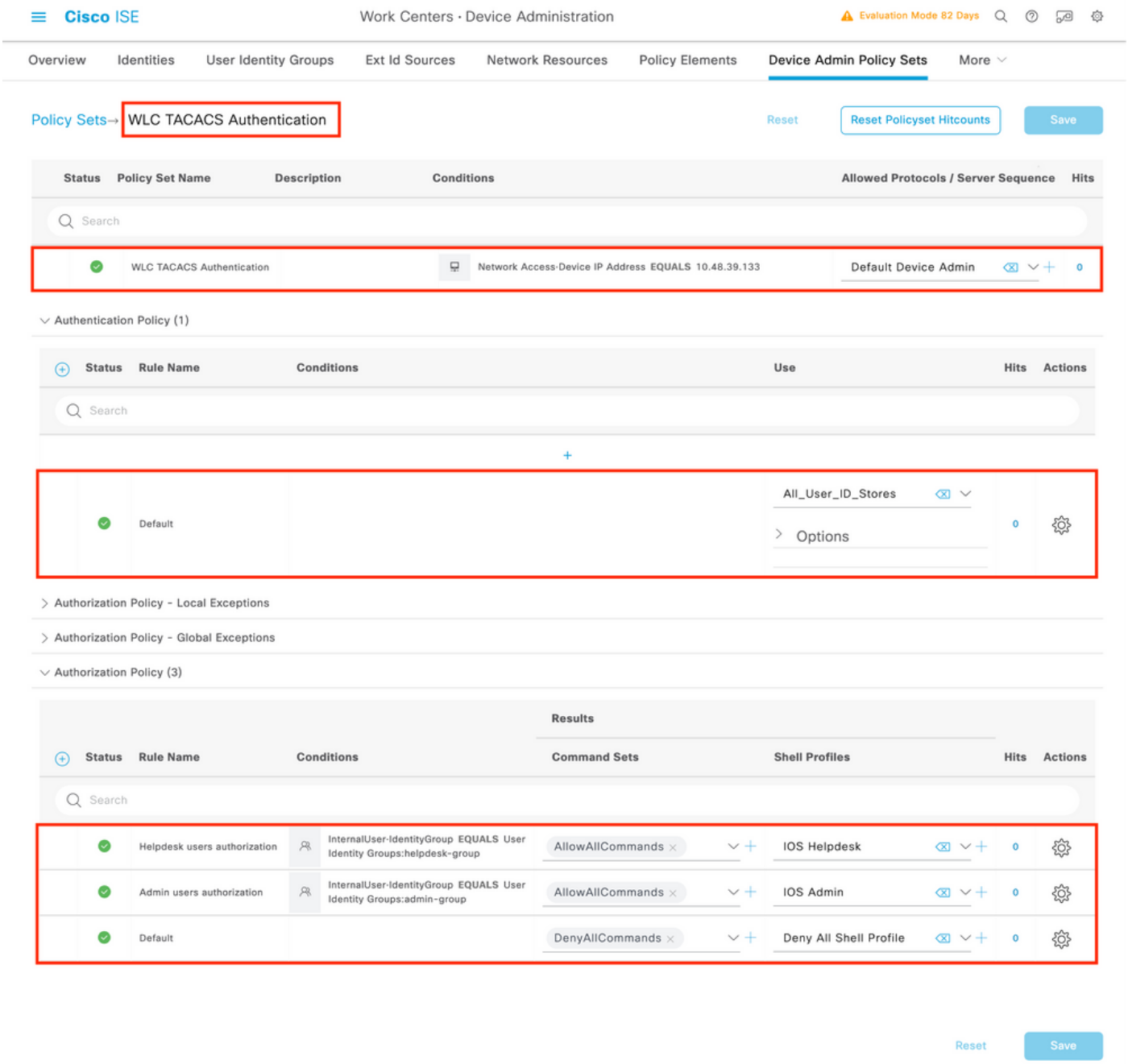
Paso 6. Cree un conjunto de directivas de administración de dispositivos.

Desde la GUI:

En cuanto al acceso RADIUS, una vez que se crean los usuarios, sus políticas de autenticación y autorización todavía deben definirse en ISE para otorgarles los derechos de acceso adecuados. La autenticación TACACS utiliza conjuntos de políticas de administración de dispositivos para ese fin, que se pueden configurar desde el Work Centers > Device Administration > Device Admin Policy Sets GUI Page como se muestra.



Para crear un conjunto de directivas de administración de dispositivos, utilice el botón agregar enmarcado en rojo en la imagen anterior. De este modo, se agrega un elemento a la lista de conjuntos de directivas. Proporcione un nombre para el conjunto recién creado, una condición bajo la cual debe aplicarse y la Secuencia Protocolos/Servidor Permitidos (aquí, Default Device Adminbasta). Utilice el Save botón para finalizar la adición del conjunto de políticas y utilice la punta de flecha de su derecha para acceder a su página de configuración, tal y como aparece en la representada.



