Autentificación del Administrador Lobby deWireless LAN Controller a través del Servidor RADIUS

Contenido

Introducción

Este documento explica los pasos de configuración involucrados para autenticar a un administrador de lobby del controlador de LAN inalámbrica (WLC) con un servidor RADIUS.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar parámetros básicos en WLC
- Conocimiento de cómo configurar un servidor RADIUS, como Cisco Secure ACS
- Conocimiento de usuarios invitados en el WLC

Componentes Utilizados

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

- Cisco 4400 Wireless LAN Controller que ejecuta la versión 7.0.216.0

- Cisco Secure ACS que ejecuta la versión de software 4.1 y se utiliza como servidor RADIUS en esta configuración.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Un administrador del vestíbulo, también conocido como embajador del vestíbulo de un WLC, puede crear y administrar cuentas de usuarios invitados en el controlador de LAN inalámbrica (WLC). El embajador del vestíbulo tiene privilegios de configuración limitados y sólo puede acceder a las páginas web utilizadas para administrar las cuentas de invitados. El embajador del vestíbulo puede especificar la cantidad de tiempo que las cuentas de usuario invitado permanecen activas. Una vez transcurrido el tiempo especificado, las cuentas de usuario invitado caducan automáticamente.

Consulte Guía de implementación: Acceso de invitado de Cisco mediante el controlador de LAN inalámbrica de Cisco para obtener más información sobre los usuarios invitados.

Para crear una cuenta de usuario invitado en el WLC, necesita iniciar sesión en el controlador como administrador del vestíbulo. Este documento explica cómo un usuario se autentica en el WLC como administrador de lobby basado en los atributos devueltos por el servidor RADIUS.

Nota: La autenticación del administrador del vestíbulo también se puede realizar en función de la cuenta del administrador del vestíbulo configurada localmente en el WLC. Refiérase a Creación de una Cuenta de Embajador en el Vestíbulo para obtener información sobre cómo crear una cuenta de administrador de lobby localmente en un controlador.

Configurar

En esta sección, se le presenta la información sobre cómo configurar el WLC y el Cisco Secure ACS para el propósito descrito en este documento.

Configuraciones

En este documento, se utilizan estas configuraciones:

- La dirección IP de la interfaz de administración del WLC es 10.77.244.212/27.
- La dirección IP del servidor RADIUS es 10.77.244.197/27.
- La clave secreta compartida que se utiliza en el punto de acceso (AP) y el servidor RADIUS es cisco123.
- El nombre de usuario y la contraseña del administrador del vestíbulo configurados en el servidor RADIUS son lobbyadmin.

En el ejemplo de configuración de este documento, a cualquier usuario que inicie sesión en el

controlador con nombre de usuario y contraseña como lobbyadmin se le asigna la función de administrador de lobby.

Configuración de WLC

Antes de iniciar la configuración WLC necesaria, asegúrese de que su controlador ejecute la versión 4.0.206.0 o posterior. Esto se debe al Id. de error de Cisco CSCsg89868 (sólo clientes registrados) en el que la interfaz web del controlador muestra páginas web equivocadas para el usuario LobbyAdmin cuando el nombre de usuario se almacena en una base de datos RADIUS. LobbyAdmin se presenta con la interfaz ReadOnly en lugar de la interfaz LobbyAdmin.

Este bug ha sido resuelto en la versión 4.0.206.0 del WLC. Por lo tanto, asegúrese de que su versión del controlador sea 4.0.206.0 o posterior. Consulte Actualización de Software del Controlador de LAN Inalámbrica (WLC) para obtener instrucciones sobre cómo actualizar el controlador a la versión adecuada.

