

Ejemplo de Configuración de Autorización de Punto de Acceso Ligero (LAP) en una Red Inalámbrica Unificada de Cisco

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Autorización ligera del Punto de acceso \(REVESTIMIENTO\)](#)

[Usando la lista interna de la autorización en el WLC](#)

[Verificación](#)

[Autorización AP contra un servidor AAA](#)

[Configure Cisco ACS seguro para autorizar los revestimientos](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento explica cómo configurar los Controladores de LAN Inalámbricos (WLC) para autorizar Lightweight Access Points (LAP) según la dirección MAC de los LAP.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de cómo configurar un Cisco Secure Access Control Server (ACS) para autenticar a los clientes de red inalámbrica
- Conocimiento de la configuración de los revestimientos y de Cisco WLCs de Cisco Aironet
- El conocimiento de Cisco unificó las soluciones de la seguridad de red inalámbrica

Componentes Utilizados

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

- Cisco 4400 Series WLC que funciona con la versión 5.0.148.0

- Revestimientos del Cisco Aironet de la serie 1000
- Revestimientos del Cisco Aironet de la serie 1200
- Cisco asegura la versión 4.2 del servidor ACS

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.

Autorización ligera del Punto de acceso (REVESTIMIENTO)

Durante el proceso de inscripción del REVESTIMIENTO, los revestimientos y el WLCs autentican mutuamente usando los Certificados X.509.

Los Certificados X.509 son quemados en el flash protegido en el punto de acceso y WLC en la fábrica por Cisco. En el AP, los Certificados instalados en fábrica se llaman fabricación los Certificados instalados (MIC). Todo el Cisco APs fabricó después de julio 18, 2005 tiene MICs.

Cisco los APs de Aironet 1200, 1130, y 1240 fabricó antes de julio 18, 2005, que se han actualizado del IOS autónomo al IOS ligero del protocolo del Punto de acceso (LWAPP), genera un certificado autofirmado (SSC) durante el proceso de actualización. Para la información sobre cómo manejar los APs con SSCs, refiera a [actualizar las puntas de acceso Aironet autónomas de Cisco al modo ligero](#).

Además de esta autenticación recíproca que ocurra durante el proceso de inscripción, el WLCs puede también restringir los revestimientos que se registran con ellos basaron en la dirección MAC del REVESTIMIENTO.

La falta de una contraseña fuerte por el uso de la dirección MAC del REVESTIMIENTO no debe ser un problema porque el regulador utiliza el MIC para autenticar el AP antes de autorizar el AP a través del servidor de RADIUS. El uso del MIC proporciona a la autenticación robusta.

La autorización del REVESTIMIENTO se puede realizar en dos maneras:

- Usando la lista interna de la autorización en el WLC
- Usando la base de datos de la dirección MAC en un servidor AAA

Los comportamientos de los revestimientos diferencian basado en el certificado usado:

- Traslapa con SSCs — El WLC utilizará solamente la lista interna de la autorización y no transmitirá a una petición un servidor de RADIUS para estos revestimientos.
- Traslapa con MICs — WLC puede utilizar la lista interna de la autorización configurada en el WLC o utilizar a un servidor de RADIUS para autorizar los revestimientos

Este documento discute la autorización del REVESTIMIENTO usando la lista interna de la autorización y el servidor AAA.

