Autenticación de servidor de RADIUS de los usuarios de administración en el ejemplo de configuración del regulador del Wireless LAN (WLC)

Contenido

Introducción

Este documento explica cómo configurar un controlador de LAN inalámbrico (WLC) y un Access Control Server (Cisco Secure ACS) de modo que el servidor AAA pueda autenticar los usuarios de administración en el controlador. El documento también explica cómo diferentes usuarios de administración pueden recibir diferentes privilegios usando los atributos específicos del vendedor (VSA) devueltos por el servidor Cisco Secure ACS 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 como el Cisco Secure ACS

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

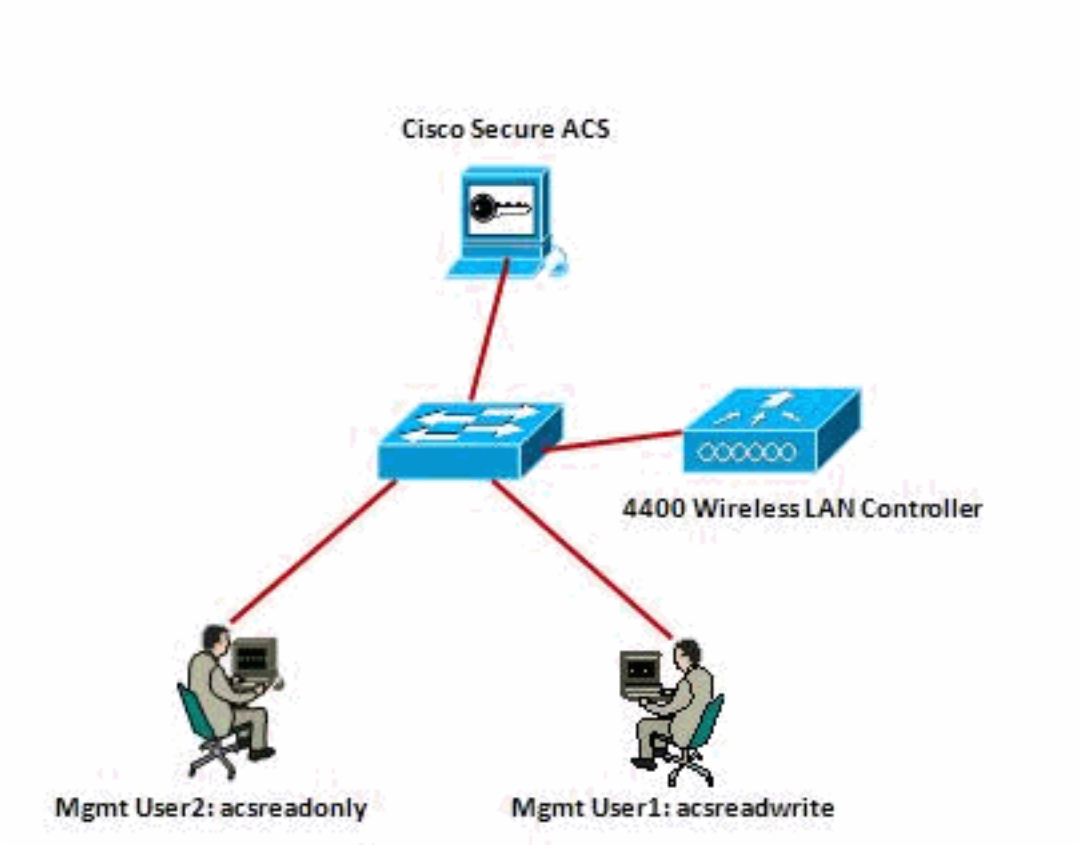
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

En esta sección, le presentan con la información sobre cómo configurar el WLC y el ACS para el propósito descrito en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este ejemplo de configuración utiliza estos parámetros:

- Dirección IP del Cisco Secure ACS — 172.16.1.1/255.255.0.0
- Dirección IP de la interfaz de administración del regulador — 172.16.1.30/255.255.0.0
- Clave secreta compartida que se utiliza en el punto de acceso y el servidor de RADIUS — asdf1234
- Éstas son las credenciales de los dos usuarios que este ejemplo configura en el ACS:Nombre de usuario - acsreadwriteContraseña - acsreadwriteNombre de usuario - acsreadonlyContraseña - acsreadonly

Usted necesita configurar el WLC y el Cisco Secure ACS seguro de Cisco para:

- Cualquier usuario que registre en el WLC con el nombre de usuario y contraseña mientras que el **acsreadwrite** se da el acceso administrativo completo al WLC.
- Dan cualquier usuario que registre en el WLC con el nombre de usuario y contraseña como **acsreadonly** acceso de sólo lectura al WLC.

Configuraciones

En este documento, se utilizan estas configuraciones:

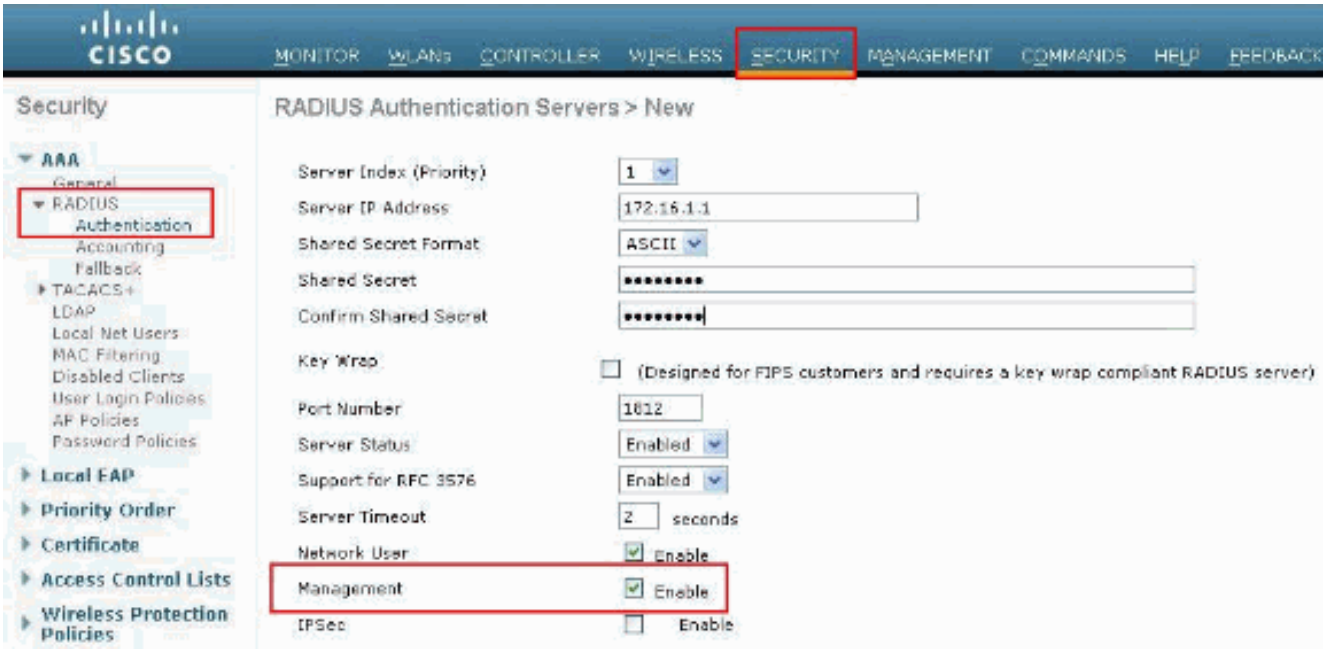
- Configuración del WLC
- Configuración del Cisco Secure ACS