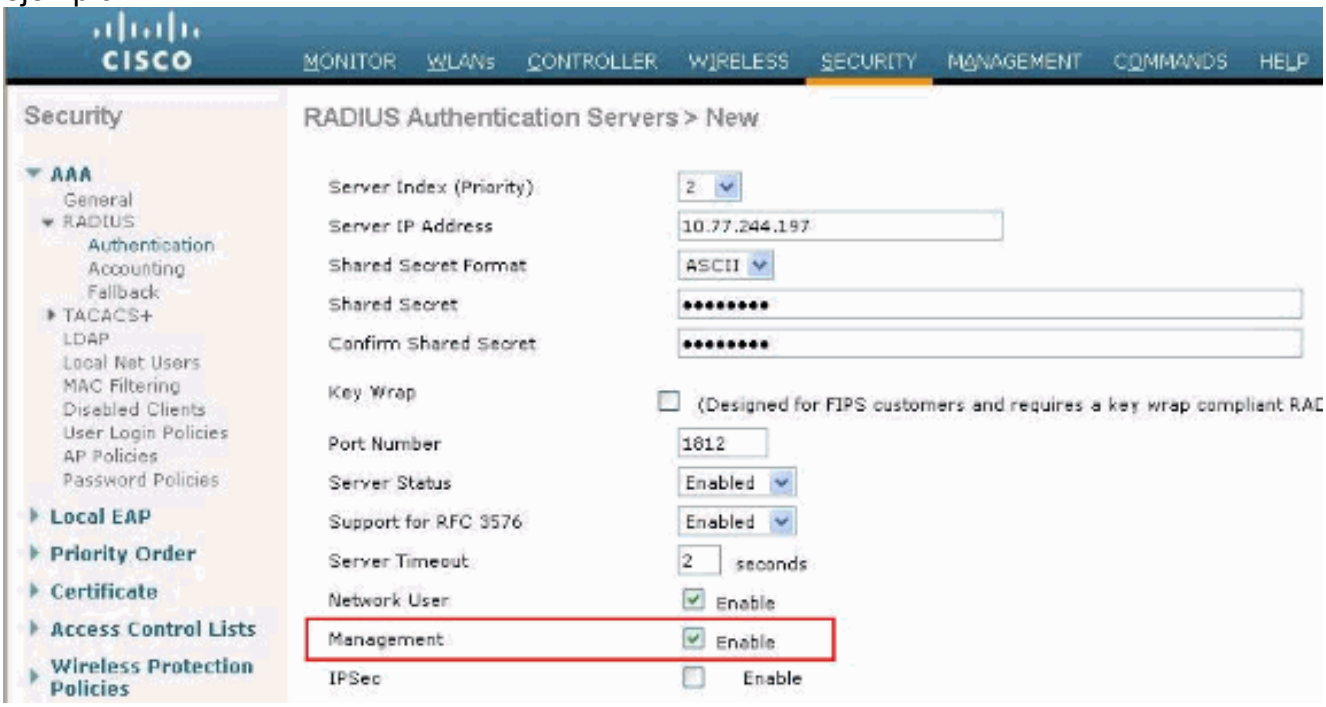
Para realizar la autenticación de administración del controlador con el servidor RADIUS, asegúrese de que el indicador **Admin-auth-via-RADIUS** esté habilitado en el controlador. Esto se puede verificar desde la salida del comando **show radius summary**.

El primer paso es configurar la información del servidor RADIUS en el controlador y establecer el alcance de la Capa 3 entre el controlador y el servidor RADIUS.

Configuración de la información del servidor RADIUS en el controlador

Complete estos pasos para configurar el WLC con detalles sobre el ACS:

1. Desde la GUI del WLC, elija la pestaña **Seguridad** y configure la dirección IP y el secreto compartido del servidor ACS.Este secreto compartido necesita ser el mismo en el ACS para que el WLC se comunique con el ACS.**Nota:** El secreto compartido ACS distingue entre mayúsculas y minúsculas. Por lo tanto, asegúrese de introducir la información secreta compartida correctamente.Esta figura muestra un ejemplo:



2. Marque la casilla de verificación **Management** para permitir que el ACS administre a los usuarios del WLC como se muestra en la figura en el paso 1. A continuación, haga clic en **Aplicar**.
3. Verifique el alcance de la Capa 3 entre el controlador y el servidor RADIUS configurado con la ayuda del comando **ping**. Esta opción de ping también está disponible en la página del servidor RADIUS configurado en la GUI del WLC en la pestaña **Security>RADIUS Authentication**.Este diagrama muestra una respuesta ping exitosa del servidor RADIUS. Por lo tanto, el alcance de la Capa 3 está disponible entre el controlador y el servidor RADIUS.

Configuración del servidor de RADIUS

Complete los pasos en estas secciones para configurar el servidor RADIUS:

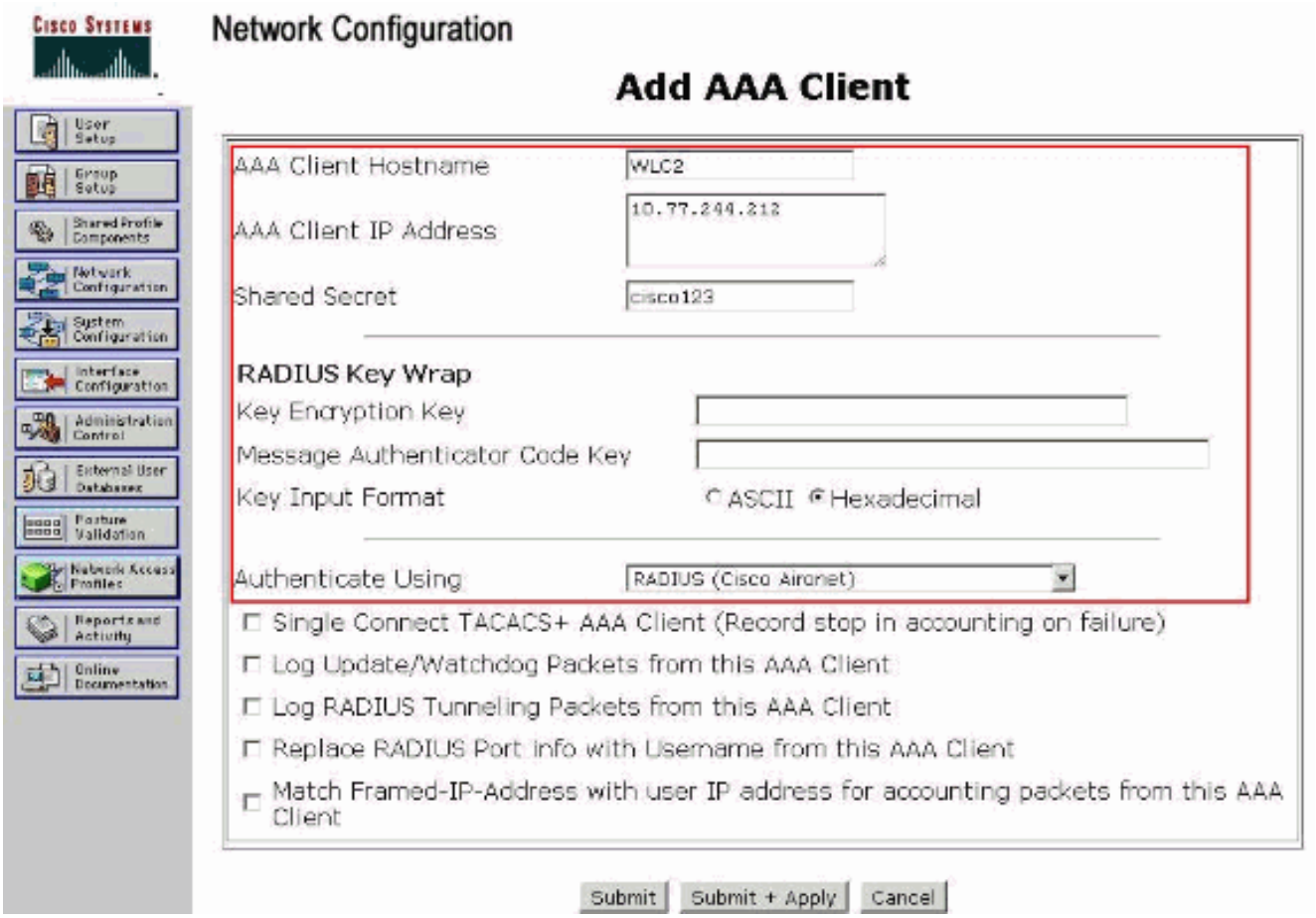
1. Agregue el WLC como cliente AAA al servidor RADIUS
2. Configure el Atributo de Tipo de Servicio RADIUS IETF Apropiado para un Administrador de Lobby

Agregue el WLC como cliente AAA al servidor RADIUS

Complete estos pasos para agregar el WLC como un cliente AAA en el servidor RADIUS. Como se mencionó anteriormente, este documento utiliza el ACS como el servidor RADIUS. Puede utilizar cualquier servidor RADIUS para esta configuración.

Complete estos pasos para agregar el WLC como un cliente AAA en el ACS:

1. Desde la GUI de ACS, elija la pestaña **Configuración de Red**.
2. En los clientes AAA, haga clic en Add Entry (Agregar entrada).
3. En la ventana Add AAA Client, ingrese el nombre de host del WLC, la dirección IP del WLC y una clave secreta compartida. Vea el diagrama de ejemplo en el paso 5.
4. En el menú desplegable Authenticate Using, elija **RADIUS (Cisco Aironet)**.
5. Haga clic en **Submit + Restart** para guardar la configuración.