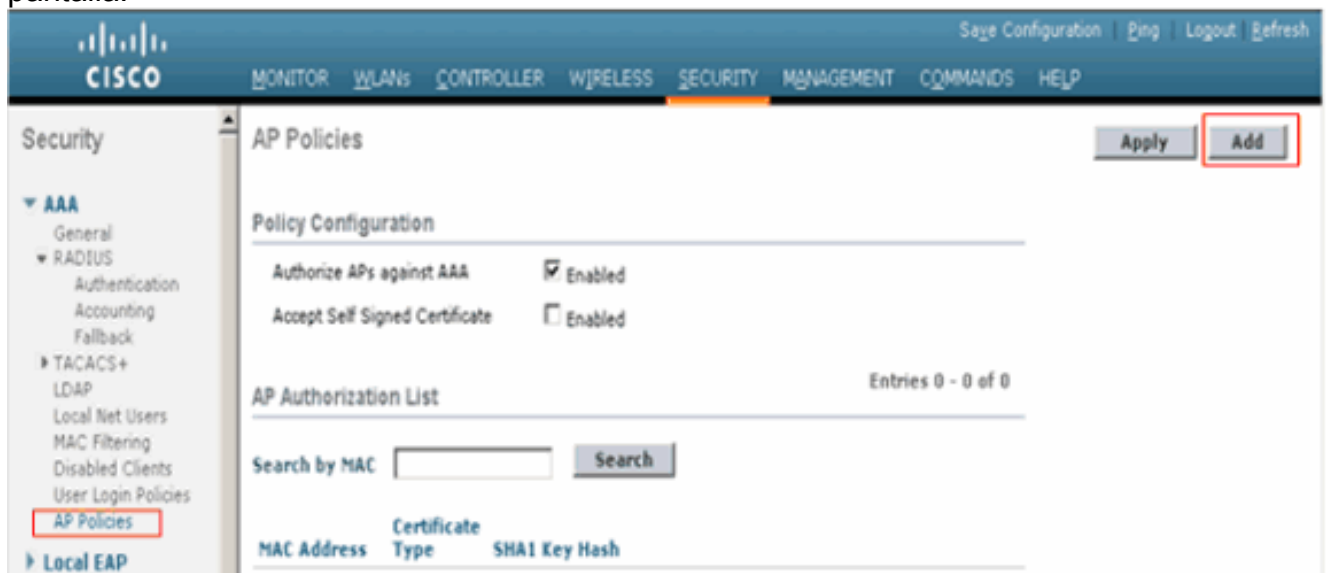
Usando la lista interna de la autorización en el WLC

En el WLC, utilice la lista de la autorización AP para restringir los revestimientos basados en su dirección MAC. La lista de la autorización AP está disponible bajo la **Seguridad > directivas AP** en el GUI WLC.

Este ejemplo muestra cómo agregar el REVESTIMIENTO con la dirección MAC **00:0b:85:5b:fb:d0**.

Complete estos pasos:

1. Del GUI del regulador WLC, haga clic la **Seguridad > las directivas AP**. La página de las directivas AP aparece.
2. Bajo configuración de la política, controle el cuadro para saber si hay **Authorize APs contra el AAA**. Cuando se selecciona este parámetro, el WLC controla la lista local de la autorización primero. Si el MAC del REVESTIMIENTO no está presente, controla al servidor de RADIUS.
3. Haga clic el **botón Add** en el Lado derecho de la pantalla.



4. Bajo agregue el AP a la lista de la autorización, ingresan el MAC address AP. Entonces, elija el tipo de certificado y el tecleo **agrega**. En este ejemplo, un REVESTIMIENTO con el certificado MIC se agrega. **Nota:** Para los revestimientos con SSCs, elija **SSC** bajo el tipo de

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

AP Policies

Policy Configuration

Authorize APs against AAA Enabled

Accept Self Signed Certificate Enabled

Add AP to Authorization List

MAC Address

Certificate Type

certificado.

El

REVESTIMIENTO se agrega a la lista de la autorización AP y es mencionado conforme a la lista de la autorización

AP Authorization List Entries 1 - 1 of 1

Search by MAC

MAC Address	Certificate Type	SHA1 Key Hash
00:0b:85:51:5a:e0	MIC	

AP.

Verificación

Para verificar esta configuración, usted necesita conectar el REVESTIMIENTO con la dirección MAC 00:0b:85:51:5a:e0 a la red y al monitor. Utilice el **permiso** y los **comandos debug aaa all enable de los eventos del lwapp de la depuración** para realizar esto.

Esta salida muestra las depuraciones cuando la dirección MAC del REVESTIMIENTO no está presente en la lista de la autorización AP:

Nota: Algunas de las líneas en la salida se han movido a la segunda línea debido a los apremios del espacio.

```
debug lwapp events enable
```

