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

Contenido

Introducción

Este documento explica los pasos para la configuración implicados para autenticar a un administrador del pasillo del regulador del Wireless LAN (WLC) con un servidor de RADIUS.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar los parámetros básicos en el WLCs
- Conocimiento de cómo configurar a un servidor de RADIUS, tal como el Cisco Secure ACS
- Conocimiento de los Usuarios invitados en el WLC

Componentes Utilizados

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

- Regulador del Wireless LAN de Cisco 4400 que funciona con la versión 7.0.216.0

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

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Un administrador del pasillo, también conocido como embajador del pasillo de un WLC, puede crear y manejar las cuentas de Usuario invitado en el regulador del Wireless LAN (WLC). El embajador del pasillo ha limitado los privilegios de la configuración y puede acceder solamente las páginas web usadas para manejar las cuentas de invitado. El embajador del pasillo puede especificar la cantidad de tiempo que las cuentas de Usuario invitado siguen siendo activas. Después de los pasajes del tiempo especificado, las cuentas de Usuario invitado expiran automáticamente.

Refiera al Guía de despliegue: Acceso de invitado de Cisco usando el controlador LAN de la tecnología inalámbrica de Cisco para más información sobre los Usuarios invitados.

Para crear una cuenta de Usuario invitado en el WLC, usted necesita iniciar sesión al regulador como administrador del pasillo. Este documento explica cómo autentican a un usuario en el WLC como un administrador del pasillo basado en los atributos volvió por el servidor de RADIUS.

Nota: La autenticación de administrador del pasillo se puede también realizar basó en la cuenta del administrador del pasillo configurada localmente en el WLC. Refiera a crear a un embajador del pasillo explican la información de cómo crear una cuenta del administrador del pasillo localmente en un regulador.

Configurar

En esta sección, le presentan con 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 de RADIUS es 10.77.244.197/27.
- La clave secreta compartida que se utiliza en el punto de acceso y el servidor de RADIUS es cisco123.
- El nombre de usuario y contraseña del administrador del pasillo configurado en el servidor de RADIUS es ambo lobbyadmin.

En el ejemplo de configuración en este documento, cualquier registro de usuario en el regulador con el nombre de usuario y contraseña como lobbyadmin se asigna el papel de un administrador del pasillo.

Configuración del WLC

Antes de que usted comience la configuración necesaria del WLC, asegúrese de que su regulador funcione con la versión 4.0.206.0 o más adelante. Esto es debido al Id. de bug Cisco CSCsg89868 (clientes registrados solamente) en las cuales la interfaz Web del regulador visualiza las páginas web incorrectas para el usuario de LobbyAdmin cuando el nombre de usuario se salva en una base de datos RADIUS. El LobbyAdmin se presenta con la interfaz inalterable en vez de la interfaz de LobbyAdmin.

Este bug se ha resuelto en la versión 4.0.206.0 del WLC. Por lo tanto, asegúrese de que su versión del regulador sea 4.0.206.0 o más adelante. Refiera a la actualización del software del regulador del Wireless LAN (WLC) para las instrucciones en cómo actualizar su regulador a la versión apropiada.