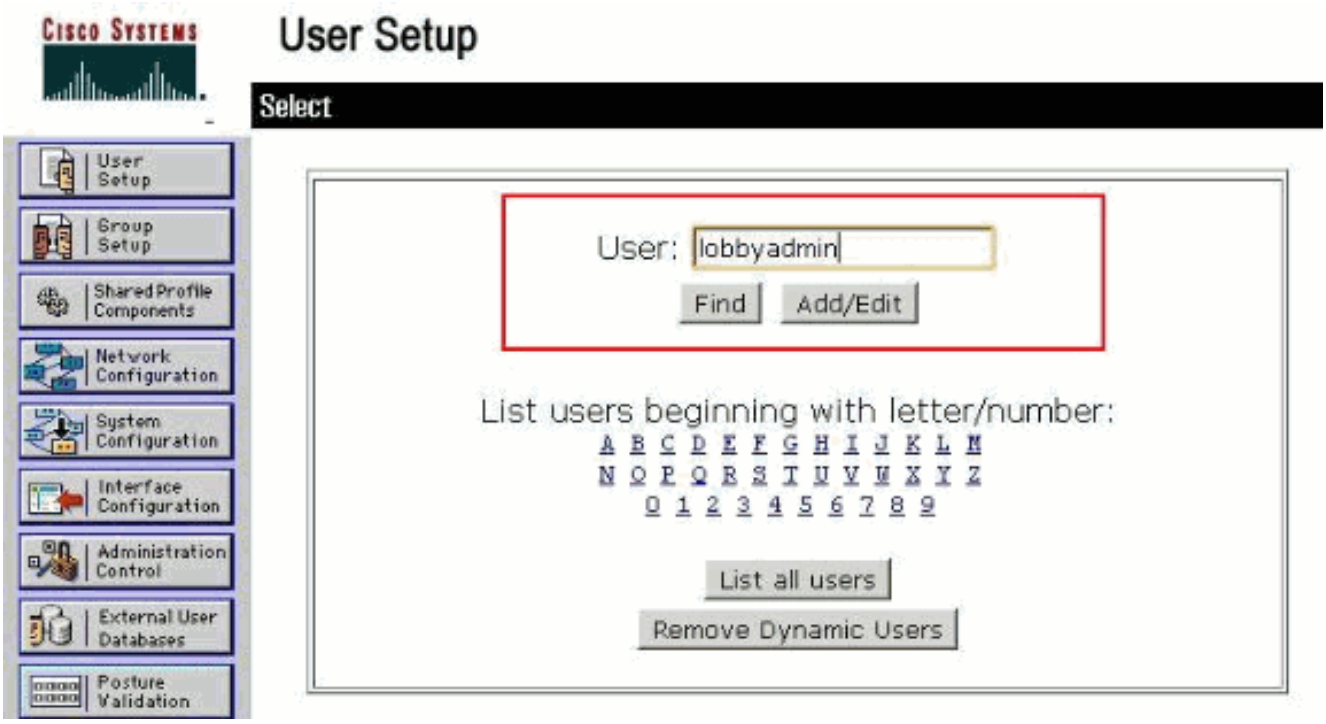


Configure el Atributo de Tipo de Servicio RADIUS IETF Apropiado para un Administrador de Lobby

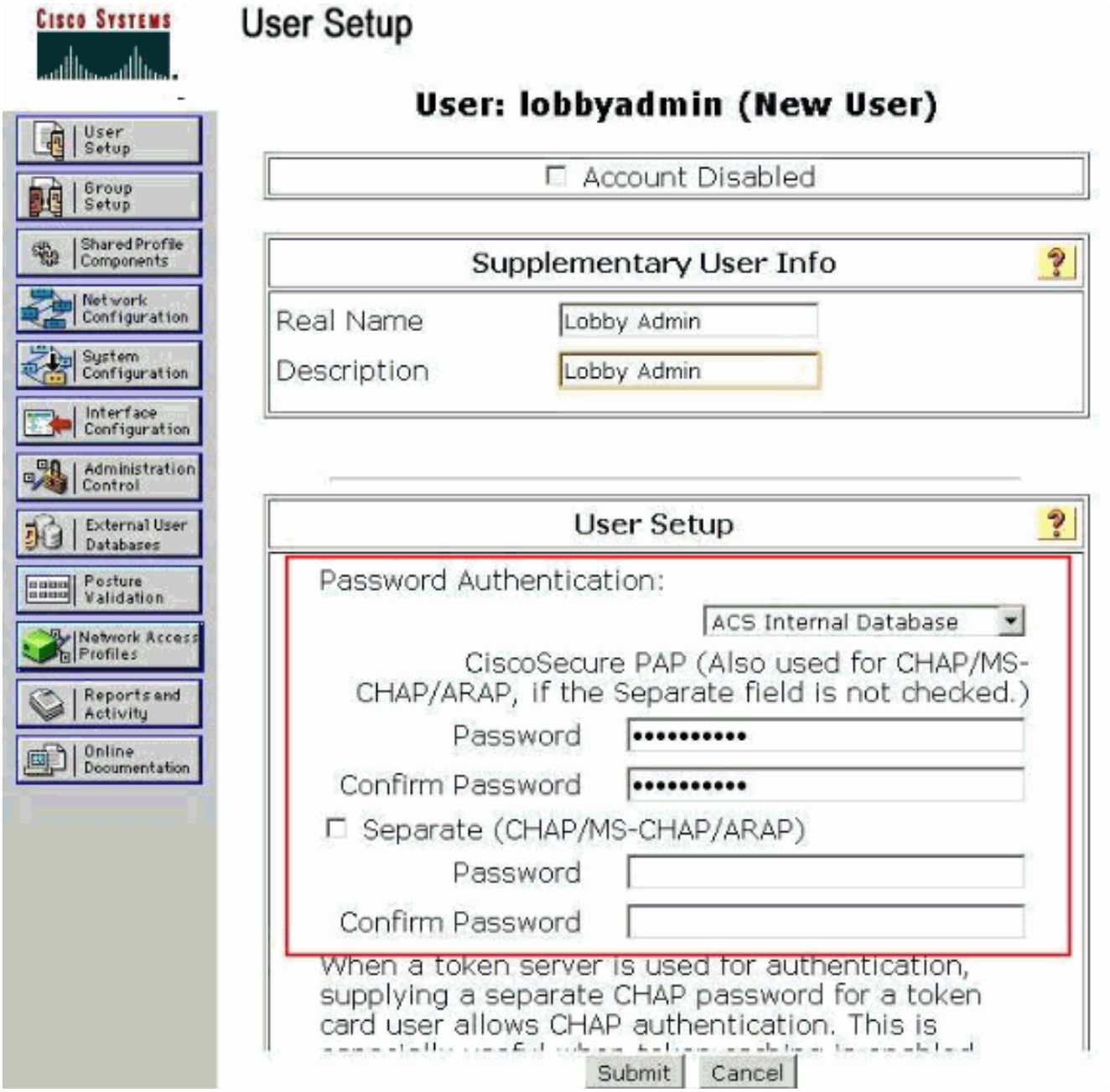
Para autenticar a un usuario de administración de un controlador como administrador de lobby a través del servidor RADIUS, debe agregar el usuario a la base de datos RADIUS con el atributo IETF RADIUS Service-Type establecido en **Callback Administrative**. Este atributo asigna al usuario específico la función de administrador de lobby en un controlador.

