

Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requisitos](#)

[Componentes usados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configure el WLC para la operación básica y registre los APs ligeros al regulador](#)

[Configure el WLC para la autenticación de RADIUS a través de un servidor de RADIUS externo](#)

[Configure los parámetros de la red inalámbrica \(WLAN\)](#)

[Configure Cisco ACS seguro como el servidor de RADIUS externo y cree una base de datos de usuarios para las Autenticaciones de clientes](#)

[Configure al cliente](#)

[Verifique](#)

[Troubleshooting](#)

[Extremidades de troubleshooting](#)

[Temporizadores de manipulación EAP](#)

[Extracción del archivo de paquete del servidor de RADIUS ACS para resolver problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento explica cómo configurar el controlador de LAN inalámbrico (WLC) para la autenticación EAP (Extensible Authentication Protocol) mediante un servidor RADIUS externo. Este ejemplo de la configuración utiliza el Cisco Secure Access Control Server (ACS) como el servidor de RADIUS externo para validar los credenciales de usuario.

[Prerequisites](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de los Puntos de acceso ligeros (APs) y de Cisco WLCs.
- Conocimiento básico del protocolo ligero AP (LWAPP).

- Conocimiento de cómo configurar a un servidor de RADIUS externo como Cisco ACS seguro.

Componentes usados

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

- Serie AP ligero de Cisco Aironet 1232AG
- Cisco 4400 Series WLC que funciona con los firmwares 5.1
- Cisco ACS seguro que funciona con la versión 4.1
- Adaptador del cliente del 802.11 a/b/g de Cisco Aironet
- Cisco utilidad Aironet Desktop (ADU) ese firmware 4.2 de los funcionamientos

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 Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Configurar

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

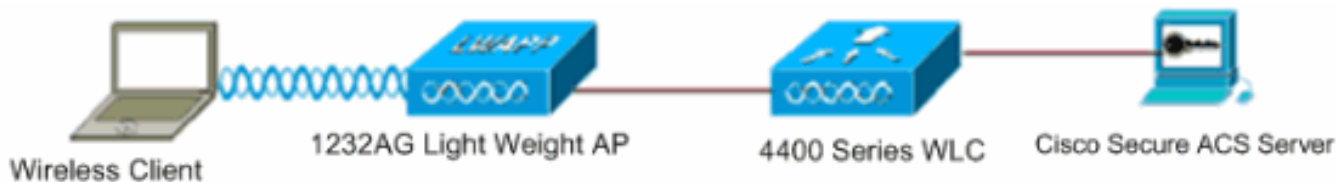
Note: Utilice la [herramienta de búsqueda de comandos \(clientes registrados solamente\)](#) para encontrar más información sobre los comandos usados en este documento.

Complete estos pasos para configurar los dispositivos para la autenticación EAP:

1. [Configure el WLC para la operación básica y registre los APs ligeros al regulador.](#)
2. [Configure el WLC para la autenticación de RADIUS a través de un servidor de RADIUS externo.](#)
3. [Configure los parámetros de la red inalámbrica \(WLAN\).](#)
4. [Configure Cisco ACS seguro como el servidor de RADIUS externo y cree una base de datos de usuarios para los clientes de autenticidad.](#)

Diagrama de la red

En esta disposición, Cisco 4400 WLC y un AP ligero está conectado a través de un concentrador. Un servidor de RADIUS externo (Cisco ACS seguro) también está conectado con el mismo concentrador. Todos los dispositivos están en la misma subred. El AP se registra inicialmente al regulador. Usted debe configurar el WLC y el AP para la autenticación del protocolo lightweight extensible authentication (SALTO). Los clientes que conectan con la autenticación LEAP del uso AP para asociarse al AP. Cisco ACS seguro se utiliza para realizar la autenticación de RADIUS.



[Configure el WLC para la operación básica y registre los APs ligeros al regulador](#)

Utilice al Asistente de la configuración de inicio en el comando line interface(cli) para configurar el WLC para la operación básica. Alternativamente, usted puede también utilizar el GUI para configurar el WLC. Este documento explica la configuración en el WLC con el Asistente de la configuración de inicio en el CLI.

Después de los cargadores del programa inicial WLC por primera vez, ingresa directamente en el Asistente de la configuración de inicio. Utilice al asistente de configuración para configurar las configuraciones básicas. Usted puede funcionar con al Asistente en el CLI o el GUI. Esta salida muestra un ejemplo del Asistente de la configuración de inicio en el CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration..
```

Estos parámetros pusieron el WLC para la operación básica. En este ejemplo de la configuración, el WLC utiliza **10.77.244.204** como la dirección IP de la interfaz de administración y **10.77.244.205** como la dirección IP del interfaz del AP-encargado.

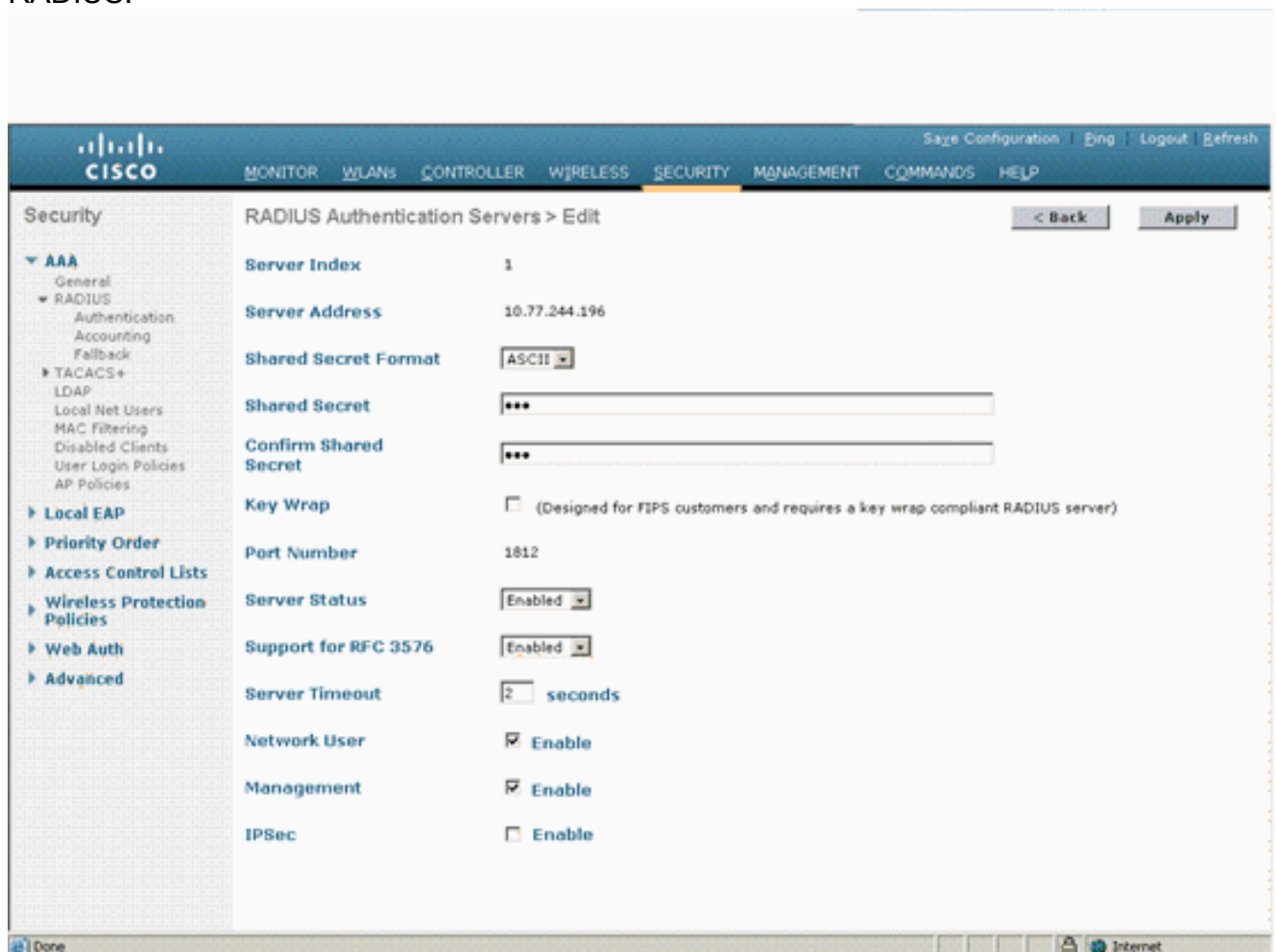
Antes de que cualquier otra función se pueda configurar en el WLCs, los APs ligeros tienen que registrarse con el WLC. Este documento asume que el AP ligero está registrado al WLC. Refiera al [registro ligero AP \(REVESTIMIENTO\) a un regulador LAN de la Tecnología inalámbrica \(WLC\)](#) para más información sobre cómo los APs ligeros se registran con el WLC.

[Configure el WLC para la autenticación de RADIUS a través de un servidor de RADIUS externo](#)

El WLC necesita ser configurado para remitir los credenciales de usuario a un servidor de RADIUS externo. El servidor de RADIUS externo después valida los credenciales de usuario y proporciona al acceso a los clientes de red inalámbrica.

Complete estos pasos para configurar el WLC para un servidor de RADIUS externo:

1. Elija 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.



2. 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. Las casillas de verificación del usuario de la red y de la Administración determinan si la autenticación basada en RADIUS solicita la Administración y los usuarios de la red WLC. Este ejemplo utiliza Cisco ACS seguro como el servidor de RADIUS con la dirección IP 10.77.244.196.
3. El servidor de RADIUS puede ahora ser utilizado por el WLC para la autenticación. Usted puede encontrar al servidor de RADIUS enumerado si usted elige la **Seguridad > el radio > la autenticación**.



El RFC 3576 se utiliza en el servidor de RADIUS del Registro de acceso de CNS de Cisco (COCHE), pero no en Cisco asegura la versión 4.0 y anterior del servidor ACS. Usted puede también utilizar la característica local del servidor de RADIUS para autenticar a los usuarios. Presentaron al servidor de RADIUS local con el código de 4.1.171.0 de la versión. WLCs que se ejecuta las versiones anteriores no tiene la característica local del radio. EAP local es un método de autenticación que permite los usuarios y a los clientes de red inalámbrica que se autenticarán localmente. Se diseña para el uso en las oficinas remotas que quieren mantener la Conectividad a los clientes de red inalámbrica cuando el sistema backend se interrumpe o va el servidor externo de la autenticación abajo. EAP local extrae los credenciales de usuario de la base de datos de usuarios locales o de la base de datos de la parte LDAP para autenticar a los usuarios. Las ayudas locales EAP SALTAN, EAP-FAST con los PACs, EAP-FAST con los Certificados, y autenticación EAP-TLS entre el regulador y los clientes de red inalámbrica. EAP local se diseña como sistema de autenticación de reserva. Si configuran a algunos servidores de RADIUS en el regulador, el regulador intenta autenticar a los clientes de red inalámbrica con los servidores de RADIUS primero. EAP local se intenta solamente si no se encuentra a ningunos servidores de RADIUS, tampoco porque los servidores de RADIUS medidos el tiempo hacia fuera o no se configuró a ningunos servidores de RADIUS. Refiera a la [autenticación local EAP en el regulador LAN de la Tecnología inalámbrica con el ejemplo de la configuración del EAP-FAST y de servidor LDAP](#) para más información sobre cómo configurar EAP local en los reguladores inalámbricos LAN.

[Configure los parámetros de la red inalámbrica \(WLAN\)](#)

Después, configure la red inalámbrica (WLAN) que los clientes utilizan para conectar con la red inalámbrica. Cuando usted configuró los parámetros básicos para el WLC, usted también configuró el SSID para la red inalámbrica (WLAN). Usted puede utilizar este SSID para la red inalámbrica (WLAN) o crear un nuevo SSID. En este ejemplo, usted crea un nuevo SSID.

Note: Usted puede configurar hasta dieciséis redes inalámbricas (WLAN) en el regulador. La solución de la red inalámbrica (WLAN) de Cisco puede controlar hasta dieciséis redes inalámbricas (WLAN) para los APs ligeros. Cada red inalámbrica (WLAN) se puede asignar las políticas de seguridad únicas. Los APs ligeros difunden toda la red inalámbrica (WLAN) activa SSID de la solución de la red inalámbrica (WLAN) de Cisco y aplican las directivas que usted define para cada red inalámbrica (WLAN).

Complete estos pasos para configurar una nueva red inalámbrica (WLAN) y sus parámetros relacionados:

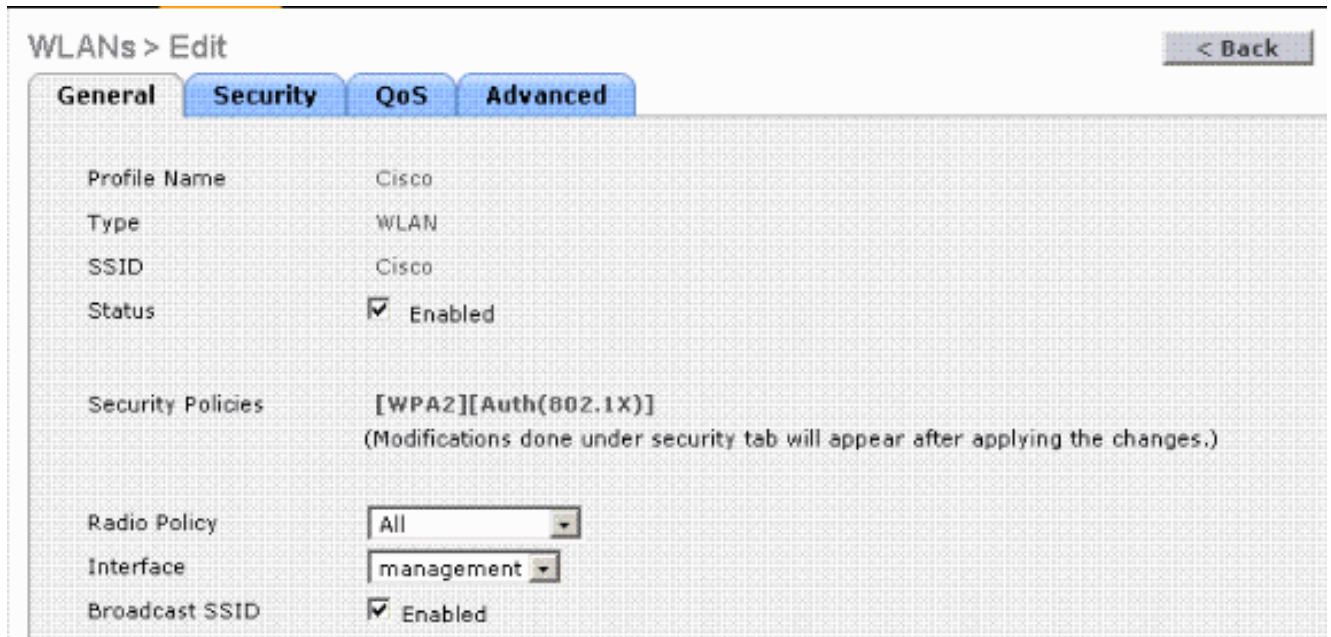
1. Haga clic las **redes inalámbricas (WLAN)** del GUI del regulador para visualizar la página de las redes inalámbricas (WLAN).Esta página enumera las redes inalámbricas (WLAN) que existe en el regulador.
2. Elija **nuevo** para crear una nueva red inalámbrica (WLAN). Ingrese el nombre del perfil y los WLAN SSID para el WLAN y el teclado **se aplican**. Este ejemplo utiliza Cisco como el SSID.



The screenshot shows the Cisco GUI for configuring WLANs. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The 'WLANs' section is active, showing a sidebar with 'WLANs' and 'Advanced' options. The main content area is titled 'WLANs > New' and contains the following fields:

Type	WLAN
Profile Name	Cisco
WLAN SSID	Cisco

3. Una vez que usted crea una nueva red inalámbrica (WLAN), la red inalámbrica (WLAN) > corrige la página para la nueva red inalámbrica (WLAN) aparece. En esta página usted puede definir los diversos parámetros específicos a esta red inalámbrica (WLAN) que incluya las políticas generales, las políticas de seguridad, las directivas QoS y otros parámetros avanzados.

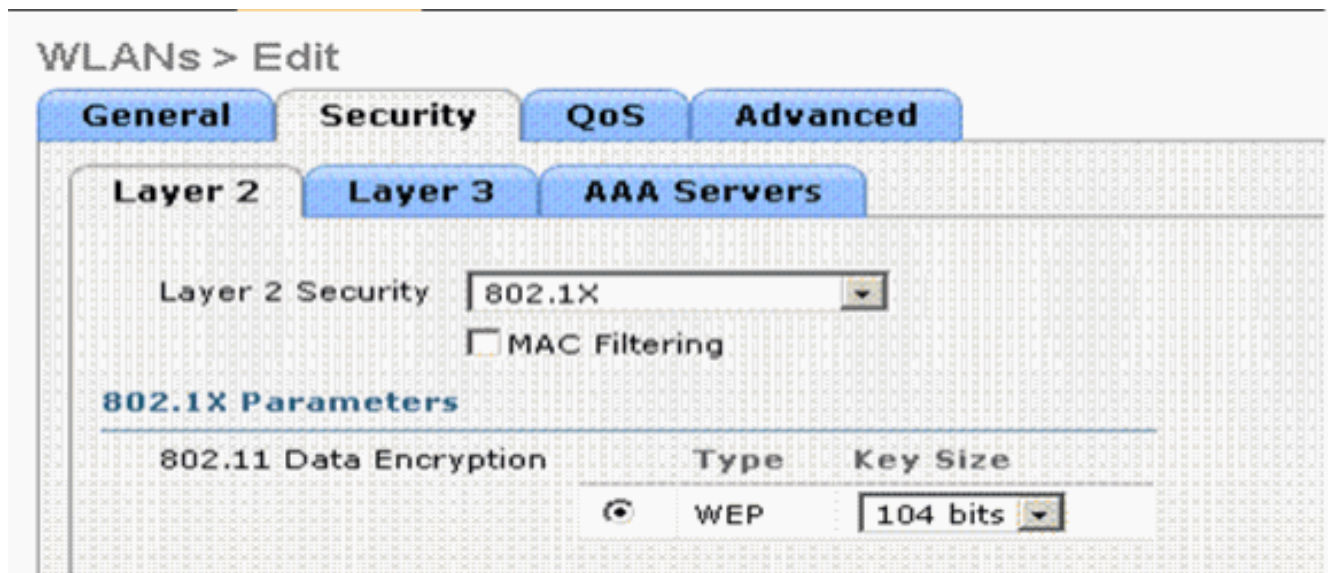


The screenshot shows the Cisco GUI for editing a WLAN. The top navigation bar is the same as the previous screenshot. The 'WLANs' section is active, showing a sidebar with 'WLANs' and 'Advanced' options. The main content area is titled 'WLANs > Edit' and contains a 'Back' button. The 'Security' tab is selected, showing the following fields:

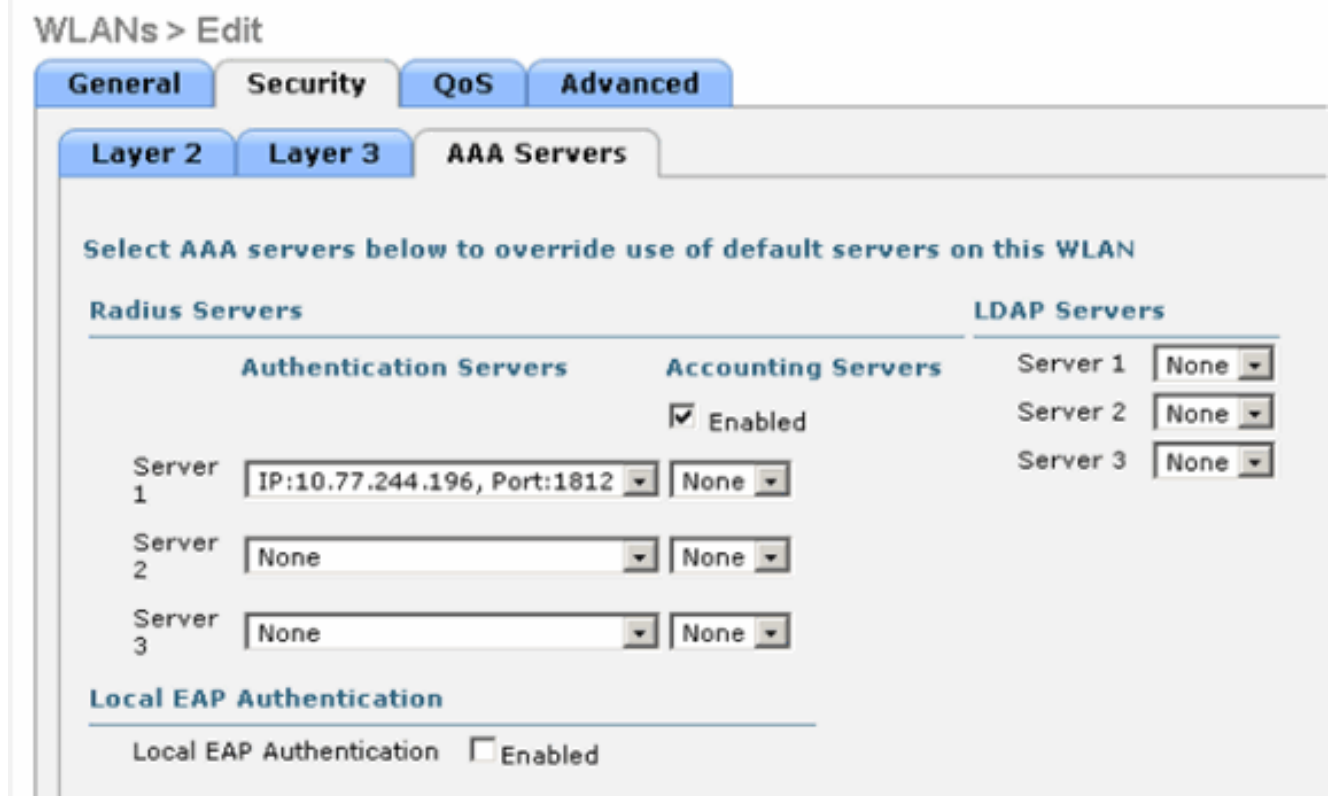
Profile Name	Cisco
Type	WLAN
SSID	Cisco
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Elija el interfaz apropiado del menú desplegable. Los otros parámetros se pueden modificar basaron en el requisito de la red de la red inalámbrica (WLAN).Controle el cuadro del **estatus** bajo políticas generales para activar la red inalámbrica (WLAN).

4. Haga clic la **ficha de seguridad** y elija la **Seguridad de la capa 2**. Del menú desplegable de la Seguridad de la capa 2, elija el **802.1x**. En los parámetros del 802.1x, elija el tamaño de la clave WEP. Este ejemplo utiliza la clave WEP del 128-bit, que es clave WEP the104-bit más el vector de inicialización 24-bit.



5. Elija los **servidores** cuadro **AAA**. Del menú desplegable de los servidores de la autenticación (RADIUS), elija al servidor de RADIUS apropiado. Este servidor se utiliza para autenticar a los clientes de red inalámbrica.

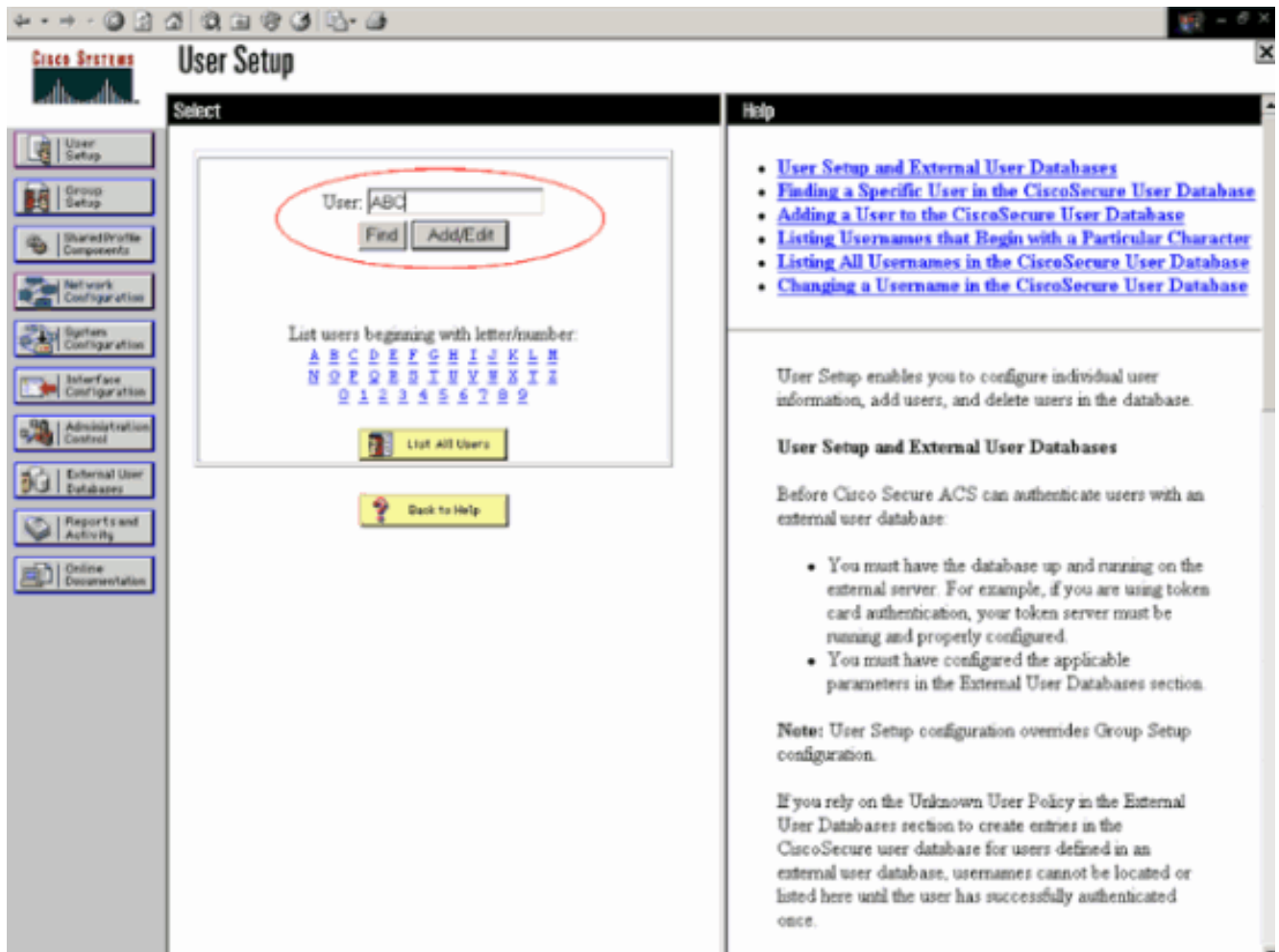


6. El tecleo **se aplica** para salvar la configuración.

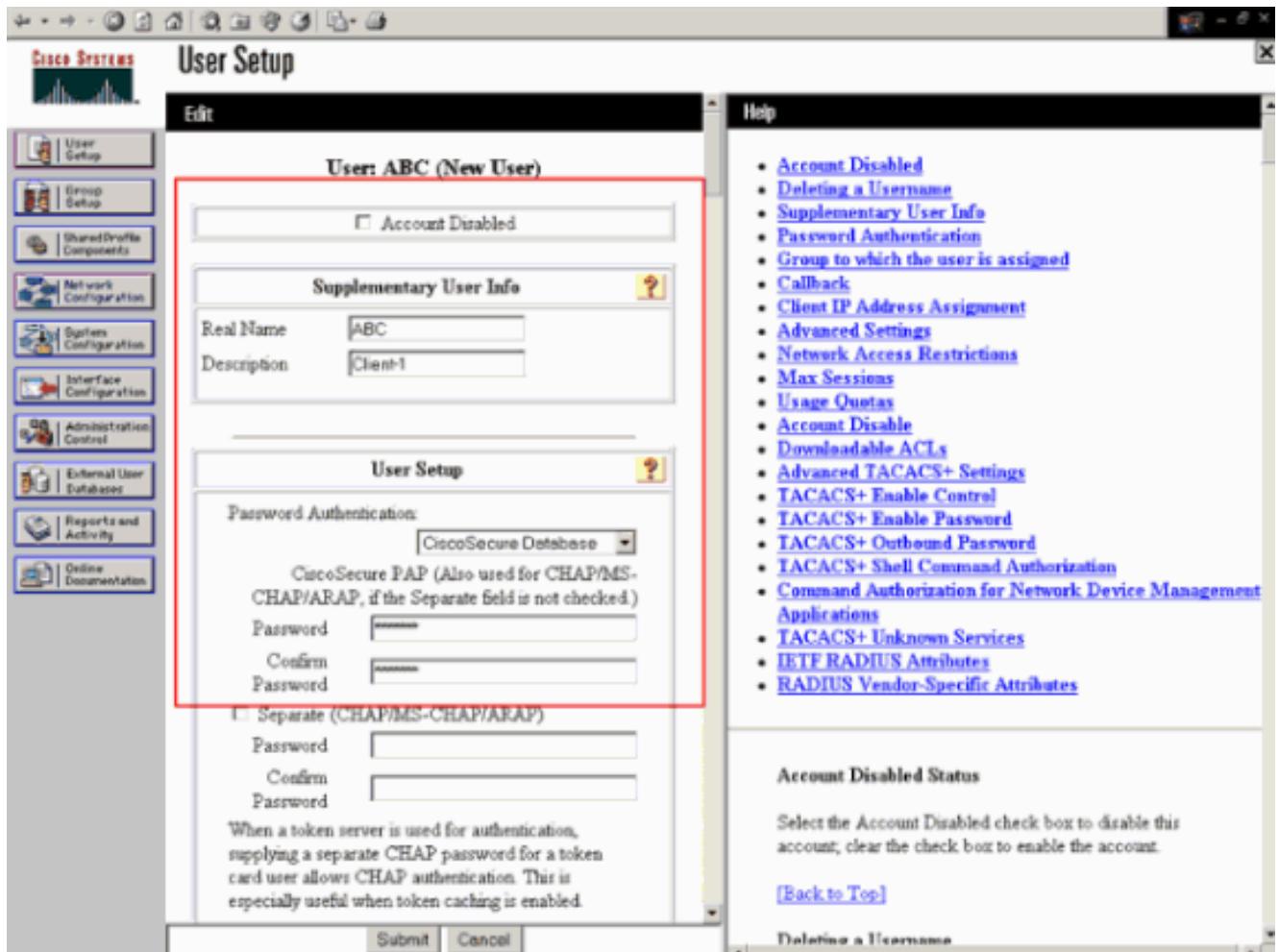
[Configure Cisco ACS seguro como el servidor de RADIUS externo y cree una base de datos de usuarios para las Autenticaciones de clientes](#)

Complete estos pasos para crear la base de datos de usuarios y para activar la autenticación EAP en Cisco ACS seguro:

1. Elija la **configuración de usuario** del GUI ACS, ingrese el username, y el tecleo **agrega/corrig**e. En este ejemplo el usuario es **ABC**.



2. Cuando aparece la página de la configuración de usuario, defina todos los parámetros específicos al usuario. En este ejemplo se configuran el username, la contraseña y la información sobre el usuario suplementaria porque usted necesita solamente estos parámetros para la autenticación EAP. Haga clic **comenzar** y relanzan el mismo proceso para agregar a más usuarios a la base de datos. Por abandono agrupan bajo grupo predeterminado y se asignan todos los usuarios la misma directiva según lo definido para el grupo. Refiera a la [sección de administración del grupo de usuarios de la guía de usuario para Cisco ACS seguro para el Servidor Windows 3.2](#) para más información si usted quiere asignar a los usuarios específicos a diversos grupos.

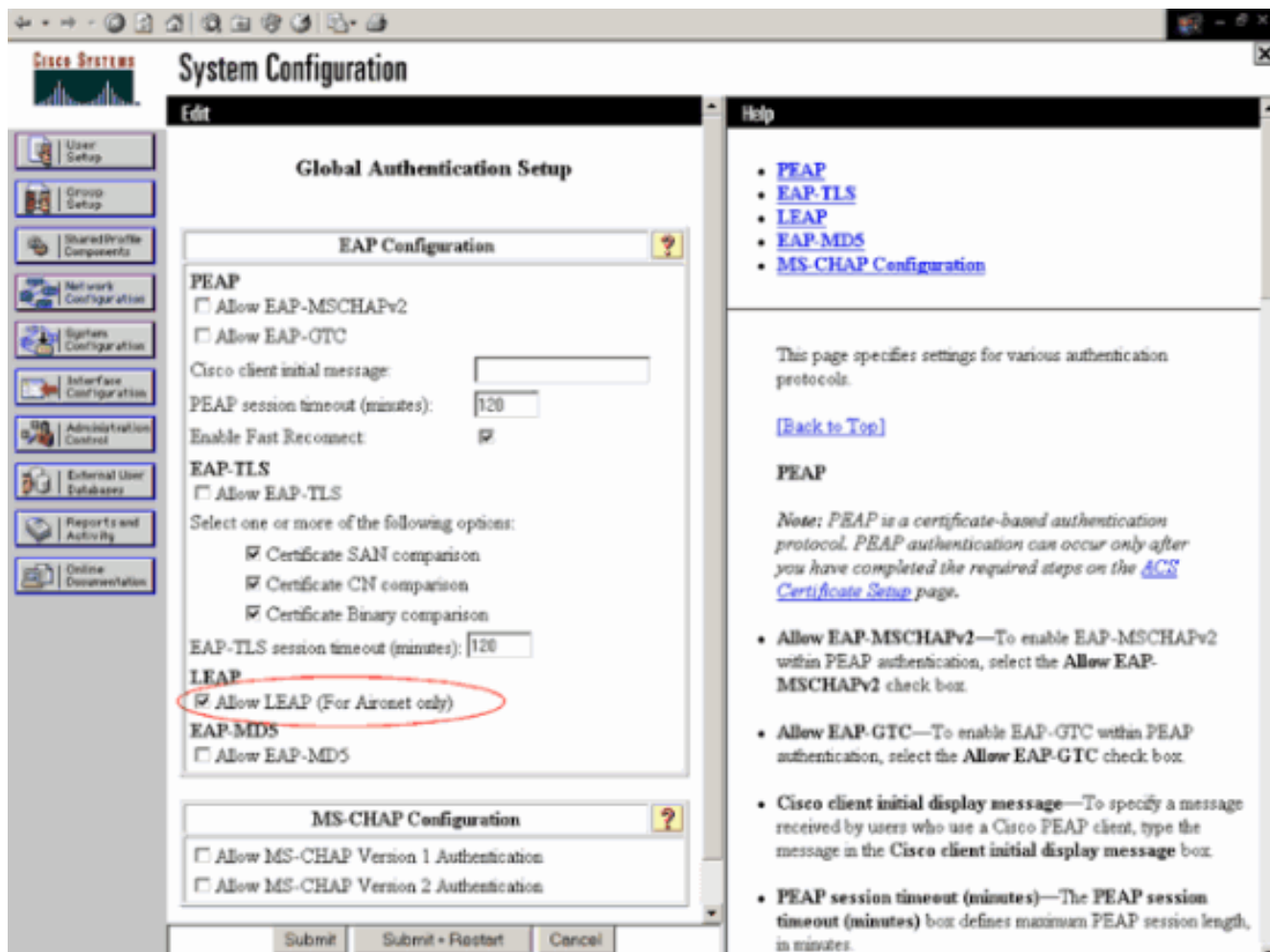


3. Defina el regulador como cliente AAA en el servidor ACS. Haga clic la **configuración de red del GUI ACS**. Cuando aparece la página de la configuración de red, defina el nombre del WLC, de la dirección IP, del secreto compartido y del método de autenticación (RADIUS Cisco Airespace). Refiera a la documentación del fabricante para otros servidores no--ACS de la autenticación. **Note:** La clave secreta compartida que usted configura en el WLC y el servidor ACS debe hacer juego. El secreto compartido es con diferenciación entre mayúsculas y minúsculas.

Add AAA Client

AAA Client Hostname	<input type="text" value="WLC-1"/>
AAA Client IP Address	<input type="text" value="10.77.244.204"/>
Shared Secret	<input type="text" value="cisco"/>
<hr/>	
RADIUS Key Wrap	
Key Encryption Key	<input type="text"/>
Message Authenticator Code Key	<input type="text"/>
Key Input Format	<input type="radio"/> ASCII <input checked="" type="radio"/> Hexadecimal
<hr/>	
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	
<input type="checkbox"/> Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	

4. La configuración del sistema del teclado y la autenticación global ponen para asegurarse de que el servidor de la autenticación está configurado para realizar el método de autenticación deseado EAP. Bajo configuraciones EAP, elija el método EAP apropiado. Este ejemplo utiliza la autenticación LEAP. El teclado **some** cuando le hacen.

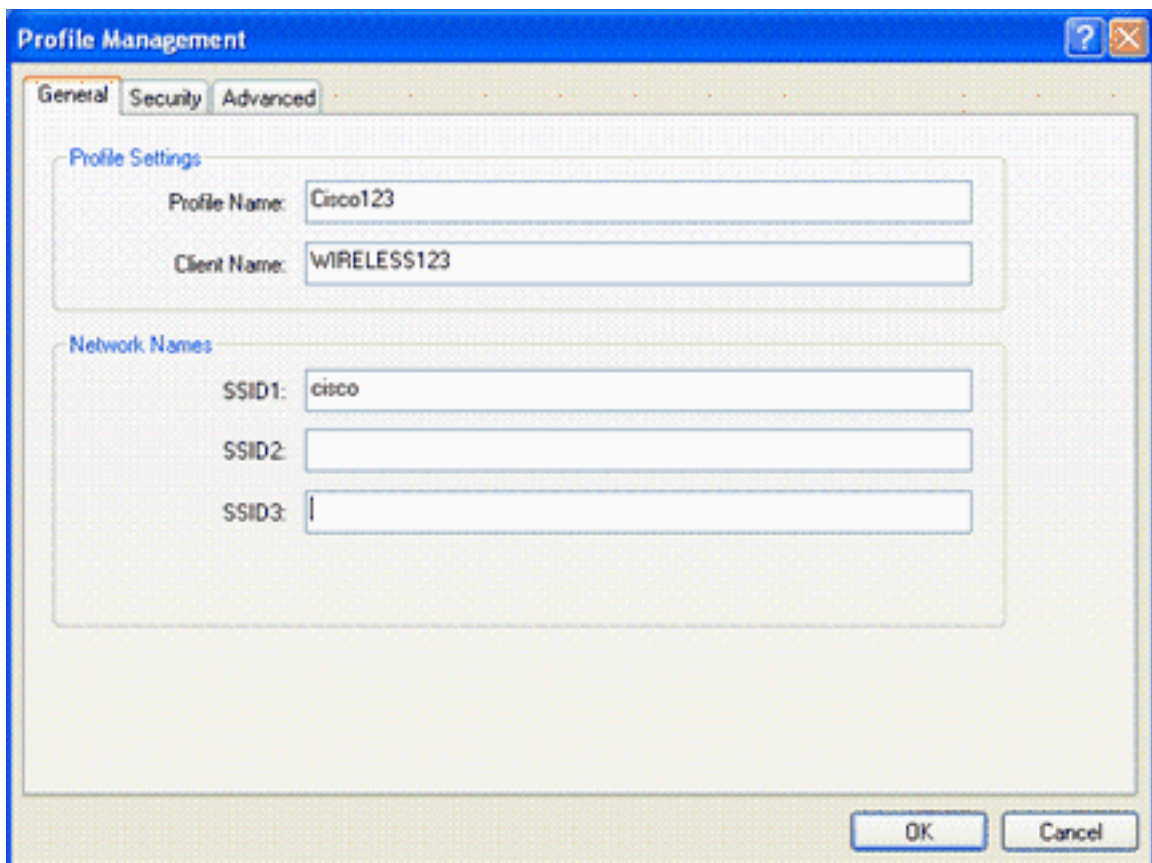


[Configure al cliente](#)

El cliente debe también ser configurado para el tipo apropiado EAP. El cliente propone el tipo EAP al servidor durante el proceso de negociación EAP. Si los soportes de servidor que el tipo EAP, él reconoce el tipo EAP. Si el tipo EAP no se utiliza, envía un reconocimiento negativo y el cliente negocia otra vez con un diverso método EAP. Este proceso continúa hasta que se negocie un tipo utilizado EAP. Este ejemplo utiliza el SALTO como el tipo EAP.

Complete estos pasos para configurar el SALTO en el cliente con utilidad Aironet Desktop.

1. Haga doble clic en el icono **utilitario de Aironet** para abrirlo.
2. Haga clic la **Administración** cuadro del perfil.
3. Haga clic en un perfil y elija **se modifican**.
4. Conforme a la ficha general, elija un *nombre del perfil*. Ingrese el **SSID** del

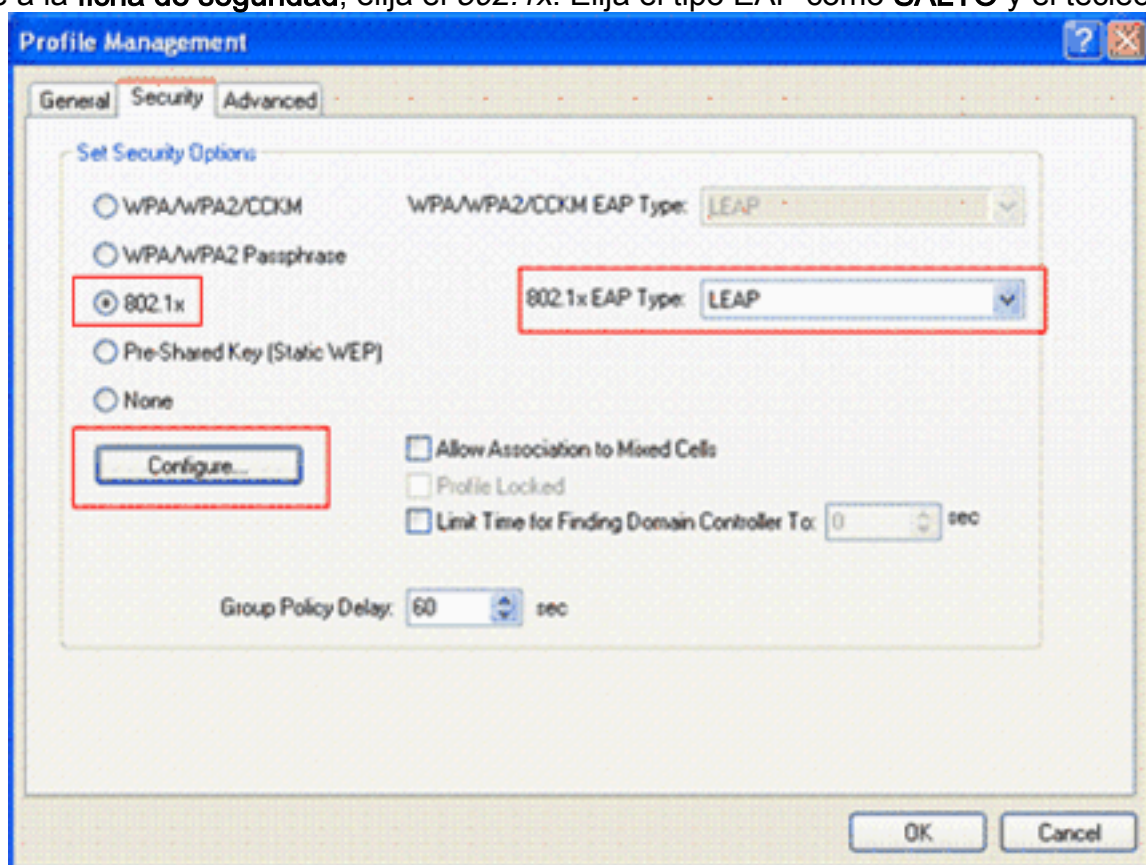


WLAN.

Not

e: El SSID es con diferenciación entre mayúsculas y minúsculas y necesita hacer juego exactamente con el SSID configurado en el WLC.

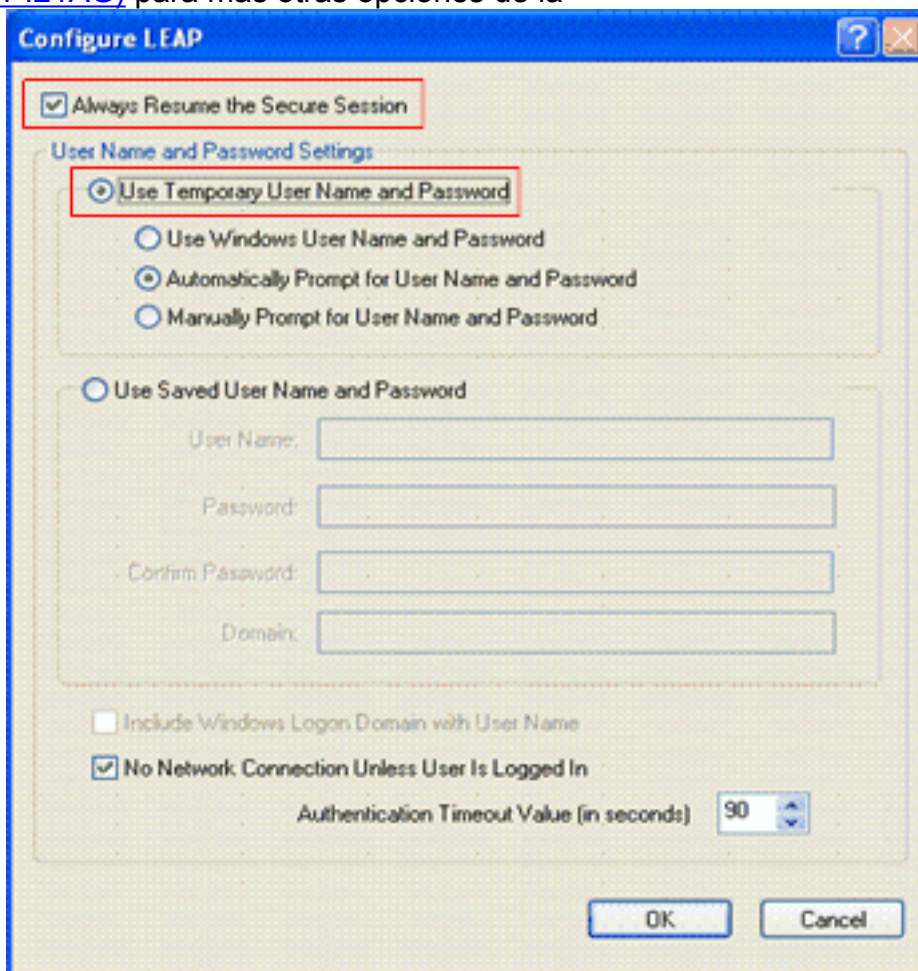
5. Conforme a la **ficha de seguridad**, elija el **802.1x**. Elija el tipo EAP como **SALTO** y el tecleo



configura.

6. Elija el **nombre de usuario y contraseña temporal del uso**, que le incita ingresar los credenciales del usuario cada vez las reinicializaciones del ordenador. Controle una de las tres opciones dadas aquí. Este ejemplo utiliza **automáticamente la guía para el nombre de usuario y contraseña**, que le requiere ingresar las credenciales del *usuario LEAP* además

del *nombre de usuario de Windows y de la contraseña* antes de que usted se abra una sesión a las ventanas. Controle **siempre el curriculum vitae** la casilla de verificación **segura de la sesión** en la cima de la ventana si usted quisiera que el suplicante del SALTO intentara siempre reanudar la sesión anterior sin la necesidad de incitarle entrar sus credenciales de nuevo siempre que el adaptador del cliente vague por y reasocie a la red. **Note:** Refiera a [configurar la sección del adaptador del cliente de la guía de instalación y configuración inalámbrica de los adaptadores del cliente LAN de Cisco Aironet 802.11a/b/g del documento \(CB21AG y PI21AG\)](#) para más otras opciones de la



información.

7. Bajo **ficha Avanzadas**, usted puede configurar la extensión del preámbulo, de Aironet y otras opciones del 802.11 tales como potencia, frecuencia y así sucesivamente.
8. **Autorización del teclado.** El cliente ahora intenta asociarse a los parámetros configurados.

Verifique

Use esta sección para confirmar que su configuración funciona correctamente.

Intente asociar a un cliente de red inalámbrica al AP ligero usando la autenticación LEAP para verificar si la configuración trabaja como se esperaba.

Note: Este documento asume que el perfil del cliente está configurado para la autenticación LEAP. Refiérase [con la autenticación EAP](#) para más información sobre cómo configurar el adaptador de red inalámbrica de cliente del 802.11 a/b/g para la autenticación LEAP.

El perfil para el cliente de red inalámbrica se activa una vez, el usuario se pide proporcionar al username/a la contraseña para la autenticación LEAP. Aquí está un ejemplo:

The image shows a Windows-style dialog box titled "Enter Wireless Network Password". The dialog has a blue title bar with a close button (X) in the top right corner. The main area has a light green background and contains the following text and fields:

- Text: "Please enter your LEAP username and password to log on to the wireless network"
- Label: "User Name :" followed by a text input field containing "ABC".
- Label: "Password :" followed by a password input field containing "xxxxxxx".
- Label: "Log on to :" followed by an empty text input field.
- Label: "Card Name :" followed by the text "Cisco Aironet 802.11 a/b/g Wireless Adapter".
- Label: "Profile Name :" followed by the text "EAP-Authentication".
- Buttons: "OK" and "Cancel" buttons at the bottom right.

El AP ligero y entonces el WLC pasa encendido los credenciales de usuario al servidor de RADIUS externo (Cisco ACS seguro) para validar las credenciales. El servidor de RADIUS compara los datos con la base de datos de usuarios y proporciona al acceso al cliente de red inalámbrica siempre que los credenciales de usuario sean válidos para verificar los credenciales de usuario. El informe pasajero de la autenticación sobre el servidor ACS muestra que el cliente ha pasado la autenticación de RADIUS. Aquí está un ejemplo:

Reports and Activity

Select

Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts
- Logged-in Users
- Disabled Accounts
- ACS Backup And Restore
- Administration Audit
- User Password Changer
- ACS Service Monitoring

Back to Help

Select

Refresh Download

Passed Authentications active.csv

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
04/04/2006	15:01:33	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30
04/04/2006	15:00:37	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30

Sobre la autenticación de RADIUS acertada el cliente de red inalámbrica se asocia al AP ligero.

LEAP Authentication Status

Card Name: Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name: EAP-Authentication

Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

Esto se puede también controlar bajo tabulación del **monitor del GUI WLC**. Elija el **monitor > a los clientes** y controle para saber si hay la dirección MAC del cliente.

Monitor Clients Items 1 to 1 of 1

Search by MAC address Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:96:ac:e6:57	ap:5b:fb:d0	00:0b:85:5b:fb:d0	Cisco123	802.11a	Associated	Yes	1	Detail Link Test Disable Banlist

Troubleshooting

Complete estos pasos para resolver problemas las configuraciones:

1. Utilice el **comando debug lwapp events enable** para controlar si el AP se registra con el WLC.
2. Controle si el servidor de RADIUS recibe y valida la petición de la autenticación del cliente de red inalámbrica. Controle el direccionamiento NAS-IP-, fecha y hora para verificar si el WLC podía alcanzar al servidor de RADIUS. Controle los informes pasajeros de las autenticaciones y de los intentos fallidos sobre el servidor ACS para lograr esto. Estos informes están disponibles bajo los informes y actividades en el servidor ACS. Aquí está un ejemplo cuando la autenticación de servidor de RADIUS falla:

Reports and Activity

Select Refresh Download

Failed Attempts active.csv

Date	Time	Message Type	User Name	Group Name	Caller ID	Authn Failure Code	Author Failure Code	Author Data	NAS Port	NAS-IP Address
04/04/2006	15:42:51	Authn failed	code		00-40-96-AC-E6-57	CS user unknown			1	172.16.1.30

Back to help

Note: Refiera a [obtener la información de la versión y de la depuración AAA para Cisco ACS seguro para Windows](#) para la información sobre cómo resolver problemas y obtener la información de la depuración sobre Cisco ACS seguro.

3. Usted puede también utilizar estos **comandos debug** para resolver problemas la autenticación AAA: **la depuración aaa todo activa** — Configura la depuración de todos los mensajes AAA. **permiso del paquete de la depuración dot1x** — Activa la depuración de todos los paquetes dot1x. Aquí está una salida de muestra del **comando enable aaa del 802.1x de la depuración:**

```
(Cisco Controller) >debug dot1x aaa enable
```

```
*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
0x1533a288.. !!!!
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8,
id=2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
....ABC
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
Response'
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1,
length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24 e8 9f
.....B:...
*Sep 23 15:15:43.799: 00000010: 41 42 43
ABC
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
00:40:96:ac:dd:05
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
index=1
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
index=2
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
```

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request =
0x1533a288.. !!!!
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2,
length=35, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed
...#.....[2.e..
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13
..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43
ABC
*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
Response'
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 **AAA Message 'Interim Response' received
for mobile 00:40:96:ac:dd:05**
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3,
length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00000000: 03 03 00 04
....
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
00:40:96:ac:dd:05
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
index=1
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
index=2
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae
.....)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] **AAA response 'Success'**
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] **Returning AAA response**
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 **AAA Message 'Success' received for
mobile 00:40:96:ac:dd:05**
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6 c3 4c
...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6 92 ce 60 a6
..i.....).V...`.

```
*Sep 23 15:15:43.918: 00000020: 41 42 43
ABC
```

```
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
vendorId 9, valueLen 16
```

```
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
vendorId 0, valueLen 21
```

```
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
vendorId 0, valueLen 16
```

Note: Algunas de las líneas en la salida de la depuración han sido envuelto debido a los apremios del espacio.

4. Vigile abre una sesión el WLC para controlar si el servidor de RADIUS recibe los credenciales de usuario. Haga clic el **monitor** para controlar los registros del GUI WLC. Del menú del lado izquierdo, haga clic las **estadísticas** y haga clic al **servidor de RADIUS de la** lista de opciones. Esto es muy importante porque en algunos casos, el servidor de RADIUS nunca recibe los credenciales de usuario si la configuración de servidor de RADIUS en el WLC es incorrecta. Éste es cómo los registros aparecen en el WLC si los parámetros de RADIUS se configuran incorrectamente:



Usted puede utilizar una combinación del **comando show wlan summary** para reconocer cuáles de sus redes inalámbricas (WLAN) emplean la autenticación de servidor de RADIUS. Entonces usted puede ver el **comando show client summary** para ver qué direcciones MAC (clientes) se autentican con éxito en las redes inalámbricas (WLAN) RADIUS. Usted puede también correlacionar esto con sus tentativas de Cisco o registros pasajeros ACS seguros de los intentos fallidos.

Extremidades de troubleshooting

- Verifique en el regulador que el servidor de RADIUS esté en el estado **activo**, y no en el recurso seguro **0** inhabilitado.
- Utilice el **comando ping** para controlar si el servidor de RADIUS es accesible del WLC.
- Controle si seleccionan al servidor de RADIUS del menú desplegable de la red inalámbrica (WLAN) (SSID).
- Si usted utiliza el WPA, después usted tiene que instalar el último hotfix de Microsoft WPA para Windows XP SP2. También, usted debe actualizar el driver para su suplicante del cliente al más último.
- Si usted hace el PEAP, por ejemplo los Certificados con XP, el SP2 donde los indicadores luminosos LED amarillo de la placa muestra gravedad menor son manejados por la utilidad de Microsoft wireless-0, usted necesita conseguir la corrección KB885453 de Microsoft. Si usted utiliza los Config cero de Windows/al suplicante del cliente, inhabilite el **permiso**

rápidamente vuelven a conectar. Usted puede hacer esto si usted elige las **propiedades > las redes inalámbricas de conexión de red inalámbrica > las redes preferidas**. Entonces elija **SSID > las propiedades > abierto > WEP > autenticación > tipo EAP > PEAP > las propiedades > permiso rápidamente vuelven a conectar**. Usted puede entonces encontrar la opción para activar o para inhabilitar en el extremo de la ventana.

- Si usted tiene indicadores luminosos LED amarillo de la placa muestra gravedad menor de Intel 2200 o 2915, refiera a las declaraciones sobre el sitio web de Intel sobre los problemas conocidos con sus indicadores luminosos LED amarillo de la placa muestra gravedad menor: [Conexión de red de Intel® PRO/Wireless 2200BG](#) [Conexión de red de Intel® PRO/Wireless 2915ABG](#) Descargue los drivers más actuales de Intel para evitar cualquier problema. Usted puede descargar los drivers de Intel en <http://downloadcenter.intel.com/>
- Si la característica **agresiva del failover** se habilita en el WLC, el WLC es demasiado agresivo marcar el servidor de AAA como no respondiendo. Pero, esto no debe ser hecha porque el servidor AAA no es posiblemente responsivo solamente a ese cliente particular, si usted hace el descarte silencioso. Puede ser una respuesta a otros clientes válidos con los certificados válidos. Pero, el WLC puede todavía marcar el servidor AAA como `no respondiendo y no funcional`. Para superar esto, inhabilite la función **aggressive failover**. Emita el comando **config radius aggressive-failover disable** controlador GUI para realizar esto. Si se inhabilita esto, después el regulador falla solamente encima al servidor siguiente AAA si hay tres clientes consecutivos que no pueden recibir una respuesta del servidor de RADIUS.

Temporizadores de manipulación EAP

Durante la autenticación del 802.1x, el usuario pudo ver el DOT1X-1-

MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: Las retransmisiones de la EAPOL-clave M1 max alcanzaron para el móvil xx: xx: xx: xx: mensaje de error xx.

Los mensajes de este error indican que el cliente no respondió a tiempo al regulador durante la negociación de la clave WPA (802.1x). El regulador fija un temporizador para una respuesta durante la negociación dominante. Típicamente, cuando usted ve este mensaje, es debido a un problema con el suplicante. Asegúrese de que usted funcione con las últimas versiones de los drivers y de los firmwares del cliente. En el WLC, hay algunos temporizadores EAP que usted puede manipular para ayudar con la autenticación de cliente. Estos temporizadores EAP incluyen:

```
(Cisco Controller) >debug dot1x aaa enable
```

```
*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
0x1533a288.. !!!!
```

*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8, id=2) for mobile 00:40:96:ac:dd:05

*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
.....ABC

*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] **Sending auth request to 'RADIUS' (proto 0x140001)**

*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response'

*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response

*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05

*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1, length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05

*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24 e8 9f
.....B:...

*Sep 23 15:15:43.799: 00000010: 41 42 43
ABC

*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7

*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!!

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=35, id=3) for mobile 00:40:96:ac:dd:05

*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed
...#.[2.e..

*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13
..O...5..k..WP..

*Sep 23 15:15:43.904: 00000020: 41 42 43
ABC

*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (proto 0x140001)

*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response'

*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response

*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 **AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05**

*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3, length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05

*Sep 23 15:15:43.907: 00000000: 03 03 00 04
....

*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05

*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0

*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1

*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2

*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3

```

*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae
.....)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for
mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6 c3 4c
...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6 92 ce 60 a6
..i.....).V...`
*Sep 23 15:15:43.918: 00000020: 41 42 43
ABC
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
vendorId 0, valueLen 21
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
vendorId 0, valueLen 16

```

Antes de que usted pueda manipular estos valores, usted necesita entender lo que hacen, y cómo el cambio de ellos afectará la red:

- **Descanso de la EAP-Identidad-petición:** Influencias de este temporizador cuánto tiempo usted espera entre las peticiones de la identidad EAP. Por abandono, éste es segundo (4.1 y más bajo) y 30 segundos (4.2 y mayor). La razón de este cambio era porque algunos clientes, helds de la mano, teléfonos, escáneres etc, tenían una dificultad que respondía rápidamente bastante. Los dispositivos como las computadoras portátiles, no requieren generalmente una manipulación de estos valores. El valor disponible es a partir la 1 a 120. ¿Así pues, qué sucede cuando este atributo se fija a un valor de 30? Cuando el cliente primero conecta, envía un comienzo EAPOL a la red, y el WLC envía abajo de un paquete EAP, pidiendo la identidad del usuario o de la máquina. Si el WLC no recibe la respuesta de la identidad, envía otra petición de la identidad 30 segundos después del primeros. Esto sucede en la conexión inicial, y cuando el cliente vaga por. ¿Qué sucede cuando aumentamos este temporizador? Si todo es bueno, no hay impacto. Sin embargo, si hay un problema en la red (problemas incluyendo del cliente, los problemas AP, o los problemas RF), puede causar los retrasos en

la conectividad de red. Por ejemplo, si usted fija el temporizador al valor máximo de 120 segundos, el WLC espera 2 minutos entre las peticiones de la identidad. Si el cliente está vagando por, y la respuesta no es recibida por el WLC, después hemos creado, al mínimo, una caída del sistema del dos-minuto para este cliente. Las recomendaciones para este temporizador son 5. En este tiempo, no hay razón para colocar este temporizador en su valor máximo.

- **Reintento máximo de la EAP-Identidad-petición:** El valor de Reintento máximo es la cantidad de veces que el WLC enviará la petición de la identidad al cliente, antes de quitar su entrada del MSCB. Una vez que se alcanzan los Reintento máximo, el WLC envía un marco de la deautenticación al cliente, forzándolos para recomenzar el proceso EAP. El valor disponible es 1 a 20. Después, miraremos esto más detalladamente. Los Reintento máximo trabajan con el descanso de la identidad. Si usted hace su descanso de la identidad fijar a 120, y sus Reintento máximo a 20 cuánto tiempo hace él toman 2400 (o $120 * 20$). Esto significa que tardaría 40 minutos para que el cliente sea quitado, y que comenzaría el proceso EAP encima otra vez. Si usted fija el descanso de la identidad a 5, con un valor de Reintento máximo de 12, después él tomará 60 (o $5 * 12$). En contraste con el ejemplo anterior, hay un minuto hasta que quiten y tenga que comenzar al cliente EAP encima. Las recomendaciones para los Reintento máximo son 12.
- **Descanso de la EAPOL-clave:** Por el valor de agotamiento del tiempo de la EAPOL-clave, el valor por defecto es 1 segundo o 1000 milisegundos. Esto significa que cuando las claves EAPOL se intercambian entre el AP y el cliente, el AP enviará la clave y la espera hasta 1 segundo por abandono para que el cliente responda. Después de esperar el valor de tiempo definido, el AP retransmitirá la clave otra vez. Usted puede utilizar el comando **avanzado los config del eapol-clave-descanso del eap <time>** para alterar esta configuración. Los valores disponibles en 6.0 son entre 200 y 5000 milisegundos, mientras que los códigos antes de 6.0 permiten los valores entre 1 y 5 segundos. Tenga presente que si usted tiene un cliente que no esté respondiendo a una tentativa dominante, extendiendo los temporizadores hacia fuera puede darles un poco más hora de responder. Sin embargo, esto podría también prolongar el tiempo que toma para el WLC/AP al deauthenticate al cliente para que el proceso entero del 802.1x comience de nuevo.
- **Reintento máximo de la EAPOL-clave:** Para el valor de Reintento máximo de la EAPOL-clave, el valor por defecto es 2. Esto significa que revisaremos la tentativa dominante original al cliente dos veces. Esta configuración se puede alterar usando el comando **avanzado los config del eapol-clave-Retries del eap <retries>**. Los valores disponibles están entre 0 y 4 recomprobaciones. Usando el valor predeterminado para el descanso de la EAPOL-clave (es decir, 1 segundo) y el valor predeterminado para la recomprobación de la EAPOL-clave (2) el proceso iría como sigue si un cliente no responde a la tentativa dominante inicial: El AP envía una tentativa dominante al cliente. Espera al segundo una contestación. Si no hay contestación, después se envía la primera recomprobación de la EAPOL-clave. Espera al segundo una contestación. Si no hay contestación, después se envía la segunda recomprobación de la EAPOL-clave. Si todavía no hay respuesta del cliente y se resuelve el valor de reintentos, después el cliente deauthenticated. Una vez más como con el descanso de la EAPOL-clave, ampliar el valor de reintentos de la EAPOL-clave podía, en algunas circunstancias, ser beneficioso. Sin embargo, la determinación de él al máximo puede otra vez ser dañina pues el mensaje del deauthenticate sería prolongado.

[Extracción del archivo de paquete del servidor de RADIUS ACS para resolver](#)

problemas

Si usted utiliza ACS como el servidor de RADIUS externo, esta sección se puede utilizar para resolver problemas su configuración. El package.cab es archivo zip que contiene todos los ficheros necesarios necesarios para resolver problemas ACS eficientemente. Usted puede utilizar la utilidad CSSupport.exe para crear el package.cab, o usted puede recoger los ficheros manualmente.

Refiera a [crear una sección del archivo package.cab de información de ObtainingVersion y de la depuración AAA para Cisco ACS seguro para Windows](#) para más información sobre cómo crear y extraer el archivo de paquete del WCS.

Información Relacionada

- [Conmutación por falla del regulador de la red inalámbrica \(WLAN\) por el ejemplo de la configuración de los Puntos de acceso ligeros](#)
- [Actualización del Software del Controlador de la LAN Inalámbrica \(WLC\)](#)
- [Referencia inalámbrica del comando controller LAN de Cisco](#)
- [Soporte técnico y documentación - Cisco Systems](#)