Configuración del WLC

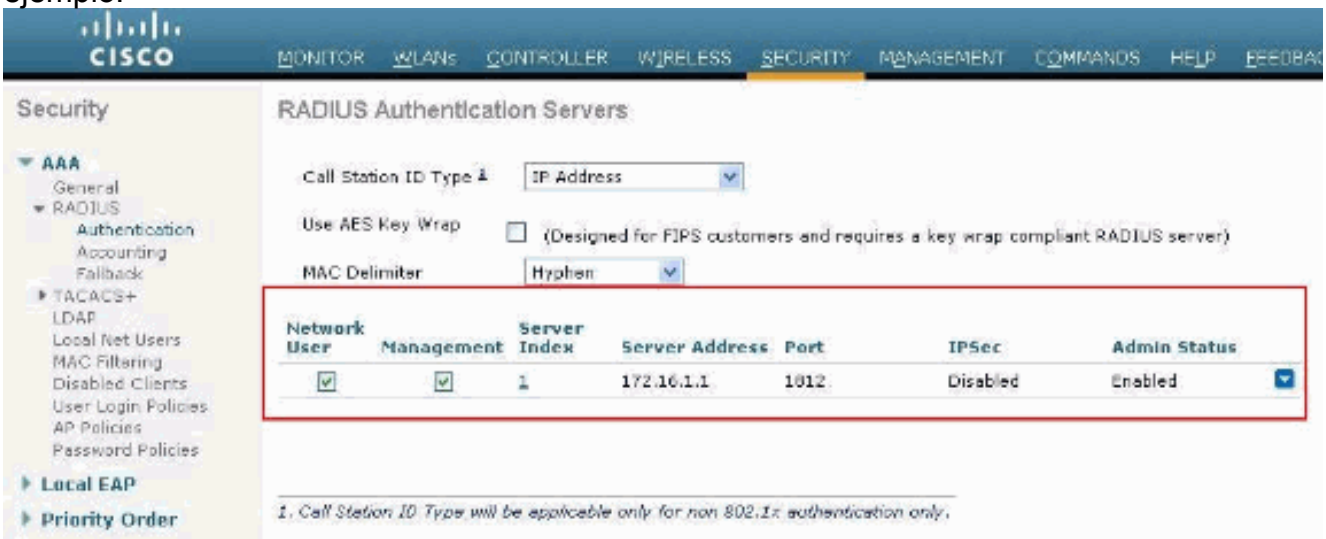
Configure el WLC para validar la Administración a través del servidor del Cisco Secure ACS

Complete estos pasos para configurar el WLC de modo que pueda comunicar con el servidor de RADIUS.

1. Del WLC GUI, haga clic la **Seguridad**. Del menú a la izquierda, haga clic **RADIUS > autenticación**. La página de los **servidores de autenticación de RADIUS** aparece. Para agregar a un nuevo servidor de RADIUS, haga clic **nuevo**. En los **servidores de autenticación de RADIUS > la nueva** página, ingresa los parámetros específicos al servidor de RADIUS. Aquí está un
ejemplo.



2. Marque el botón de radio de la **Administración** para permitir que el servidor de RADIUS autentique a los usuarios que inician sesión el WLC.**Nota:** Asegúrese de que el secreto compartido configurado en esta página haga juego con el secreto compartido configurado en el servidor de RADIUS. Solamente entonces el WLC puede comunicar con el servidor de RADIUS.
3. Verifique si el WLC esté configurado para ser manejado por el Cisco Secure ACS. Para hacer esto, haga clic la **Seguridad del** WLC GUI. La ventana resultante GUI aparece similar a este
ejemplo.



Usted puede ver que la **casilla de verificación Management (Administración)** está habilitada para el servidor de RADIUS 172.16.1.1. Esto ilustra que el ACS está permitido autenticar a los usuarios de administración en el WLC.

Configuración del Cisco Secure ACS

Complete los pasos en estas secciones para configurar el ACS:

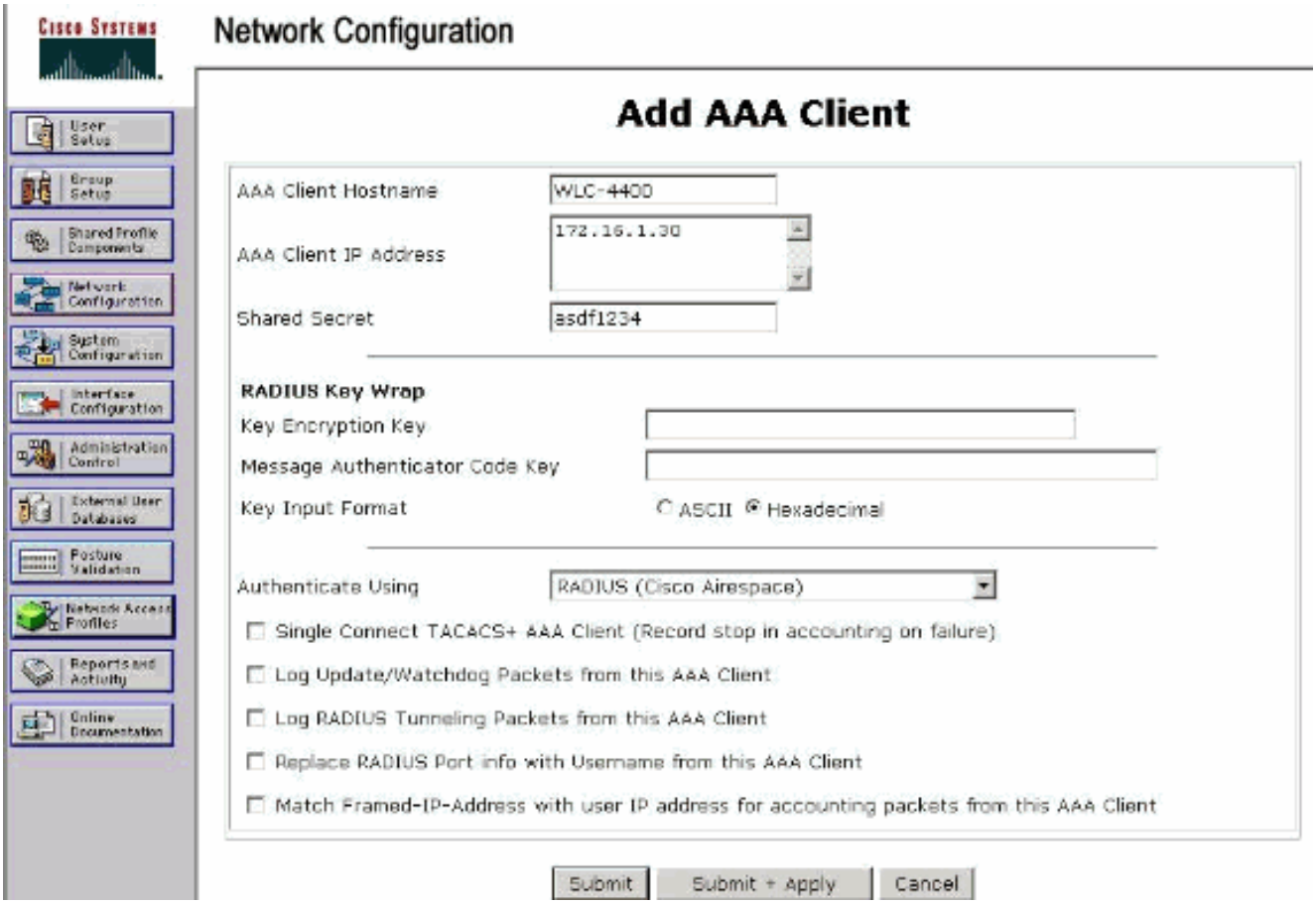
1. Agregue el WLC como cliente AAA al servidor de RADIUS.
2. Configure los usuarios y sus atributos apropiados RADIUS IETF.
3. Configure a un usuario con el acceso de lectura/escritura.