Este documento muestra el ejemplo de usuario lobbyadmin como administrador de lobby. Para configurar este usuario, complete estos pasos en el ACS:

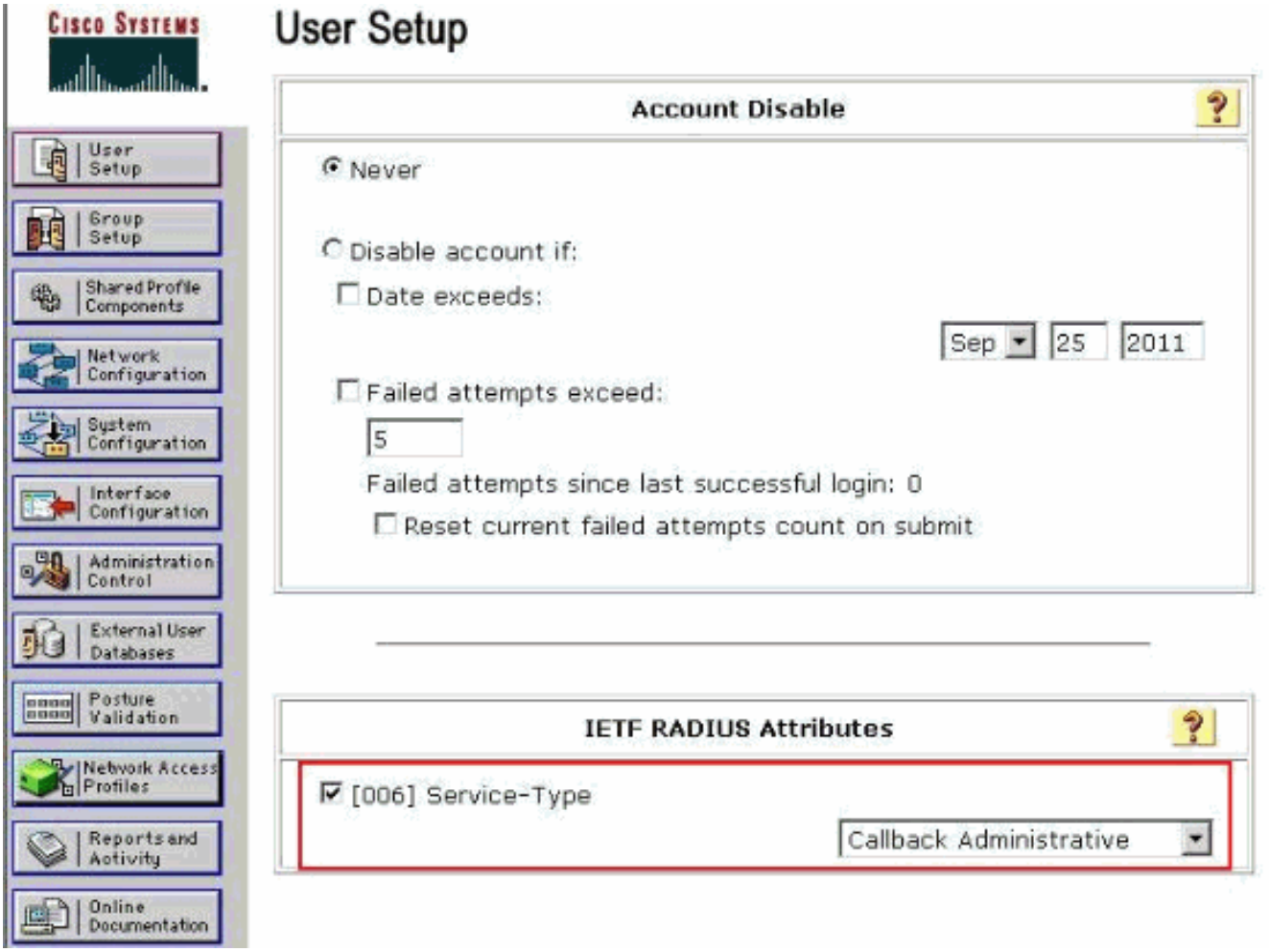
1. Desde la GUI de ACS, elija la pestaña **User Setup** .
2. Ingrese el nombre de usuario que se agregará al ACS como muestra esta ventana de ejemplo:



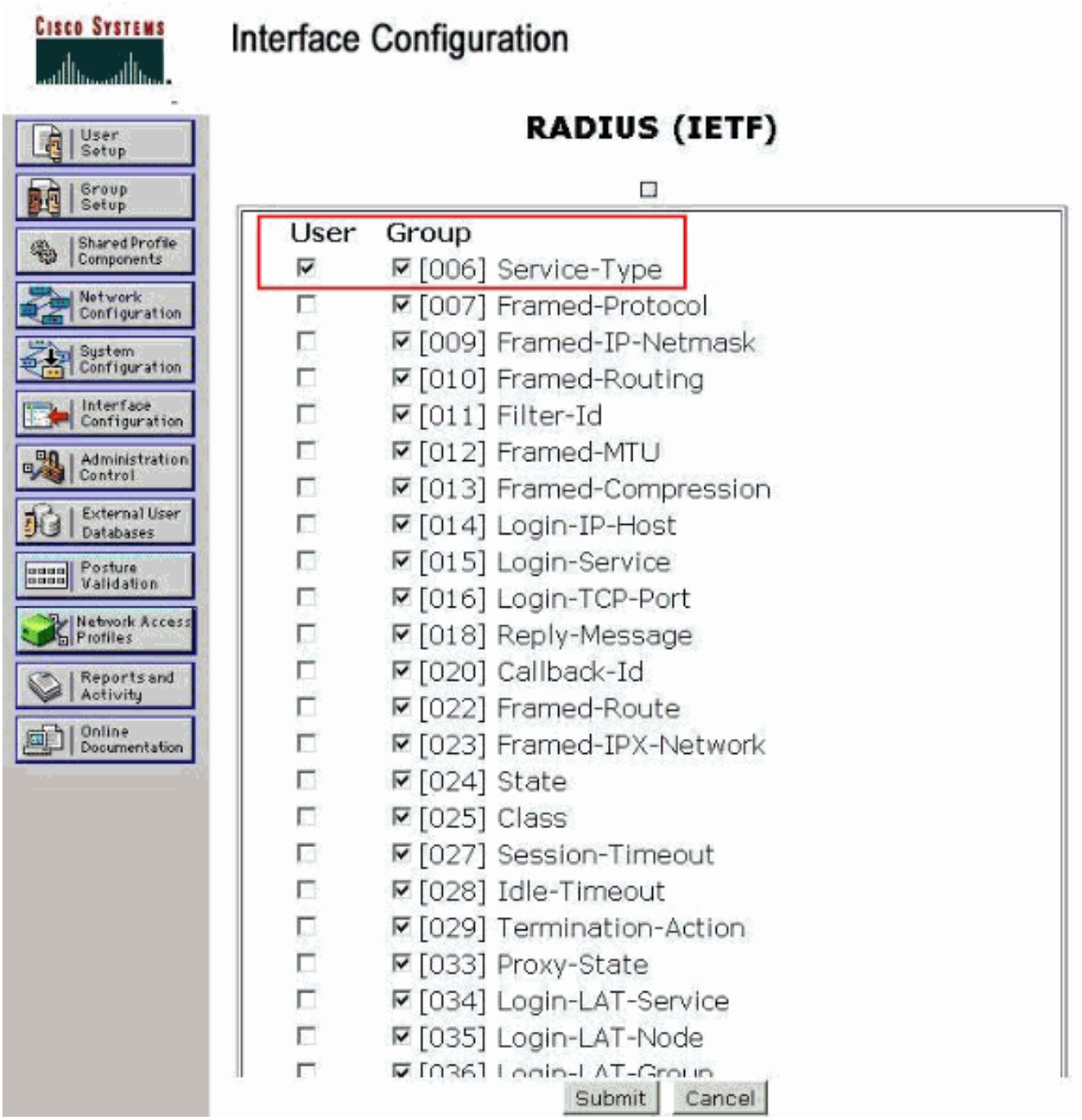
3. Haga clic en **Add/Edit** para ir a la página User Edit.
4. En la página User Edit (Editar usuario), proporcione los detalles de Nombre real, Descripción y Contraseña de este usuario.En este ejemplo, el nombre de usuario y la contraseña utilizados son
   lobbyadmin.