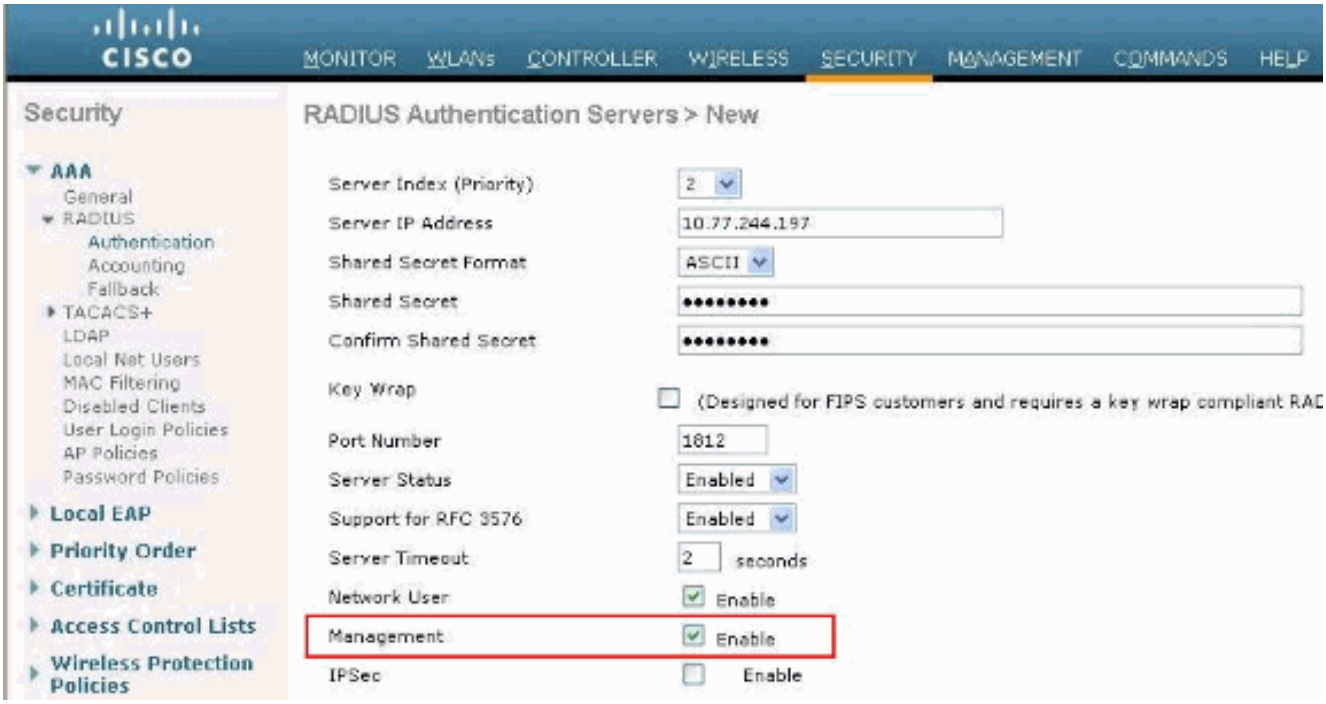
Para realizar la autenticación de la Administración del regulador con el servidor de RADIUS, asegúrese de que el indicador Admin-auth-vía-**RADIUS** está habilitado en el regulador. Esto se puede verificar de la salida del **comando summary del radio de la demostración**.

El primer paso es configurar la información del servidor de RADIUS sobre el regulador y establecer el accesibilidad de la capa 3 entre el regulador y el servidor de RADIUS.

Información del servidor de RADIUS de la configuración sobre el regulador

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

1. Del WLC GUI, elija la **ficha de seguridad** y configure la dirección IP y el secreto compartido del servidor ACS.Este secreto compartido necesita ser lo mismo en el ACS para que el WLC comunique con el ACS.**Nota:** El secreto compartido ACS es con diferenciación entre mayúsculas y minúsculas. Por lo tanto, aseegurese ingresar la información secreta compartida correctamente.Esta figura muestra un ejemplo:



2. Marque la **casilla de verificación Management (Administración)** para permitir que el ACS maneje a los usuarios del WLC tal y como se muestra en de la figura en el paso 1. Entonces, el tecleo **se aplica**.
3. Verifique el accesibilidad de la capa 3 entre el regulador y el servidor Radius configurado con la ayuda del **comando ping**. Esta opción del ping está también disponible en la página del servidor Radius configurado en el WLC GUI en la lengueta de la **autenticación de Security>RADIUS**.Este diagrama muestra una contestación del ping exitoso del servidor de RADIUS. Por lo tanto, el accesibilidad de la capa 3 está disponible entre el regulador y el servidor de
RADIUS.

Configuración del servidor de RADIUS

Complete los pasos en estas secciones para configurar al servidor de RADIUS:

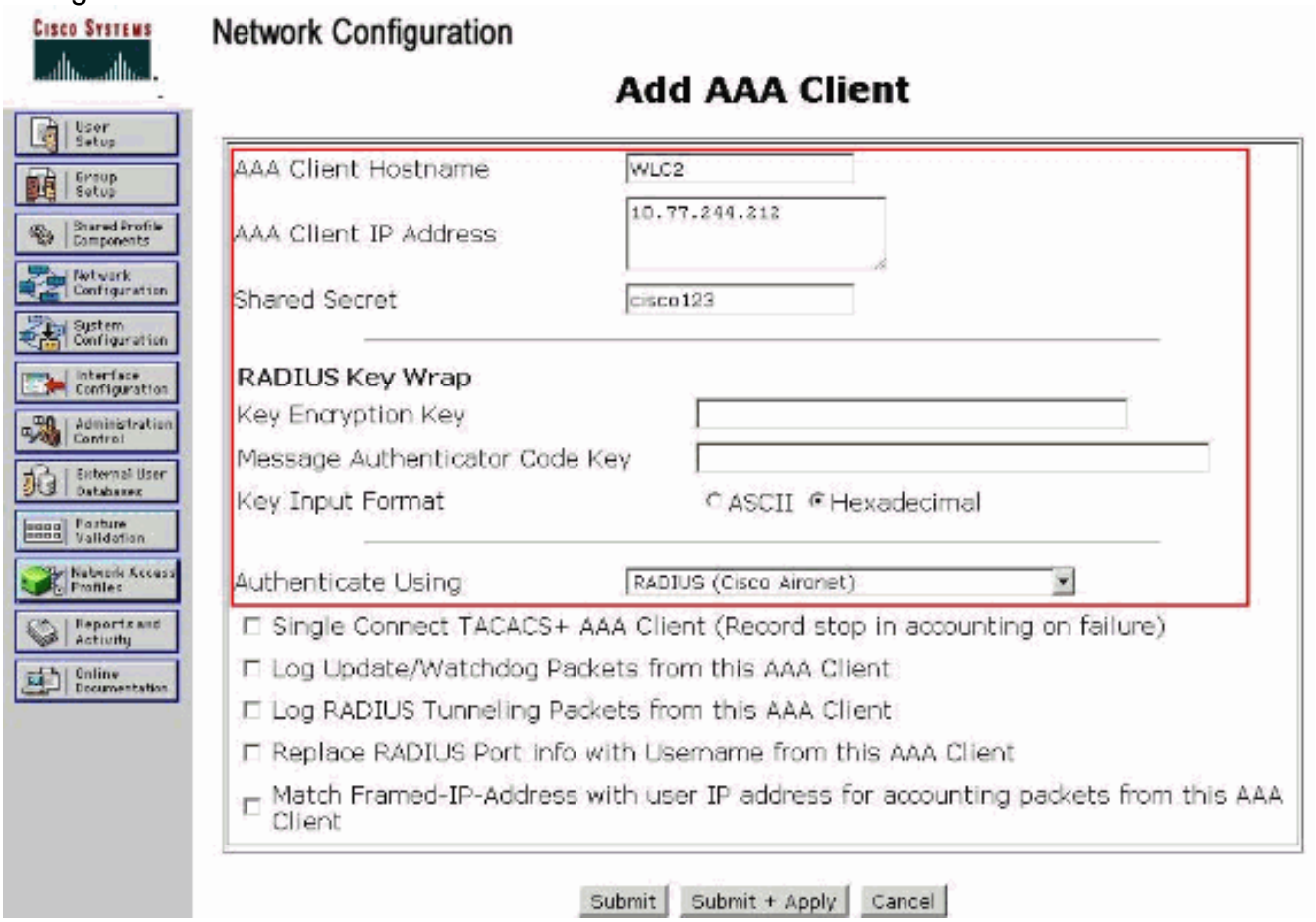
1. Agregue el WLC como cliente AAA al servidor de RADIUS
2. Configure el atributo de tipo de servicio apropiado RADIUS IETF para un administrador del pasillo

Agregue el WLC como cliente AAA al servidor de RADIUS

Complete estos pasos para agregar el WLC como cliente AAA en el servidor de RADIUS. Según lo mencionado anterior, este documento utiliza el ACS como el servidor de RADIUS. Usted puede utilizar a cualquier servidor de RADIUS para esta configuración.

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

1. Del ACS GUI, elija la lengueta de la **configuración de red**.
2. En los clientes AAA, haga clic en Add Entry (Agregar entrada).
3. En la ventana del cliente AAA del agregar, ingrese el nombre del host del WLC, el IP Address del WLC, y una clave secreta compartida. Vea el diagrama del ejemplo bajo paso 5.
4. De la autenticidad usando el menú desplegable, elija **RADIUS (Cisco Aironet)**.
5. Haga clic **Submit + Restart** para salvar la configuración.

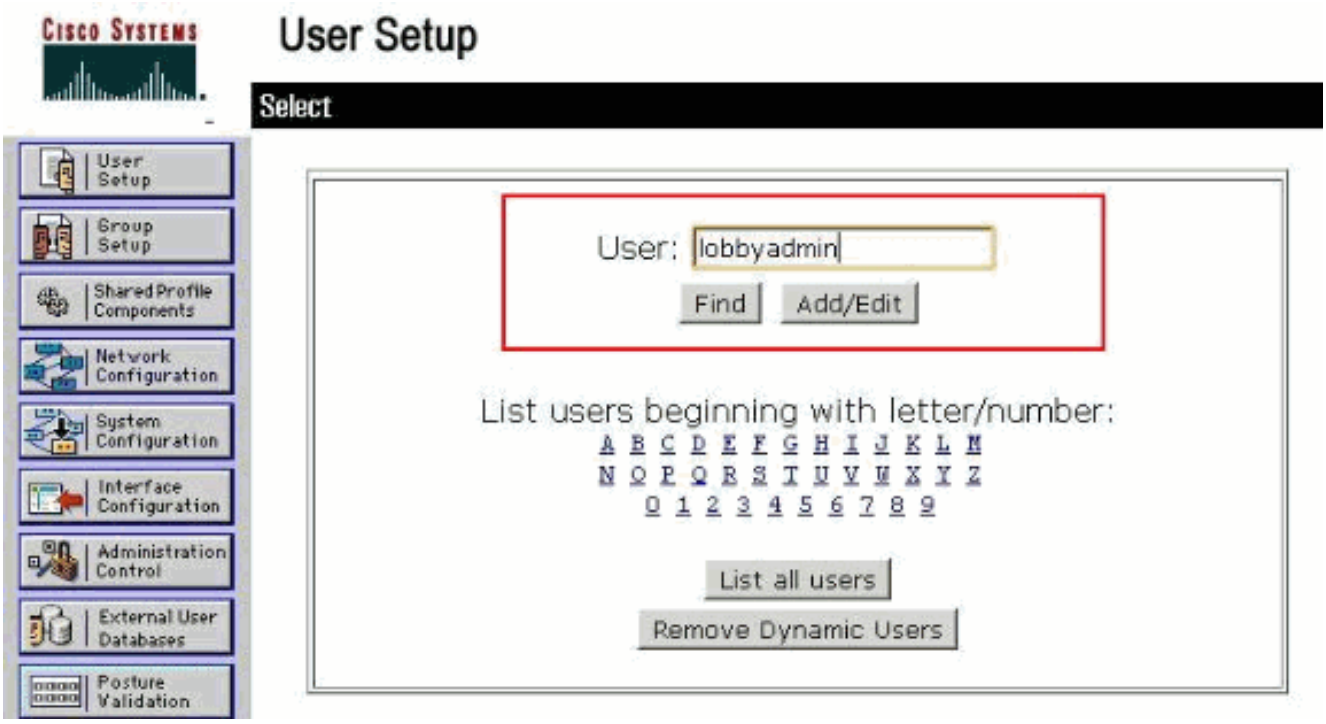


Configure el atributo de tipo de servicio apropiado RADIUS IETF para un administrador del pasillo