4. Configure a un usuario con acceso de sólo lectura.

Agregue el WLC como cliente AAA al servidor de RADIUS

Complete estos pasos para agregar el WLC como cliente AAA en el Cisco Secure ACS.

1. Del ACS GUI, haga clic 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.En este ejemplo, éstas son las configuraciones:Nombre del host del cliente AAA está el WLC-4400172.16.1.30/16 es la dirección IP del cliente AAA, que, en este caso es el WLC.La clave secreta compartida es el "asdf1234".



   Esta clave secreta compartida debe ser lo mismo que la clave secreta compartida que usted configura en el WLC.
4. De la autenticidad usando el menú desplegable, elija **RADIUS (Airespace de Cisco)**.
5. Haga clic **Submit + Restart** para salvar la configuración.

Configure los usuarios y sus atributos apropiados RADIUS IETF

Para autenticar a un usuario vía un servidor de RADIUS, para el login del regulador y la Administración, usted debe agregar al usuario a la base de datos RADIUS con el *tipo de servicio del* atributo IETF RADIUS fijado al valor apropiado según los privilegios del usuario.

- Para fijar los privilegios de lectura/grabación para el usuario, fije el atributo de *tipo de servicio a* **administrativo**.
- Para fijar los privilegios solo lecturas para el usuario, fije el NAS-**prompt del** atributo de *tipo de*

servicio.

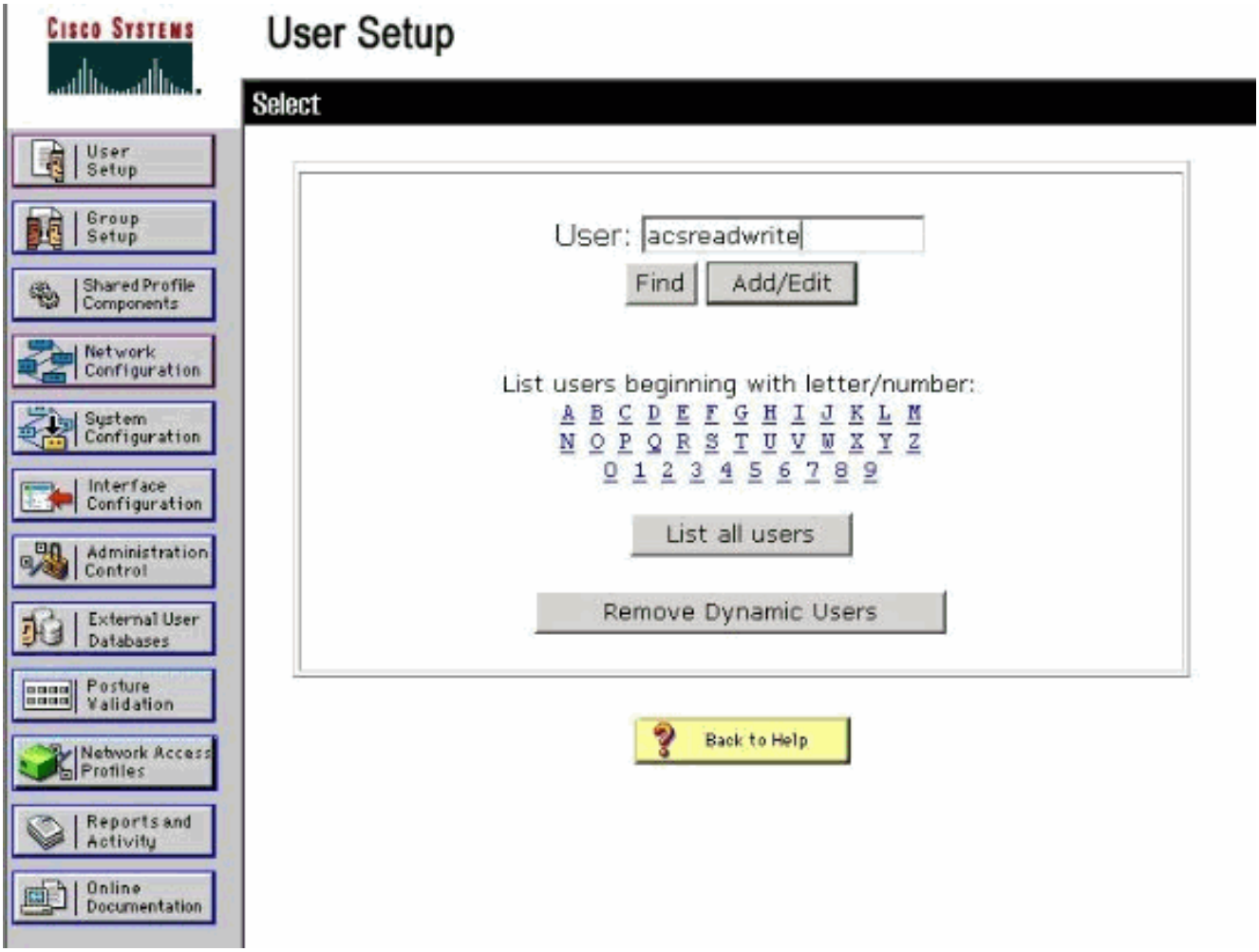
Configure a un usuario con el acceso de lectura/escritura

El primer ejemplo muestra la configuración de un usuario con el acceso total al WLC. Cuando este usuario intenta iniciar sesión al regulador, el servidor de RADIUS autentica y proporciona a este usuario con el acceso administrativo completo.

