

Configuración de la autenticación EAP con controladores WLAN (WLC)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configure el WLC para el Funcionamiento Básico y Registre los AP Ligeros al Controlador](#)

[Configuración del WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo](#)

[Configurar parámetros WLAN](#)

[Configure Cisco Secure ACS como servidor RADIUS externo y cree una base de datos de usuario para clientes de autenticación](#)

[Configuración del cliente](#)

[Verificación](#)

[Troubleshoot](#)

[Consejos de Troubleshooting](#)

[Manipulación de Temporizadores EAP](#)

[Extracción del archivo de paquete del servidor RADIUS ACS para la resolución de 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 configuración utiliza Cisco Secure Access Control Server (ACS) como servidor RADIUS externo para validar las credenciales del usuario.

[Prerequisites](#)

[Requirements](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de puntos de acceso ligeros (AP) y WLC de Cisco.
- Conocimiento básico del protocolo ligero AP (LWAPP).
- Conocimiento de cómo configurar un servidor RADIUS externo como Cisco Secure ACS.

Componentes Utilizados

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

- Punto de acceso ligero (LAP) Cisco Aironet de la serie 1232AG
- WLC de la serie 4400 de Cisco que ejecuta firmware 5.1
- Cisco Secure ACS que ejecuta la versión 4.1
- Adaptador de cliente Cisco Aironet 802.11 a/b/g
- Cisco Aironet Desktop Utility (ADU) que ejecuta firmware 4.2

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 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.

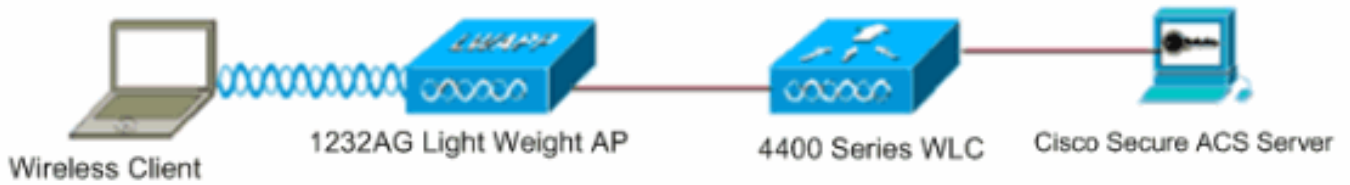
Nota: Use la [Command Lookup Tool](#) (sólo para clientes registrados) para encontrar más información sobre los comandos usados en este documento.

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

1. [Configure el WLC para el funcionamiento básico y registre los AP ligeros al controlador.](#)
2. [Configure el WLC para la autenticación RADIUS a través de un servidor RADIUS externo.](#)
3. [Configure los parámetros WLAN.](#)
4. [Configure Cisco Secure ACS como el servidor RADIUS externo y cree una base de datos de usuarios para autenticar clientes.](#)

Diagrama de la red

En esta configuración, un Cisco 4400 WLC y un Lightweight AP están conectados a través de un hub. Un servidor RADIUS externo (Cisco Secure ACS) también está conectado al mismo hub. Todos los dispositivos están en la misma subred. El AP se registra inicialmente al controlador. Debe configurar el WLC y el AP para la autenticación del protocolo de autenticación extensible ligero (LEAP). Los clientes que se conectan al AP utilizan la autenticación LEAP para asociarse con el AP. Cisco Secure ACS se utiliza para realizar la autenticación RADIUS.



[Configure el WLC para el Funcionamiento Básico y Registre los AP Ligeros al Controlador](#)

Utilice el asistente de configuración de inicio en la interfaz de línea de comandos (CLI) para configurar el WLC para el funcionamiento básico. Alternativamente, también puede utilizar la GUI para configurar el WLC. Este documento explica la configuración en el WLC con el asistente de configuración de inicio en la CLI.

Después de que el WLC se inicie por primera vez, ingresa directamente al asistente de configuración de inicio. Utilice el asistente de configuración para configurar los parámetros básicos. Puede ejecutar el asistente en la CLI o en la GUI. Este resultado muestra un ejemplo del asistente de configuración de inicio en la 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 configuran el WLC para el funcionamiento básico. En este ejemplo de 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 de la interfaz del administrador de AP.

Antes de que se puedan configurar otras funciones en los WLC, los AP ligeros deben registrarse con el WLC. Este documento asume que el Lightweight AP está registrado en el WLC. Refiérase al [Registro del Lightweight AP \(LAP\) a un Wireless LAN Controller \(WLC\)](#) para obtener más

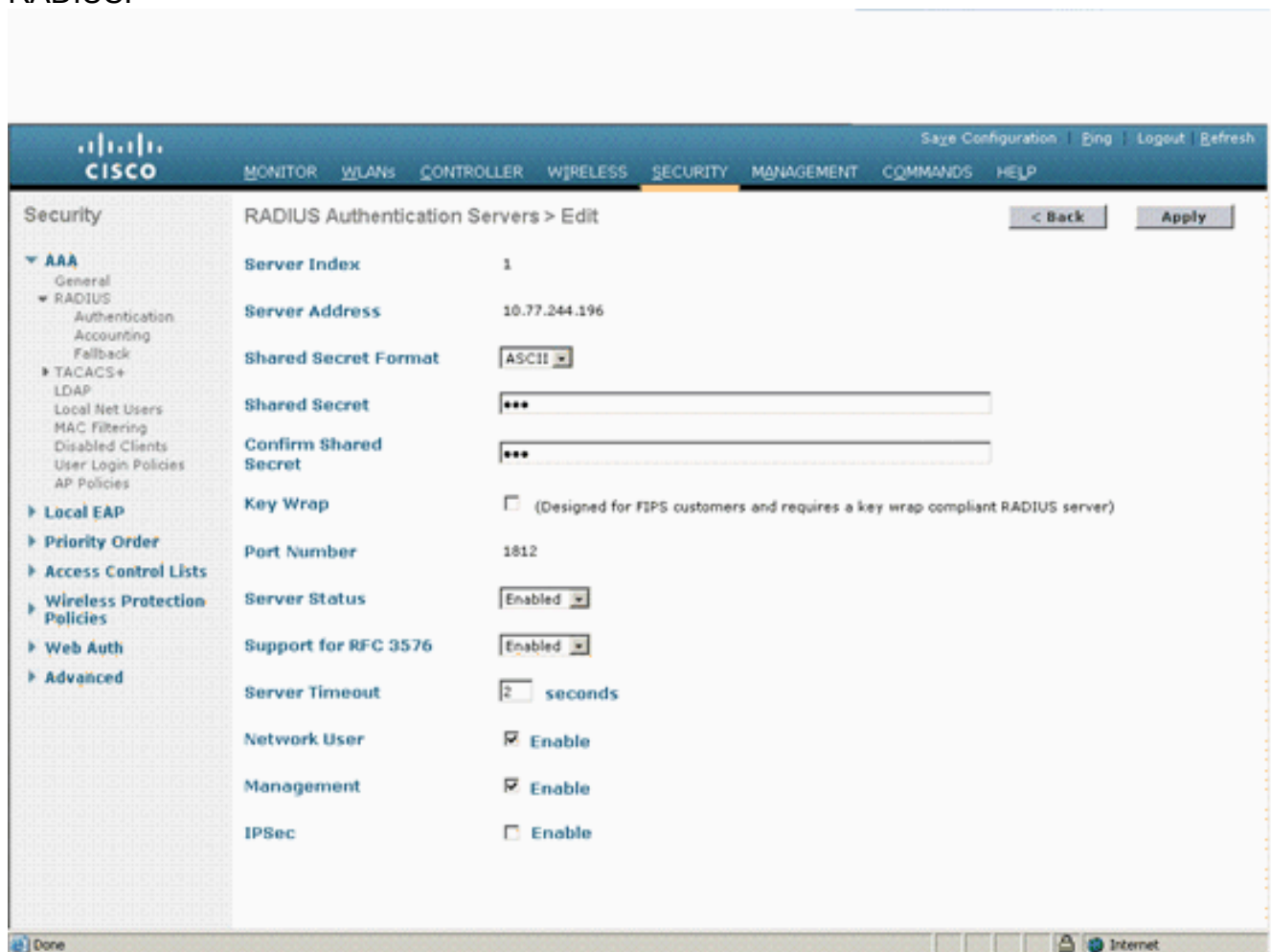
información sobre cómo se registran los Lightweight AP con el WLC.

Configuración del WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo

El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo. A continuación, el servidor RADIUS externo valida las credenciales del usuario y proporciona acceso a los clientes inalámbricos.

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

1. Elija **Seguridad y Autenticación RADIUS** en la GUI del controlador para mostrar la página Servidores de Autenticación RADIUS. A continuación, haga clic en **Nuevo** para definir un servidor RADIUS.



The screenshot shows the Cisco WLC GUI with the 'SECURITY' tab selected. The left sidebar shows the navigation tree with 'AAA' > 'RADIUS' expanded. The main content area is titled 'RADIUS Authentication Servers > Edit' and shows configuration for a single server (Server Index 1). The configuration fields are as follows:

Parameter	Value
Server Index	1
Server Address	10.77.244.196
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

2. Defina los parámetros del servidor RADIUS en la página Servidores de autenticación RADIUS > Nueva. Estos parámetros incluyen la dirección IP del servidor RADIUS, el secreto compartido, el número de puerto y el estado del servidor. Las casillas de verificación Network User and Management determinan si la autenticación basada en RADIUS se aplica a la administración del WLC y a los usuarios de red. Este ejemplo utiliza Cisco Secure ACS como el servidor RADIUS con la dirección IP 10.77.244.196.
3. El WLC ahora puede utilizar el servidor Radius para la autenticación. Puede encontrar el Servidor Radius en la lista si elige **Seguridad > Radius > Autenticación**.

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.77.244.196	1812	Disabled	Enabled

RFC 3576 es compatible con el servidor RADIUS Cisco CNS Access Registrar (CAR), pero no con Cisco Secure ACS Server versión 4.0 y anteriores. También puede utilizar la función de servidor RADIUS local para autenticar a los usuarios. El servidor RADIUS local se introdujo con el código de la versión 4.1.171.0. Los WLC que ejecutan versiones anteriores no tienen la función de radio local. EAP local es un método de autenticación que permite autenticar a usuarios y clientes inalámbricos de forma local. Se ha diseñado para su uso en oficinas remotas que desean mantener la conectividad con clientes inalámbricos cuando el sistema backend se interrumpe o el servidor de autenticación externo se desactiva. EAP local recupera las credenciales de usuario de la base de datos de usuario local o de la base de datos de backend LDAP para autenticar a los usuarios. EAP local admite LEAP, EAP-FAST con PAC, EAP-FAST con certificados y autenticación EAP-TLS entre el controlador y los clientes inalámbricos. EAP local está diseñado como un sistema de autenticación de respaldo. Si hay servidores RADIUS configurados en el controlador, el controlador intenta autenticar primero a los clientes inalámbricos con los servidores RADIUS. El EAP local se intenta solamente si no se encuentran servidores RADIUS, ya sea porque los servidores RADIUS agotaron el tiempo de espera o porque no se configuraron servidores RADIUS. Refiérase a [Ejemplo de Autenticación EAP Local en el Controlador de LAN Inalámbrico con EAP-FAST y Configuración de Servidor LDAP](#) para obtener más información sobre cómo configurar EAP local en los controladores de LAN Inalámbrica.

[Configurar parámetros WLAN](#)

A continuación, configure la WLAN que utilizan los clientes para conectarse a la red inalámbrica. Cuando configuró los parámetros básicos para el WLC, también configuró el SSID para la WLAN. Puede utilizar este SSID para la WLAN o crear un nuevo SSID. En este ejemplo, se crea un nuevo SSID.

Nota: Puede configurar hasta dieciséis WLAN en el controlador. La solución WLAN de Cisco puede controlar hasta dieciséis WLAN para AP ligeros. A cada WLAN se le pueden asignar políticas de seguridad únicas. Los AP ligeros emiten todos los SSID de WLAN de la solución WLAN de Cisco activos y aplican las políticas que define para cada WLAN.

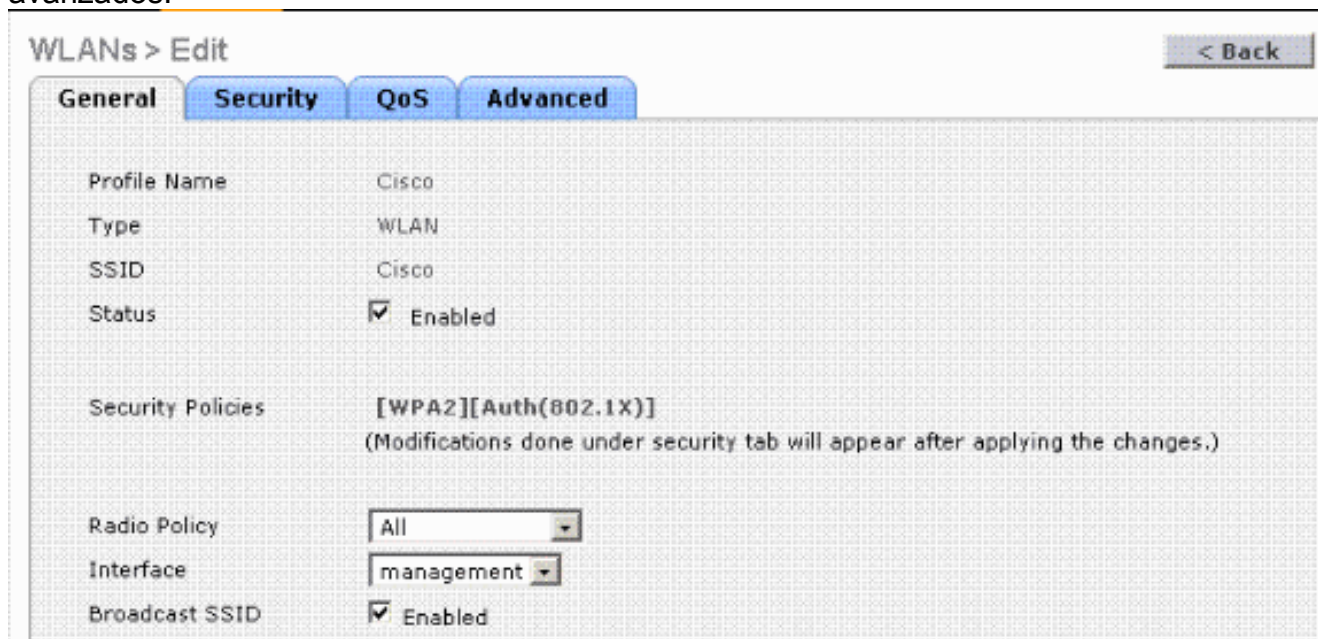
Complete estos pasos para configurar una nueva WLAN y sus parámetros relacionados:

1. Haga clic en **WLANs** desde la GUI del controlador para mostrar la página de WLANs. Esta página enumera las WLANs que existen en el controlador.
2. Elija **New** para crear una nueva WLAN. Ingrese el nombre del perfil y el SSID de WLAN para la WLAN y haga clic en **Aplicar**. Este ejemplo utiliza Cisco como

SSID.

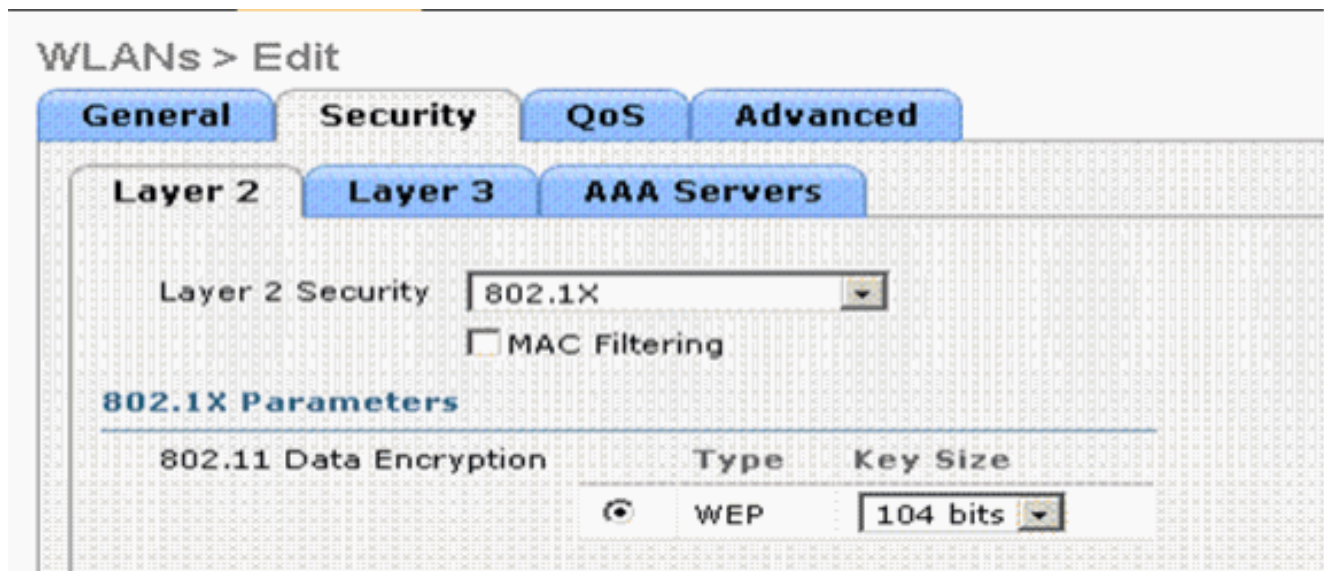


- Una vez que se crea una nueva WLAN, aparece la página WLAN > Edit para la nueva WLAN. En esta página puede definir varios parámetros específicos de esta WLAN que incluyen políticas generales, políticas de seguridad, políticas de QoS y otros parámetros avanzados.

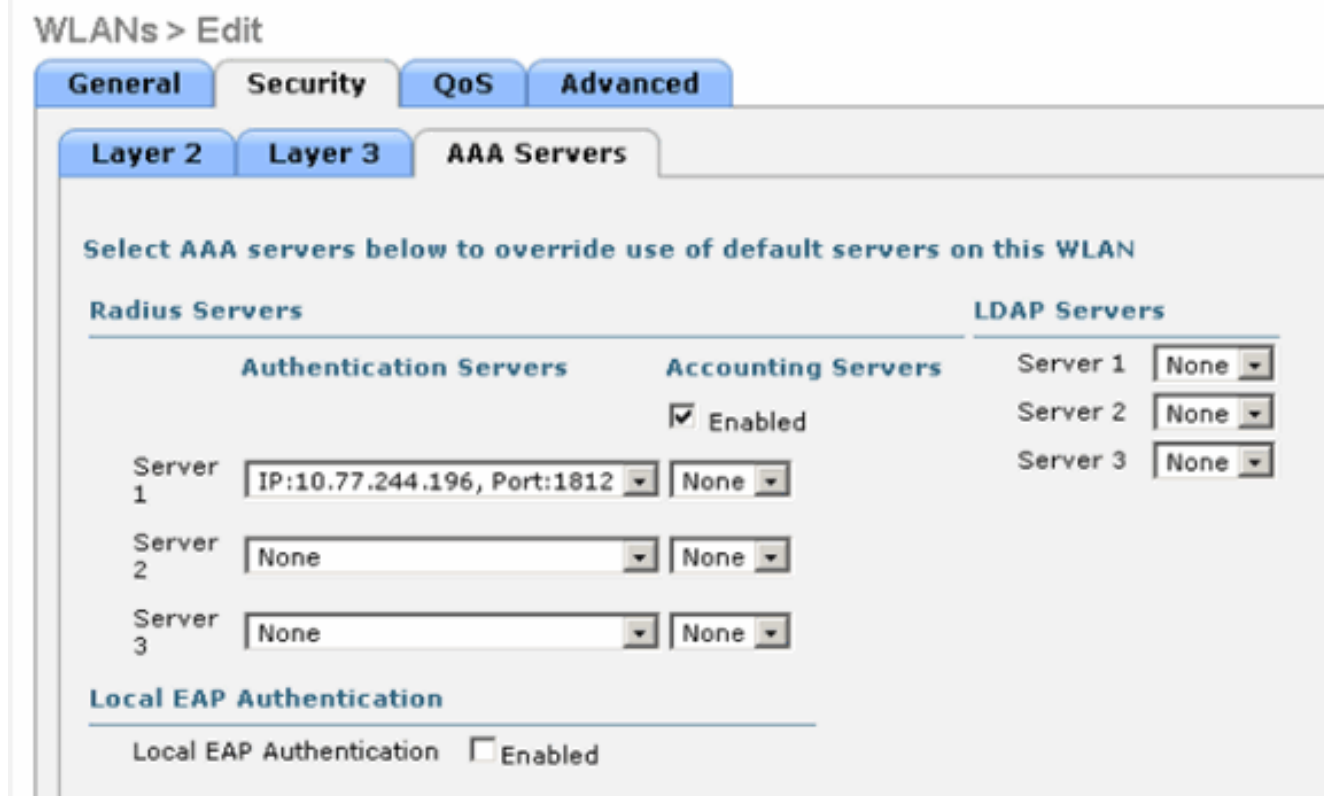


Elija la interfaz adecuada en el menú desplegable. Los otros parámetros se pueden modificar en función de los requisitos de la red WLAN. Marque la casilla **Status** en General Policies para habilitar la WLAN.

- Haga clic en la pestaña **Seguridad** y elija **Seguridad de Capa 2**. En el menú desplegable Layer 2 Security, elija **802.1x**. En los parámetros 802.1x, elija el tamaño de la clave WEP. Este ejemplo utiliza la clave WEP de 128 bits, que es la clave WEP de 104 bits más el vector de inicialización de 24 bits.



5. Elija la pestaña **Servidores AAA**. En el menú desplegable Authentication Servers (RADIUS) (Servidores de autenticación), elija el servidor RADIUS adecuado. Este servidor se utiliza para autenticar los clientes inalámbricos.

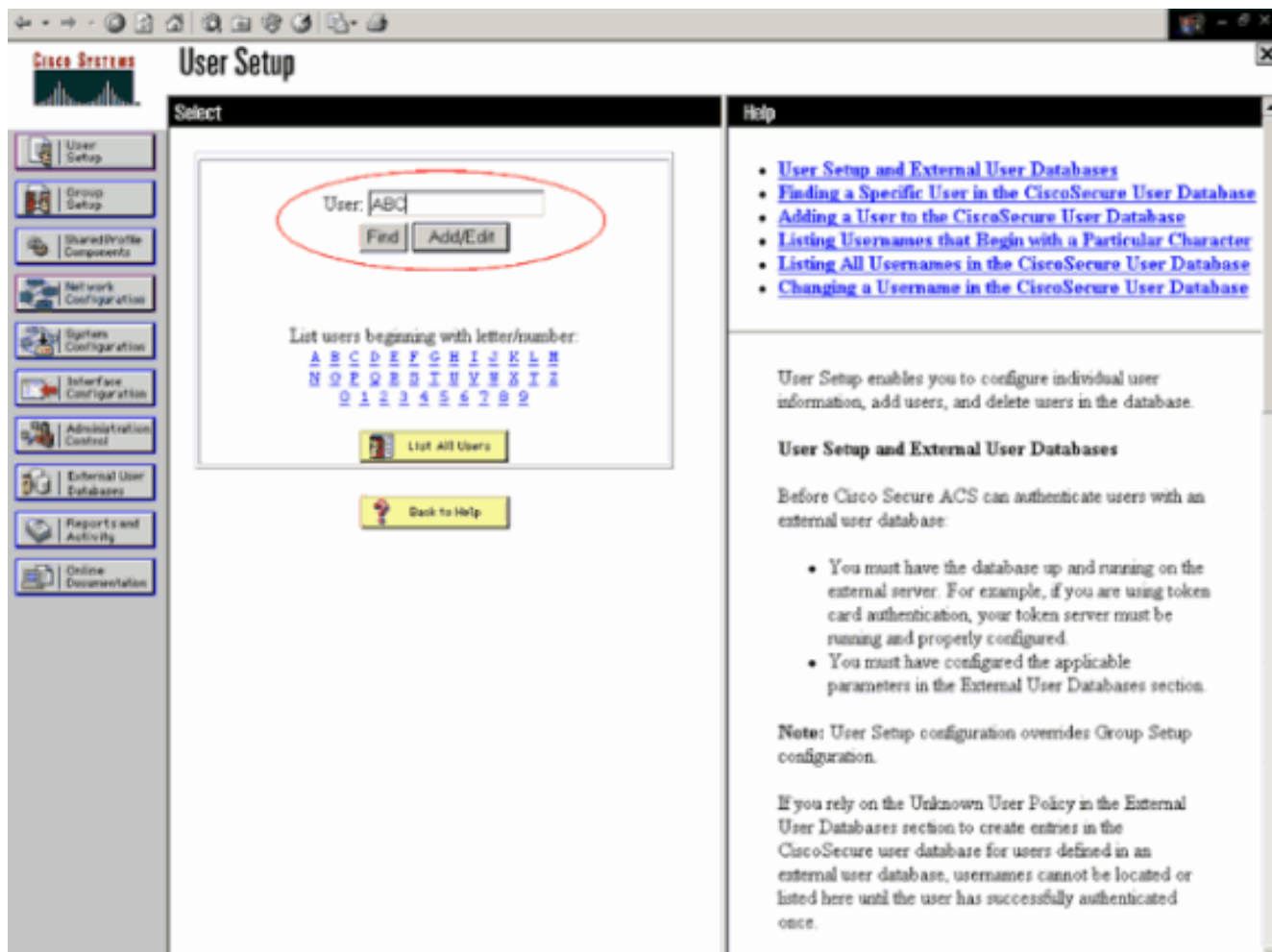


6. Haga clic en **Aplicar** para guardar la configuración.

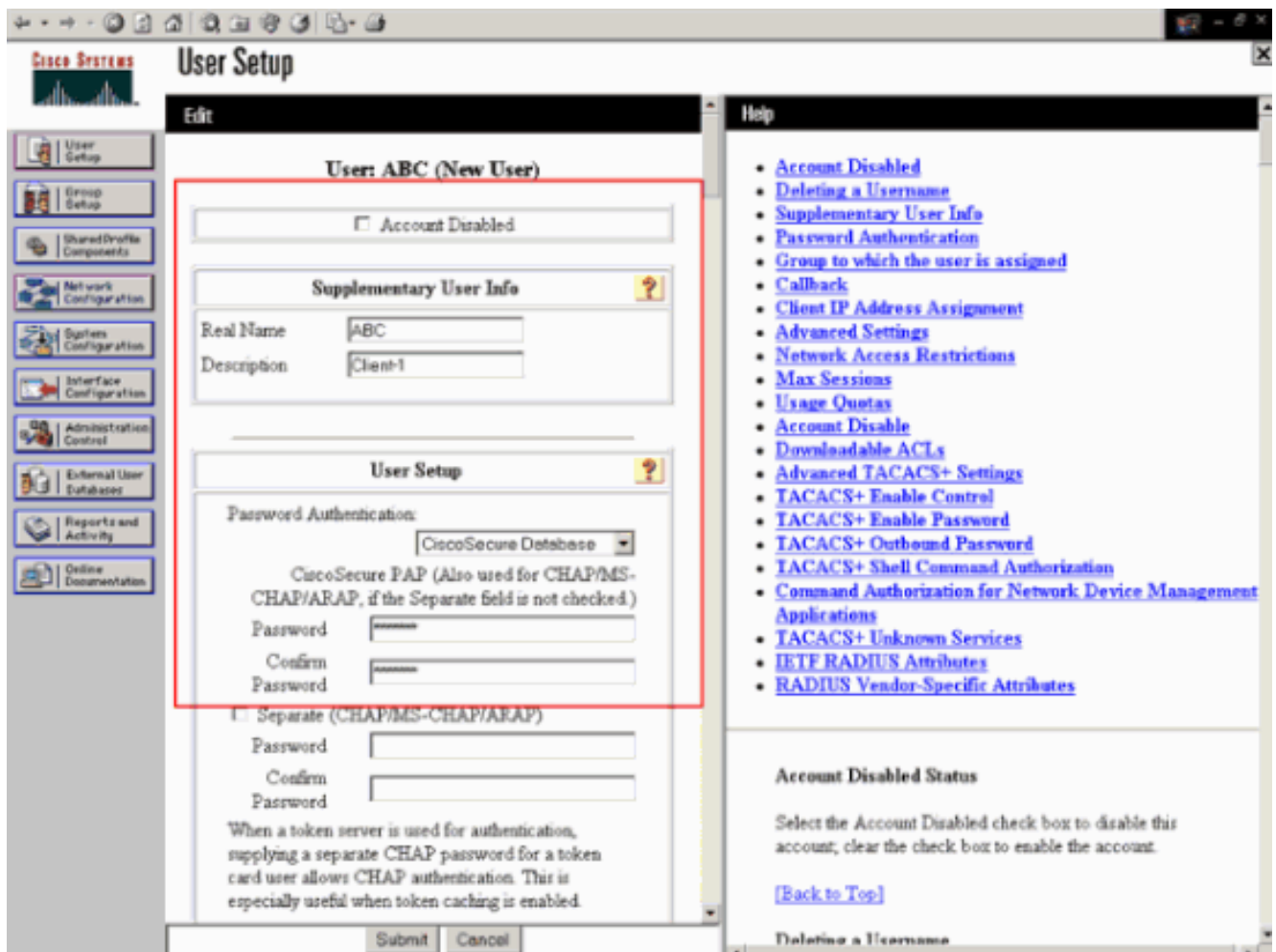
[Configure Cisco Secure ACS como servidor RADIUS externo y cree una base de datos de usuario para clientes de autenticación](#)

Complete estos pasos para crear la base de datos del usuario y habilitar la autenticación EAP en Cisco Secure ACS:

1. Elija **User Setup** en la GUI de ACS, ingrese el nombre de usuario y haga clic en **Add/Edit**. En este ejemplo, el usuario es **ABC**.



2. Cuando aparezca la página User Setup (Configuración de usuario), defina todos los parámetros específicos del usuario. En este ejemplo se configuran el nombre de usuario, la contraseña y la información de usuario adicional porque sólo necesita estos parámetros para la autenticación EAP. Haga clic en **Enviar** y repita el mismo proceso para agregar más usuarios a la base de datos. De forma predeterminada, todos los usuarios se agrupan en el grupo predeterminado y se les asigna la misma política que se define para el grupo. Refiérase a la sección [Administración de Grupos de Usuarios de la Guía del Usuario para Cisco Secure ACS para Windows Server 3.2](#) para obtener más información si desea asignar usuarios específicos a diferentes grupos.

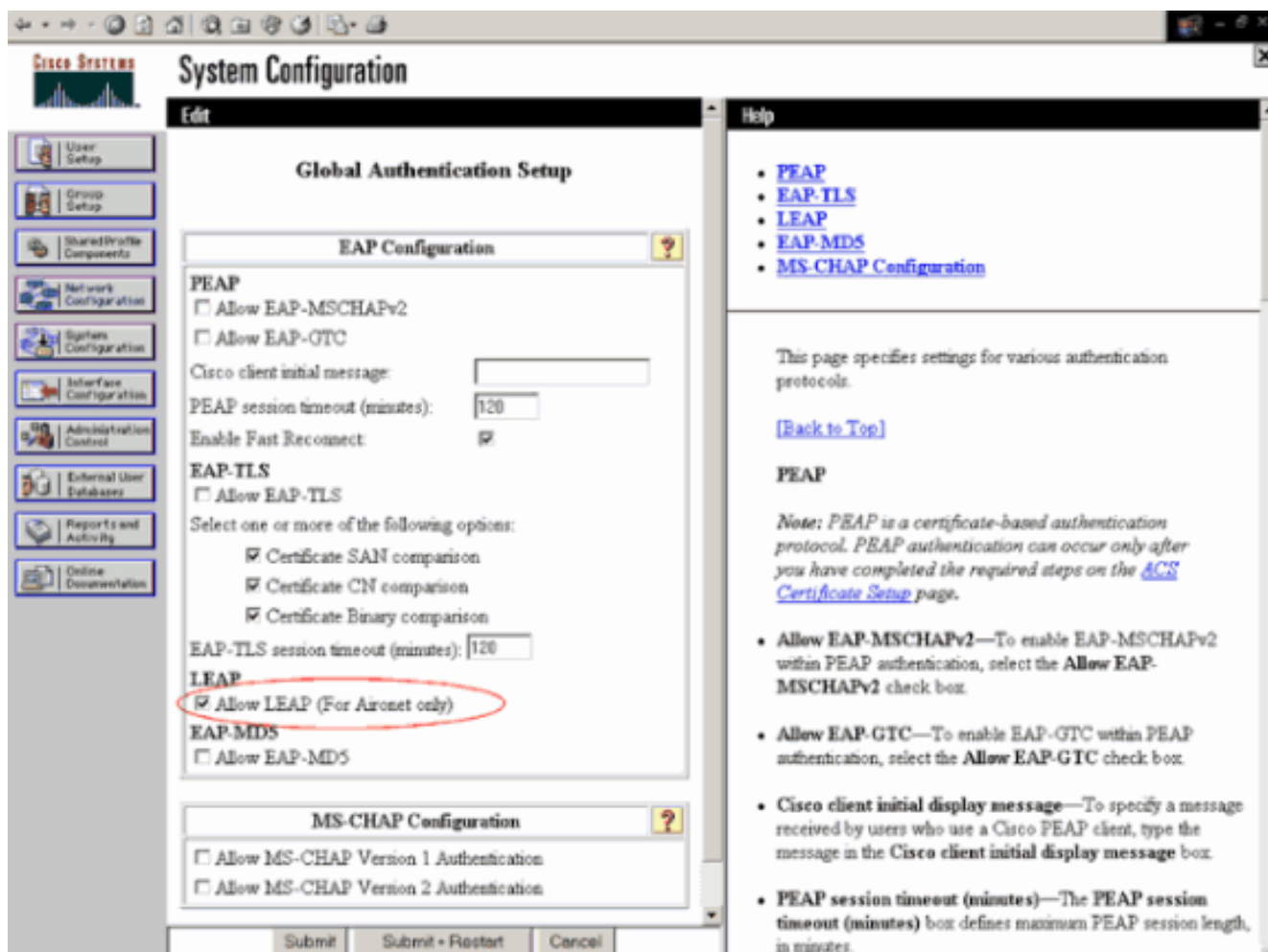


3. Defina el controlador como un cliente AAA en el servidor ACS. Haga clic en **Configuración de red** en la GUI de ACS. Cuando aparezca la página Network Configuration (Configuración de red), defina el nombre del WLC, la dirección IP, el secreto compartido y el método de autenticación (RADIUS Cisco Airespace). Consulte la documentación del fabricante para otros servidores de autenticación no ACS. **Nota:** La clave secreta compartida que configura en el WLC y el servidor ACS debe coincidir. El secreto compartido distingue 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. Haga clic en **Configuración del sistema** y **Configuración de autenticación global** para asegurarse de que el servidor de autenticación esté configurado para realizar el método de autenticación EAP deseado. En la configuración EAP, elija el método EAP adecuado. Este ejemplo utiliza autenticación LEAP. Haga clic en **Enviar** cuando haya terminado.

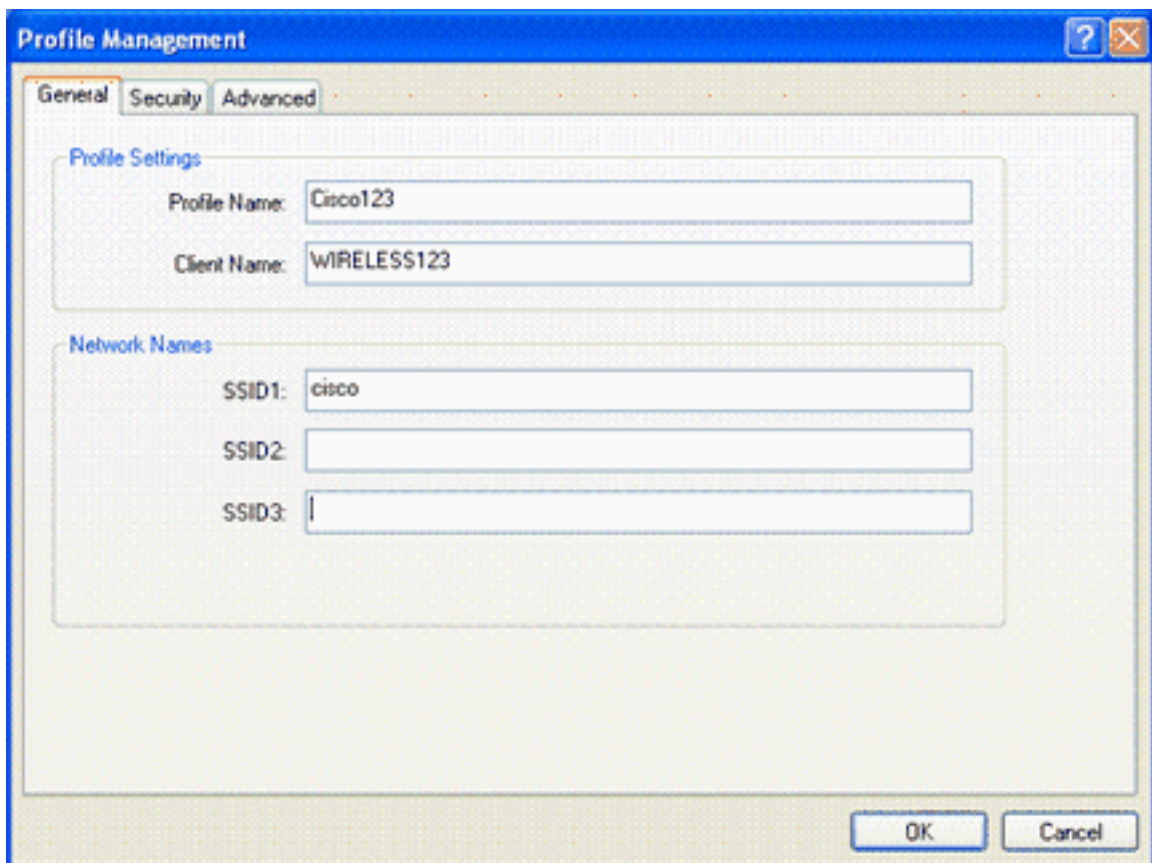


Configuración del cliente

El cliente también se debe configurar para el tipo EAP apropiado. El cliente propone el tipo EAP al servidor durante el proceso de negociación EAP. Si el servidor soporta ese tipo EAP, reconoce el tipo EAP. Si no se admite el tipo EAP, envía un reconocimiento negativo y el cliente vuelve a negociar con un método EAP diferente. Este proceso continúa hasta que se negocie un tipo EAP admitido. Este ejemplo utiliza LEAP como tipo EAP.

Complete estos pasos para configurar LEAP en el cliente con Aironet Desktop Utility .

1. Haga doble clic en el icono **Aironet Utility** para abrirlo.
2. Haga clic en la pestaña **Administración de perfiles**.
3. Haga clic en un perfil y elija **Modificar**.
4. En la ficha General, elija un *nombre de perfil*. Ingrese el **SSID** de la

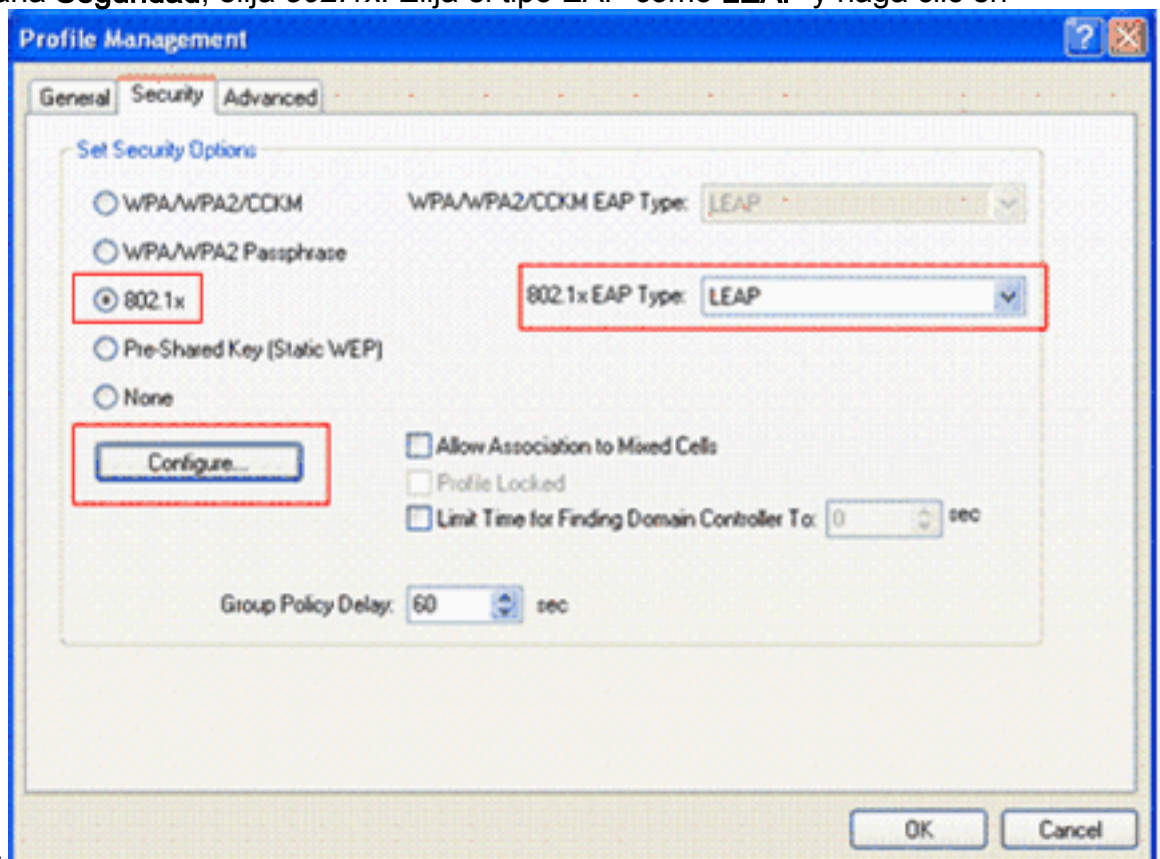


WLAN.

Not

a: SSID distingue entre mayúsculas y minúsculas y necesita coincidir exactamente con el SSID configurado en el WLC.

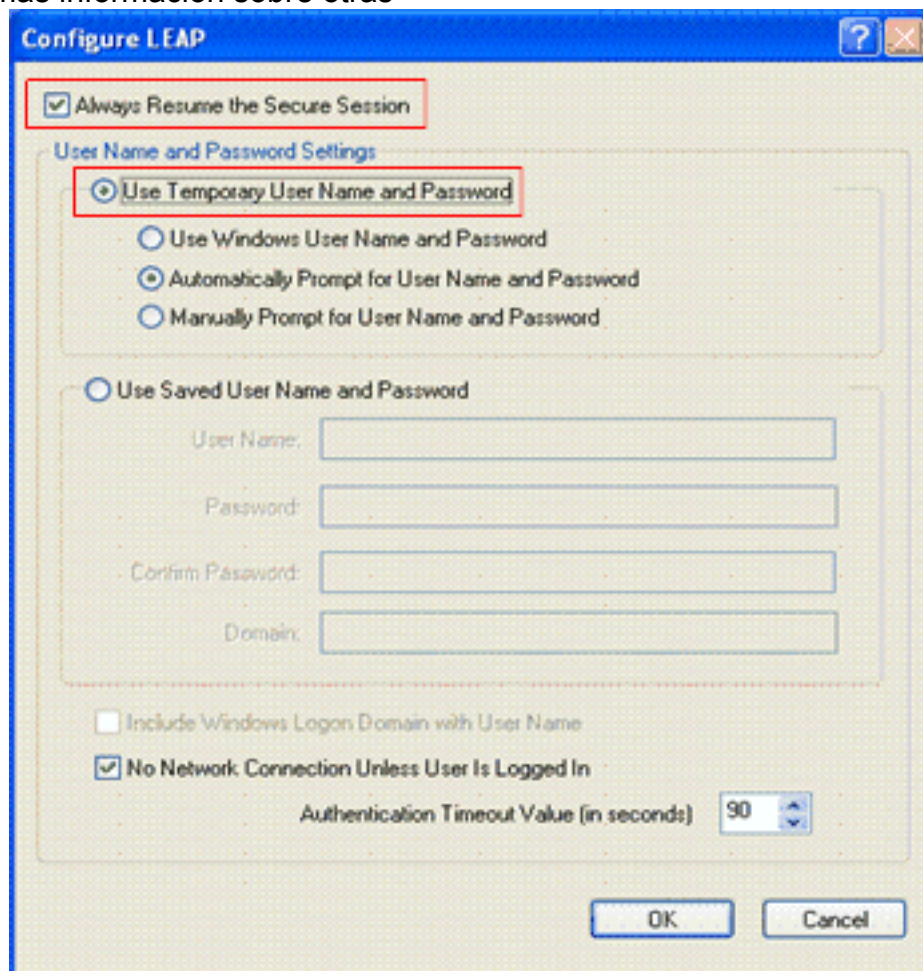
5. En la pestaña **Seguridad**, elija **802.1x**. Elija el tipo EAP como **LEAP** y haga clic en



Configurar.

6. Elija **Usar nombre de usuario temporal y contraseña**, que le solicita que introduzca las credenciales de usuario cada vez que se reinicie el equipo. Compruebe una de las tres opciones que se ofrecen aquí. Este ejemplo utiliza **Solicitud Automática para Nombre de Usuario y Contraseña**, que requiere que ingrese las credenciales de usuario **LEAP** además

de las *Contraseña y Nombre de Usuario de Windows* antes de iniciar sesión en Windows. Marque la casilla de verificación **Reanudar siempre la sesión segura** en la parte superior de la ventana si desea que el suplicante LEAP siempre intente reanudar la sesión anterior sin necesidad de pedirle que vuelva a ingresar sus credenciales cada vez que el adaptador del cliente se desplace y se reasocie a la red. **Nota:** Refiérase a la sección [Configuración del Adaptador de Cliente del documento Guía de Instalación y Configuración de Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters \(CB21AG e PI21AG\)](#) para obtener más información sobre otras



opciones.

7. En la pestaña **Avanzadas**, puede configurar el Preámbulo, la extensión Aironet y otras opciones 802.11 como Alimentación, Frecuencia, etc.
8. Click OK. El cliente ahora intenta asociarse con los parámetros configurados.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Intente asociar un cliente inalámbrico con el Lightweight AP usando la autenticación LEAP para verificar si la configuración funciona como se esperaba.

Nota: Este documento asume que el perfil del cliente está configurado para la autenticación LEAP. Refiérase a [Uso de la Autenticación EAP](#) para obtener más información sobre cómo configurar el 802.11 a/b/g Wireless Client Adapter para la autenticación LEAP.

Una vez que se activa el perfil del cliente inalámbrico, se solicita al usuario que proporcione el nombre de usuario/contraseña para la autenticación LEAP. Aquí tiene un ejemplo:

Enter Wireless Network Password [X]

Please enter your LEAP username and password to log on to the wireless network

User Name :

Password :

Log on to :

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

Profile Name : EAP-Authentication

El Lightweight AP y luego el WLC transfieren las credenciales del usuario al servidor RADIUS externo (Cisco Secure ACS) para validar las credenciales. El servidor RADIUS compara los datos con la base de datos del usuario y proporciona acceso al cliente inalámbrico siempre que las credenciales del usuario sean válidas para verificar las credenciales del usuario. El informe de Autenticación Pasada en el servidor ACS muestra que el cliente ha pasado la autenticación RADIUS. Aquí tiene un ejemplo:

The screenshot shows the Cisco Reports and Activity interface. On the left is a navigation menu with categories like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Database, Reports and Activity, and Online Documentation. The main area is titled 'Reports and Activity' and contains a list of reports such as TACACS+ Accounting, RADIUS Accounting, VoIP Accounting, Passed Authentications, Failed Attempts, Logged-in Users, Disabled Accounts, ACS Backup And Restore, Administration Audit, User Password Changer, and ACS Service Monitoring. A 'Back to Help' button is also visible.

The 'Passed Authentications active.csv' table displays the following data:

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

Tras la autenticación RADIUS exitosa, el cliente inalámbrico se asocia con el AP ligero.

The screenshot shows the 'LEAP Authentication Status' dialog box. It displays the following information:

- 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

At the bottom, there is a checkbox for 'Show minimized next time' and a 'Cancel' button.

Esto también se puede verificar bajo la pestaña **Monitor** de la GUI del WLC. Elija **Monitor > Clients** y verifique la dirección MAC del cliente.

The screenshot shows the Cisco Systems WLC Monitor interface. The 'Clients' section is active, displaying a table of connected clients. A red circle highlights the first row of the table, which contains the following data:

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

Troubleshoot

Complete estos pasos para resolver problemas de las configuraciones:

1. Utilice el comando **debug lwapp events enable** para verificar si el AP se registra con el WLC.
2. Verifique si el servidor RADIUS recibe y valida la solicitud de autenticación del cliente inalámbrico. Verifique la dirección NAS-IP-, la fecha y la hora para verificar si el WLC pudo alcanzar el servidor Radius. Verifique los informes de Autenticaciones Pasadas e Intentos Fallidos en el servidor ACS para lograr esto. Estos informes están disponibles en Informes y actividades en el servidor ACS. Este es un ejemplo cuando falla la autenticación del servidor RADIUS:

The screenshot shows the Cisco Systems Reports and Activity page. The 'Reports' section is active, displaying a table of failed authentication attempts. A red circle highlights the table, which contains the following data:

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

Nota: Refiérase a [Obtención de Información de Depuración de Versión y AAA para Cisco Secure ACS para Windows](#) para obtener información sobre cómo resolver problemas y

obtener información de depuración en Cisco Secure ACS.

3. También puede utilizar estos comandos **debug** para resolver problemas de autenticación
- AAA:debug aaa all enable:** configura la depuración de todos los mensajes AAA.
 - debug dot1x packet enable:** habilita la depuración de todos los paquetes dot1x.
- A continuación se muestra un ejemplo de salida del comando **debug 802.1x aaa enable:**

```
(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,
```

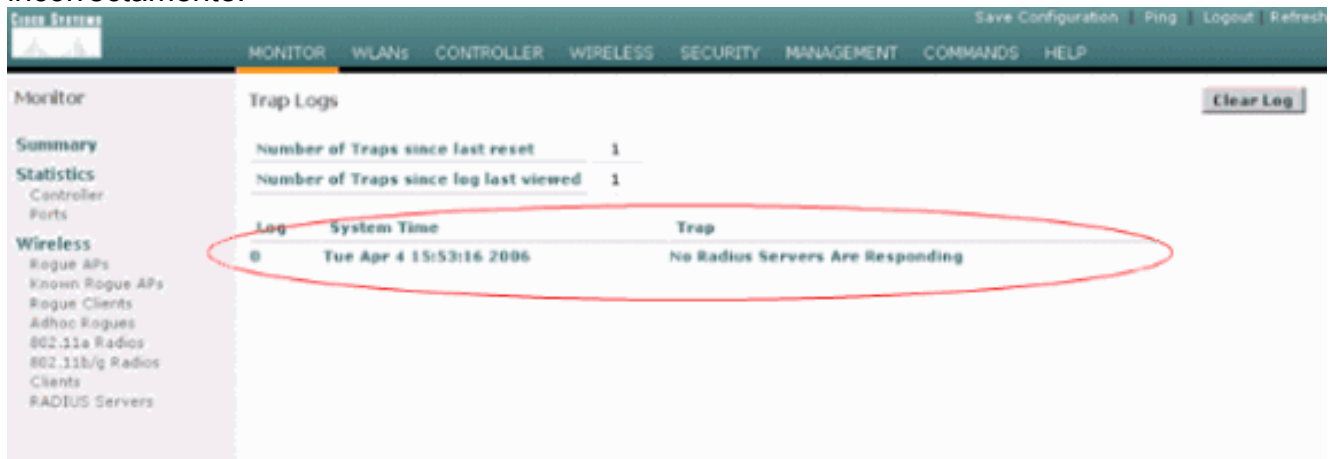
```
length=35, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed
...#.....[2.e..
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13
..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43
ABC
*Sep 23 15:15:43.904: 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, dotlxcb->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
```

Nota: Algunas de las líneas de la salida de depuración se han ajustado debido a restricciones de espacio.

4. Monitoree los registros en el WLC para verificar si el servidor RADIUS recibe las credenciales del usuario. Haga clic en **Monitor** para verificar los registros desde la GUI del WLC. En el menú de la izquierda, haga clic en **Estadísticas** y haga clic en **Servidor Radius** en la lista de opciones. Esto es muy importante porque en algunos casos, el servidor RADIUS nunca recibe las credenciales del usuario si la configuración del servidor RADIUS en el WLC es incorrecta. Así es como los registros aparecen en el WLC si los parámetros RADIUS están configurados incorrectamente:



Puede utilizar una combinación del comando **show wlan summary** para reconocer cuál de sus WLAN emplea autenticación del servidor RADIUS. A continuación, puede ver el comando **show client summary** para ver qué direcciones MAC (clientes) se autentican correctamente en las WLAN RADIUS. También puede relacionar esto con los registros de intentos fallidos o intentos fallidos de Cisco Secure ACS.

Consejos de Troubleshooting

- Verifique en el controlador que el servidor RADIUS esté en estado **activo** y no en **espera** o **inhabilitado**.
- Utilice el comando **ping** para verificar si el servidor Radius es accesible desde el WLC.
- Compruebe si el servidor RADIUS está seleccionado en el menú desplegable WLAN (SSID).
- Si utiliza WPA, debe instalar el último parche de Microsoft WPA para Windows XP SP2. Además, debe actualizar el controlador para el suplicante de su cliente a la versión más reciente.
- Si hace PEAP, por ejemplo certificados con XP, SP2 donde las tarjetas son administradas por la utilidad wireless-0 de Microsoft, necesita obtener el parche KB885453 de Microsoft. Si utiliza Windows Zero Config/client supplicant, inhabilite **Enable Fast Reconnect**. Puede hacerlo si elige **Wireless Network Connection Properties > Wireless Networks > Preferred networks**. A continuación, elija **SSID > Properties > Open > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect**. A continuación, puede encontrar la opción para activar o desactivar al final de la ventana.
- Si tiene tarjetas Intel 2200 o 2915, consulte las declaraciones en el sitio web de Intel sobre los problemas conocidos con sus tarjetas: [Conexión de red Intel® PRO/Wireless](#)

[2200BGConexión de red Intel® PRO/Wireless 2915ABG](http://downloadcenter.intel.com/) Descargue los controladores Intel más actuales para evitar cualquier problema. Puede descargar controladores 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 debería hacerse porque el servidor AAA posiblemente no responda solamente a ese cliente en particular, si hace descarte silencioso. Puede ser una respuesta a otros clientes válidos con certificados válidos. Pero, el WLC todavía puede 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 esto se inhabilita, entonces el controlador solamente falla en el siguiente servidor AAA si hay tres clientes consecutivos que no reciben una respuesta del servidor RADIUS.

Manipulación de Temporizadores EAP

Durante la autenticación 802.1x, el usuario podría ver el `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE:` Se alcanzaron las retransmisiones de la clave EAPOL MÁX1 para el mensaje de error `xx:xx:xx:xx:xx` para móvil.

Este mensaje de error indica que el cliente no respondió a tiempo al controlador durante la negociación de la clave WPA (802.1x). El controlador configura un temporizador para una respuesta durante la negociación de clave. Normalmente, cuando ve este mensaje, se debe a un problema con el solicitante. Asegúrese de ejecutar las últimas versiones de los controladores de cliente y el firmware. En el WLC, hay algunos temporizadores EAP que puede manipular para ayudar con la autenticación del cliente. Estos temporizadores EAP incluyen:

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

Antes de poder manipular estos valores, debe comprender lo que hacen y cómo su cambio afectará a la red:

- **Tiempo de espera de solicitud de identidad EAP:** Este temporizador afecta al tiempo que espera entre las Solicitudes de Identidad de EAP. De forma predeterminada, esto es un segundo (4.1 y inferior) y 30 segundos (4.2 y superior). La razón de este cambio fue que algunos clientes, dispositivos de mano, teléfonos, escáneres, etc., tuvieron dificultades para responder lo suficientemente rápido. Los dispositivos como los portátiles no suelen requerir una manipulación de estos valores. El valor disponible es de 1 a 120. Entonces, ¿qué sucede cuando este atributo se establece en un valor de 30? Cuando el cliente se conecta por primera vez, envía un EAPOL Start a la red, y el WLC envía un paquete EAP, solicitando la identidad del usuario o la máquina. Si el WLC no recibe la respuesta de identidad, envía otra solicitud de identidad 30 segundos después de la primera. Esto sucede en la conexión inicial y cuando el cliente se traslada. ¿Qué ocurre cuando aumentamos este temporizador? Si todo está bien, no hay impacto. Sin embargo, si hay un problema en la red (incluidos problemas de cliente, problemas de AP o problemas de RF), puede causar retrasos en la conectividad de

red. Por ejemplo, si configura el temporizador en el valor máximo de 120 segundos, el WLC espera 2 minutos entre Solicitudes de Identidad. Si el cliente está en roaming y el WLC no recibe la respuesta, entonces hemos creado, como mínimo, una interrupción de dos minutos para este cliente. Las recomendaciones para este temporizador son 5. En este momento, no hay razón para colocar este temporizador en su valor máximo.

- **Reintentos máximos de Solicitud de Identidad de EAP:** El valor Max Retries es el número de veces que el WLC enviará la Solicitud de Identidad al cliente, antes de remover su entrada del MSCB. Una vez que se alcanza el Max Retries, el WLC envía una trama de desautenticación al cliente, obligándolos a reiniciar el proceso EAP. El valor disponible es de 1 a 20. A continuación, analizaremos esto con más detalle. El método Max Retries funciona con el tiempo de espera de identidad. Si el tiempo de espera de su identidad se establece en 120 y el máximo se reinicia en 20, ¿cuánto tiempo tarda 2400 (o $120 * 20$)? Esto significa que tardaría 40 minutos en que el cliente se quitara y en que el proceso EAP se reanudara. Si establece el tiempo de espera de identidad en 5, con un valor de Max Retries de 12, tomará 60 (o $5 * 12$). A diferencia del ejemplo anterior, hay un minuto hasta que el cliente se quita y tiene que iniciar EAP nuevamente. Las recomendaciones para las devoluciones máximas son 12.
- **Límite de tiempo de clave EAPOL:** Para el valor de Tiempo de espera de clave EAPOL, el valor predeterminado es 1 segundo o 1000 milisegundos. Esto significa que cuando se intercambian las claves EAPOL entre el AP y el cliente, el AP enviará la clave y esperará hasta 1 segundo de forma predeterminada para que el cliente responda. Después de esperar el valor de tiempo definido, el AP volverá a transmitir la clave. Puede utilizar el comando **config advanced eap eapol-key-timeout <time>** para modificar esta configuración. Los valores disponibles en 6.0 están entre 200 y 5000 milisegundos, mientras que los códigos anteriores a 6.0 permiten valores entre 1 y 5 segundos. Tenga en cuenta que si tiene un cliente que no responde a un intento clave, extender los temporizadores puede darles un poco más de tiempo para responder. Sin embargo, esto también podría prolongar el tiempo que toma el WLC/AP para desautenticar al cliente para que todo el proceso 802.1x comience nuevamente.
- **Reintentos máximos de claves EAPOL:** Para el valor de Reintentos máximos de clave EAPOL, el valor predeterminado es 2. Esto significa que volveremos a intentar la clave original dos veces al cliente. Esta configuración se puede modificar usando el comando **config advanced eapol-key-retries <retries>**. Los valores disponibles están entre 0 y 4 reintentos. Utilizando el valor predeterminado para el tiempo de espera de la clave EAPOL (es decir, 1 segundo) y el valor predeterminado para la reintentos de la clave EAPOL (2), el proceso sería el siguiente si un cliente no responde al intento de la clave inicial: El AP envía un intento de clave al cliente. Espera un segundo para una respuesta. Si no hay respuesta, se envía el primer reintentos de clave EAPOL. Espera un segundo para una respuesta. Si no hay respuesta, se envía el segundo reintentos de clave EAPOL. Si todavía no hay respuesta del cliente y se cumple el valor de reintentos, el cliente se desautentica. Una vez más, al igual que con el tiempo de espera de clave EAPOL, extender el valor de reintentos de clave EAPOL podría, en algunas circunstancias, ser beneficioso. Sin embargo, establecer el valor máximo puede ser perjudicial de nuevo, ya que el mensaje de desautenticación se prolongará.

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

Si utiliza ACS como servidor RADIUS externo, esta sección se puede utilizar para resolver

problemas de configuración. Package.cab es un archivo Zip que contiene todos los archivos necesarios para resolver problemas de ACS de manera eficiente. Puede usar la utilidad CSSupport.exe para crear el package.cab o puede recolectar los archivos en forma manual.

Refiérase a la sección [Creación de un Archivo package.cab de Obtención de Información de Depuración de Versión y AAA para Cisco Secure ACS para Windows](#) para obtener más información sobre cómo crear y extraer el archivo de paquete de WCS.

[Información Relacionada](#)

- [Ejemplo de Configuración de Failover del Controlador WLAN para Puntos de Acceso Ligeros](#)
- [Actualización del Software del Controlador de la LAN Inalámbrica \(WLC\)](#)
- [Referencia de Comandos de Cisco Wireless LAN Controller](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).