Configuración de un Servidor RADIUS y WLC para la Asignación de VLAN Dinámica

Contenido

Introducción

Este documento presenta el concepto de asignación de VLAN dinámica. El documento explica cómo configurar el controlador de LAN inalámbrico (WLC) y un servidor RADIUS para asignar dinámicamente clientes de LAN inalámbrica (WLAN) a una VLAN específica.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Tener conocimientos básicos del WLC y los Lightweight Access Points (LAP)
- Tener conocimiento funcional del servidor AAA
- Conozca a fondo las redes inalámbricas y los problemas de seguridad inalámbrica
- Tener conocimiento básico del protocolo ligero AP (LWAPP)

Componentes Utilizados

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

- Cisco 4400 WLC que ejecuta firmware versión 5.2
- LAP de la serie 1130 de Cisco
- Adaptador de cliente inalámbrico Cisco 802.11a/b/g que utiliza firmware versión 4.4
- Cisco Aironet Desktop Utility (ADU) que ejecuta la versión 4.4
- CiscoSecure Access Control Server (ACS) que ejecuta la versión 4.1
- Cisco 2950 Series Switch

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.

Asignación de VLAN Dinámica con Servidor RADIUS

En la mayoría de los sistemas WLAN, cada WLAN tiene una política estática que se aplica a todos los clientes asociados a un identificador de conjunto de servicios (SSID) o WLAN en la terminología del controlador. Aunque poderoso, este método tiene limitaciones porque requiere que los clientes se asocien con diferentes SSID para heredar diferentes QoS y políticas de seguridad.

Sin embargo, la solución de WLAN de Cisco admite redes de identidad. Esto permite que la red anuncie un solo SSID, pero permite a usuarios específicos heredar diferentes QoS o políticas de seguridad basadas en las credenciales del usuario.

La asignación de VLAN dinámica es una de estas funciones que colocan a un usuario inalámbrico en una VLAN específica en función de las credenciales suministradas por el usuario. Esta tarea de asignar usuarios a una VLAN específica es manejada por un servidor de autenticación RADIUS, como CiscoSecure ACS. Esto se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en la misma VLAN a medida que se desplaza dentro de una red de campus.

Por lo tanto, cuando un cliente intenta asociarse a un LAP registrado con un controlador, el LAP pasa las credenciales del usuario al servidor RADIUS para la validación. Cuando la autenticación es correcta, el servidor RADIUS transmite una serie de atributos del Grupo de trabajo en ingeniería de Internet (IETF) al usuario. Estos atributos de RADIUS deciden la ID de VLAN que se debe asignar al cliente inalámbrico. El SSID (WLAN, en términos de WLC) del cliente no importa porque el usuario siempre está asignado a este ID de VLAN predeterminado.

Los atributos del usuario de RADIUS que se utilizan para la asignación del ID de VLAN son:

- IETF 64 (Tipo de túnel): Defina esto en VLAN.
- IETF 65 (tipo de túnel medio): establezca este valor en 802

- IETF 81 (ID de grupo privado de túnel): Defina esta opción en ID de VLAN.

La ID de VLAN es 12 bits y recibe un valor entre 1 y 4094, ambos incluidos. Debido a que el Tunnel-Private-Group-ID es de tipo string, como se define en RFC2868 para su uso con IEEE 802.1X, el valor entero de ID de VLAN se codifica como una cadena. Una vez que se envían estos atributos del túnel, es necesario rellenar el campo Tag (Etiqueta).

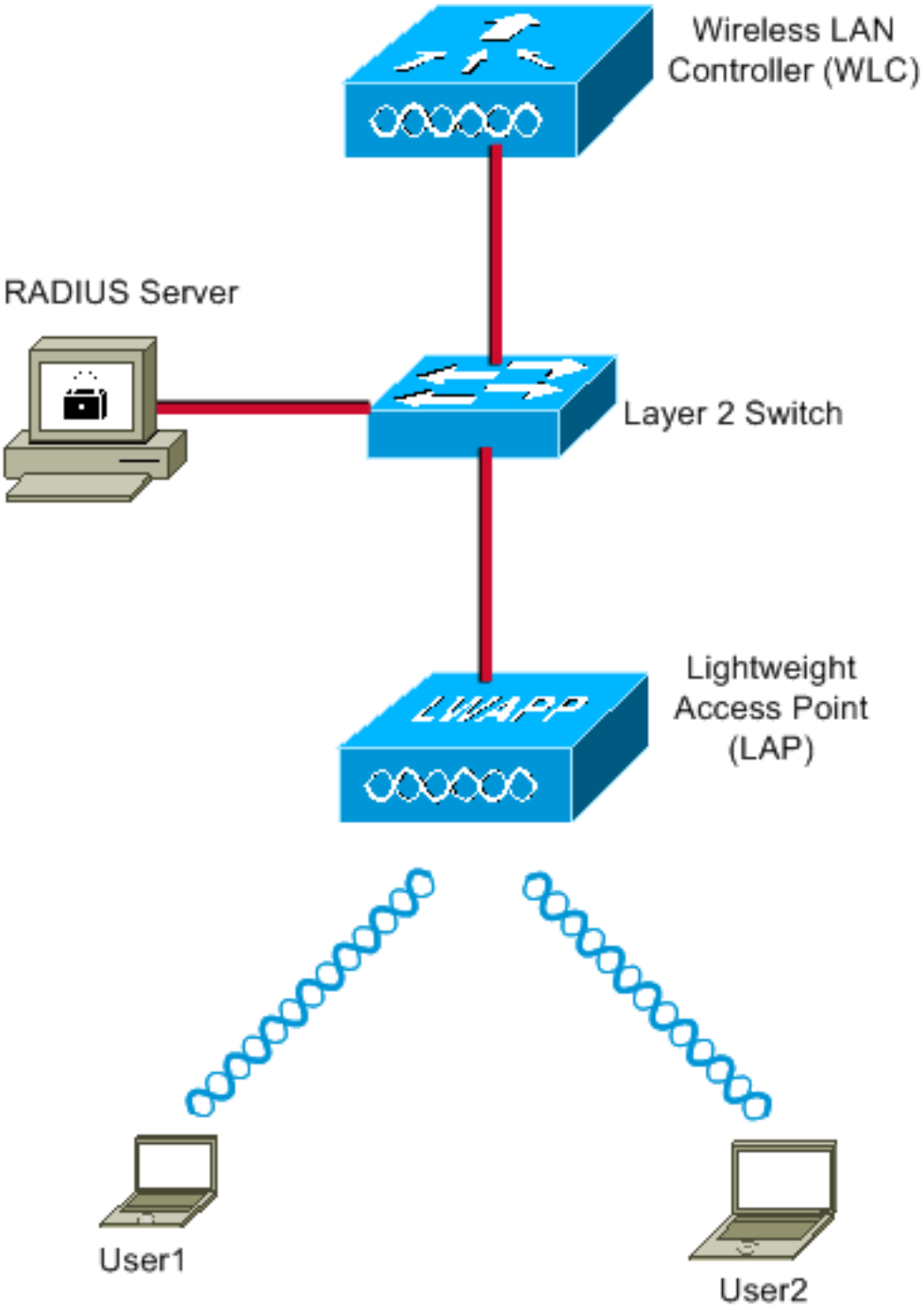
Como se indica en RFC2868 , sección 3.1: **El campo Tag (etiqueta) tiene un octeto de longitud y está diseñado para proporcionar un medio de agrupamiento de atributos en el mismo paquete que hace referencia al mismo túnel.** Los valores válidos para este campo son de 0x01 a 0x1F, ambos incluidos. Si el campo Tag (Etiqueta) no se utiliza, debe tener el valor cero (0x00). Consulte RFC 2868 para obtener más información sobre todos los atributos de RADIUS.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 172.16.1.1.
- La dirección de la interfaz de administración del WLC es 172.16.1.30.
- La dirección de la interfaz del administrador de AP del WLC es 172.16.1.31.
- La dirección del servidor DHCP 172.16.1.1 se utiliza para asignar direcciones IP al LWAPP. **El servidor DHCP interno del controlador se utiliza para asignar la dirección IP a los clientes inalámbricos.**
- VLAN10 y VLAN11 se utilizan a lo largo de esta configuración. El usuario1 está configurado para ubicarse en la VLAN10 y el usuario2 está configurado para ser colocado en la VLAN11 por el servidor RADIUS.**Nota:** Este documento sólo muestra toda la información de configuración relacionada con user1. Complete el mismo procedimiento explicado en este documento para el usuario2.
- Este documento utiliza 802.1x con LEAP como mecanismo de seguridad.**Nota:** Cisco recomienda utilizar métodos de autenticación avanzados, como EAP-FAST y autenticación

EAP-TLS, para proteger la WLAN. Este documento utiliza LEAP sólo para simplificar.

Configuración

Antes de la configuración, este documento asume que el LAP ya está registrado con el WLC. Consulte Ejemplo de Configuración Básica del Controlador de LAN Inalámbrica y del Punto de Acceso Ligero para obtener más información. Consulte Registro de Lightweight AP (LAP) en un controlador de LAN inalámbrica (WLC) para obtener información sobre el procedimiento de registro involucrado.

Configuration Steps

Esta configuración se divide en tres categorías:

1. Configuración del servidor de RADIUS
2. Configuración del Switch para Varias VLAN
3. Configuración de WLC
4. Configuración de la utilidad del cliente inalámbrico

Configuración del servidor de RADIUS

La configuración requiere estos pasos:

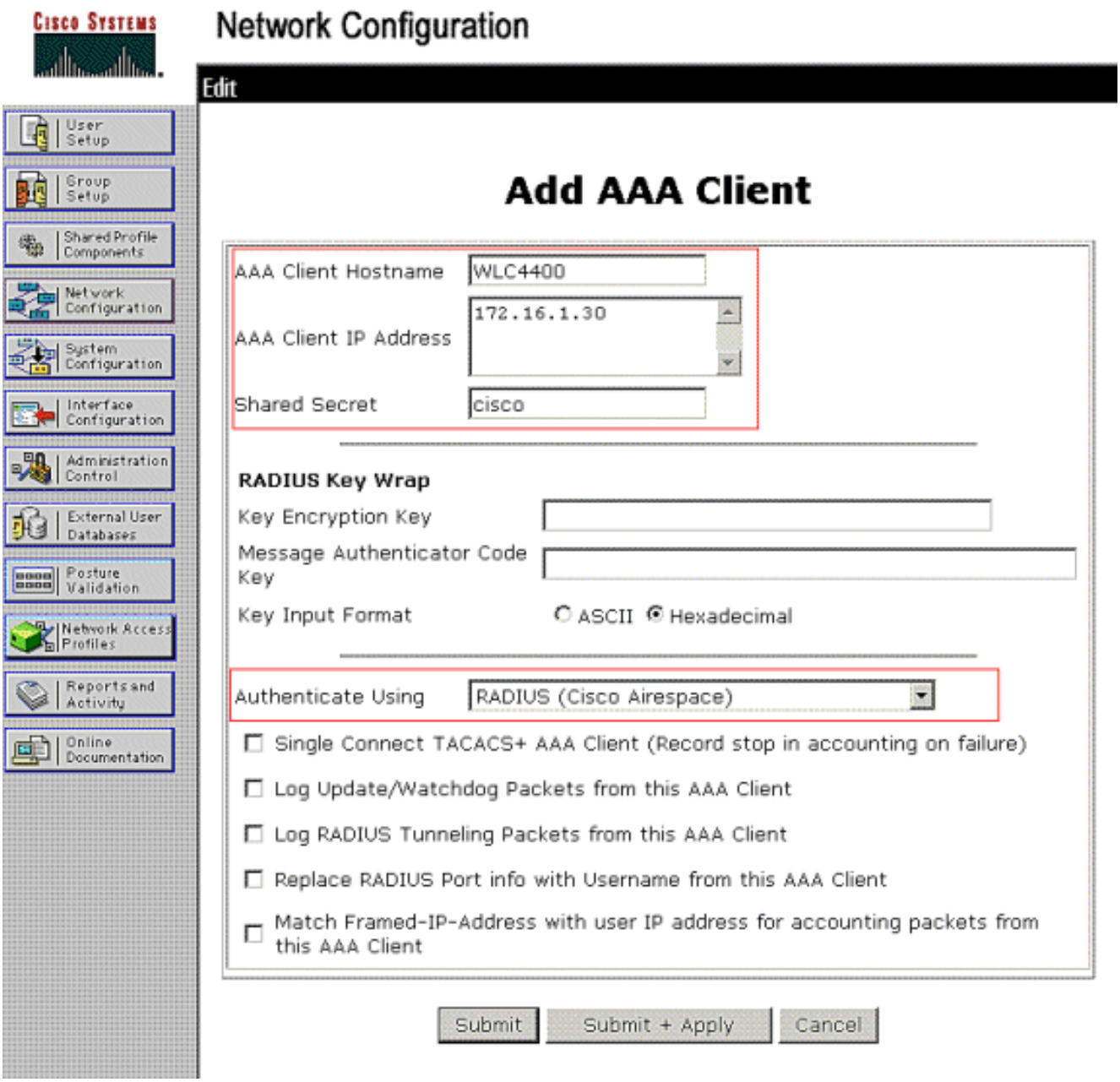
- Configure el WLC como un Cliente AAA en el Servidor RADIUS
- Configure los Usuarios y los Atributos RADIUS (IETF) Utilizados para la Asignación de VLAN Dinámica en el Servidor RADIUS

Configure el Cliente AAA para el WLC en el Servidor RADIUS

Este procedimiento explica cómo agregar el WLC como un cliente AAA en el servidor RADIUS para que el WLC pueda pasar las credenciales del usuario al servidor RADIUS.