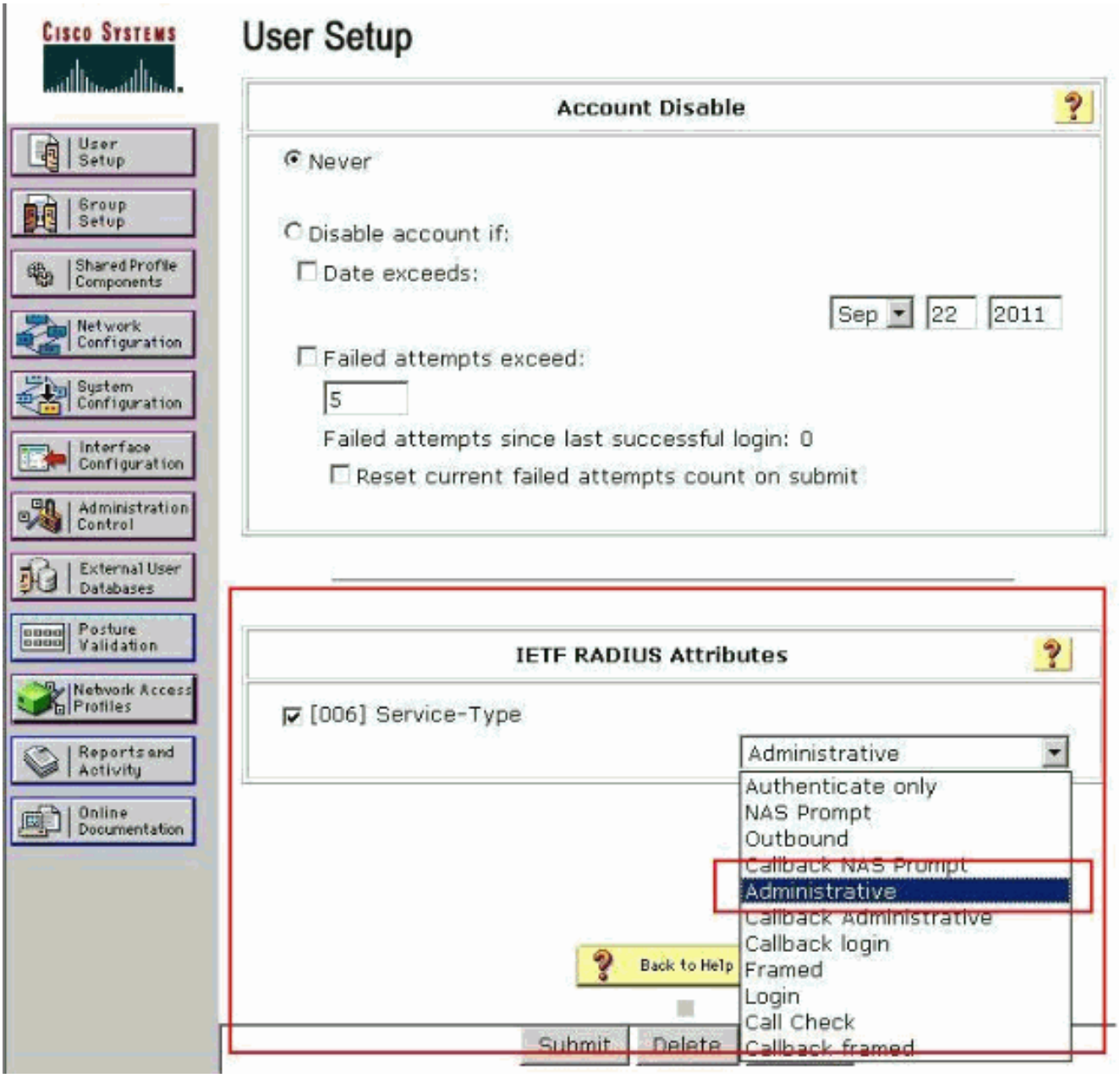
En este ejemplo, el nombre de usuario y contraseña es **acsreadwrite**.

Complete estos pasos en el Cisco Secure ACS.

1. Del ACS GUI, haga clic la **configuración de usuario**.
2. Teclee el nombre de usuario que se agregará al ACS como esta ventana de muestra muestra.

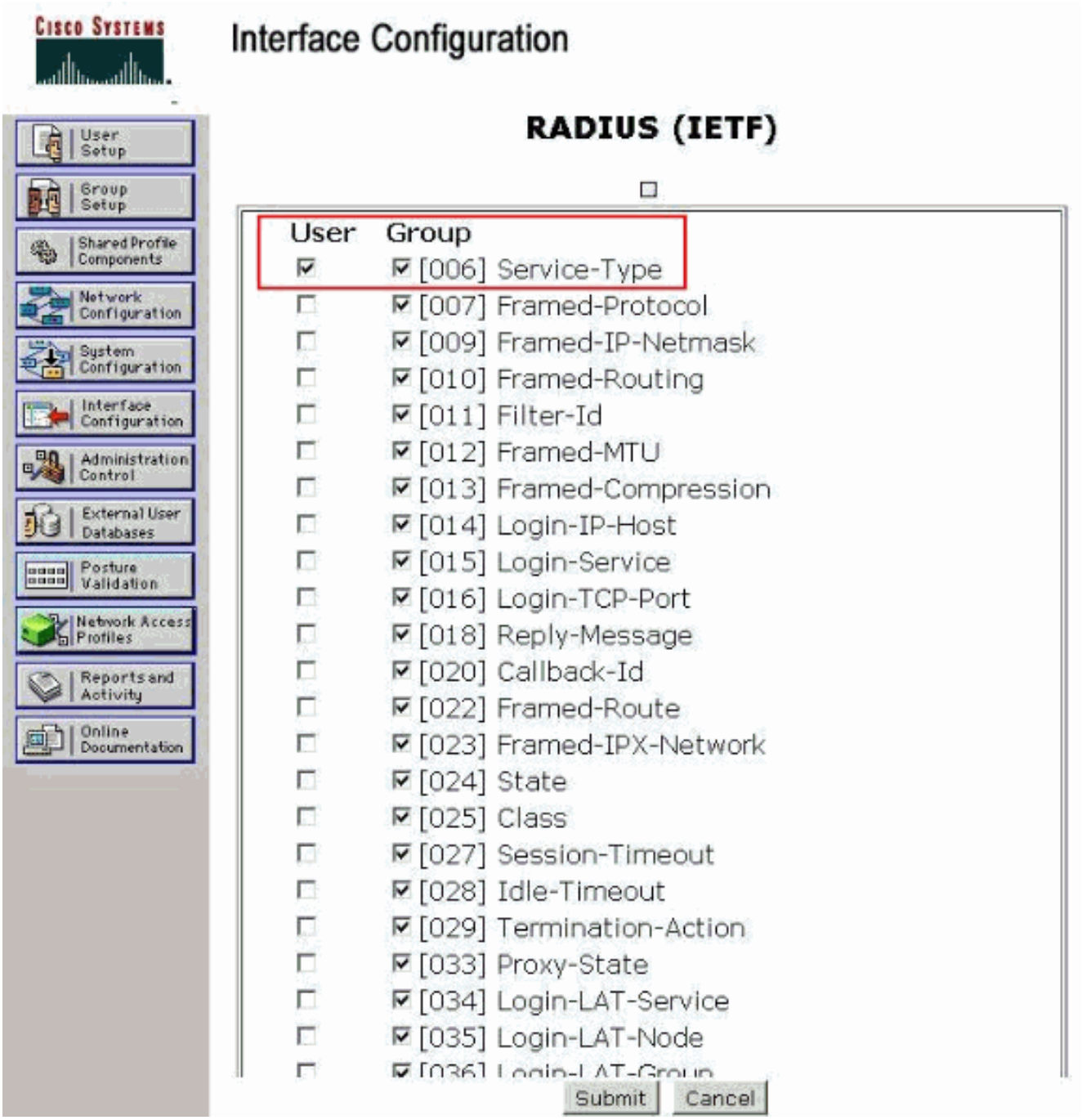


3. El tecleo **agrega/edita** para ir al usuario edita la página.
4. En el usuario edite la página, proporcione a los detalles del Nombre real, de la descripción y de la contraseña de este usuario.
5. Navegue hacia abajo a los atributos IETF RADIUS que fijan y al **atributo de tipo de servicio del** control.
6. Puesto que, en este ejemplo, el acsreadwrite del usuario necesita ser dado el acceso total, elija **administrativo** para el menú desplegable del tipo de servicio y el tecleo **somete**.Esto se asegura de que este usuario determinado tenga acceso de lectura/escritura al WLC.



A veces, este atributo de tipo de servicio no es visible bajo ajustes de usuario. En estos casos, complete estos pasos para hacerlo visible.

1. 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 lleva a la página Configuración RADIUS (IETF).
2. 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, habilite 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 para información detallada sobre cómo configurar y manejar a los grupos.