El conjunto de políticas específico 'WLC TACACS Authentication' en este ejemplo filtra las solicitudes con la dirección IP igual a la dirección IP del WLC C9800 de ejemplo.

Como política de autenticación, se ha dejado la regla predeterminada porque satisface las necesidades del caso de uso. Se han establecido dos reglas de autorización:

- La primera se activa cuando el usuario pertenece al grupo definido admin-group. Permite todos los comandos (mediante la regla predeterminada Permit_all) y asigna el privilegio 15 (mediante el perfil TACACS definidoIOS_Admin).

- El segundo se activa cuando el usuario pertenece al grupo definido helpdesk-group. Permite todos los comandos (a través de la Permit_all regla predeterminada) y asigna el privilegio 1 (a través del perfil TACACS definidoIOS_Helpdesk).

Después de que este paso se haya completado, las credenciales configuradas para adminuser y loshelpdesk usuarios se pueden utilizar para

autenticar en el WLC vía la GUI o con Telnet/SSH.

Troubleshoot

Si su servidor RADIUS espera que se envíe el atributo RADIUS del tipo de servicio, puede agregar en el WLC :

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

Resolución de problemas de WLC GUI o CLI RADIUS/TACACS+ acceso a través de WLC CLI

Para resolver problemas del acceso TACACS+ a la GUI o CLI del WLC, ejecute el debug tacacs comando, junto con el monitor de terminal uno y vea la salida en vivo cuando se realiza un intento de inicio de sesión.

Por ejemplo, un inicio de sesión correcto seguido de un cierre de sesión del adminuser usuario genera este resultado.

```
<#root>

WLC-9800#

terminal monitor

WLC-9800#

debug tacacs

TACACS access control debugging is on
WLC-9800#
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

Se puede ver en estos registros que el servidor TACACS+ devuelve el privilegio correcto (que es AV priv-lvl=15).

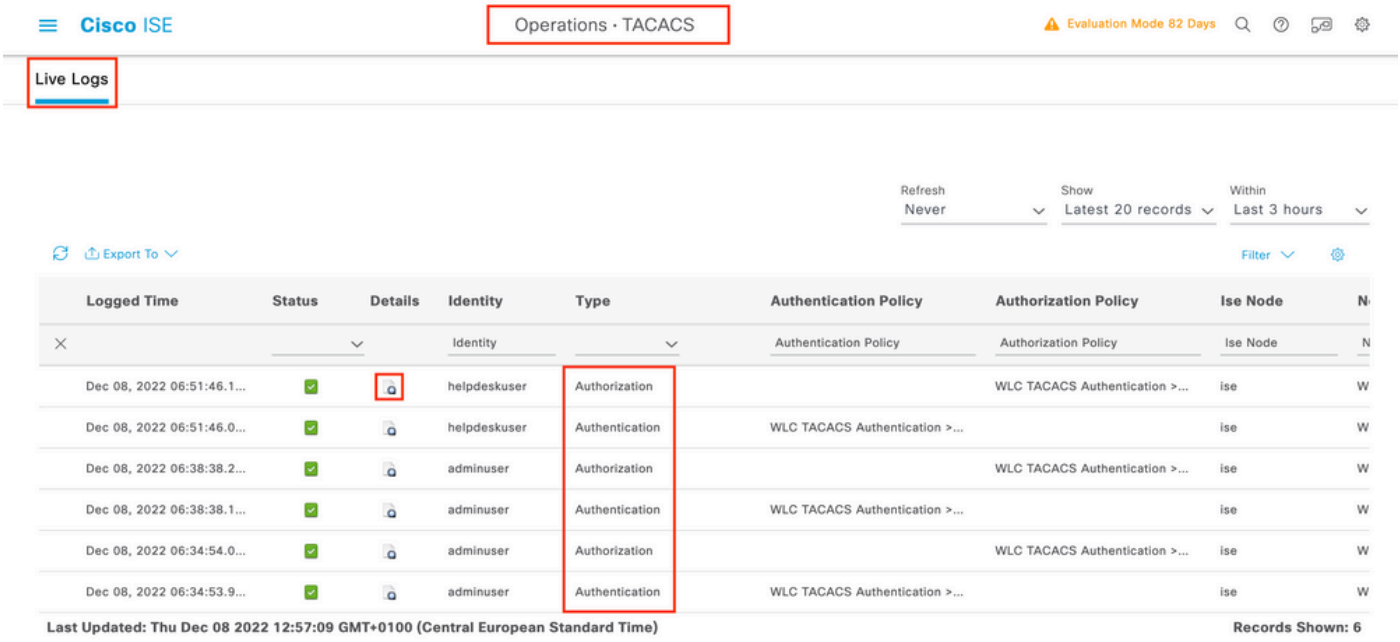
Cuando realiza la autenticación RADIUS, se muestra una salida de depuración similar, que concierne al tráfico RADIUS.

Los comandos debug aaa authentication y debug aaa authorization en su lugar, muestran qué lista de métodos es elegida por el WLC cuando el

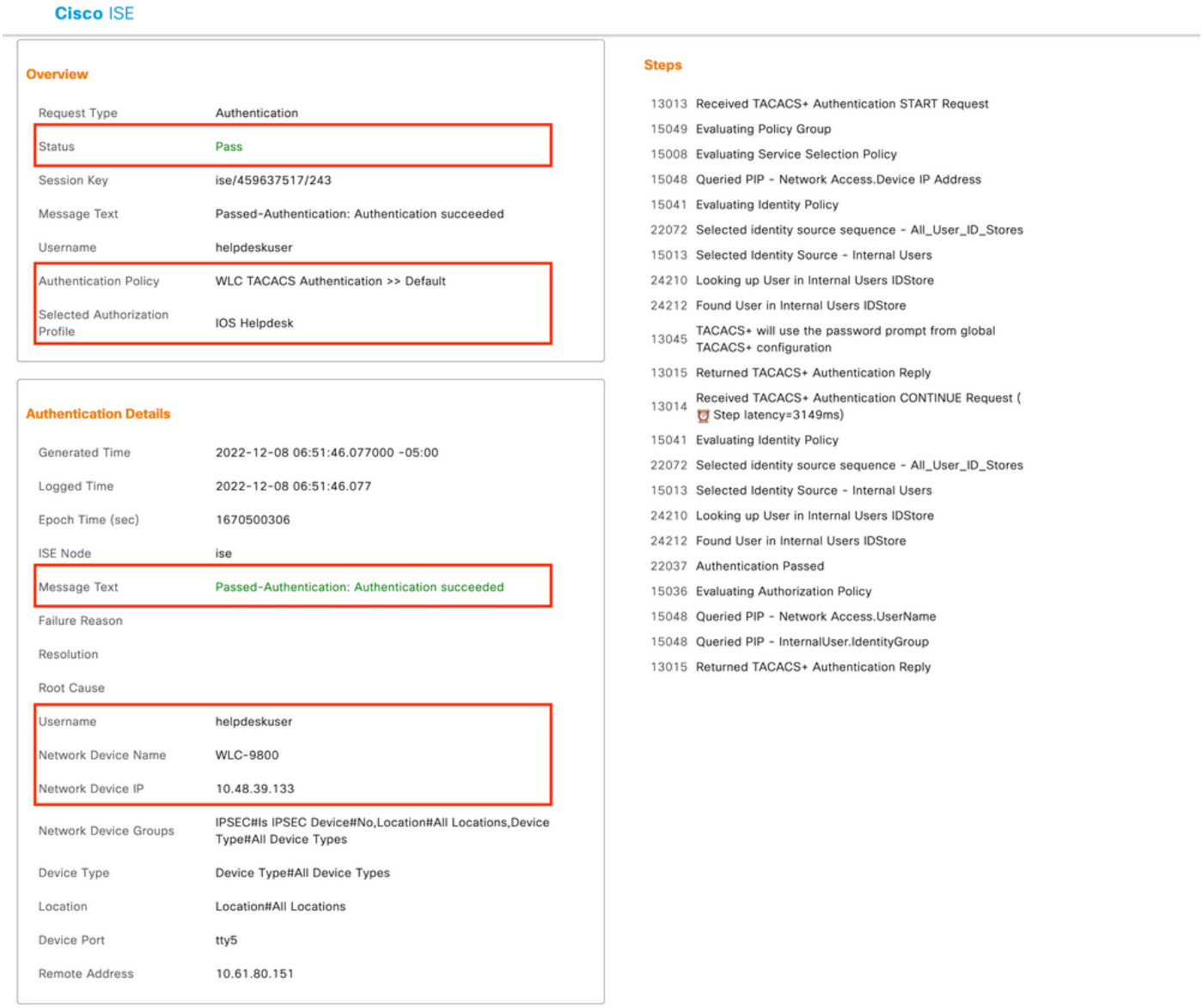
usuario intenta iniciar sesión.

Resolución de problemas de WLC GUI o CLI TACACS+ Access a través de ISE GUI

Desde la página Operations > TACACS > Live Logs, se puede ver cada autenticación de usuario realizada con TACACS+ hasta las últimas 24 horas. Para ampliar los detalles de una autorización o autenticación TACACS+, utilice el botón Detalles relacionado con este evento.



Cuando se expande, un intento de autenticación correcto para el helpdeskuser se ve así:



A partir de esto, puede ver que el usuario helpdeskuser se ha autenticado correctamente en el dispositivo de red WLC-9800 con la ayuda de la política de autenticación WLC TACACS Authentication > Default. Además, el perfil de autorización IOS Helpdesk se ha asignado a este usuario y se le ha concedido el nivel de privilegio 1.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).