5. Desplácese hacia abajo hasta la configuración IETF RADIUS Attributes y marque la casilla de verificación **Service-Type Attribute** .
6. Elija **Callback Administrative** en el menú desplegable Service-Type y haga clic en **Submit**.Este es el atributo que asigna a este usuario la función de administrador del vestíbulo.



A veces, este atributo de tipo de servicio no está visible en la configuración del usuario. En tales casos, complete estos pasos para hacerlo visible:Desde la GUI de ACS, elija **Interface Configuration > RADIUS (IETF)** para habilitar los atributos de IETF en la ventana User Configuration.Esto le lleva a la página de configuración de RADIUS (IETF).En la página Configuración de RADIUS (IETF), puede activar el atributo IETF que debe estar visible en la configuración de usuario o grupo. Para esta configuración, verifique **Tipo de servicio** para la columna Usuario y haga clic en **Enviar**.Esta ventana muestra un ejemplo:



Nota: En este ejemplo se especifica la autenticación por usuario. También puede realizar la autenticación en función del grupo al que pertenece un usuario concreto. En tales casos, active la casilla de verificación **Grupo** para que este atributo esté visible en la configuración Grupo.**Nota:** Además, si la autenticación se realiza en grupo, debe asignar usuarios a un grupo determinado y configurar los atributos IETF de configuración de grupo para proporcionar privilegios de acceso a los usuarios de ese grupo. Refiérase a Administración de Grupos de Usuarios para obtener información detallada sobre cómo configurar y administrar grupos.

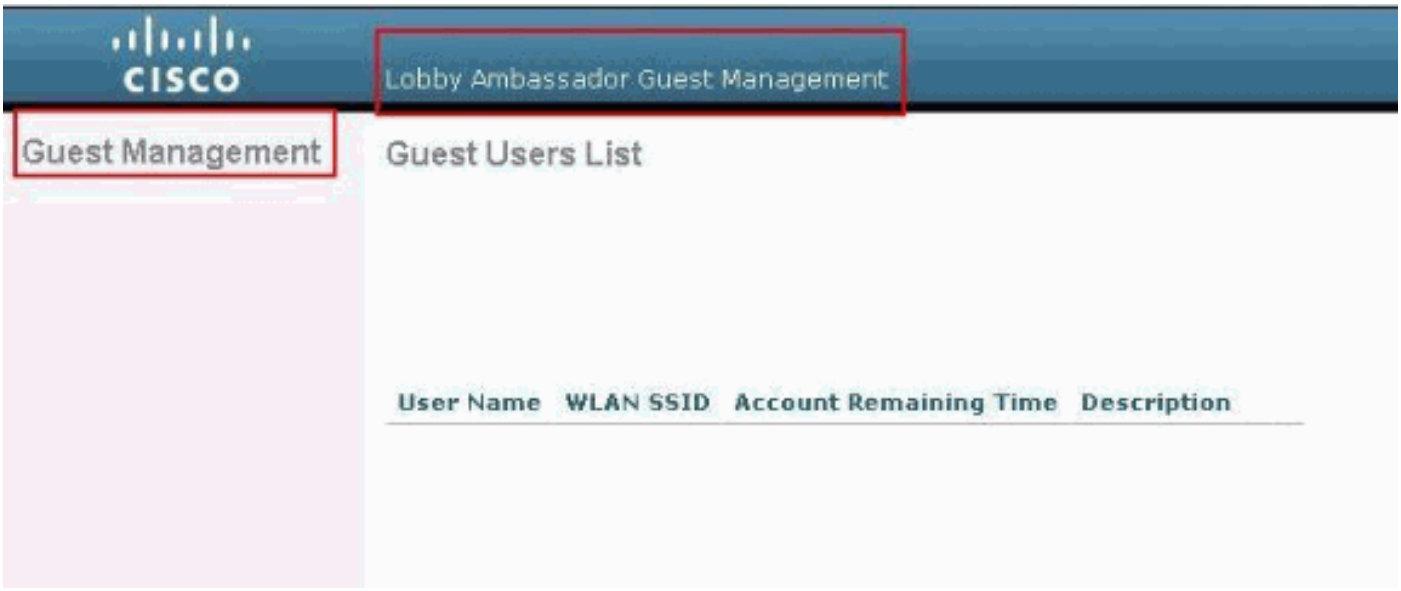
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar que su configuración funcione correctamente, acceda al WLC a través del modo GUI (HTTP/HTTPS).

Nota: Un embajador de lobby no puede acceder a la interfaz CLI del controlador y, por lo tanto, puede crear cuentas de usuario invitado solamente desde la GUI del controlador.