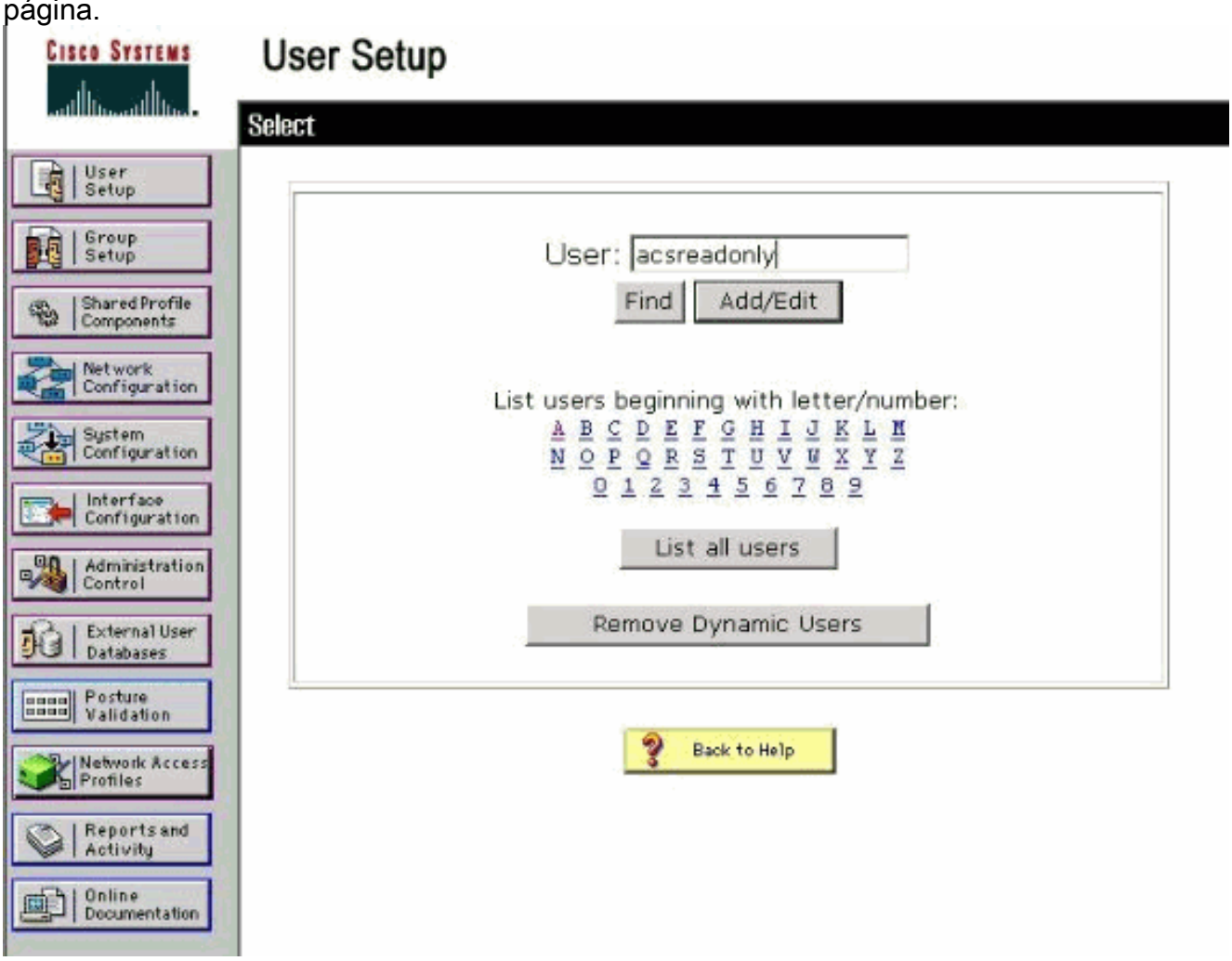
Configure a un usuario con acceso de sólo lectura

Este ejemplo muestra la configuración de un usuario con acceso de sólo lectura al WLC. Cuando este usuario intenta iniciar sesión al regulador, el servidor de RADIUS autentica y proporciona a este usuario con acceso de sólo lectura.

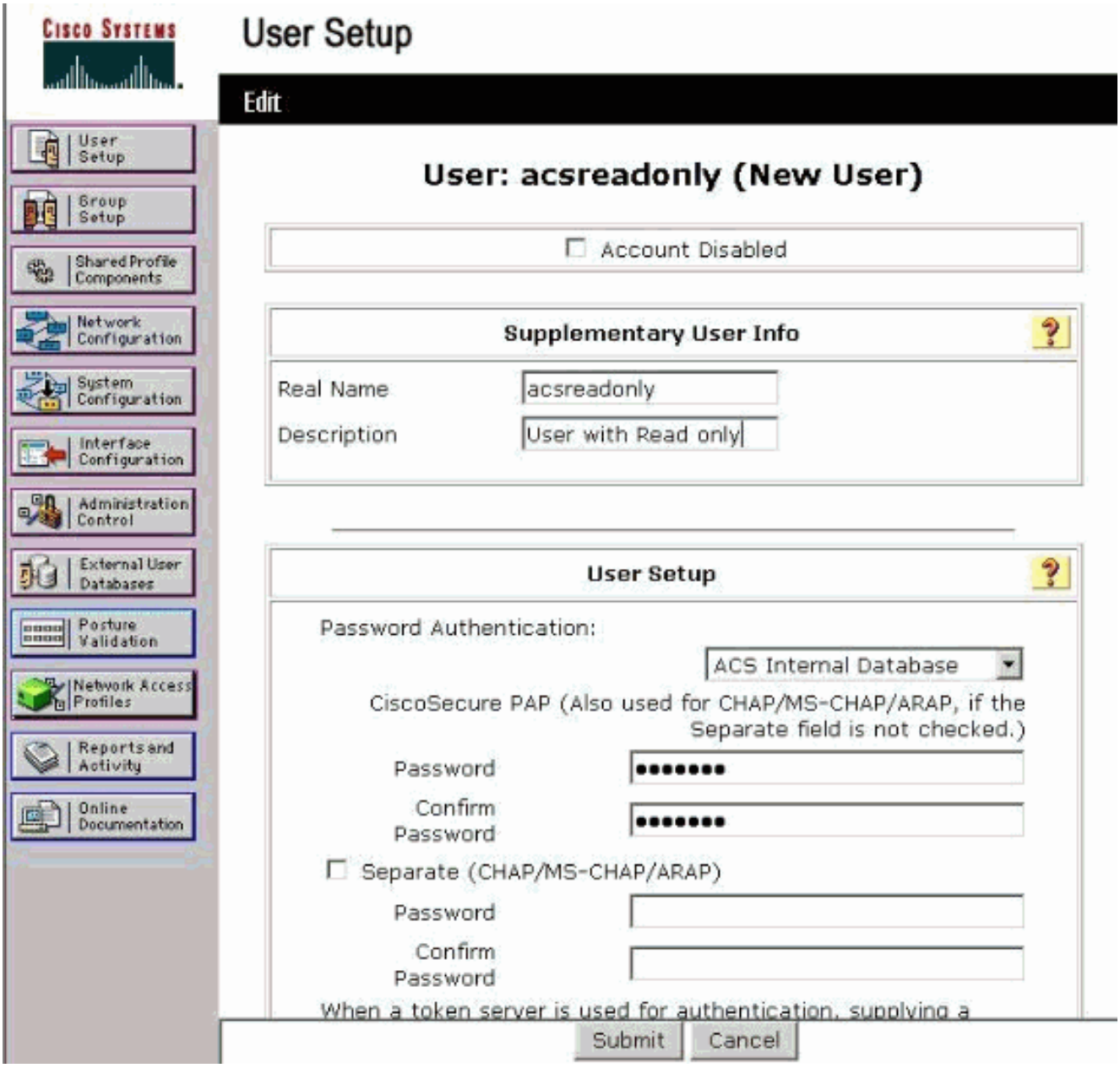
En este ejemplo, el nombre de usuario y contraseña está **acsreadonly**.