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80
rxNonce 00:0B:85:51:5A:E0
```

Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007: **spamRadiusProcessResponse: AP Authorization failure for 00:0b:85:51:5a:e0**

debug aaa all enable

Wed Sep 12 17:56:26 2007: **Unable to find requested user entry for 000b85515ae0**
Wed Sep 12 17:56:26 2007: AuthenticationRequest: 0xac476e8
Wed Sep 12 17:56:26 2007: Callback.....0x8108e2c
Wed Sep 12 17:56:26 2007: protocolType.....0x00000001
Wed Sep 12 17:56:26 2007: proxyState.....00:0B:85:51:5A:E0-00:00
Wed Sep 12 17:56:26 2007: Packet contains 8 AVPs (not shown)
Wed Sep 12 17:56:26 2007: **00:0b:85:51:5a:e0 Returning AAA Error 'No Server' (-7)**
for mobile 00:0b:85:51:5a:e0
Wed Sep 12 17:56:26 2007: AuthorizationResponse: 0xbadff7d4
Wed Sep 12 17:56:26 2007: structureSize.....28
Wed Sep 12 17:56:26 2007: resultCode.....-7
Wed Sep 12 17:56:26 2007: protocolUsed.....0xffffffff
Wed Sep 12 17:56:26 2007: proxyState.....00:0B:85:51:5A:E0-00:00
Wed Sep 12 17:56:26 2007: Packet contains 0 AVPs:
Wed Sep 12 17:56:31 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:31 2007: AuthenticationRequest: 0xac476e8
Wed Sep 12 17:56:31 2007: Callback.....0x8108e2c
Wed Sep 12 17:56:31 2007: protocolType.....0x00000001
Wed Sep 12 17:56:31 2007: proxyState.....00:0B:85:51:5A:E0-00:00
Wed Sep 12 17:56:31 2007: Packet contains 8 AVPs (not shown)
Wed Sep 12 17:56:31 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No Server' (-7)
for mobile 00:0b:85:51:5a:e0

Esta demostración de la salida las depuraciones cuando la dirección MAC del REVESTIMIENTO se agrega a la lista de la autorización AP:

Nota: Algunas de las líneas en la salida se han movido a la segunda línea debido a los apremios del espacio.

debug lwapp events enable

Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'**
Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1**
Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'**
Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1**
Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'**
Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0
Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0**
Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0 (index 58)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0
Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0**
Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Register LWAPP event for

```
AP 00:0b:85:51:5a:e0 slot 0
Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Register LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
```

```
debug aaa all enable
```

```
Wed Sep 12 17:57:44 2007: User 000b85515ae0 authenticated
Wed Sep 12 17:57:44 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'Success' (0)
for mobile 00:0b:85:51:5a:e0
Wed Sep 12 17:57:44 2007: AuthorizationResponse: 0xbadff96c
Wed Sep 12 17:57:44 2007: structureSize.....70
Wed Sep 12 17:57:44 2007: resultCode.....0
Wed Sep 12 17:57:44 2007: protocolUsed.....0x00000008
Wed Sep 12 17:57:44 2007: proxyState.....00:0B:85:51:5A:E0-00:00
Wed Sep 12 17:57:44 2007: Packet contains 2 AVPs:
Wed Sep 12 17:57:44 2007:     AVP[01] Service-Type.....
        0x00000065 (101) (4 bytes)
Wed Sep 12 17:57:44 2007:     AVP[02] Airespace / WLAN-Identifier.....
        0x00000000 (0) (4 bytes)
```

[Autorización AP contra un servidor AAA](#)

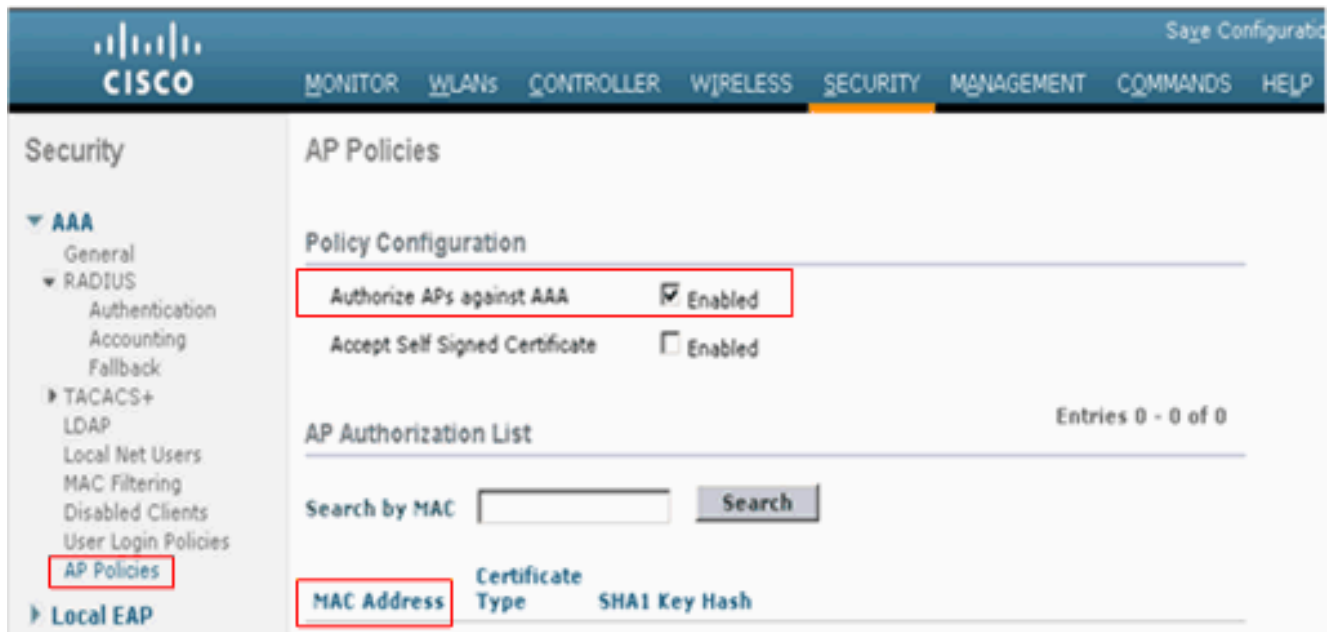
Usted puede también configurar WLCs para utilizar a los servidores de RADIUS para autorizar los APs usando MICs. El WLC utiliza la dirección MAC de un REVESTIMIENTO como ambos el nombre de usuario y contraseña al enviar la información a un servidor de RADIUS. Por ejemplo, si la dirección MAC del AP es 000b85229a70, ambos el nombre de usuario y contraseña usado por el regulador para autorizar el AP son 000b85229a70.

Nota: Si usted utiliza la dirección MAC como el nombre de usuario y contraseña para la autenticación AP en un servidor RADIUS AAA, no utilice el mismo servidor AAA para la autenticación de cliente. La razón de esto es si los hackers descubren la dirección MAC AP, después pueden utilizar ese MAC como las credenciales del nombre de usuario y contraseña para conseguir sobre la red.

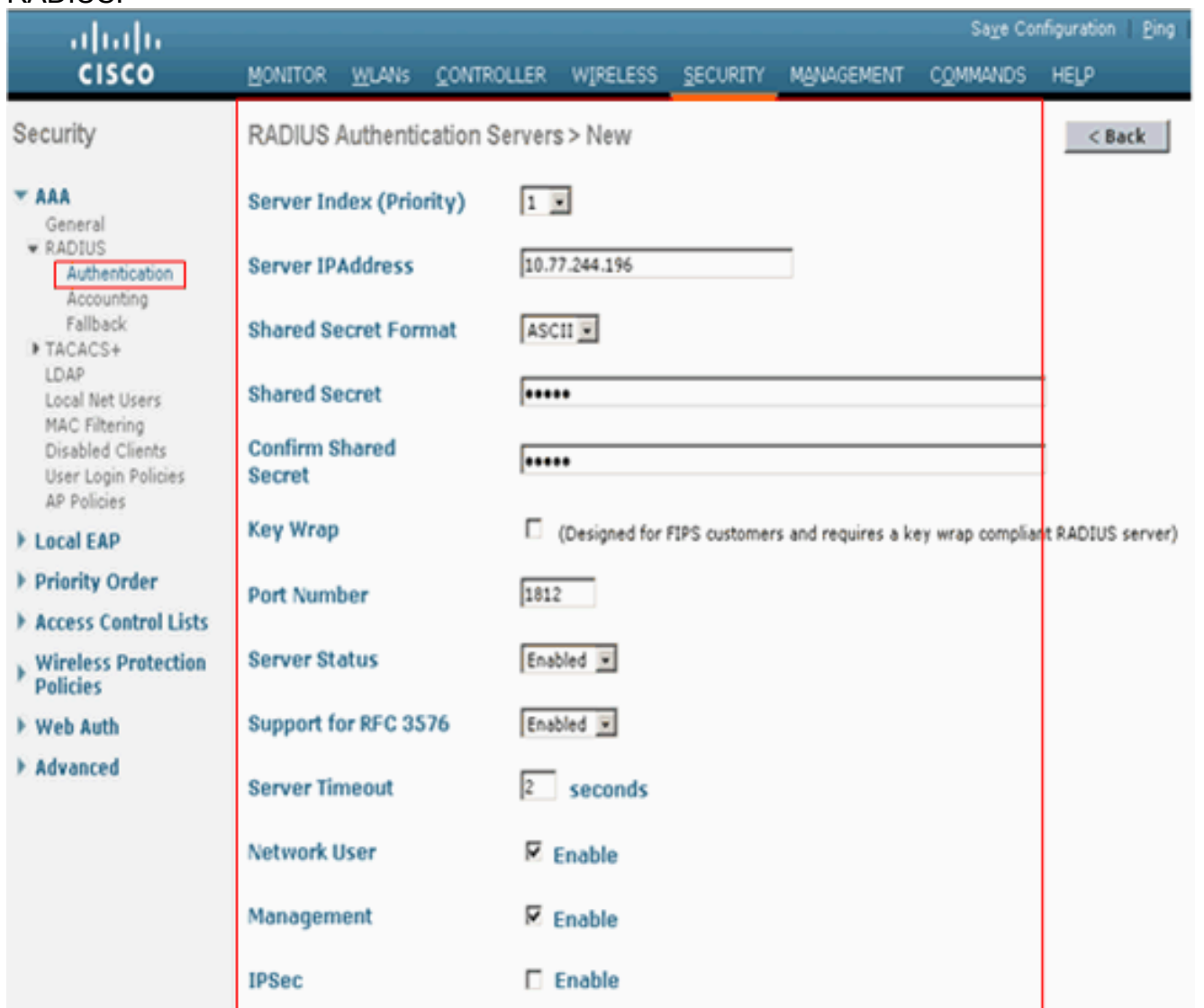
Este ejemplo muestra cómo configurar el WLCs para autorizar los revestimientos usando Cisco ACS seguro.

Complete estos pasos en el WLC:

1. Del GUI del regulador WLC, haga clic la **Seguridad > las directivas AP**. La página de las directivas AP aparece.
2. Bajo configuración de la política, controle el cuadro para saber si hay **Authorize APs contra el AAA**. Cuando se selecciona este parámetro, el WLC controla la base de datos del MAC local primero. Por este motivo, asegúrese de que la base de datos local esté vacía borrando las direcciones MAC conforme a la lista de la autorización AP. Si la dirección MAC del REVESTIMIENTO no está presente, entonces controla al servidor de RADIUS.



- Haga clic la **Seguridad** y la **autenticación de RADIUS** del GUI del regulador para visualizar la página de los servidores de autenticación de RADIUS. Entonces, haga clic **nuevo** para definir a un servidor de RADIUS.



- Defina los parámetros del servidor de RADIUS en los **servidores de autenticación de RADIUS > nueva** página. Estos parámetros incluyen la dirección IP, el secreto compartido,

el número del puerto, y el estado del servidor del servidor de RADIUS. Este ejemplo utiliza Cisco ACS seguro como el servidor de RADIUS con la dirección IP 10.77.244.196.

5. Haga clic en Apply (Aplicar).

[Configure Cisco ACS seguro para autorizar los revestimientos](#)

Para permitir a Cisco ACS seguro autorizar los revestimientos, usted necesita completar estos pasos:

1. [Configure el WLC como cliente AAA en Cisco ACS seguro](#)
2. [Agregue las direcciones MAC del REVESTIMIENTO a la base de datos de usuarios en Cisco ACS seguro](#)