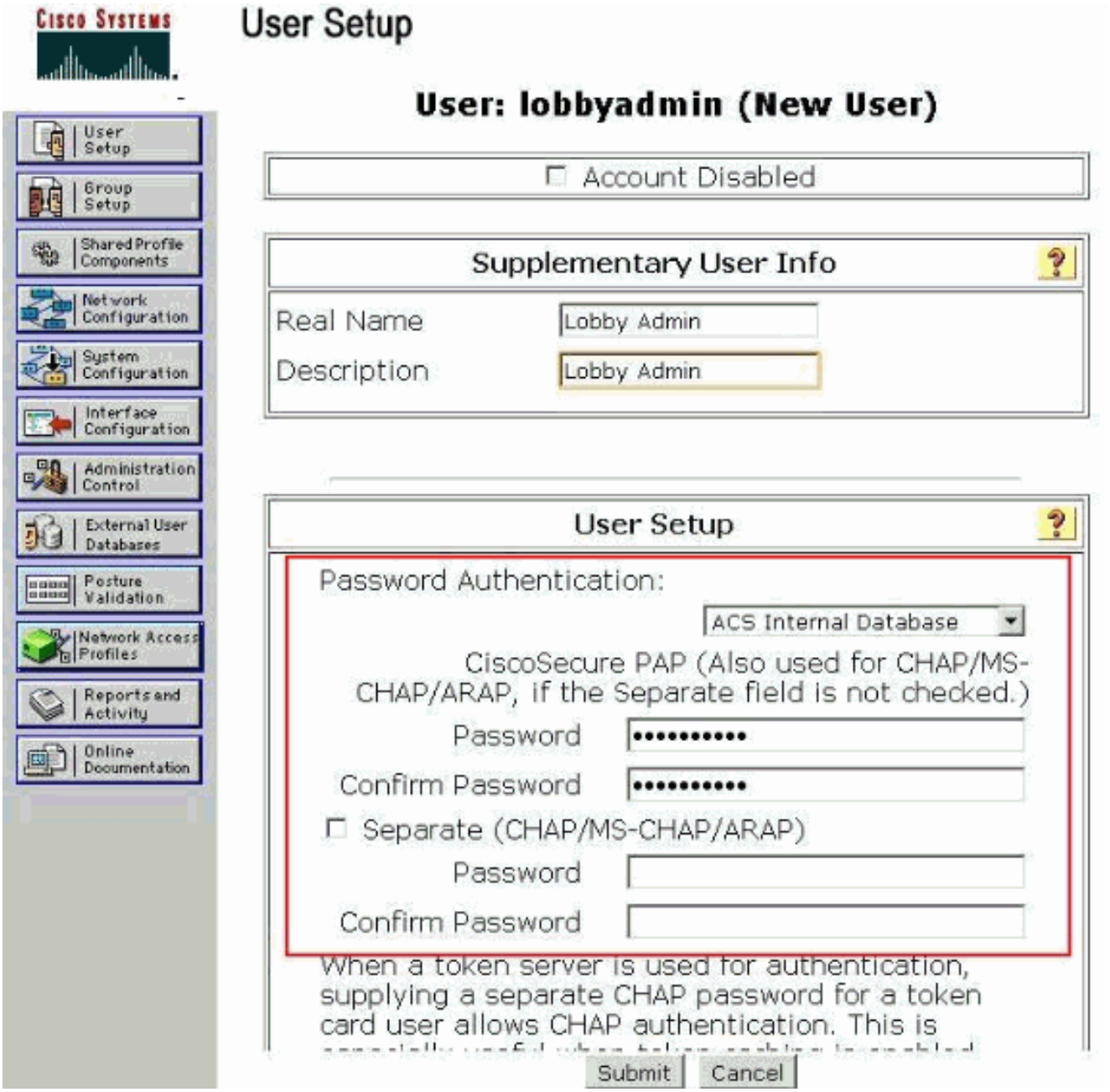
Para autenticar a un usuario de administración de un regulador como administrador del pasillo vía el servidor de RADIUS, usted debe agregar al usuario a la base de datos RADIUS con el atributo de tipo de servicio del IETF RADIUS fijado al **servicio repetido administrativo**. Este atributo asigna a usuario específico el papel de un administrador del pasillo en un regulador.

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

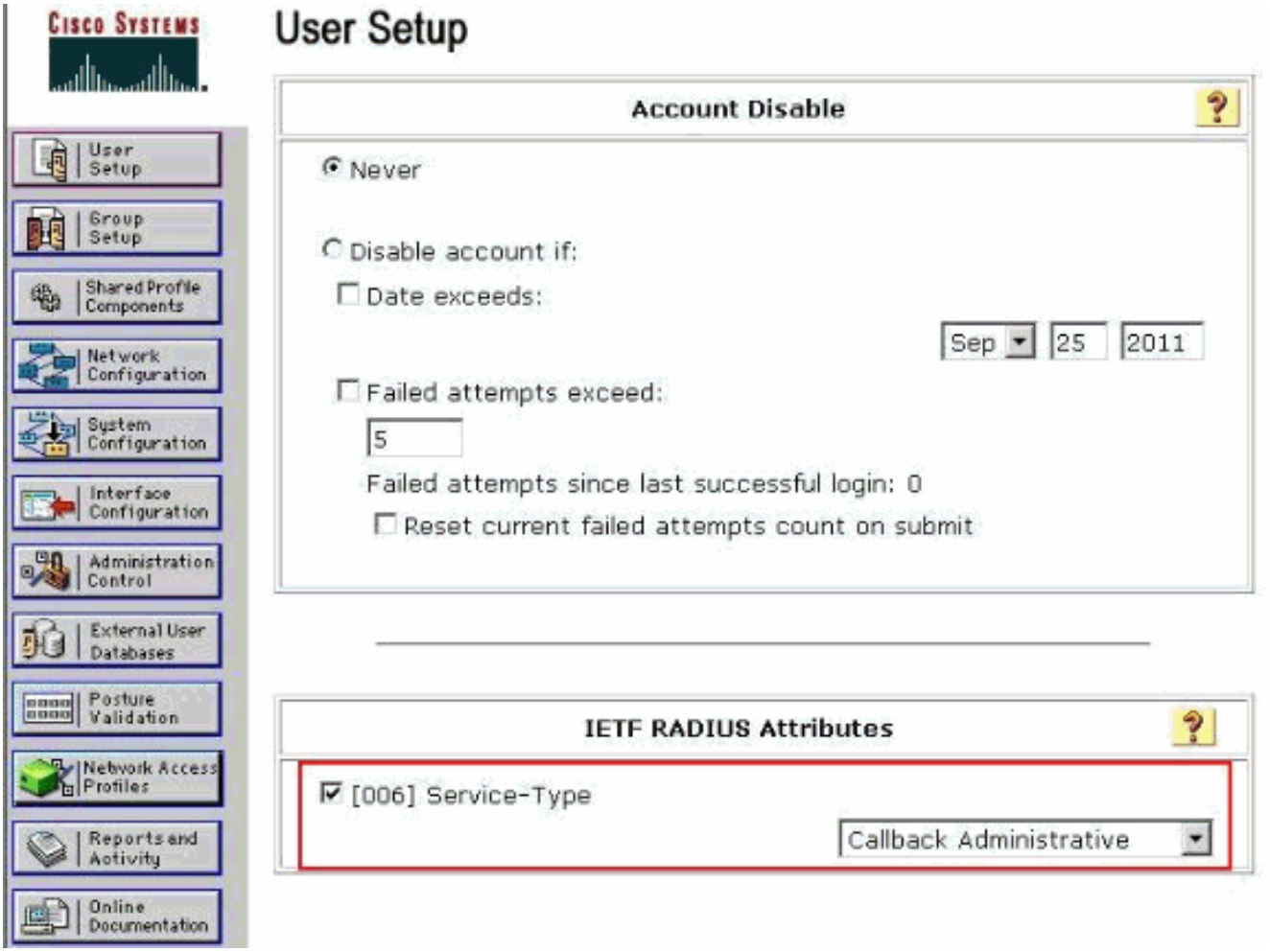
1. Del ACS GUI, elija la lengueta de la **configuración de usuario**.
2. Ingrese el nombre de usuario que se agregará al ACS como esta ventana de muestra muestra:



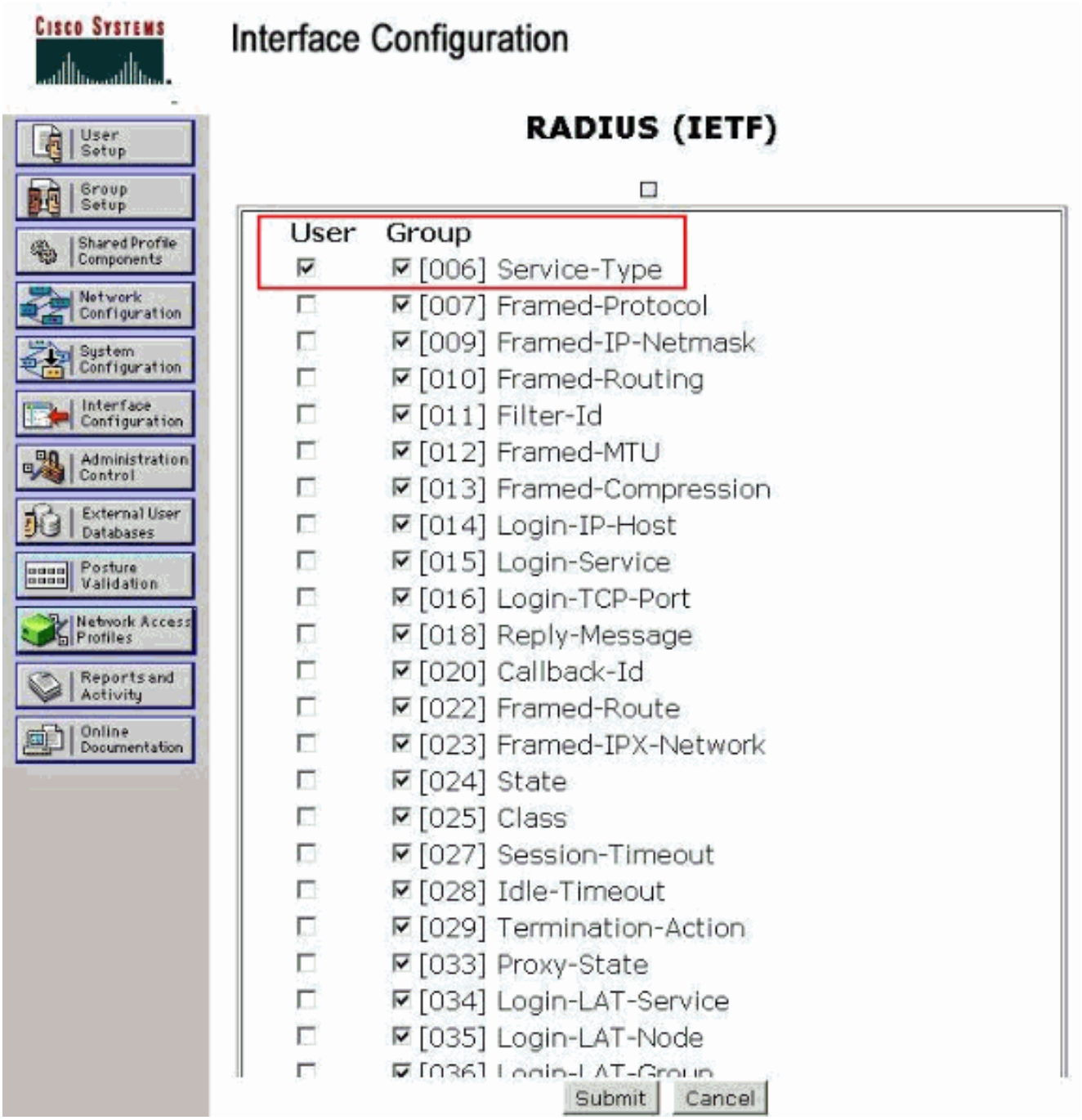
3. El tecleo **agrega/edita** para ir al usuario edita la página.
4. En el usuario edite la página, proporcione a los detalles del Nombre real, de la descripción y de la contraseña de este usuario.En este ejemplo, el nombre de usuario y contraseña usado es ambo
   lobbyadmin.



5. Navegue hacia abajo a los atributos IETF RADIUS que fijan y marque la casilla de verificación del **atributo de tipo de servicio**.
6. Elija el **servicio repetido administrativo del** menú desplegable del tipo de servicio y el tecleo **somete**.Éste es el atributo que asigna a este usuario el papel de un administrador del pasillo.



A veces, este atributo de tipo de servicio no es visible bajo ajustes de usuario. En estos casos, complete estos pasos para hacerlo visible:Del ACS GUI, elija la **configuración de la interfaz > RADIUS (IETF)** para habilitar los atributos IETF en la ventana de la configuración de usuario.Esto le trae a la página Configuración RADIUS (IETF).De la página Configuración RADIUS (IETF), usted puede habilitar el atributo IETF que necesita ser visible bajo el usuario o configuraciones de grupo. Para esta configuración, el **tipo de servicio del** control para la columna usuario y el tecleo **someten**.Esta ventana muestra un ejemplo:



Nota: Este ejemplo especifica la autenticación en por usuario una base. Usted puede también realizar la autenticación basada en el grupo a quien un usuario determinado pertenece. En estos casos, marque el cuadro de **casilla del grupo** de modo que este atributo sea visible bajo configuraciones de grupo.**Nota:** También, si la autenticación está sobre una base del grupo, usted necesita asignar a los usuarios a un grupo determinado y configurar los atributos de la configuración de grupo IETF para proporcionar los privilegios de acceso a los usuarios de ese grupo. Refiera a la Administración del grupo de usuarios para información detallada sobre cómo configurar y manejar a los grupos.

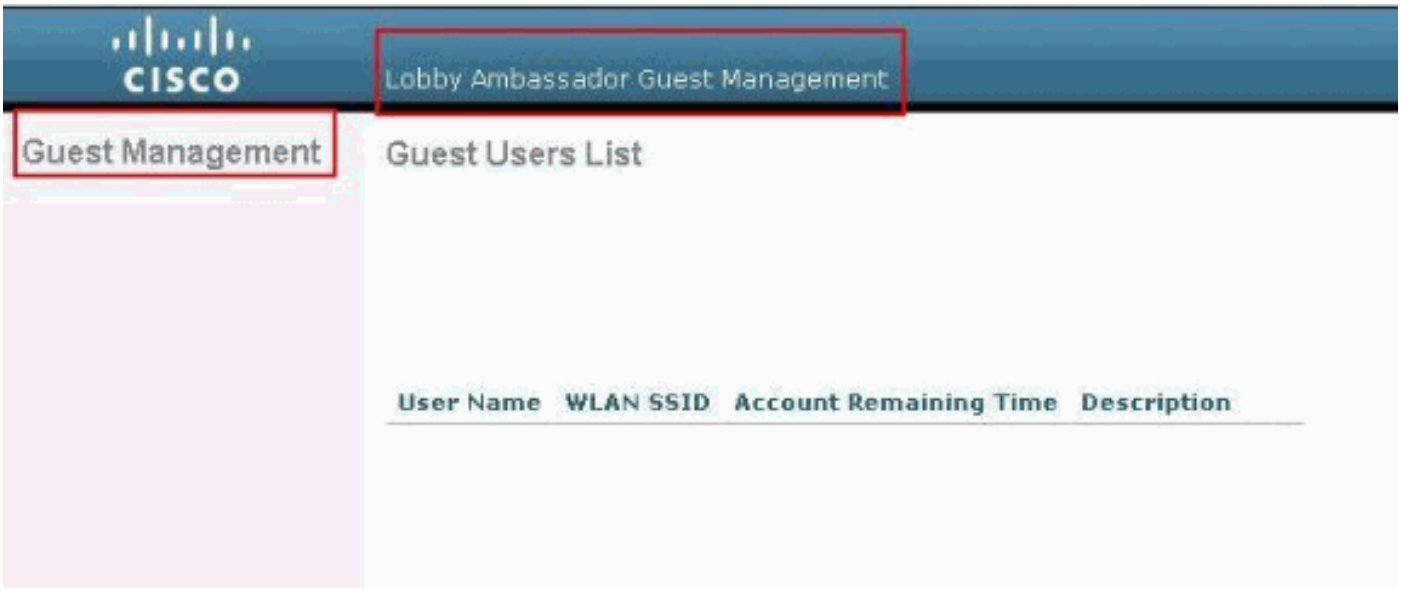
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar que su configuración trabaje correctamente, acceda el WLC con el modo GUI (HTTP/HTTPS).

Nota: Un embajador del pasillo no puede acceder la interfaz CLI del regulador y por lo tanto puede crear las cuentas de Usuario invitado solamente del regulador GUI.

Cuando aparece el prompt de inicio de sesión, ingrese el nombre de usuario y contraseña según lo configurado en el ACS. Si usted tiene las configuraciones correctas, le autentican con éxito en el WLC como **administrador del pasillo**. Este ejemplo muestra cómo el GUI de un administrador del pasillo se ocupa la autenticación satisfactoria:



Nota: Usted puede ver que un administrador del pasillo no tiene ninguna otra opción aparte de la Administración del Usuario invitado.

Para verificarla del modo CLI, Telnet en el regulador como administrador de lectura/grabación. Publique el **comando debug aaa all enable** en el regulador CLI.

```
(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 esta salida, usted puede ver que el atributo de tipo de servicio 11 (servicio repetido administrativo) está pasado sobre el regulador del servidor ACS y del usuario está abierto una sesión como administrador del pasillo.

Estos comandos pudieron estar de ayuda adicional:

- **permiso de los detalles aaa del debug**
- **permiso de los eventos aaa del debug**
- **permiso de los paquetes aaa del debug**

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Troubleshooting

Cuando usted inicia sesión a un regulador con los privilegios del embajador del pasillo, usted no puede crear una cuenta de Usuario invitado con “un valor del tiempo de la vida del **0"**, que es una cuenta que nunca expira. En estas situaciones, usted recibe el `valor del curso de la vida no puede ser 0` mensajes de error.

El es debido al Id. de bug Cisco CSCsf32392 (clientes registrados solamente), que se encuentra principalmente con la versión 4.0 del WLC. Este bug se ha resuelto en la versión 4.1 del WLC.

Información Relacionada

- Autenticación de servidor de RADIUS de los usuarios de administración en el ejemplo de la configuración de controlador
- Configuración de la red TACACS+ del Cisco Unified Wireless
- Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 4.0 - Manejo de las cuentas de usuario
- ACL en el ejemplo de la configuración de controlador del Wireless LAN
- Regulador del Wireless LAN (WLC) FAQ
- ACL en los reguladores del Wireless LAN: Reglas, limitaciones, y ejemplos
- Ejemplo de configuración de autenticación Web externa con controladores inalámbricos
- 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