Complete estos pasos en el Cisco Secure ACS:

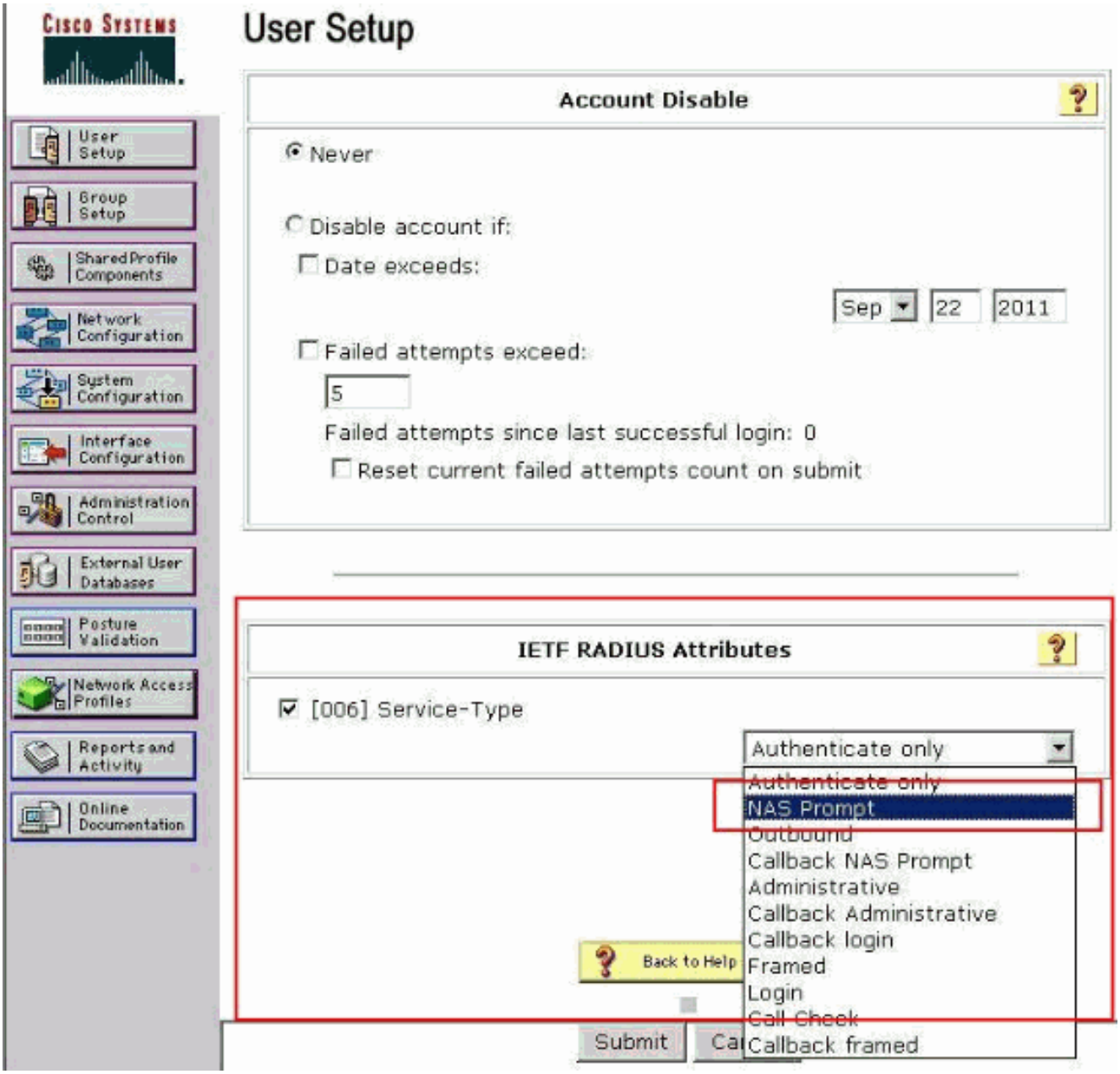
1. Del ACS GUI, haga clic la **configuración de usuario**.
2. Teclee el nombre de usuario que usted quiere agregar al ACS y al tecleo **agrega/edita** para ir al usuario edita la
página.



3. Proporcione el Nombre real, la descripción y la contraseña de este usuario. Esta ventana muestra un
ejemplo.

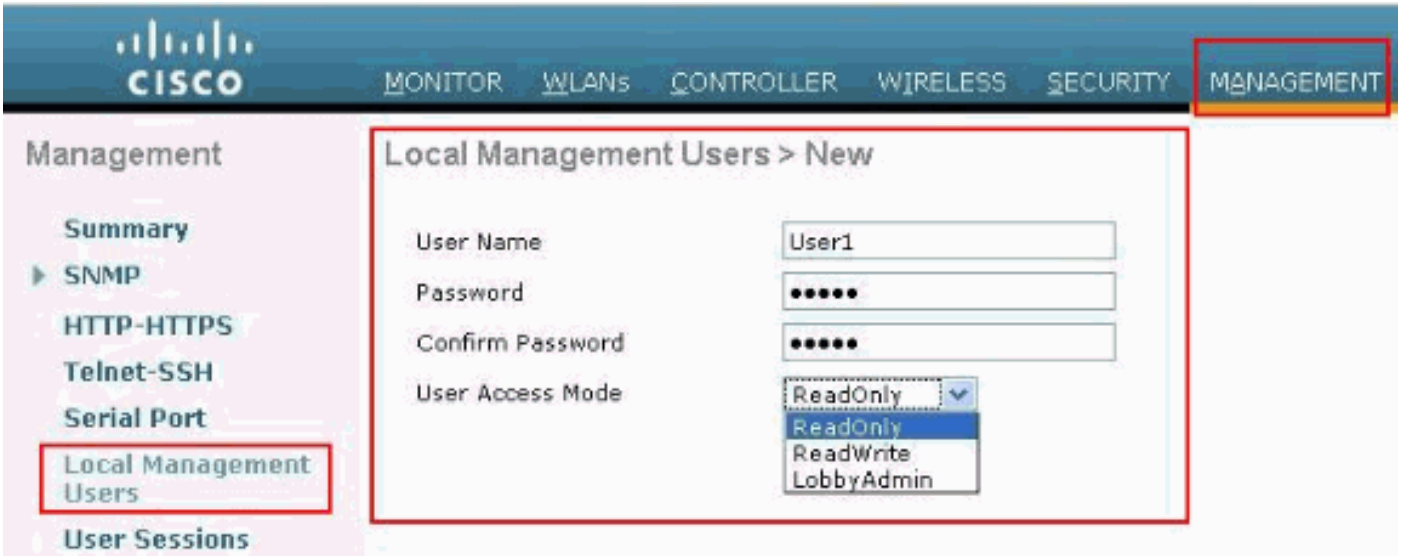


4. Navegue hacia abajo a los atributos IETF RADIUS que fijan y al **atributo de tipo de servicio del** control.
5. Puesto que, en este ejemplo, el usuario acsreadonly necesita tener acceso de sólo lectura, elegir el **prompt NAS del** menú desplegable y del tecleo del tipo de servicio **someta**.Esto se asegura de que este usuario determinado tenga acceso de sólo lectura al WLC.