[Configure el WLC como cliente AAA en Cisco ACS seguro](#)

Complete estos pasos para configurar el WLC como cliente AAA en Cisco ACS seguro:

1. **La Configuración de la red del teclado agrega al cliente AAA.** La página del cliente AAA del agregar aparece.
2. En esta página, defina el nombre del sistema WLC, dirección IP de la interfaz de administración, secreto compartido, y autentiqúelo usando RADIUS Airespace. **Nota:** Alternativamente, usted puede intentar la opción de la autenticidad usando RADIUS Aironet. Aquí tiene un ejemplo:

The screenshot shows the 'AAA Client Setup for wlc1' configuration page in Cisco ACS. The form is enclosed in a red border. The fields are as follows:

- AAA Client IP Address: 10.77.244.212
- Shared Secret: cisco
- RADIUS Key Wrap:
 - Key Encryption Key: [Empty]
 - Message Authenticator Code Key: [Empty]
 - Key Input Format: ASCII Hexadecimal
- Authenticate Using: RADIUS (Cisco Airespace)
- Options (all unchecked):
 - Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
 - Log Update/Watchdog Packets from this AAA Client
 - Log RADIUS Tunneling Packets from this AAA Client
 - Replace RADIUS Port info with Username from this AAA Client
 - Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Buttons at the bottom: Submit, Submit + Apply, Delete, Delete + Apply, Cancel.

The Help sidebar on the right contains the following text:

AAA Client IP Address

Type the IP address information for this AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

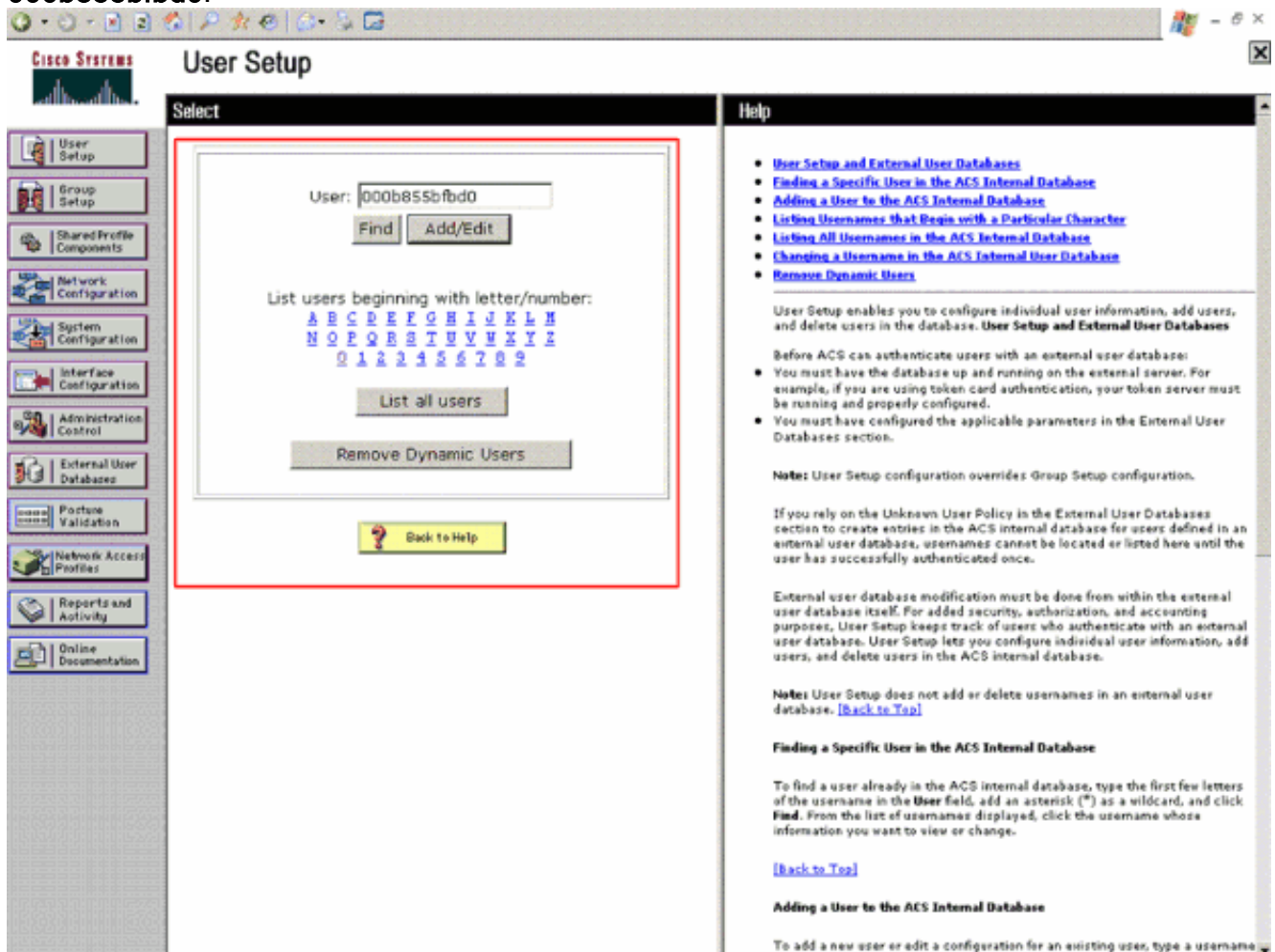
You can define ranges within an octet of an IP address. For

3. El teclado **somete + se aplica**.

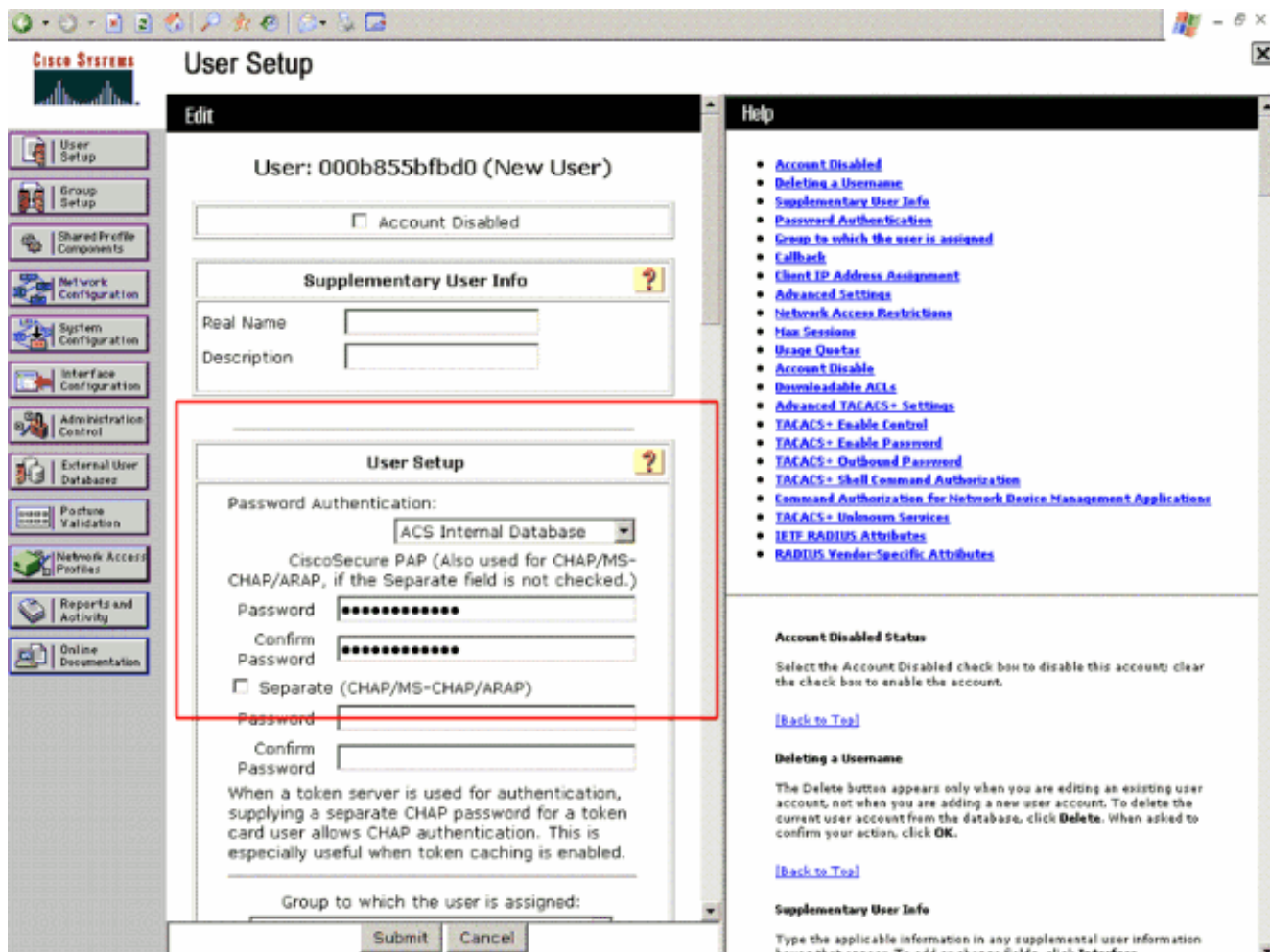
[Agregue las direcciones MAC del REVESTIMIENTO a la base de datos de usuarios en Cisco ACS seguro](#)

Complete estos pasos para agregar las direcciones MAC del REVESTIMIENTO a Cisco ACS seguro:

1. Elija la **configuración de usuario del GUI ACS**, ingrese el username, y el teclado **agrega/corrig**e. El username debe ser la dirección MAC del REVESTIMIENTO que usted quiere autorizar. La dirección MAC no debe contener los dos puntos o los guiones. En este ejemplo, el REVESTIMIENTO se agrega con la dirección MAC **000b855bfd0**:



2. Cuando aparece la página de la configuración de usuario, defina la contraseña para este REVESTIMIENTO en el campo de contraseña como se muestra. La contraseña debe también ser la dirección MAC del REVESTIMIENTO. En este ejemplo, es **000b855bfd0**.



3. Haga clic en Submit (Enviar).
4. Relance este procedimiento para agregar más revestimientos a Cisco aseguran la base de datos ACS.

Verificación

Para verificar esta configuración, usted necesita conectar el REVESTIMIENTO con la dirección MAC 00:0b:85:51:5a:e0 a la red y al monitor. Utilice el **permiso** y los **comandos debug aaa all enable de los eventos del lwapp de la depuración** para realizar esto.

Según lo visto de las depuraciones, el WLC pasajero en la dirección MAC del REVESTIMIENTO al servidor de RADIUS 10.77.244.196, y el servidor ha autenticado con éxito el REVESTIMIENTO. El REVESTIMIENTO entonces se registra con el regulador.

Nota: Algunas de las líneas en la salida se han movido a la segunda línea debido a los apremios del espacio.

```
debug aaa all enable
```

```
Thu Sep 13 13:54:39 2007: AuthenticationRequest: 0xac48778
Thu Sep 13 13:54:39 2007: Callback.....0x8108e2c
Thu Sep 13 13:54:39 2007: protocolType.....0x00000001
Thu Sep 13 13:54:39 2007: proxyState.....00:0B:85:51:5A:E0-00:00
Thu Sep 13 13:54:39 2007: Packet contains 8 AVPs (not shown)
Thu Sep 13 13:54:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
Authentication Packet (id 123) to 10.77.244.196:1812,
```

```
proxy state 00:0b:85:51:5a:e0-85:51
Thu Sep 13 13:54:39 2007: 00000000: 01 7b 00 72 00 00 00 00 00 00 00 00 00 00 00 00
.{r.....
Thu Sep 13 13:54:39 2007: 00000010: 00 00 00 00 01 0e 30 30 30 62 38 35 35 31 35 61
.....000b85515a
Thu Sep 13 13:54:39 2007: 00000020: 65 30 1e 13 30 30 2d 30 62 2d 38 35 2d 33 33 2d
e0..00-0b-85-33-
Thu Sep 13 13:54:39 2007: 00000030: 35 32 2d 38 30 1f 13 30 30 2d 30 62 2d 38 35 2d
52-80..00-0b-85-
Thu Sep 13 13:54:39 2007: 00000040: 35 31 2d 35 61 2d 65 30 05 06 00 00 00 01 04 06
51-5a-e0.....
Thu Sep 13 13:54:39 2007: 00000050: 0a 4d f4 d4 20 06 77 6c 63 31 02 12 03 04 0e 12
.M...wlc1.....
Thu Sep 13 13:54:39 2007: 00000060: 84 9c 03 8f 63 40 2a be 9d 38 42 91 06 06 00 00
....c@*..8B....
Thu Sep 13 13:54:39 2007: 00000070: 00 0a
..
Thu Sep 13 13:54:40 2007: 00000000: 02 7b 00 30 aa fc 40 4b fe 3a 33 10 f6 5c 30 fd
.{.0..@K.:3..\0.
Thu Sep 13 13:54:40 2007: 00000010: 12 f3 6e fa 08 06 ff ff ff ff 19 16 43 41 43 53
..n.....CACS
Thu Sep 13 13:54:40 2007: 00000020: 3a 30 2f 39 37 37 2f 61 34 64 66 34 64 34 2f 31
:0/977/a4df4d4/1
Thu Sep 13 13:54:40 2007: ****Enter processIncomingMessages: response code=2
Thu Sep 13 13:54:40 2007: ****Enter processRadiusResponse: response code=2
Thu Sep 13 13:54:40 2007: 00:0b:85:51:5a:e0 Access-Accept received
from RADIUS server 10.77.244.196 for mobile 00:0b:85:51:5a:e0 receiveId = 0
Thu Sep 13 13:54:40 2007: AuthorizationResponse: 0x9845500
Thu Sep 13 13:54:40 2007: structureSize.....84
Thu Sep 13 13:54:40 2007: resultCode.....0
Thu Sep 13 13:54:40 2007: protocolUsed.....0x00000001
Thu Sep 13 13:54:40 2007: proxyState.....00:0B:85:51:5A:E0-00:00
Thu Sep 13 13:54:40 2007: Packet contains 2 AVPs:
Thu Sep 13 13:54:40 2007: AVP[01] Framed-IP-Address.....
0xffffffff (-1) (4 bytes)
Thu Sep 13 13:54:40 2007: AVP[02] Class.....
CACS:0/977/a4df4d4/1 (20 bytes)
```

debug lwapp events enable

```
Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80
rxNonce 00:0B:85:51:5A:E0
Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 LWAPP Join-Request MTU path
from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for
AP 00:0b:85:51:5a:e0(index 57)Switch IP: 10.77.244.213, Switch Port: 12223,
intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0
Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Successfully transmission of
LWAPP Join-Reply to AP 00:0b:85:51:5a:e0
Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Register LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Register LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
```

Troubleshooting

Utilice estos comandos de resolver problemas su configuración:

Nota: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un **comando debug**.

- **ponga a punto el permiso de los eventos del lwapp** — Configura la depuración de los eventos y de los errores LWAPP.
- **permiso del paquete del lwapp de la depuración** — Configura la depuración del rastro del paquete LWAPP.
- **la depuración aaa todo activa** — Configura la depuración de todos los mensajes AAA.

Información Relacionada

- [Actualizar los puntos de acceso autónomos del Cisco Aironet al modo ligero](#)
- [Consejos de Troubleshooting de la Herramienta de Upgrade de LWAPP](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)