Cuando aparezca el mensaje de inicio de sesión, ingrese el nombre de usuario y la contraseña tal como se configuró en el ACS. Si usted tiene las configuraciones correctas, se autentica exitosamente en el WLC como **administrador de lobby**. Este ejemplo muestra cómo la GUI de un administrador de lobby se ocupa de la autenticación exitosa:



Nota: Puede ver que un administrador del vestíbulo no tiene otra opción aparte de la administración de usuarios invitados.

Para verificarlo desde el modo CLI, Telnet en el controlador como administrador de lectura-escritura. Ejecute el comando **debug aaa all enable** en la CLI del controlador.

```
(Cisco Controller) >debug aaa all enable

(Cisco Controller) >
*aaaQueueReader: Aug 26 18:07:35.072: ReProcessAuthentication previous proto 28,
 next proto 20001
*aaaQueueReader: Aug 26 18:07:35.072: AuthenticationRequest: 0x3081f7dc
*aaaQueueReader: Aug 26 18:07:35.072:   Callback.....................................0x10756dd0
*aaaQueueReader: Aug 26 18:07:35.072:   protocolType.................................0x00020001
*aaaQueueReader: Aug 26 18:07:35.072:
proxyState.....................................00:00:00:40:
00:00-00:00
*aaaQueueReader: Aug 26 18:07:35.072:   Packet contains 5 AVPs (not shown)
*aaaQueueReader: Aug 26 18:07:35.072: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes
srcAddr:
0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful transmission of
Authentication
Packet (id 39) to 10.77.244.212:1812, proxy state 00:00:00:40:00:00-00:01
*aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00  00 00 00 00 00 00 00 00
.'.G............
*aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00 00 00 01 0c 6c 6f  62 62 79 61 64 6d 69 6e
......lobbyadmin
*aaaQueueReader: Aug 26 18:07:35.073: 00000020: 02 12 5f 5b 5c 12 c5 c8  52 d3 3f 4f 4f 8e 9d 38
 .._[\...R.?OO..8
*aaaQueueReader: Aug 26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07  04 06 0a 4e b1 1a 20 09
B..........N....
```

```
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1
f8  .'.@~.mS=.y.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06 ff ffff ff 06 06 00 00
00
0b  .Z.O............
*radiusTransportThread: Aug 26 18:07:35.080: 00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f
61
34  ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69
6e  eb11a/lobbyadmin
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: 00:00:00:40:00:00 Access-Accept received from
RADIUS
server 10.77.244.212 for mobile 00:00:00:40:00:00 receiveId = 0
*radiusTransportThread: Aug 26 18:07:35.080: AuthorizationResponse: 0x13c73d50
*radiusTransportThread: Aug 26 18:07:35.080:    structureSize.............................118
*radiusTransportThread: Aug 26 18:07:35.080:    resultCode.................................0
*radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.............................0x00000001
*radiusTransportThread: Aug 26 18:07:35.080:
proxyState.................................00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080:    Packet contains 3 AVPs:
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[01] Framed-IP-
Address.....................0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[02] Service-
Type.............................0x0000000b (11) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[03]
Class.....................................
CACS:0/ae26/a4eb11a/lobbyadmin (30 bytes)
*emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

En la información resaltada en este resultado, puede ver que el atributo de tipo de servicio 11 (Callback Administrative) se pasa al controlador desde el servidor ACS y el usuario se conecta como administrador de lobby.

Estos comandos pueden ser de ayuda adicional:

- **debug aaa details enable**
- **debug aaa events enable**
- **debug aaa packets enable**

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

Troubleshoot

Cuando inicia sesión en un controlador con privilegios de embajador en el vestíbulo, no puede crear una cuenta de usuario invitado con un valor **de "0"** de tiempo de vida, que es una cuenta que nunca caduca. En estas situaciones, recibe el mensaje de error `Lifetime no puede ser 0`.

Esto se debe al Id. de bug Cisco CSCsf32392 (sólo clientes registrados) , que se encuentra principalmente con la versión 4.0 del WLC. Este bug ha sido resuelto en la versión 4.1 del WLC.

Información Relacionada

- Ejemplo de Autenticación de Servidor RADIUS de Usuarios de Administración en la Configuración del Controlador
- Configuración de la red inalámbrica unificada de Cisco TACACS+
- Guía de configuración del controlador LAN inalámbrico Cisco, versión 4.0: Administración de cuentas de usuario
- Ejemplo de Configuración de ACL en el Controlador de LAN Inalámbrica
- Preguntas frecuentes sobre Wireless LAN Controller (WLC)
- ACL en Controladores de LAN Inalámbricos: Reglas, limitaciones y ejemplos
- Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica
- Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico
- Ejemplo de Configuración de WLAN Guest y WLAN Interna mediante WLCs
- Soporte Técnico y Documentación - Cisco Systems