Maneje el WLC localmente así como a través del servidor de RADIUS

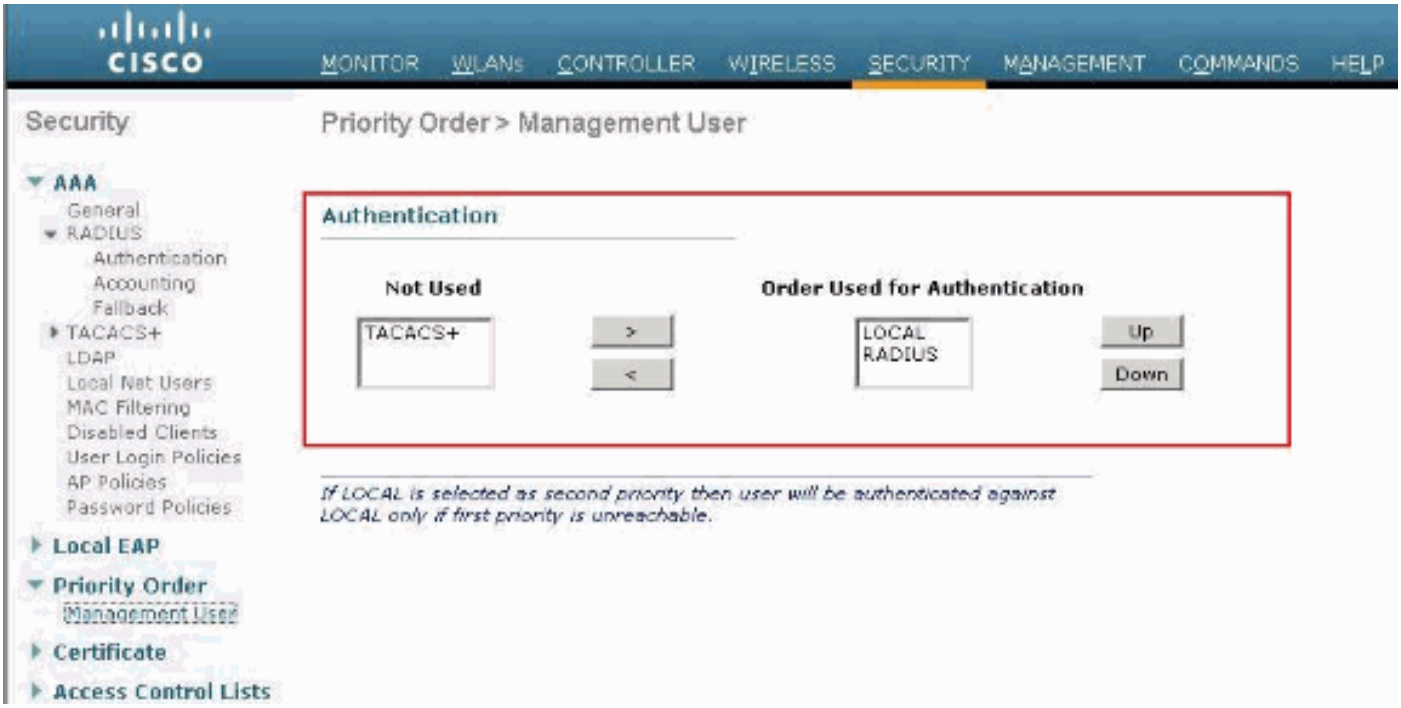
Usted puede también configurar a los usuarios de administración localmente en el WLC. Esto se puede hacer del regulador GUI, bajo los **usuarios de la Administración > de la administración local**.



Asuma que el WLC está configurado con los usuarios de administración localmente así como en el servidor de RADIUS con la **casilla de verificación Management (Administración)** habilitada. En tal escenario, por abandono, cuando un usuario intenta iniciar sesión al WLC, el WLC se comporta de este modo:

1. El WLC primero mira a los usuarios de la administración local definidos para validar al usuario. Si el usuario existe en su lista local, después permite la autenticación para este usuario. Si no aparece este usuario localmente, después mira al servidor de RADIUS.
2. Si el mismo usuario existe localmente así como en el servidor de RADIUS pero con diversos privilegios de acceso, después el WLC autentica al usuario con los privilegios especificados localmente. Es decir la configuración local en el WLC toma siempre la precedencia cuando está comparada al servidor de RADIUS.

La orden de la autenticación para los usuarios de administración se puede cambiar en el WLC. Para hacer esto, de la **página Seguridad** en el WLC, **orden de la prioridad del** tecleo **> usuario de administración**. De esta página usted puede especificar la orden de la autenticación. Aquí está un ejemplo.



Nota: Si el LOCAL se selecciona como segunda prioridad, después autenticarán al usuario

usando este método solamente si el método definido como la primera prioridad (RADIUS/TACACS) es inalcanzable.

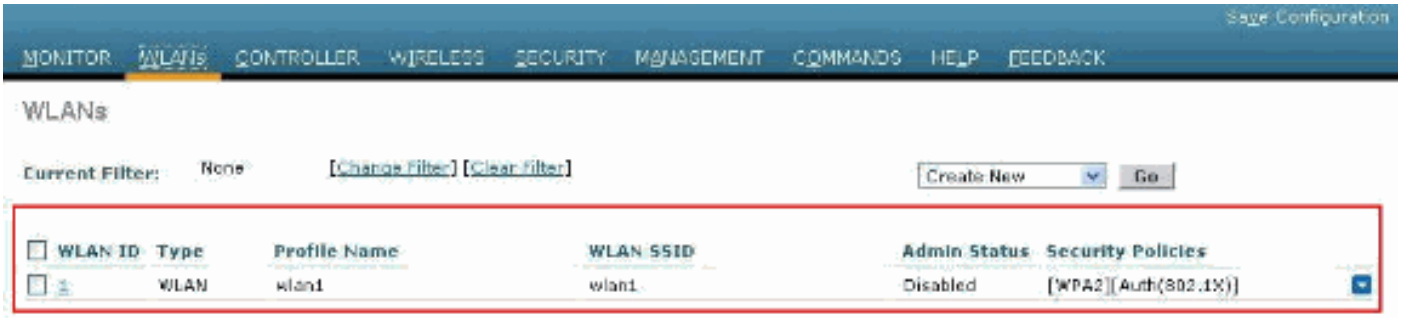
Verificación

Para verificar si sus trabajos de la configuración correctamente, accedan el WLC con el modo CLI o GUI (HTTP/HTTPS). Cuando aparece el prompt de inicio de sesión, teclee el nombre de usuario y contraseña según lo configurado en el Cisco Secure ACS.