Complete estos pasos:

1. Desde la GUI de ACS, haga clic en **Configuración de Red**.
2. Haga clic en la sección **Agregar entrada** en el campo Clientes AAA.
3. Introduzca la dirección IP y la clave del cliente AAA.La dirección IP debe ser la dirección IP de la interfaz de administración del WLC.Asegúrese de que la clave que ingresa sea la misma que la configurada en el WLC bajo la ventana Seguridad. Esta es la clave secreta utilizada para la comunicación entre el cliente AAA (WLC) y el servidor RADIUS.
4. Elija **RADIUS (Cisco Airespace)** del campo Authenticate Using para el tipo de autenticación.

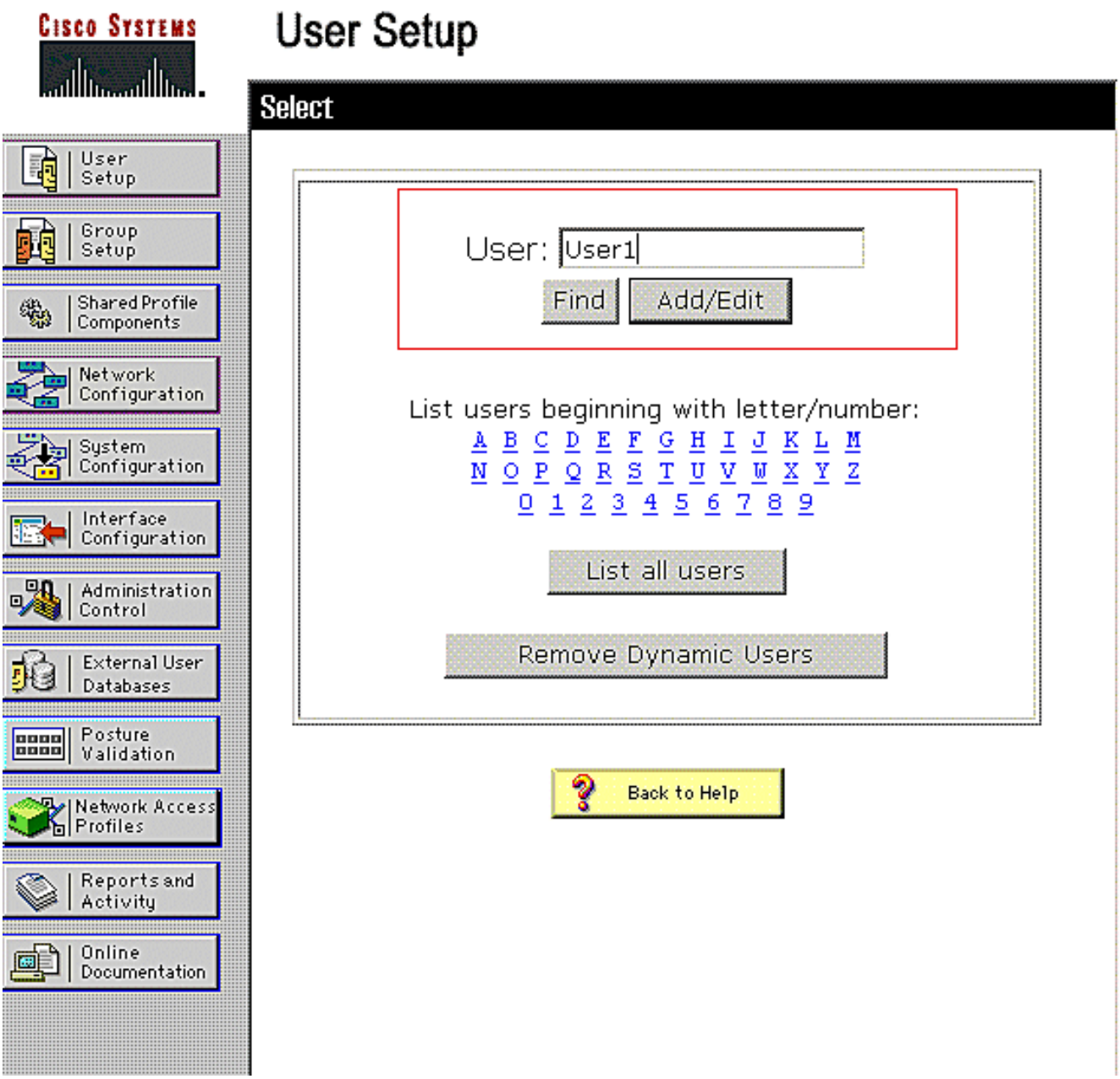


Configure los Usuarios y los Atributos RADIUS (IETF) Utilizados para la Asignación de VLAN Dinámica en el Servidor RADIUS

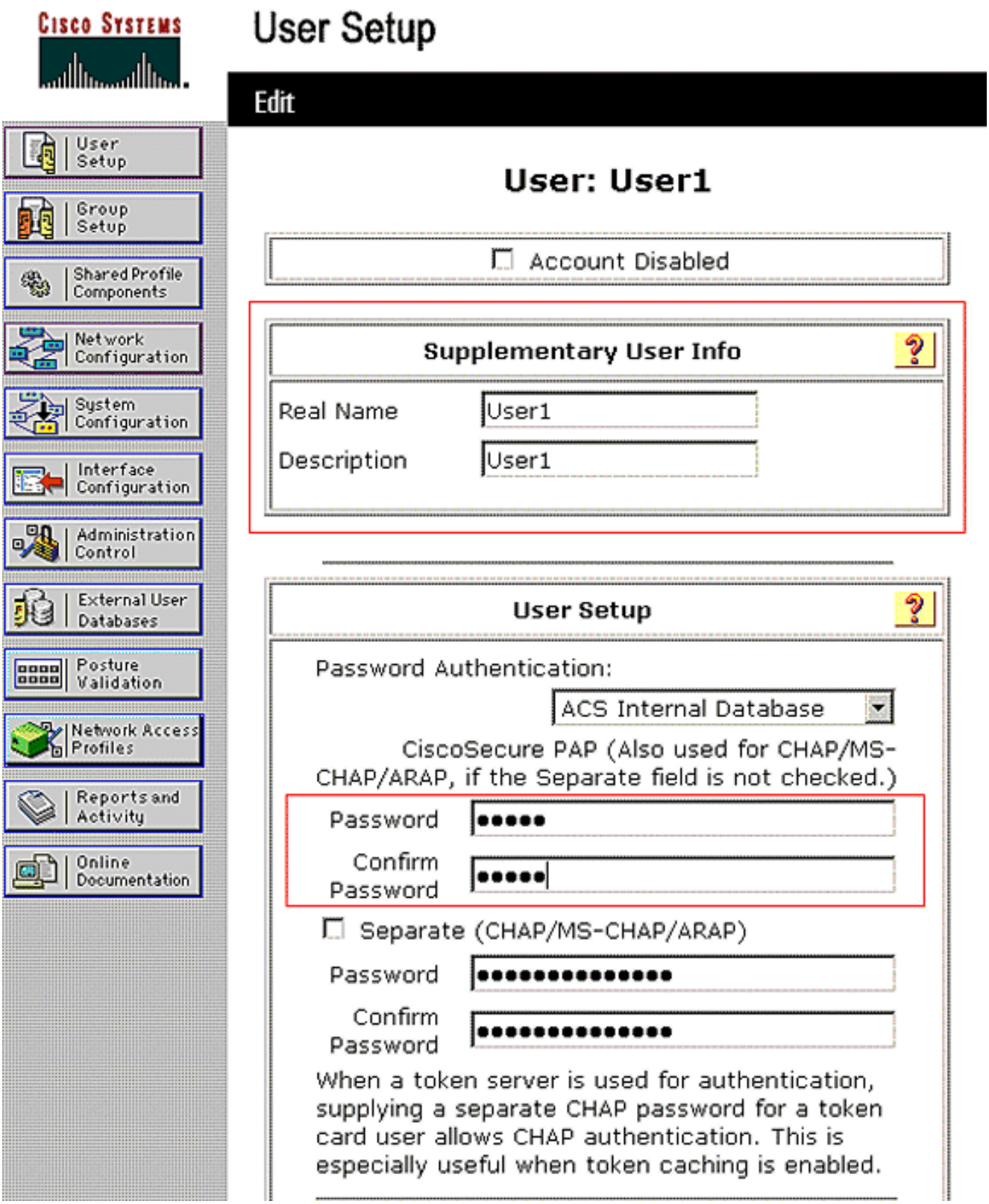
Este procedimiento explica cómo configurar los usuarios en el servidor RADIUS y los atributos RADIUS (IETF) utilizados para asignar ID de VLAN a estos usuarios.

Complete estos pasos:

1. Desde la GUI de ACS, haga clic en **User Setup**.
2. En la ventana User Setup (Configuración de usuario), introduzca un nombre de usuario en el campo User (Usuario) y haga clic en **Add/Edit (Agregar/Editar)**.

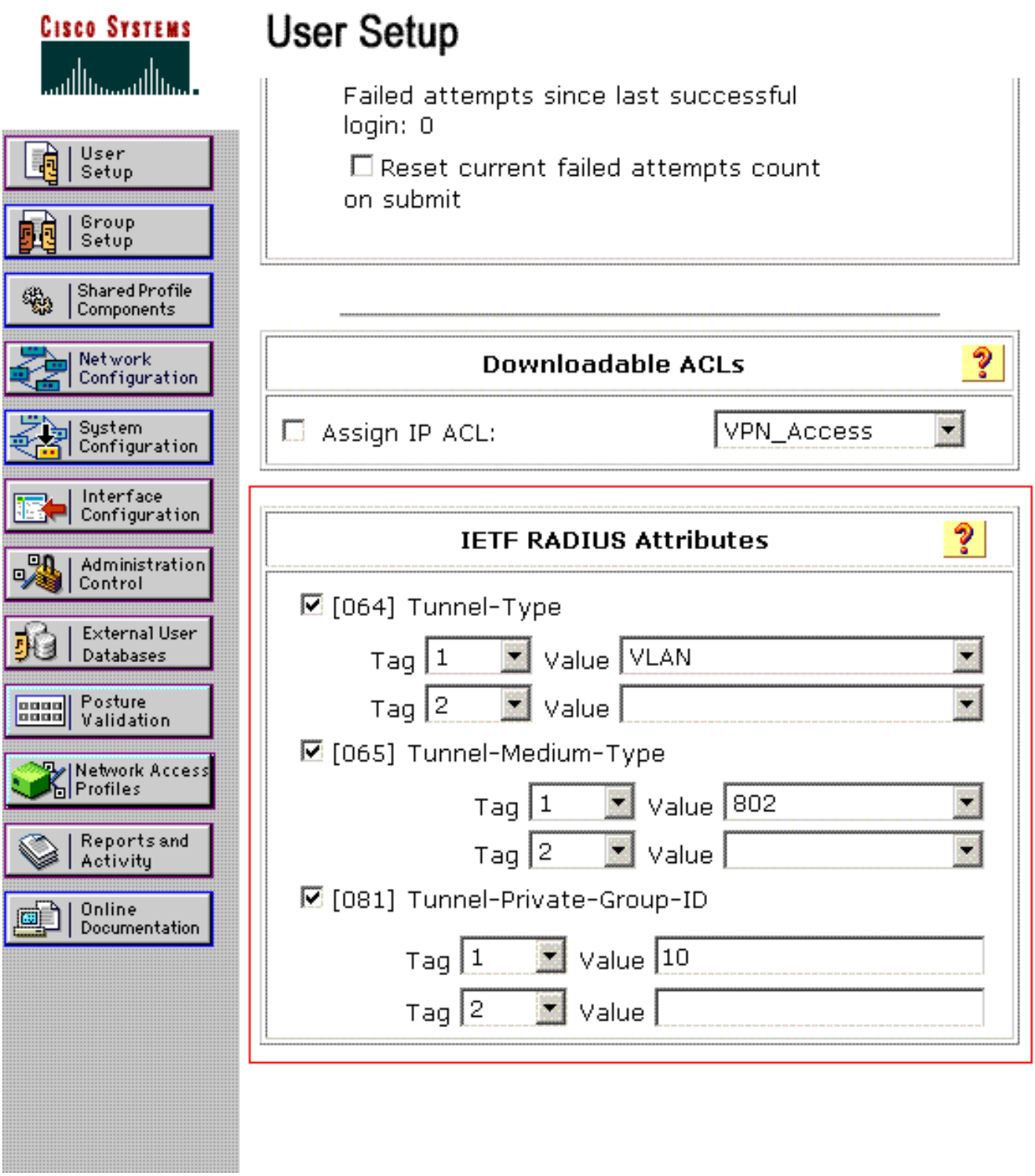


3. En la página Editar, introduzca la información de usuario necesaria como se muestra aquí:

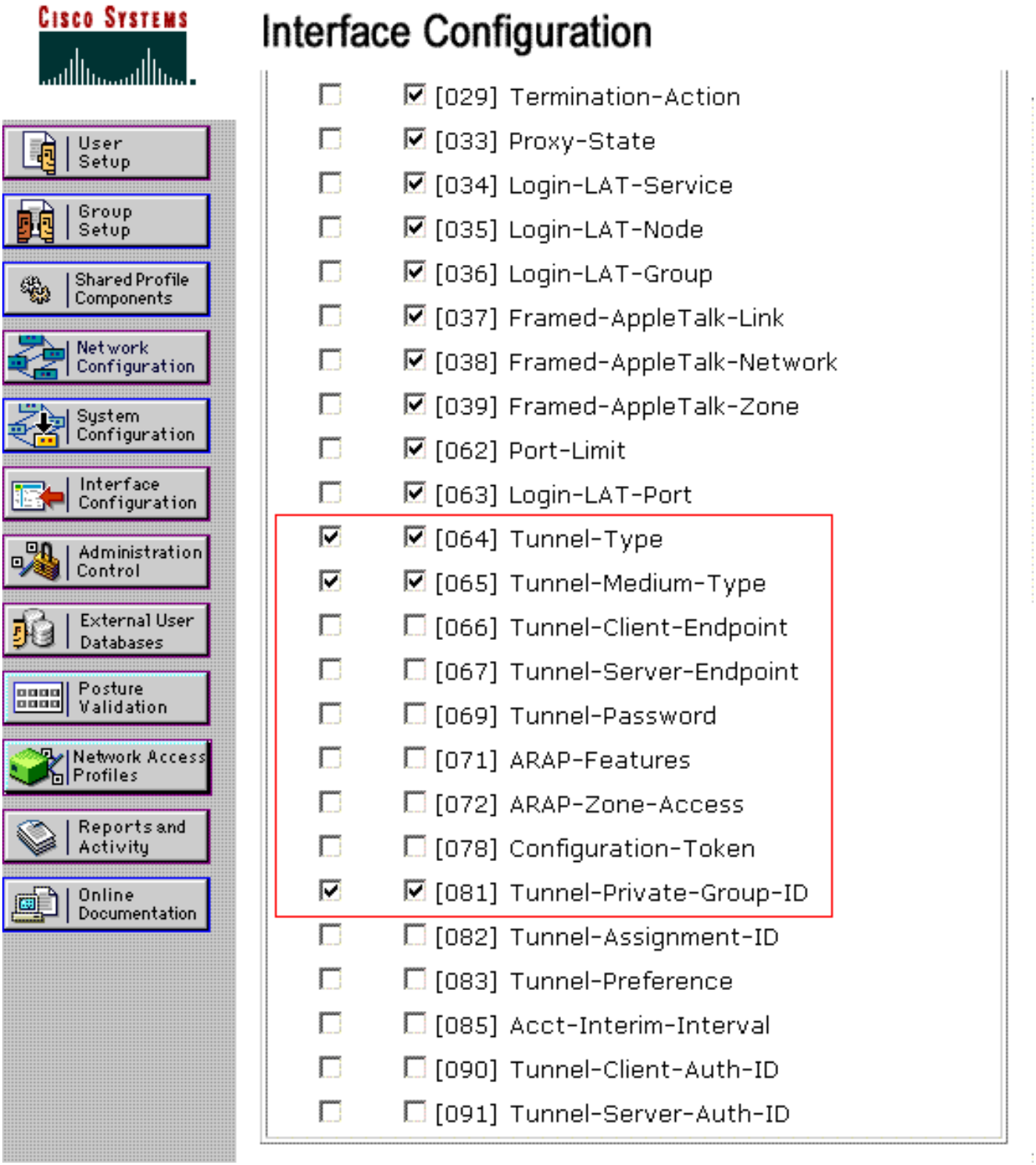


En este diagrama, observe que la contraseña que proporciona en la sección User Setup (Configuración de usuario) debe ser la misma que la proporcionada en el lado cliente durante la autenticación de usuario.

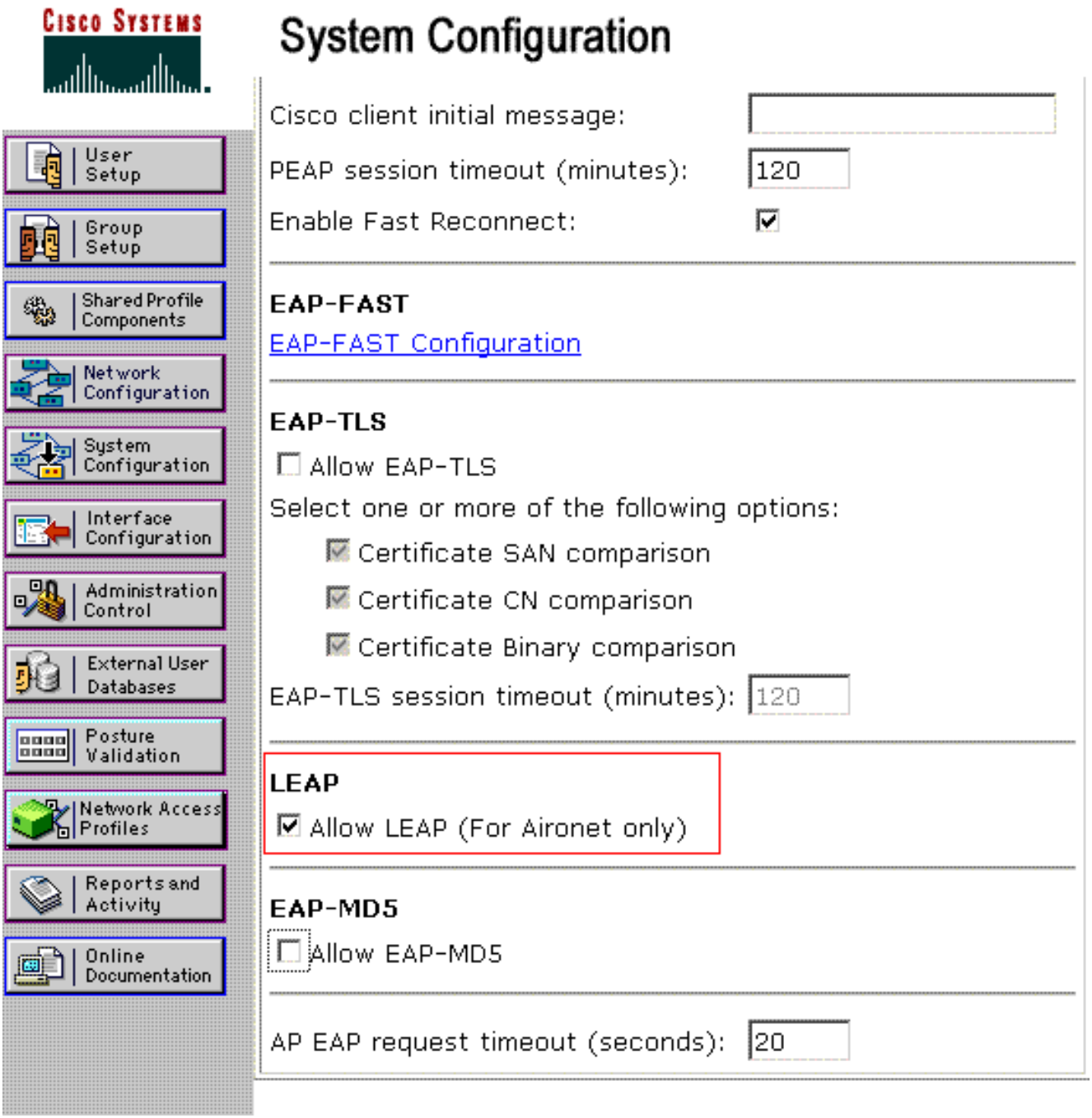
4. Desplácese hacia abajo en la página Edit (Editar) y busque el campo **IETF RADIUS Attributes (Atributos RADIUS de IETF)**.
5. En el campo IETF RADIUS Attributes (Atributos RADIUS de IETF), active las casillas de verificación situadas junto a los tres atributos del túnel y configure los valores de atributo como se muestra
aquí:



Nota: En la configuración inicial del servidor ACS, es posible que no se muestren los atributos RADIUS IETF.Elija **Interface Configuration > RADIUS (IETF)** para habilitar los atributos IETF en la ventana de configuración del usuario.A continuación, active las casillas de verificación de los atributos **64, 65 y 81** en las columnas Usuario y Grupo.



Nota: Para que el servidor RADIUS asigne dinámicamente el cliente a una VLAN específica, **es necesario que la VLAN-ID configurada bajo el campo IETF 81 (Tunnel-Private-Group-ID) del servidor RADIUS exista en el WLC.**Marque la casilla de verificación **Per User TACACS+/RADIUS** en Interface Configuration > Advanced Options para habilitar el servidor RADIUS para las configuraciones por usuario.Además, dado que LEAP se utiliza como protocolo de autenticación, asegúrese de que LEAP esté habilitado en la ventana Configuración del sistema del servidor RADIUS como se muestra aquí:



Configure el ACS con los Atributos VSA de Cisco Airespace para la Asignación de VLAN Dinámica

En las últimas versiones de ACS, también puede configurar el atributo Cisco Airespace [VSA (Específico del Proveedor)] para asignar un usuario autenticado correctamente con un nombre de interfaz VLAN (no el ID de VLAN) según la configuración del usuario en el ACS. Para lograrlo, realice los pasos de esta sección.

Nota: Esta sección utiliza la versión ACS 4.1 para configurar el atributo VSA de Cisco Airespace.

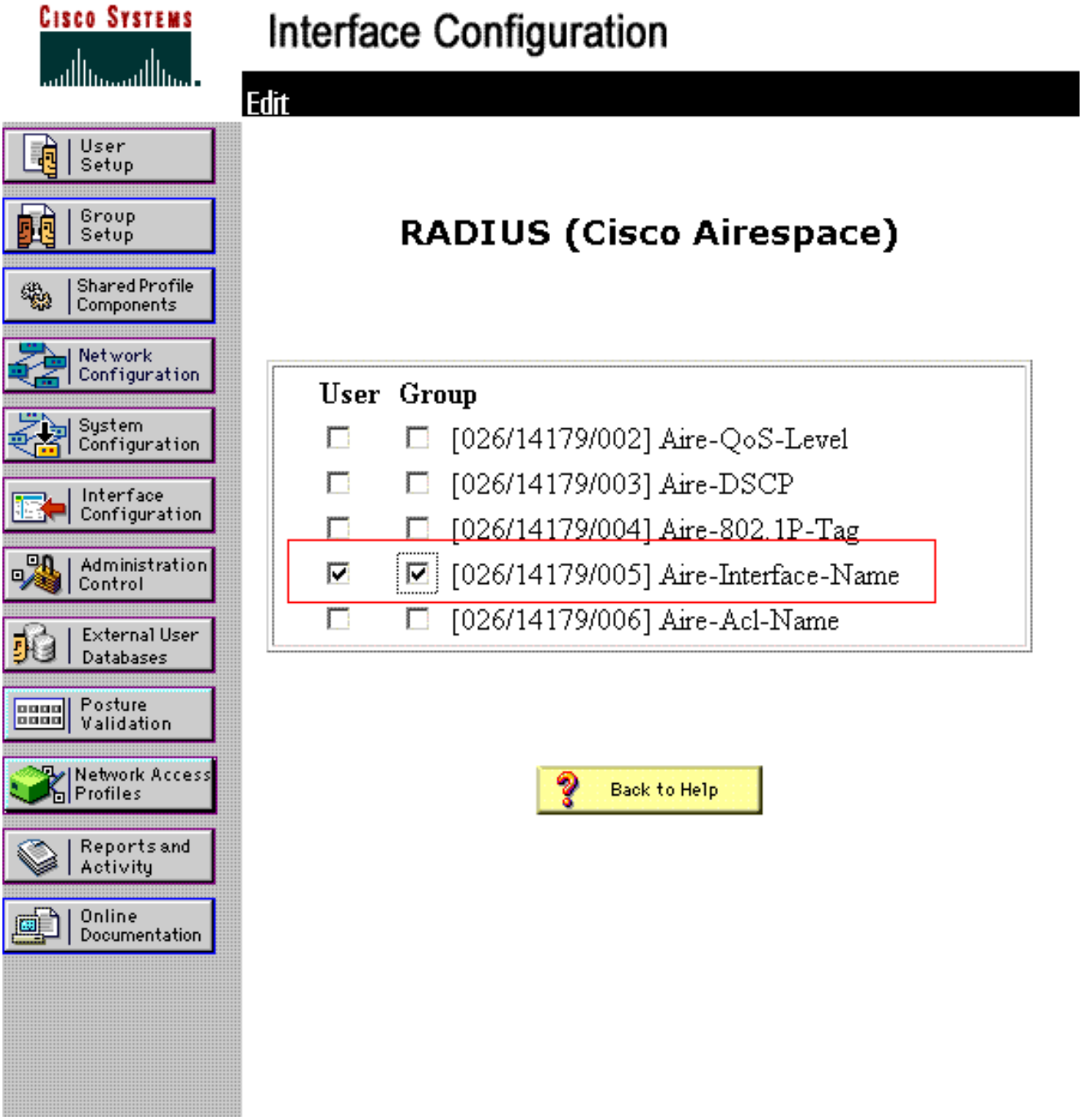
Configuración del Grupo ACS con la Opción de Atributo VSA de Cisco Airespace

Complete estos pasos:

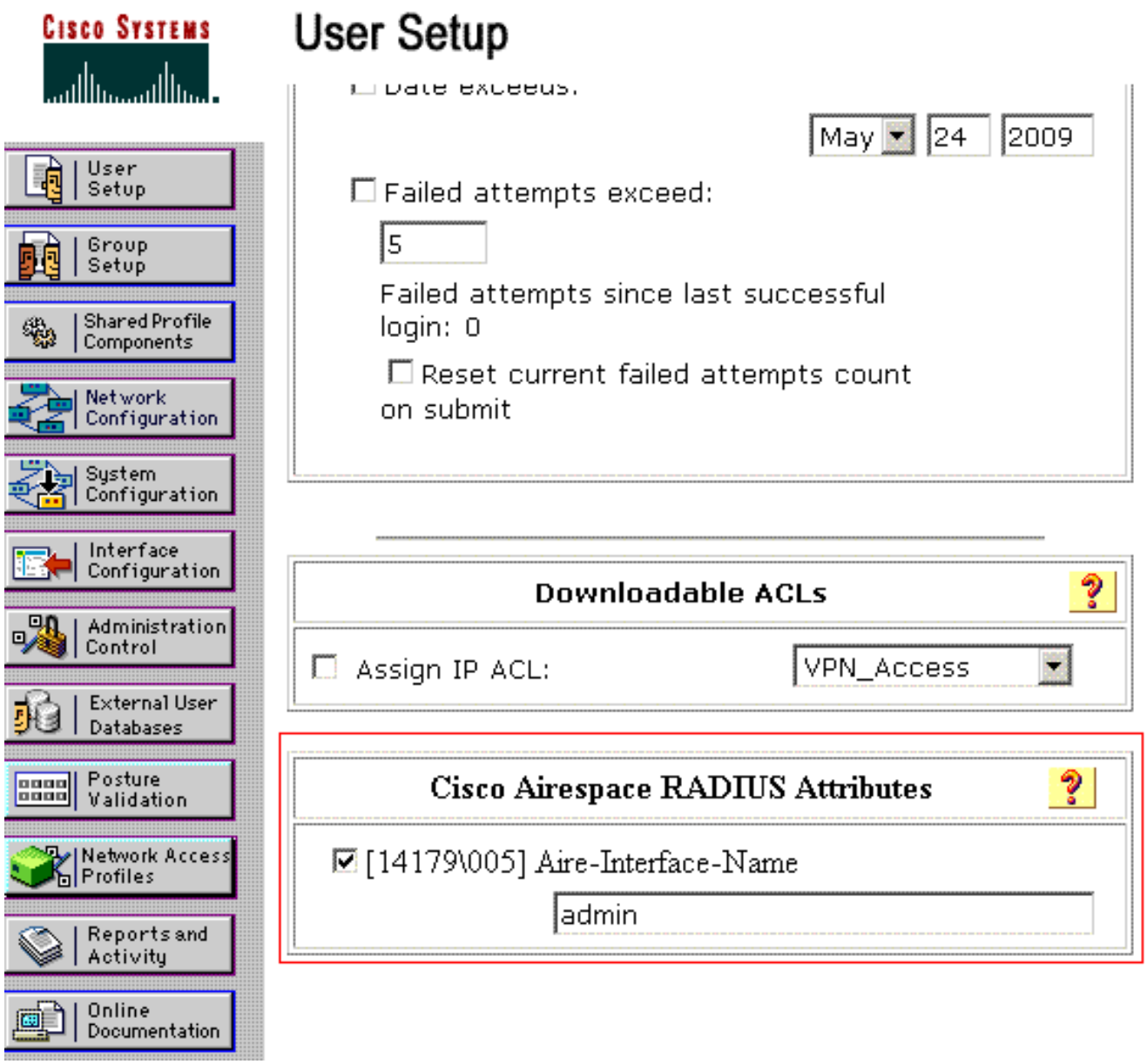
1. Desde la GUI de ACS 4.1, haga clic en **Interface Configuration** en la barra de navegación. A

continuación, seleccione **RADIUS (Cisco Airespace)** en la página Interface Configuration para configurar la opción de atributo Cisco Airespace.

2. Desde la ventana RADIUS (Cisco Airespace), marque la casilla de verificación Usuario (casilla de verificación Grupo si es necesario) junto a **Aire-Interface-Name** para mostrarla en la página User Edit. A continuación, haga clic en **Enviar**.



3. Vaya a la página Editar del usuario1.
4. Desde la página User Edit (Editar usuario), desplácese hacia abajo hasta la sección **Cisco Airespace RADIUS Attributes (Atributos RADIUS de Cisco Airespace)**. Marque la casilla de verificación junto al atributo **Aire-Interface-Name** y especifique el nombre de la interfaz dinámica que se asignará tras la autenticación de usuario correcta.Este ejemplo asigna el usuario a la VLAN **admin**.



5. Haga clic en Submit (Enviar).

Configuración del Switch para Varias VLAN

Para permitir varias VLAN a través del switch, debe ejecutar estos comandos para configurar el puerto del switch conectado al controlador:

1. Switch(config-if)#**switchport mode trunk**
2. Switch(config-if)#**switchport trunk encapsulation dot1q**

Nota: De forma predeterminada, la mayoría de los switches permiten todas las VLAN creadas en ese switch a través del puerto troncal.

Estos comandos varían para un switch del sistema operativo Catalyst (CatOS).

Si hay una red con cables conectada al switch, se puede aplicar la misma configuración al puerto del switch que se conecta a la red con cables. Esto habilita la comunicación entre las mismas VLAN en la red por cable e inalámbrica.

Nota: Este documento no analiza la comunicación entre VLAN. Esto está fuera del alcance de este documento. Debe comprender que para el ruteo entre VLAN, se necesita un switch de Capa

3 o un router externo con configuraciones VLAN y troncales adecuadas. Hay varios documentos que explican la configuración de ruteo entre VLAN.

Configuración de WLC

La configuración requiere estos pasos:

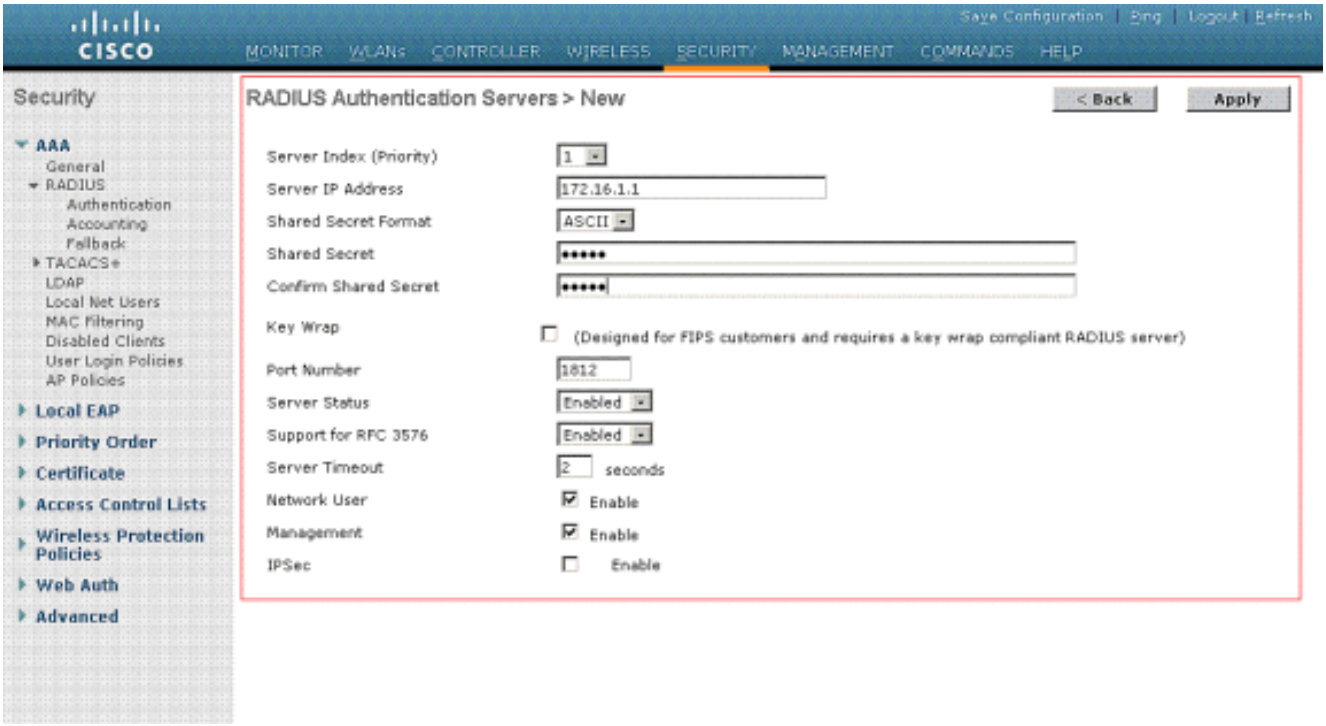
- Configure el WLC con los detalles del servidor de autenticación
- Configuración de las interfaces dinámicas (VLAN)
- Configuración de WLAN (SSID)

Configure el WLC con los detalles del servidor de autenticación

Es necesario configurar el WLC para que se pueda comunicar con el servidor RADIUS para autenticar a los clientes, y también para cualquier otra transacción.

Complete estos pasos:

1. Desde la GUI del controlador, haga clic en **Seguridad**.
2. Introduzca la dirección IP del servidor RADIUS y la clave secreta compartida utilizada entre el servidor RADIUS y el WLC.Esta clave secreta compartida debe ser la misma que la configurada en el servidor RADIUS en Configuración de red > Clientes AAA > Agregar entrada. Esta es una ventana de ejemplo del WLC:



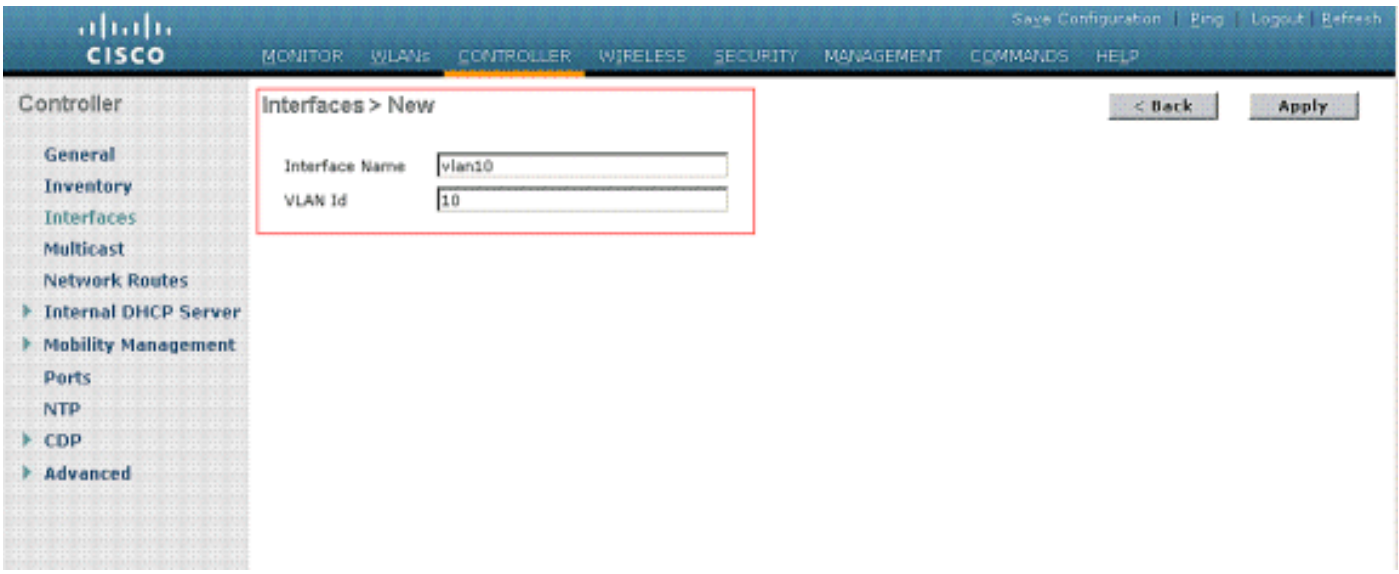
Configuración de las interfaces dinámicas (VLAN)

Este procedimiento explica cómo configurar las interfaces dinámicas en el WLC. Como se explicó anteriormente en este documento, el ID de VLAN especificado en el atributo de ID de grupo privado de túnel del servidor RADIUS también debe existir en el WLC.

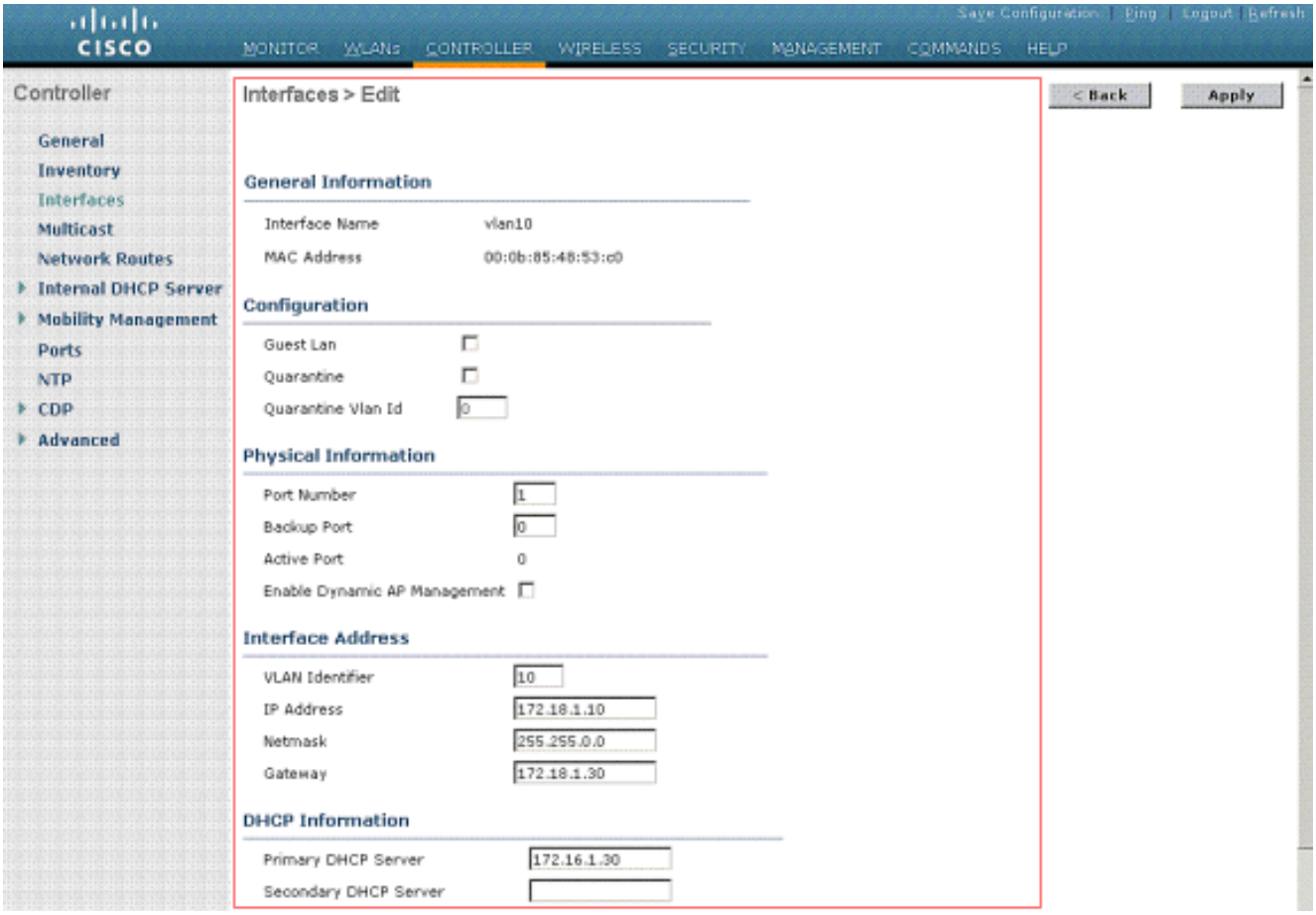
En el ejemplo, el usuario1 se especifica con el **ID de túnel-grupo privado de 10 (VLAN =10)** en el

servidor RADIUS. Consulte la sección Atributos RADIUS IETF de la ventana User Setup user1.

Puede ver la misma interfaz dinámica (VLAN=10) configurada en el WLC en este ejemplo. Desde la GUI del controlador, bajo la ventana Controller > Interfaces , se configura la interfaz dinámica.



1. Haga clic en **Aplicar** en esta ventana.Esto lo lleva a la ventana de edición de esta interfaz dinámica (VLAN 10 aquí).
2. Introduzca la dirección IP y la puerta de enlace predeterminada de esta interfaz dinámica.



Nota: Debido a que este documento utiliza un servidor DHCP interno en el controlador, el campo de servidor DHCP primario de esta ventana señala a la Interfaz de Administración del WLC mismo. También puede utilizar un servidor DHCP externo, un router o el propio servidor RADIUS como servidor DHCP para los clientes inalámbricos. En tales casos, el

campo del servidor DHCP primario apunta a la dirección IP de ese dispositivo utilizado como servidor DHCP. Consulte la documentación del servidor DHCP para obtener más información.

3. Haga clic en Apply (Aplicar).Ahora está configurado con una interfaz dinámica en su WLC. De manera similar, puede configurar varias interfaces dinámicas en su WLC. Sin embargo, recuerde que el mismo ID de VLAN también debe existir en el servidor RADIUS para que esa VLAN en particular se asigne al cliente.

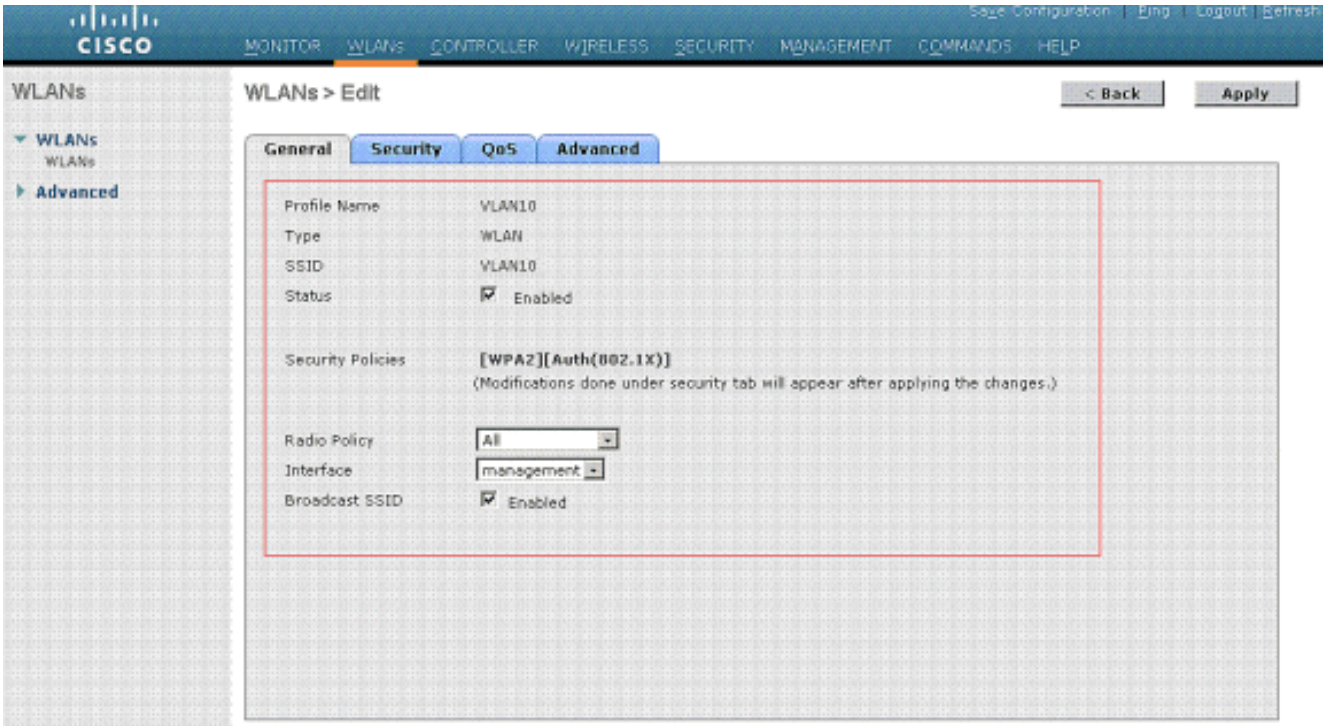
Configuración de WLAN (SSID)

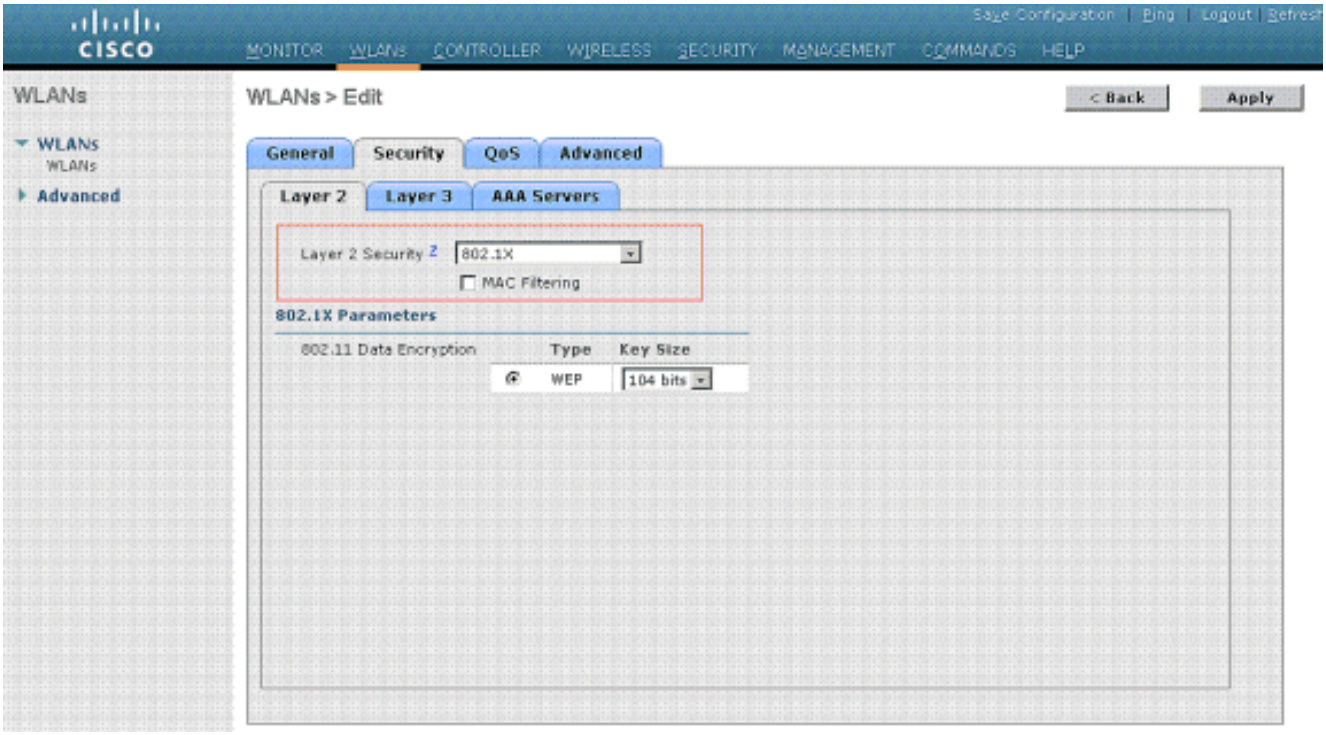
Este procedimiento explica cómo configurar las WLAN en el WLC.

Complete estos pasos:

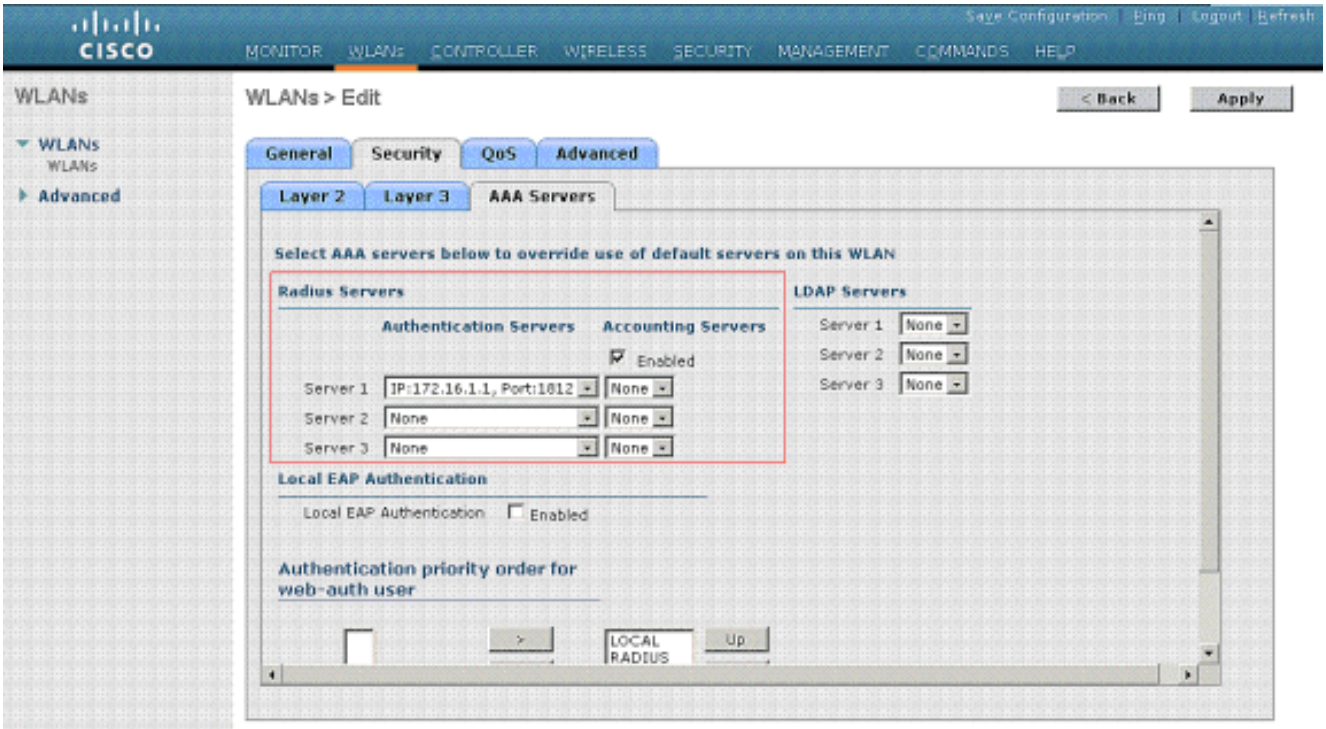
1. Desde la GUI del controlador, elija **WLANs > New** para crear una nueva WLAN.Se muestra la ventana Nuevas WLAN.
2. Introduzca la información de WLAN ID y WLAN SSID.Puede introducir cualquier nombre para que sea el WLAN SSID. Este ejemplo utiliza VLAN10 como el WLAN SSID.

3. Haga clic en **Aplicar** para ir a la ventana Editar del WLAN SSID10.





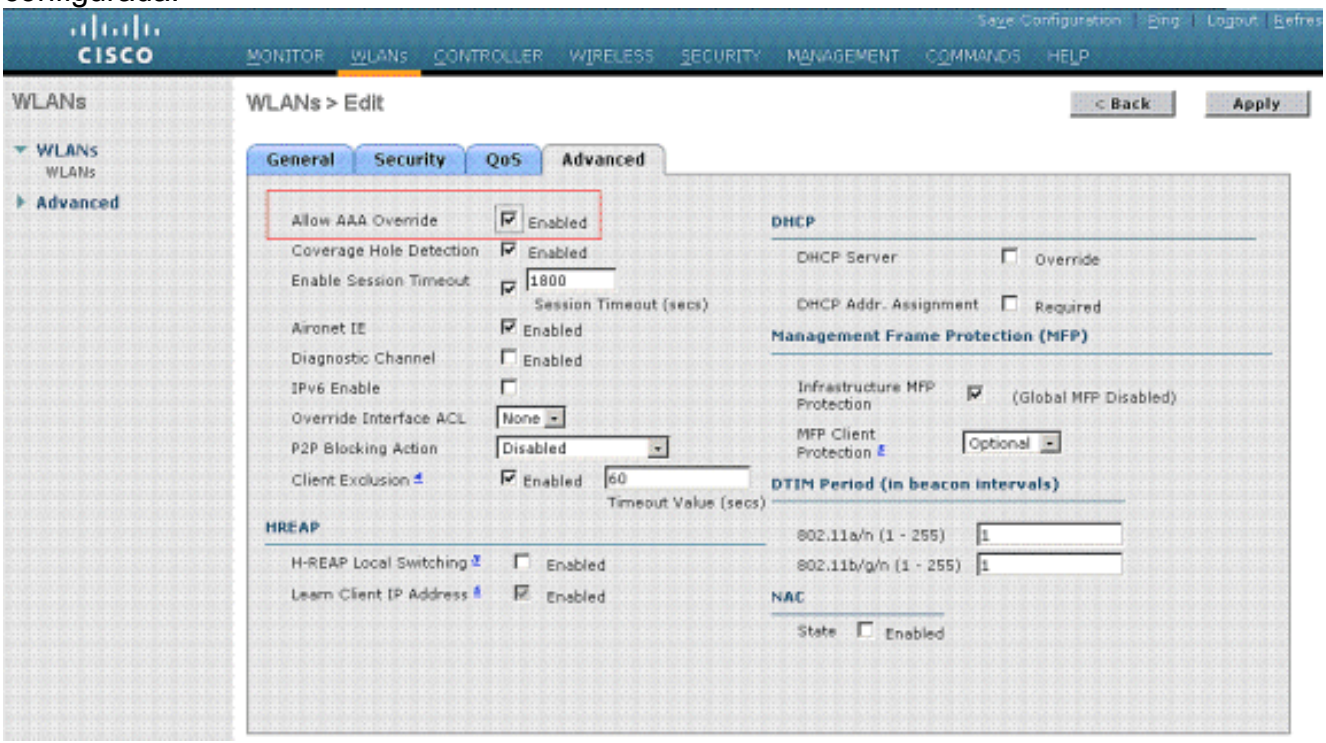
Normalmente, en un controlador de LAN inalámbrica, cada WLAN se asigna a una VLAN específica (SSID) de modo que un usuario determinado que pertenece a esa WLAN se coloque en la VLAN específica asignada. Este mapping se realiza normalmente bajo el campo Interface Name de la ventana WLAN
SSID.



En el ejemplo proporcionado, es tarea del servidor RADIUS asignar un cliente inalámbrico a una VLAN específica después de una autenticación exitosa. Las WLANs no necesitan ser mapeadas a una interfaz dinámica específica en el WLC. O, aunque la WLAN a la correspondencia de interfaz dinámica se realiza en el WLC, el servidor RADIUS invalida este mapping y asigna al usuario que llega a través de esa WLAN a la VLAN especificada bajo el **campo** usuario **Tunnel-Group-Private-ID** en el servidor RADIUS.

4. Marque la casilla de verificación **Allow AAA Override para invalidar las configuraciones del WLC por el servidor RADIUS.**

5. Active la opción Permitir anulación de AAA en el controlador para cada WLAN (SSID) configurada.



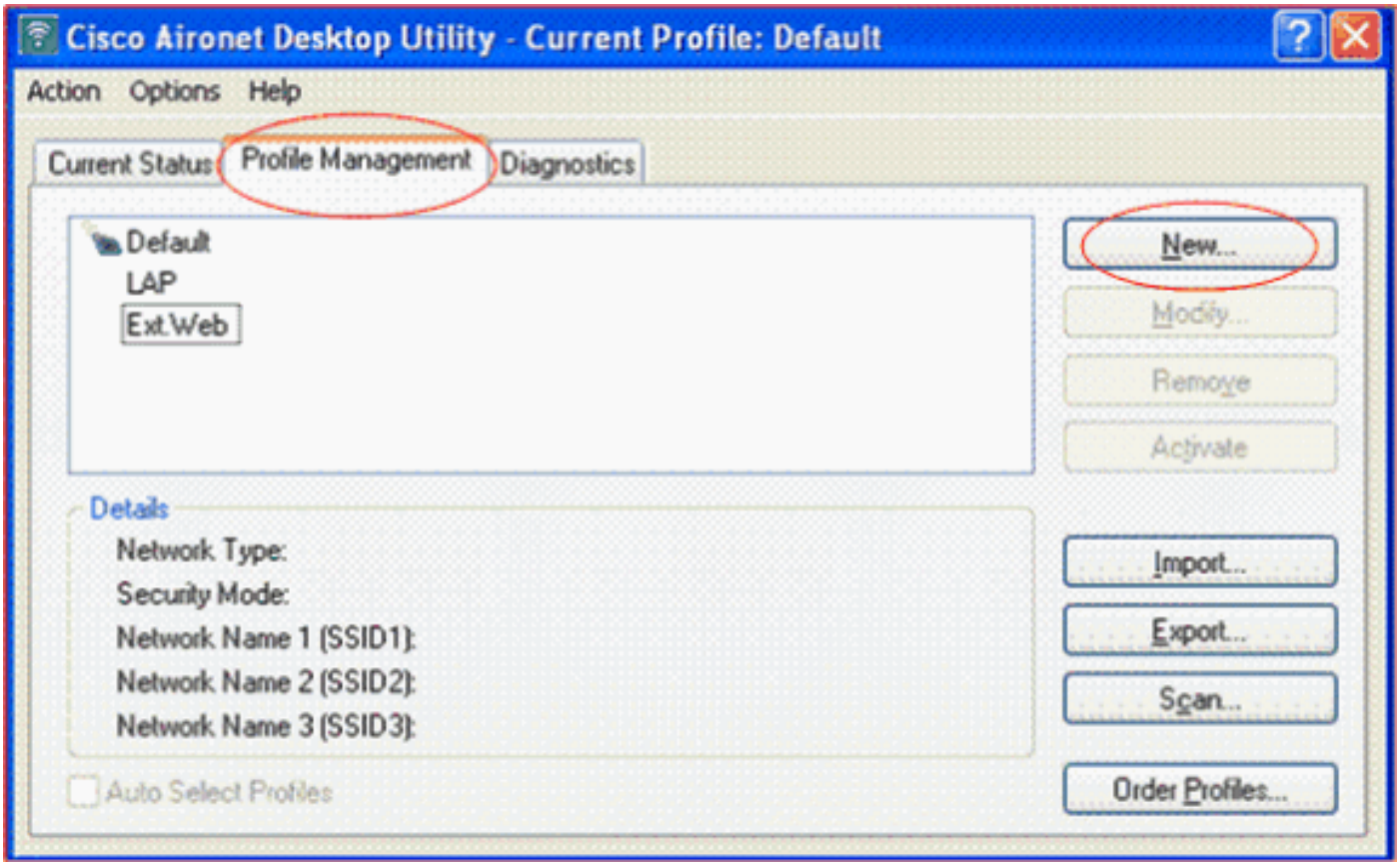
Cuando se habilita la anulación de AAA y un cliente tiene parámetros de autenticación de AAA y WLAN del controlador que entran en conflicto, la autenticación del cliente se realiza mediante el servidor AAA (RADIUS). Como parte de esta autenticación, el sistema operativo mueve los clientes a una VLAN devuelta por el servidor AAA. Esto está predefinido en la configuración de la interfaz del controlador.Por ejemplo, si la WLAN corporativa utiliza principalmente una interfaz de administración asignada a la VLAN 2 y si la anulación de AAA devuelve una redirección a la VLAN 100, el sistema operativo redirige todas las transmisiones de cliente a la VLAN 100 incluso si el puerto físico al que se asigna la VLAN 100. Cuando se inhabilita la invalidación de AAA, todos los valores predeterminados de autenticación de cliente son los parámetros de autenticación de controlador, y la autenticación es realizada solamente por el servidor AAA si la WLAN del controlador no contiene ningún parámetro de autenticación específico del cliente.

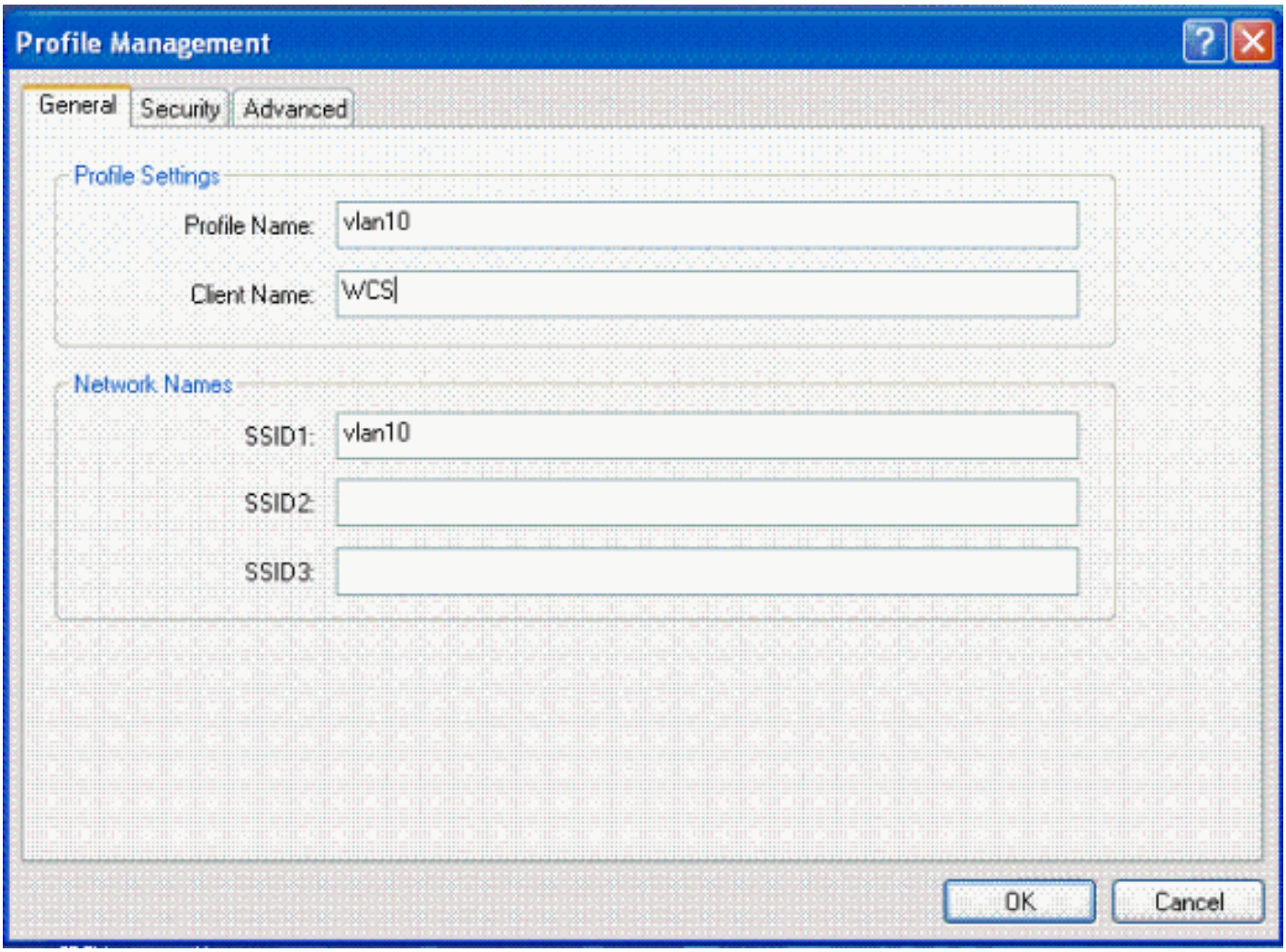
Configuración de la utilidad del cliente inalámbrico

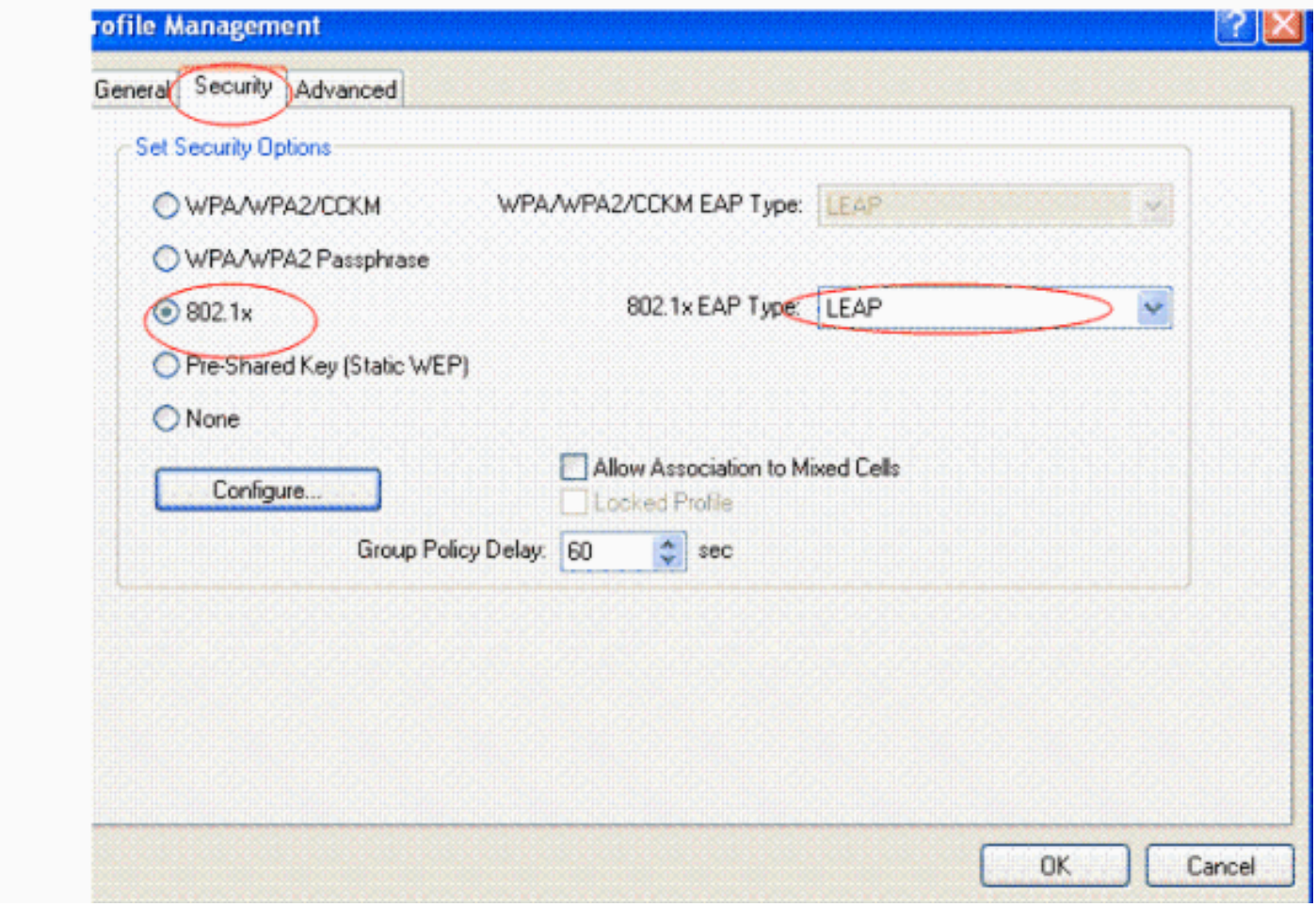
Este documento utiliza ADU como la utilidad del cliente para la configuración de los perfiles de usuario. Esta configuración también utiliza LEAP como protocolo de autenticación. Configure la ADU como se muestra en el ejemplo de esta sección.

En la barra de menú ADU, elija **Profile Management > New** para crear un nuevo perfil.

El cliente de ejemplo se configura para que forme parte de SSID VLAN10. Estos diagramas muestran cómo configurar un perfil de usuario en un cliente:


Cisco Aironet Desktop Utility - Current Profile: Default
Action Options Help
Current Status
Profile Management
Diagnostics
Default
LAP
Ext.Web
New...
Modify...
Remove
Activate
Details
Network Type:
Security Mode:
Network Name 1 (SSID1):
Network Name 2 (SSID2):
Network Name 3 (SSID3):
Import...
Export...
Scan...
Auto Select Profiles
Order Profiles...


Profile Management
General
Security
Advanced
Profile Settings
Profile Name:
vlan10
Client Name:
WCS
Network Names
SSID1:
vlan10
SSID2:
SSID3:
OK
Cancel



Verificación

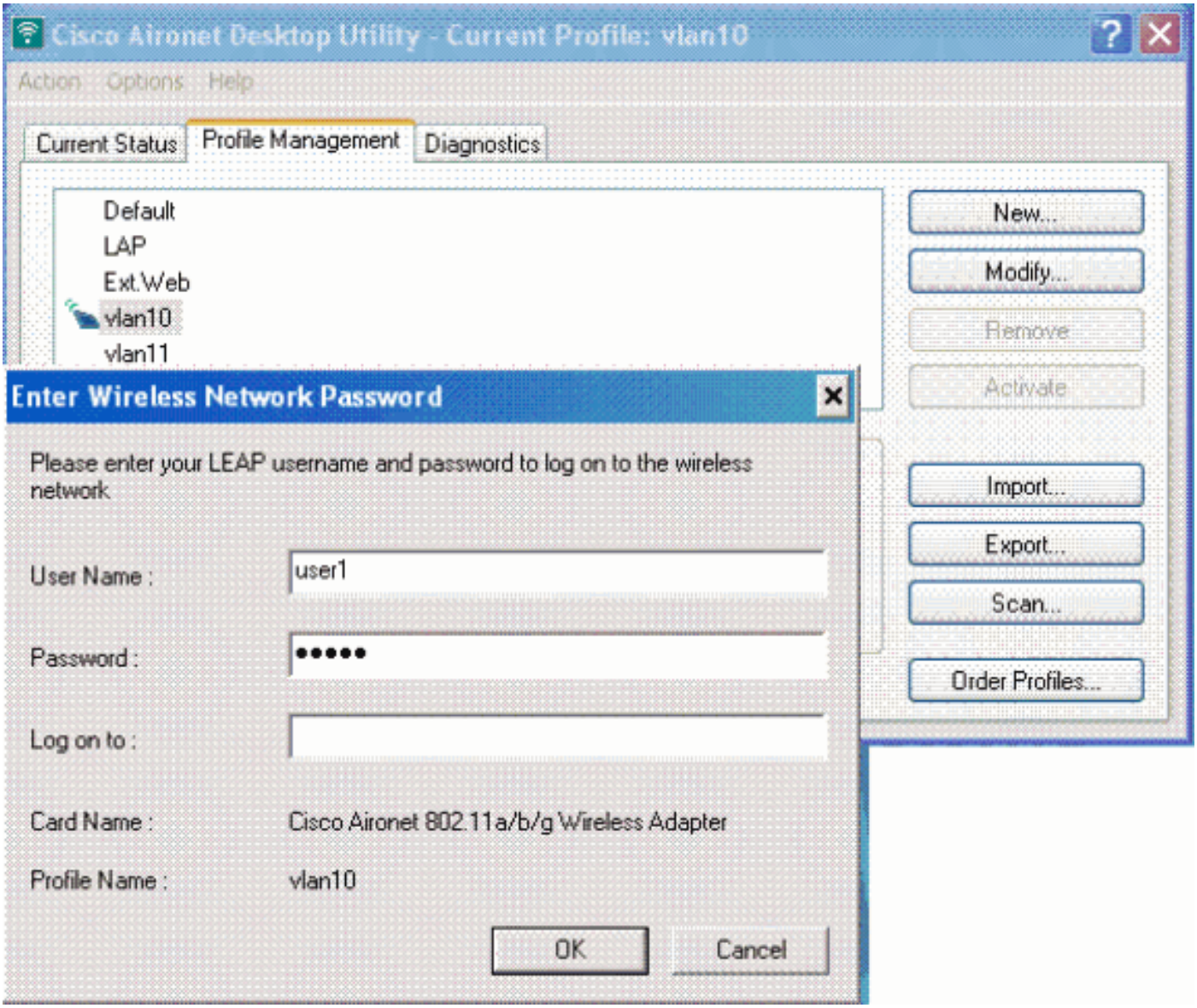
Active el perfil de usuario que ha configurado en la ADU. Según la configuración, se le solicitará un nombre de usuario y una contraseña. También puede indicar a la ADU que utilice el nombre de usuario y la contraseña de Windows para la autenticación. Hay varias opciones desde las cuales el cliente puede recibir la autenticación. Puede configurar estas opciones en la ficha Security > Configure del perfil de usuario que ha creado.

En el ejemplo anterior, observe que user1 está asignado a la VLAN10 como se especifica en el servidor RADIUS.

Este ejemplo utiliza este nombre de usuario y contraseña del lado del cliente para recibir la autenticación y ser asignados a una VLAN por el servidor RADIUS:

- Nombre de usuario = usuario1
- Contraseña = user1

Este ejemplo muestra cómo se le solicita al SSID VLAN10 el nombre de usuario y la contraseña. El nombre de usuario y la contraseña se ingresan en este ejemplo:



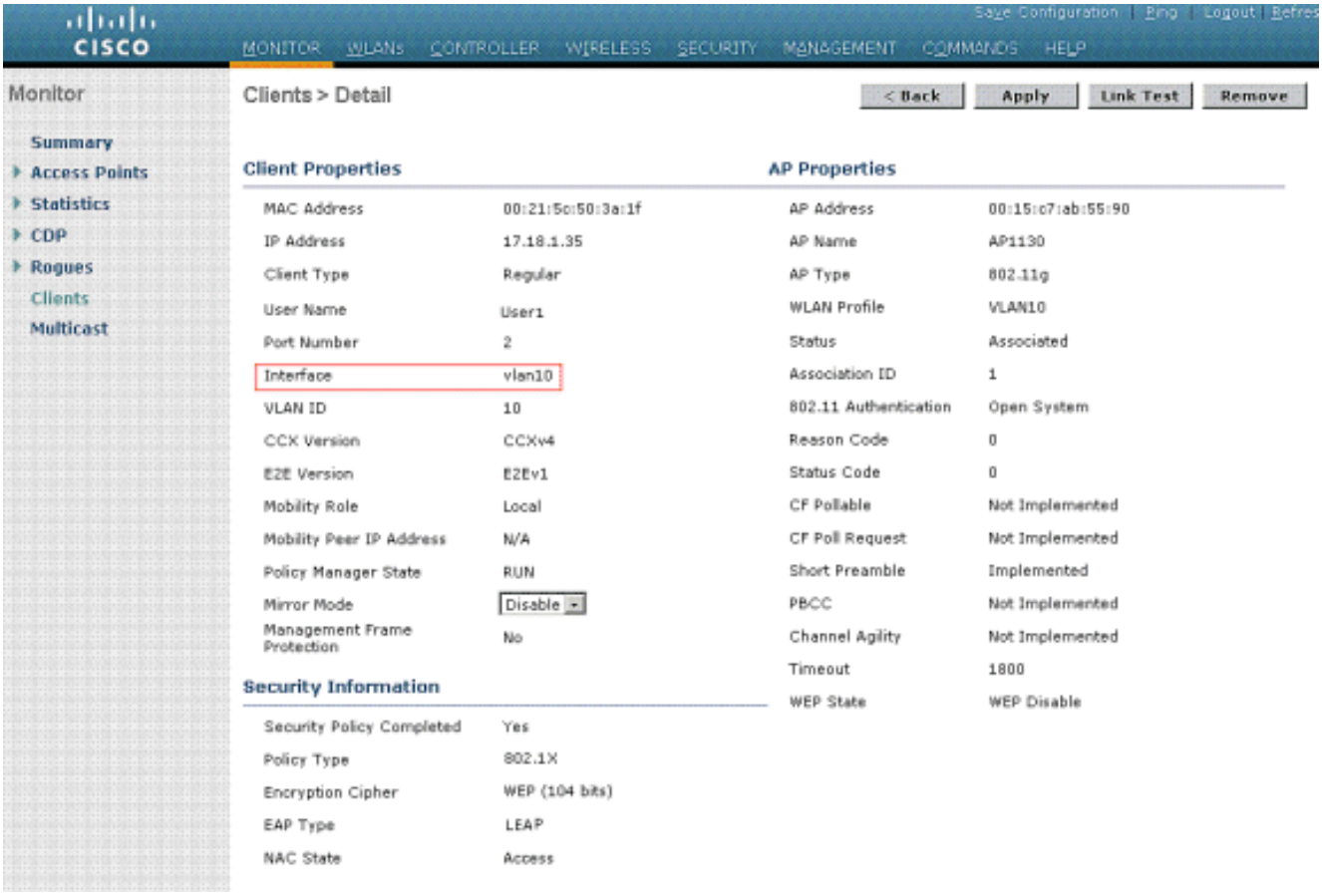
Una vez que la autenticación y la validación correspondiente se hayan realizado correctamente, recibirá el mensaje de estado correcto.

Luego, debe verificar que su cliente esté asignado a la VLAN adecuada según los atributos RADIUS enviados. Complete estos pasos para lograr esto:

1. Desde la GUI del controlador, elija **Wireless > AP**.
2. Haga clic en **Clientes**, que aparece en la esquina izquierda de la ventana Puntos de acceso (AP).Se muestran las estadísticas del cliente.

3. Haga clic en **Detalles** para identificar los detalles completos del cliente, como la dirección IP, la VLAN a la que se asigna, etc.Este ejemplo muestra estos detalles del cliente,

user1:



Desde esta ventana, puede observar que este cliente está asignado a VLAN10 según los atributos RADIUS configurados en el servidor RADIUS.**Nota:** Si la asignación de VLAN dinámica se basa en el parámetro **Atributo VSA de Cisco Airespace**, el **nombre de la interfaz lo mostrará como admin** según este ejemplo en la página de detalles del cliente.

Use esta sección para confirmar que su configuración funciona correctamente.

- **debug aaa events enable**: este comando se puede utilizar para asegurar la transferencia exitosa de los atributos RADIUS al cliente a través del controlador. Esta parte del resultado de depuración asegura una transmisión exitosa de los atributos RADIUS:

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
........44 a9 da 6c 36 94 0a f3  <D..16...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
```

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800
```

- Estos comandos también pueden ser útiles:**debug dot1x aaa enabledebug aaa packets enable**

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Nota: La asignación de VLAN dinámica no funciona para la autenticación web desde un WLC.

Información Relacionada

- Autenticación del EAP con servidor RADIUS
- LEAP de Cisco
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Soporte Técnico y Documentación - Cisco Systems