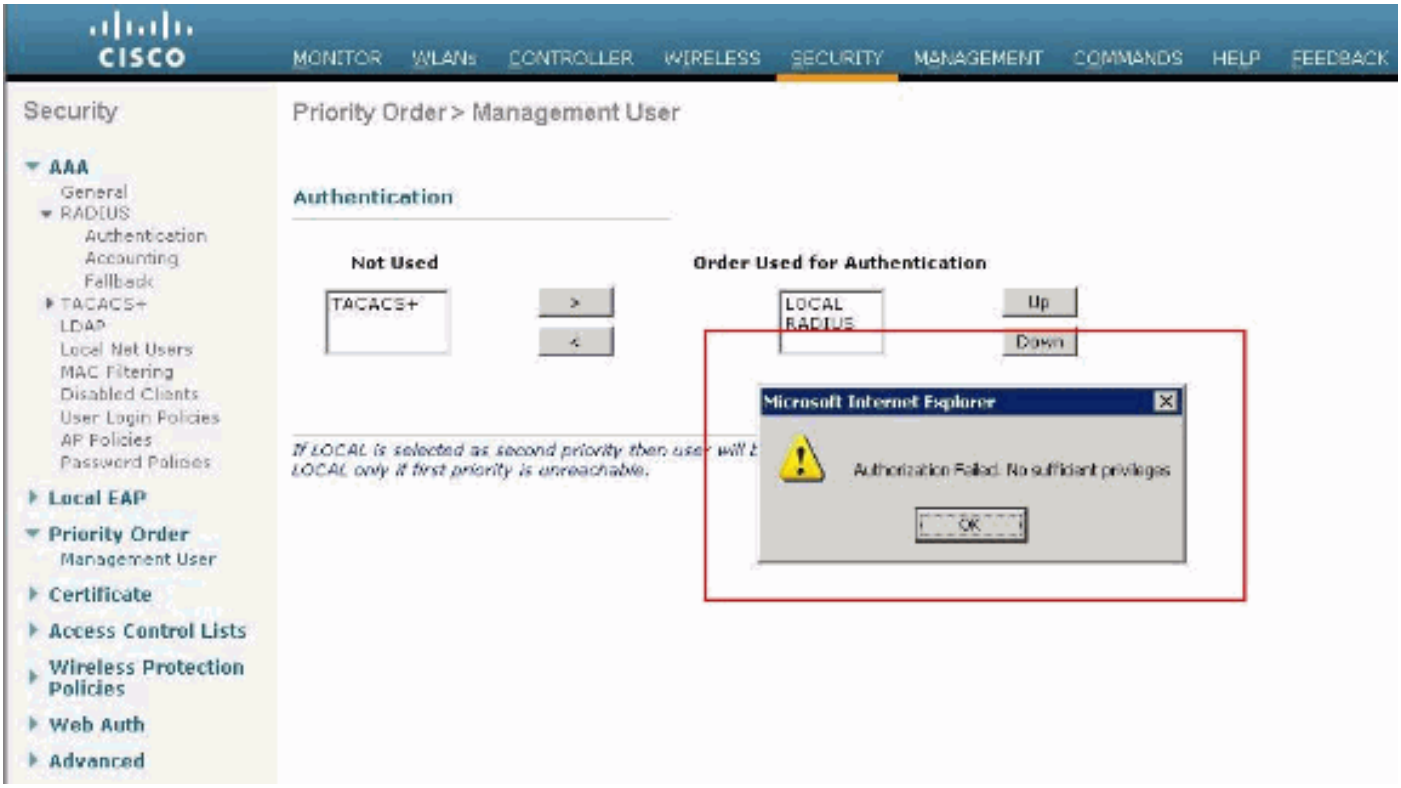
Si usted tiene las configuraciones correctas, le autentican con éxito en el WLC.

Usted puede también asegurarse de si proporcionen el usuario autenticado las restricciones de acceso según lo especificado por el ACS. Para hacer así pues, acceda el WLC GUI con el HTTP/HTTPS (asegúrese de que el WLC esté configurado para permitir el HTTP/HTTPS).

Un usuario con el conjunto de acceso de lectura/escritura en el ACS tiene varios privilegios configurables en el WLC. Por ejemplo, un usuario de lectura/grabación tiene el privilegio de crear una nueva red inalámbrica (WLAN) conforme a la página WLAN del WLC. Esta ventana muestra un ejemplo.



Cuando un usuario con los provileges del read only intenta alterar la configuración en el regulador, el usuario ve este mensaje.



Estas restricciones de acceso se pueden también verificar con el CLI del WLC. En este resultado, se muestra un ejemplo.

```
(Cisco Controller) >?

debug           Manages system debug options.
help            Help
linktest        Perform a link test to a specified MAC address.
logout          Exit this session. Any unsaved changes are lost.
show            Display switch options and settings.

(Cisco Controller) >config

Incorrect usage.  Use the '?' or <TAB> key to list commands.
```

¿Como esta salida de ejemplo muestra, a**?** en el regulador el CLI visualiza una lista de comandos disponibles para el Usuario usuario actual. También note que el **comando config** no está disponible en esta salida de ejemplo. Esto ilustra que un usuario solo lectura no tiene el privilegio de hacer ninguna configuraciones en el WLC. Considerando que, un usuario de lectura/grabación tiene los privilegios de hacer las configuraciones en el regulador (GUI y modo CLI).

Nota: Incluso después usted autentica a un usuario del WLC a través del servidor de RADIUS, pues usted hojea de la página para paginar, el servidor del [S] HTTP todavía autentica completamente al cliente cada vez. La única razón que le no indican para la autenticación en cada página es que sus cachés del buscador y juega de nuevo sus credenciales.

Troubleshooting

Hay ciertas circunstancias cuando un regulador autentica a los usuarios de administración vía el ACS, los finales de la autenticación con éxito (access-accept), y usted no ve ningún error de la autorización en el regulador. *Pero, indican al usuario otra vez para la autenticación.*

En estos casos, usted no puede interpretar cuál es incorrecto y por porqué el usuario no puede registrar en el WLC apenas usando el **comando enable de los eventos aaa del debug**. En lugar, el regulador visualiza otro prompt para la autenticación.

Una razón posible de esto es que el ACS no está configurado para transmitir el atributo de tipo de servicio para ese usuario determinado o para agruparlo aunque el nombre de usuario y contraseña se configura correctamente en el ACS.

La salida del **comando enable de los eventos aaa del debug** no indica que un usuario no tiene los atributos requeridos (por este ejemplo, el atributo de tipo de servicio) aunque un **access-accept** se devuelve del servidor de AAA. Esta salida del **comando enable de los eventos aaa del debug del** ejemplo muestra un ejemplo.

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

Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c

Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40
```

```
Mon Aug 13 20:14:33 2011: protocolType.............................0x00020001

Mon Aug 13 20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept
received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0

Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:14:33 2011: structureSize.............................28

Mon Aug 13 20:14:33 2011: resultCode.................................0

Mon Aug 13 20:14:33 2011: protocolUsed.............................0x00000001

Mon Aug 13 20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

En esta primera salida del **comando enable de los eventos aaa del debug del** ejemplo, usted ve que el access-accept está recibido con éxito del servidor de RADIUS pero el atributo de tipo de servicio no está pasado sobre el WLC. Esto es porque no configuran al usuario determinado con este atributo en el ACS.

El Cisco Secure ACS necesita ser configurado para volver el atributo de tipo de servicio después de la autenticación de usuario. El valor de atributo del tipo de servicio se debe fijar a **administrativo** o al NAS-**prompt** según los privilegios del usuario.

Este segundo ejemplo muestra el **comando enable de los eventos aaa del debug** hecho salir otra vez. Sin embargo, este vez el atributo de tipo de servicio se fija a **administrativo** en el ACS.

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


Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c

Mon Aug 13 20:17:02 2011: Callback.................................0x8250c40

Mon Aug 13 20:17:02 2011: protocolType.............................0x00020001

Mon Aug 13 20:17:02 2011: proxyState.....................1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2
```

```
Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:17:02 2011: structureSize.............................100

Mon Aug 13 20:17:02 2011: resultCode.................................0

Mon Aug 13 20:17:02 2011: protocolUsed.............................0x00000001

Mon Aug 13 20:17:02 2011: proxyState.....................1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type..........0x00000006 (6) (4 bytes)

Mon Aug 13 20:17:02 2011: AVP[02] Class.........
CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)
```

Usted puede ver en esta salida de ejemplo que el atributo de tipo de servicio está pasado sobre el WLC.

Información Relacionada

- Configurar la guía de configuración de controlador del Wireless LAN
- Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica
- Asignación del VLAN dinámico con el servidor de RADIUS y el ejemplo de la configuración de controlador del Wireless LAN
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Ejemplo de Configuración de VLANs de Grupo de AP con Controladores de LAN Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems