

# Acceso protegido Wi-Fi 2 (ejemplo de la configuración WPA 2)

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Ayuda WPA2 con el equipo Aironet de Cisco](#)

[Configure en el modo de la empresa](#)

[Configuración de la red](#)

[Configure el AP](#)

[Configuración de CLI](#)

[Configure el adaptador del cliente](#)

[Verificación](#)

[Troubleshooting](#)

[Configure en el modo personal](#)

[Configuración de la red](#)

[Configure el AP](#)

[Configure el adaptador del cliente](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento explica las ventajas del uso del Acceso protegido por Wi-Fi 2 (WPA 2) en una red inalámbrica (WLAN). El documento proporciona dos ejemplos de configuración de cómo implementar WPA 2 en una WLAN. El primer ejemplo muestra cómo configurar WPA 2 en el modo de empresa, y el segundo ejemplo configura WPA 2 en el modo personal.

**Nota:** El WPA trabaja con el Protocolo de Autenticación Extensible (EAP).

## [prerrequisitos](#)

## [Requisitos](#)

Asegúrese de que usted tenga conocimiento básico de estos temas antes de que usted intente

esta configuración:

- WPA
- Soluciones de la Seguridad de WLAN **Nota:** Refiera a la [descripción de la Seguridad de LAN del Aironet de red inalámbrica de Cisco](#) para la información sobre las soluciones de la Seguridad de WLAN de Cisco.

## Componentes Utilizados

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

- Punto de acceso /Bridge de Cisco Aironet 1310G que funciona con el Software Release 12.3(2)JA de Cisco IOS®
- Adaptador del cliente de Aironet 802.11a/b/g CB21AG que funciona con los firmwares 2.5
- Utilidad Aironet Desktop (ADU) ese firmware 2.5 de los funcionamientos

**Nota:** El Aironet CB21AG y el software del adaptador del cliente PI21AG es incompatibles con el otro software del adaptador del cliente de Aironet. Usted debe utilizar el ADU con los indicadores luminosos LED amarillo de la placa muestra gravedad menor CB21AG y PI21AG, y usted debe utilizar la utilidad de cliente de Aironet (ACU) el resto de los adaptadores del cliente de Aironet. Refiera a [instalar el adaptador del cliente](#) para más información sobre cómo instalar el indicador luminoso LED amarillo de la placa muestra gravedad menor CB21AG y el ADU.

**Nota:** Este documento utiliza un AP/bridge que tenga una antena integrada. Si usted utiliza un AP/bridge que requiera una antena externa, asegúrese de que las Antenas estén conectadas con el AP/bridge. Si no, el AP/bridge no puede conectar con la red inalámbrica. Ciertos modelos AP/bridge vienen con las Antenas integradas, mientras que otros necesitan una antena externa para el funcionamiento general. Para la información sobre los modelos AP/bridge que vienen con interno o las antenas externas, refiera a la guía/al guía de productos que ordenan del dispositivo apropiado.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

## Antecedentes

El WPA es una solución estándar-basada de la Seguridad del Wi-Fi Alliance que dirige las vulnerabilidades en las redes inalámbricas (WLAN) nativas. El WPA proporciona a la protección de datos y al control de acceso aumentados para los sistemas de la red inalámbrica (WLAN). El WPA dirige todas las vulnerabilidades sabidas del Wired Equivalent Privacy (WEP) en la instrumentación de seguridad original del 802.11 de IEEE y trae una solución inmediata de la Seguridad a las redes inalámbricas (WLAN) en la empresa y la oficina pequeña, los entornos de la oficina en el hogar (SOHO).

El WPA2 es la última generación de Seguridad del Wi-Fi. El WPA2 es la puesta en práctica interoperable del Wi-Fi Alliance del estándar ratificado de IEEE 802.11i. El WPA2 ejecuta el National Institute of Standards and Technology (NIST) - algoritmo de encriptación recomendado del Advanced Encryption Standard (AES) con el uso del modo contrario con el bloque de la cifra que encadena el protocolo del código de autenticación de mensaje (CCMP). El modo contrario AES es un cifrado en bloque que cifra los bloques del 128-bit de los datos al mismo tiempo con una clave de encriptación del 128-bit. El algoritmo CCMP produce un código de la Integridad del mensaje (MIC) que proporcione a la autenticación del origen de datos y a la integridad de datos para la trama de red inalámbrica.

**Nota:** CCMP también se refiere como CBC-MAC.

El WPA2 ofrece un de alto nivel de la Seguridad que el WPA porque AES ofrece un cifrado más fuerte que el Temporal Key Integrity Protocol (TKIP). El TKIP es el algoritmo de encriptación que el WPA utiliza. El WPA2 crea las claves de la sesión frescas en cada asociación. Las claves de encriptación que se utilizan para cada cliente en la red son únicas y específicas a ese cliente. En última instancia, cada paquete que se envía sobre el aire se cifra con una clave única. La Seguridad se aumenta con el uso de una nueva y única clave de encriptación porque no hay reutilización dominante. El WPA todavía se considera seguro y el TKIP no ha estado quebrado. Sin embargo, Cisco recomienda que transición de los clientes al WPA2 cuanto antes.

El WPA y el WPA2 ambos utilizan dos modos de operación:

- Modo de la empresa
- Modo personal

Este documento discute la puesta en práctica de estos dos modos con el WPA2.

## [Ayuda WPA2 con el equipo Aironet de Cisco](#)

El WPA2 se utiliza en este equipo:

- Serie de Aironet 1130AG AP y serie 1230AG AP
- Aironet 1100 series AP
- Aironet 1200 series AP
- Aironet 1300 series AP

**Nota:** Equipe estos APs de las radios 802.11g y utilice el Cisco IOS Software Release 12.3(2)JA o Posterior.

El WPA2 y AES también se utilizan encendido:

- Las 1200 Series de Aironet radian los módulos con los numeros de parte AIR-RM21A y AIR-RM22A**Nota:** El módulo de radio de Aironet 1200 con el numero de parte AIR-RM20A no utiliza el WPA2.
- Adaptadores del cliente de Aironet 802.11a/b/g con la versión de firmware 2.5

**Nota:** Los Productos del Cisco Aironet de la serie 350 no utilizan el WPA2 porque su ayuda de la falta AES de las radios.

**Nota:** Los puentes inalámbricos del Cisco Aironet de la serie 1400 no utilizan el WPA2 o AES.

## [Configure en el modo de la empresa](#)

**El modo de la empresa del término** refiere a los Productos que se prueban para ser interoperables en la clave previamente compartida (PSK) y los modos de operación del 802.1x de IEEE para la autenticación. El 802.1x se considera ser más seguro que los marcos de autenticación uces de los de la herencia debido a su flexibilidad en apoyo de una variedad de mecanismos de autenticación y de algoritmos de encriptación más fuertes. El WPA2 en el modo de la empresa realiza la autenticación en dos fases. La configuración de la autenticación abierta ocurre en la primera fase. La segunda fase es autenticación del 802.1x con uno de los métodos EAP. AES proporciona al mecanismo de encriptación.

En el modo de la empresa, los clientes y los servidores de la autenticación se autentican con el uso de un método de autenticación EAP, y el cliente y servidor genera en parejas una clave principal (PMK). Con el WPA2, el servidor genera el PMK dinámicamente y pasa el PMK al AP.

Esta sección discute la configuración que es necesaria ejecutar el WPA2 en el modo de operación de la empresa.

## [Configuración de la red](#)

En esta disposición, un Aironet 1310G AP/Bridge que se ejecuta protocolo lightweight extensible authentication de Cisco (SALTO) autentica a un usuario con un adaptador del cliente WPA 2-compatible. La administración de claves ocurre con el uso del WPA2, en el cual se configura el cifrado AES-CCMP. El AP se configura como servidor de RADIUS local que ejecute la autenticación LEAP. Usted debe configurar el adaptador del cliente y el AP para ejecutar esta disposición. Las secciones [configuran el AP](#) y [configuran la](#) demostración del [adaptador del cliente la](#) configuración en el AP y el adaptador del cliente.

## [Configure el AP](#)

Complete estos pasos para configurar el AP usando el GUI:

1. Configure el AP como servidor de RADIUS local que ejecute la autenticación LEAP. Elija la **Seguridad > al administrador de servidor** en el menú a la izquierda y defina la dirección IP, los puertos, y el secreto compartido del servidor de RADIUS. Porque esta configuración configura el AP como servidor de RADIUS local, utilice la dirección IP del AP. Utilice los puertos 1812 y 1813 para la operación local del servidor de RADIUS. En el área de prioridades del servidor del valor por defecto, defina la prioridad de la autenticación del valor por defecto EAP como 10.0.0.1. **Nota:** 10.0.0.1 es el servidor de RADIUS local.

**Cisco Aironet 1300 Series Wireless Bridge**

SERVER MANAGER GLOBAL PROPERTIES

Hostname bridge bridge uptime is 7 minutes

**Security: Server Manager**

**Backup RADIUS Server**

Backup RADIUS Server:  (Hostname or IP Address)  
 Shared Secret:

Apply Delete Cancel

**Corporate Servers**

Current Server List

(Hostname or IP Address)

Server:  (Hostname or IP Address)  
 Shared Secret:

Authentication Port (optional):  (0-65536)  
 Accounting Port (optional):  (0-65536)

Apply Cancel

**Default Server Priorities**

EAP Authentication MAC Authentication Accounting

Priority 1:  Priority 1:  Priority 1:

2. Elija al **encargado de la Seguridad > del cifrado del menú** a la izquierda y complete estos pasos: Del menú de la cifra, elija **AES CCMP**. Esta opción activa la encriptación AES con el uso del modo contrario con CBC-MAC.

**Cisco Aironet 1300 Series Wireless Bridge**

Hostname bridge bridge uptime is 5 minutes

**Security: Encryption Manager**

**Encryption Modes**

None

WEP Encryption

Cisco Compliant TKIP Features:  Enable Message Integrity Check (MIC)  
 Enable Per Packet Keying (PPK)

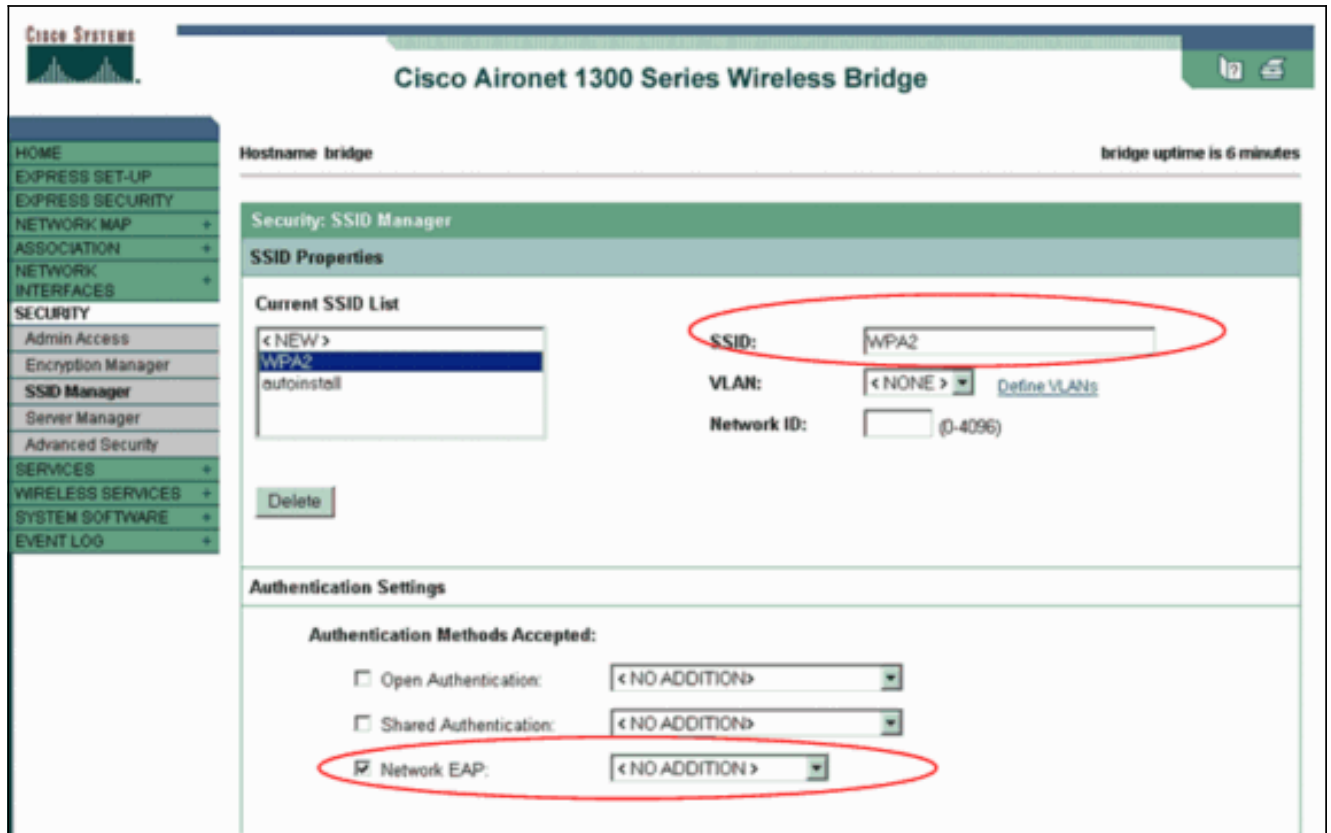
Cipher

**Encryption Keys**

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>

Haga clic en Apply (Aplicar).

3. Elija la **Seguridad > al administrador SSID** y cree un nuevo Service Set Identifier (SSID) para el uso con el WPA2. Controle **Casilla de verificación EAP de la red**. adentro el área validada de los métodos de autenticación.



**Nota:** Utilice estas guías de consulta cuando usted configura el tipo de la autenticación en la interfaz radio: Clientes de Cisco — Utilice la red EAP. Clientes de tercera persona (que incluyen las Extensiones compatibles de Cisco que el [CCX] - los Productos obedientes) — utiliza la autenticación abierta con EAP. Una combinación de ambo Cisco y clientes de tercera persona — elija la red EAP y la autenticación abierta con EAP. Enrolle abajo la ventana del administrador SSID de la Seguridad al área autenticada de la administración de claves y complete estos pasos: Del menú de la administración de claves, elija **obligatorio**. Controle la casilla de verificación **WPA** a la derecha. Haga clic en Apply (Aplicar). **Nota:** La definición de los VLA N es opcional. Si usted define los VLA N, los dispositivos cliente que se asocian al uso de este SSID se agrupan en el VLA N. Refiera a [configurar los VLA N](#) para más información sobre cómo ejecutar los VLA N.

**Authenticated Key Management**

**Key Management:**   CCCKM  WPA

**WPA Pre-shared Key:**   ASCII  Hexadecimal

---

**Accounting Settings**

Enable Accounting

**Accounting Server Priorities:**

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

---

**General Settings**

Advertise Extended Capabilities of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional):  [Define Filter](#)

4. Elija la **Seguridad > servidor de RADIUS local** y complete estos pasos: Haga clic la tabulación **general de la disposición** situada en la cima de la ventana. Controle la casilla de verificación del **SALTO** y el tecleo **se aplica**. En el área de los servidores del acceso a la red, defina la dirección IP y el secreto compartido del servidor de RADIUS. Para el servidor de RADIUS local, utilice la dirección IP del AP.

The screenshot shows the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page is titled "Cisco Aironet 1300 Series Wireless Bridge" and has three tabs: "STATISTICS", "GENERAL SET-UP", and "EAP-FAST SET-UP". The "GENERAL SET-UP" tab is active. The page displays the following information:

- Hostname: bridge
- bridge uptime is 0 minutes
- Security: Local RADIUS Server - General Set-Up
- Local Radius Server Authentication Settings
  - Enable Authentication Protocols:
    - EAP FAST
    - LEAP
    - MAC
- Network Access Servers (AAA Clients)
  - Current Network Access Servers
    - < NEW >
    - 10.0.0.1
  - Network Access Server: 10.0.0.1 (IP Address)
  - Shared Secret: [Redacted]
- Individual Users

Haga clic en Apply (Aplicar).

5. Enrolle abajo la ventana general de la disposición al área de usuarios individuales y defina a los usuarios individuales. La definición de los grupos de usuarios es opcional.



Esta configuración define a un usuario con el nombre el "user1" y una contraseña. También, la configuración selecciona el hash de NT para la contraseña. Tras completar el procedimiento en esta sección, el AP está listo para validar las peticiones de la autenticación de los clientes. El siguiente paso es configurar el adaptador del cliente.

## [Configuración de CLI](#)

### Punto de acceso

```
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. !! aaa group server radius rad_eap
server 10.0.0.1 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.0.0.1 on ports
1812 and 1813. . . . aaa authentication login
eap_methods group rad_eap
!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use
server group "rad_eap". . . . ! bridge irb ! interface
```

```

Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
    12345678901234567890123456 transmit-key
!---This step is optional !--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
!--- This defines the policy for the use of Wired
Equivalent Privacy (WEP). !--- If more than one VLAN is
used, !--- the policy must be set to mandatory for each
VLAN. broadcast-key vlan 1 change 300
    !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1
!--- Create a SSID Assign a vlan to this SSID
authentication open eap eap_methods
    authentication network-eap eap_methods
    !--- Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local
!--- Engages the Local RADIUS Server feature. nas
10.0.0.1 key shared_secret
!--- Identifies itself as a RADIUS server, reiterates !-
-- "localness" and defines the key between the server
(itself) and the access point(itself). ! group testuser
!--- Groups are optional. ! user user1 ntnash password1
group testuser
!--- Individual user user user2 ntnash password2 group
testuser
!--- Individual user !--- These individual users
comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port
1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end

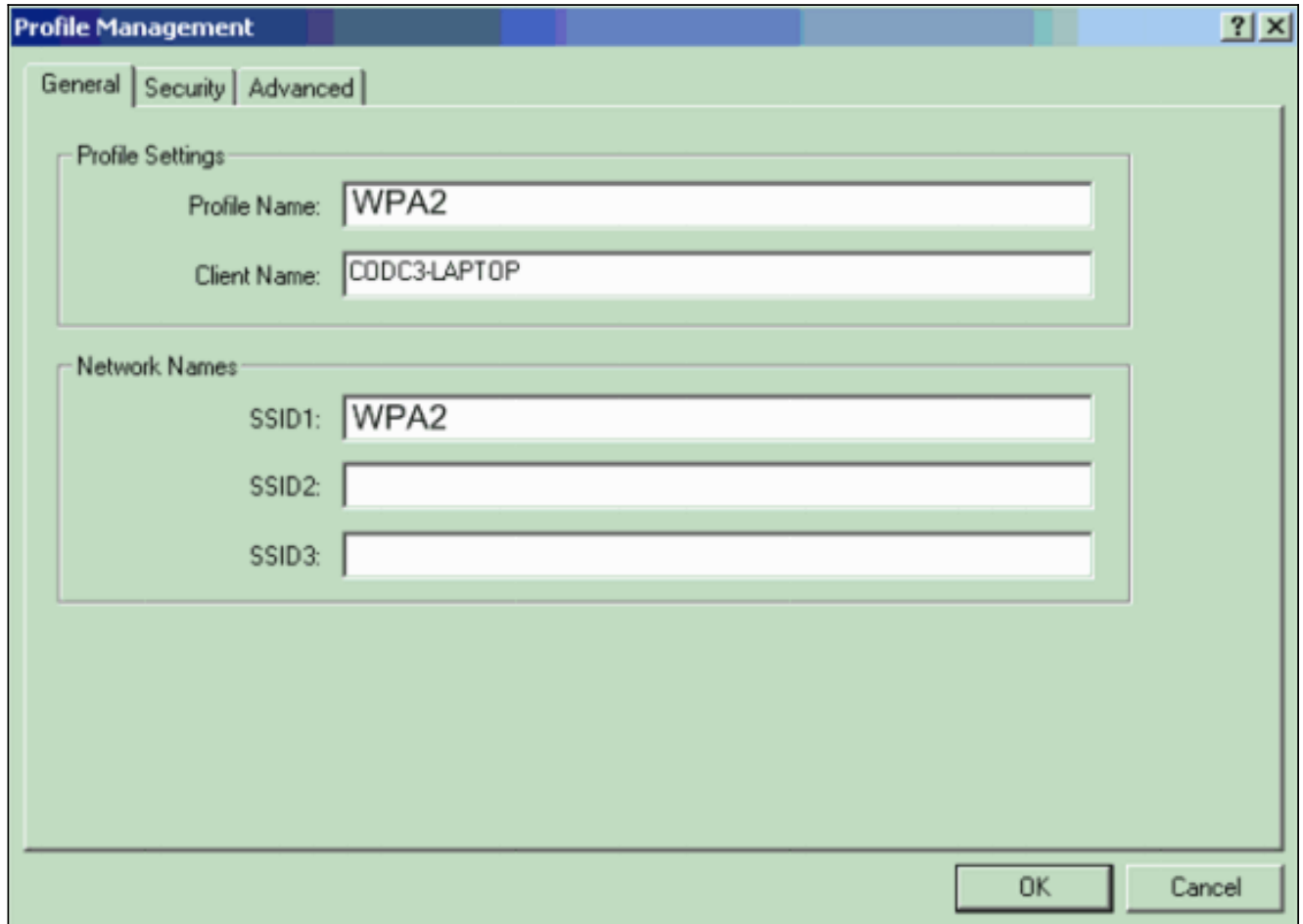
```

## [Configure el adaptador del cliente](#)

Complete estos pasos:

**Nota:** Este documento utiliza un adaptador del cliente de Aironet 802.11a/b/g que funcione con los firmwares 2.5 y explique la configuración del adaptador del cliente con la versión 2.5 ADU.

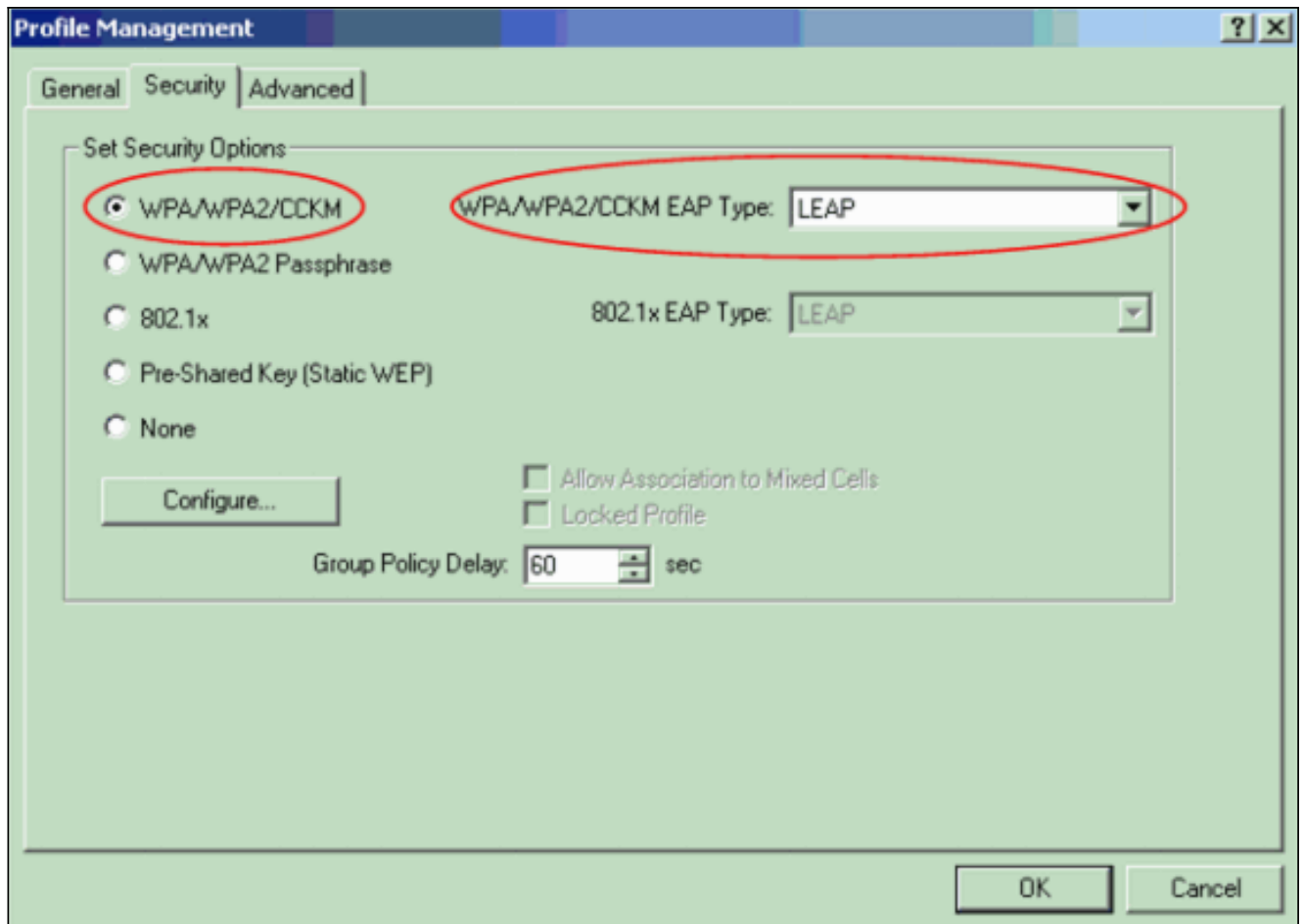
1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil. Visualizaciones de una nueva ventana donde usted puede fijar la configuración para la operación del modo de la empresa WPA2. Conforme a la ficha general, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará. En este ejemplo, el nombre del perfil y el SSID son WPA2: **Nota:** El SSID debe hacer juego el SSID que usted configuró en el AP para el WPA2.



The screenshot shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. It contains two sections: 'Profile Settings' and 'Network Names'. In 'Profile Settings', 'Profile Name' is 'WPA2' and 'Client Name' is 'C0DC3-LAPTOP'. In 'Network Names', 'SSID1' is 'WPA2', and 'SSID2' and 'SSID3' are empty. 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Profile Name	WPA2
Client Name	C0DC3-LAPTOP
SSID1	WPA2
SSID2	
SSID3	

2. Haga clic la **ficha de seguridad**, haga clic **WPA/WPA2/CCKM**, y elija el **SALTO** del tipo menú WPA/WPA2/CCKM EAP. Esta acción activa el WPA o el WPA2, cualquiera usted configura en el AP.



3. El teclado **configura** para definir las configuraciones del SALTO.
4. Elija las configuraciones apropiadas del nombre de usuario y contraseña, sobre la base de los requisitos, y haga clic la **AUTORIZACIÓN**. Esta configuración elige la opción incita automáticamente para el Nombre de usuario y la contraseña. Esta opción le permite ingresar manualmente el Nombre de usuario y la contraseña cuando ocurre la autenticación LEAP.

**LEAP Settings** [?] [X]

Always Resume the Secure Session

Username and Password Settings

Use Temporary User Name and Password

Use Windows User Name and Password

Automatically Prompt for User Name and Password

Manually Prompt for User Name and Password

Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

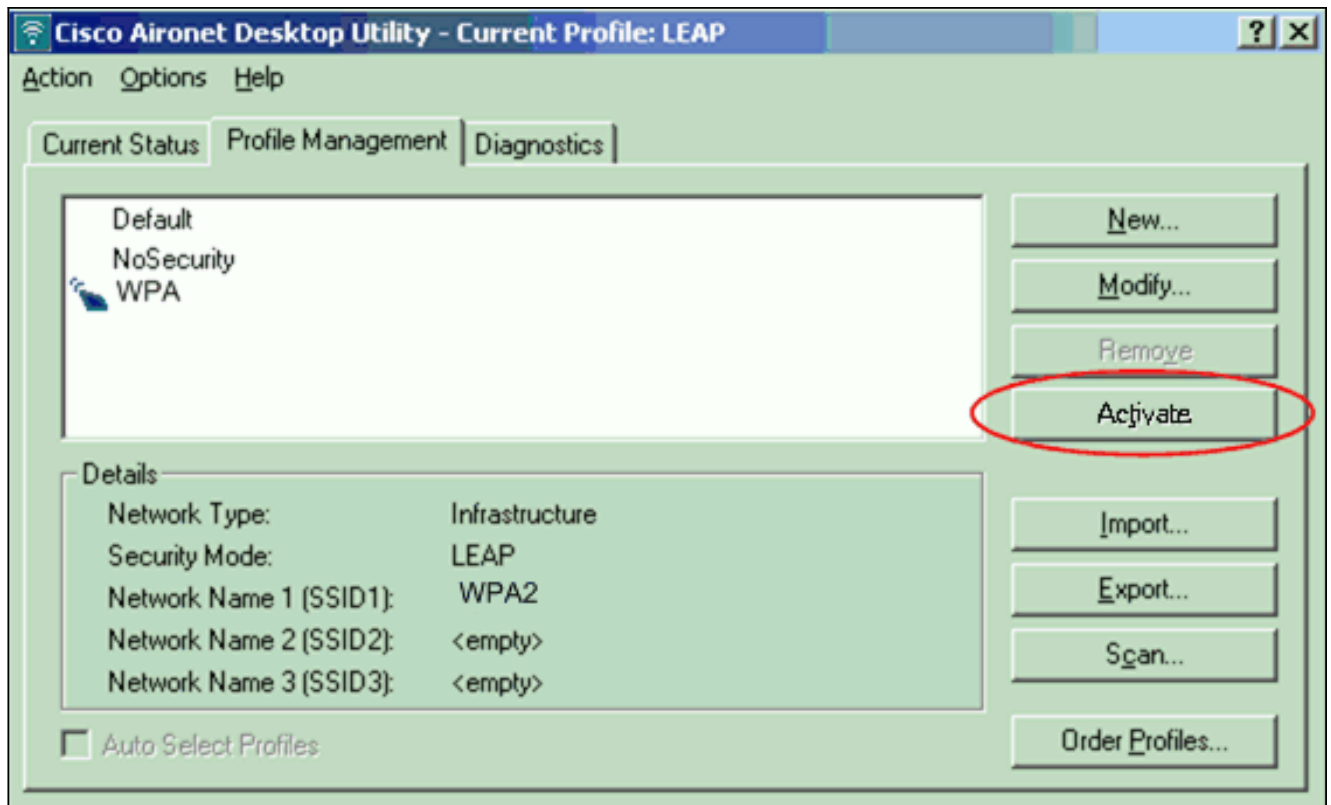
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

5. **AUTORIZACIÓN** del teclado para salir la ventana de administración del perfil.
6. El teclado **activa** para activar este perfil en el adaptador del cliente.



**Nota:** Si usted utiliza la configuración de la Tecnología inalámbrica cero de Microsoft (WZC) para configurar el adaptador del cliente, por abandono, el WPA2 no está disponible con WZC. Así pues, para permitir WZC-activó a los clientes ejecutar el WPA2, usted debe instalar un arreglo caliente para el Microsoft Windows XP. Refiera al [centro de descarga de Microsoft - Actualización para Windows XP \(KB893357\)](#) para la instalación. Después de que usted instale el arreglo caliente, usted puede configurar el WPA2 con WZC.

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

1. Cuando las visualizaciones de la ventana de contraseña de la red inalámbrica del ingresar, ingresan el Nombre de usuario y la

**Enter Wireless Network Password**

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 : WPA2

contraseña.

La próxima ventana es estatus de la autenticación LEAP. Esta fase verifica los credenciales de usuario contra el servidor de RADIUS local.

2. Controle el área del estatus para ver el resultado de la autenticación.

**LEAP Authentication Status**

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

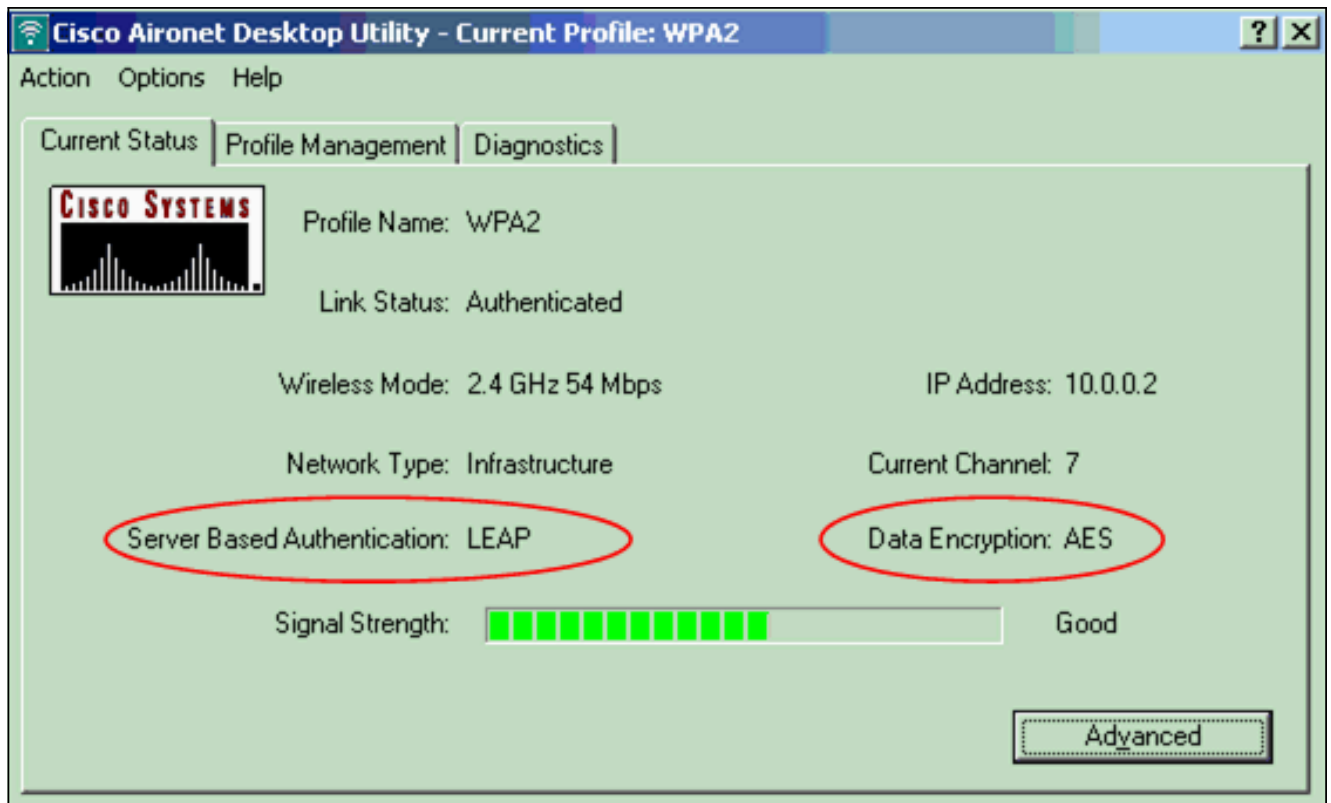
Profile Name: WPA2

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

Cuando la autenticación es acertada, el cliente conecta con el LAN de la Tecnología inalámbrica.

3. Controle el estado actual ADU para verificar que el cliente utiliza la encriptación AES y la autenticación LEAP. Esto muestra que usted ha ejecutado el WPA2 con la autenticación LEAP y la encriptación AES en la red inalámbrica (WLAN).



4. Controle la orden de la clave del evento AP/bridge para verificar que han autenticado al cliente con éxito con el WPA2.



## Troubleshooting

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

## Configure en el modo personal

El modo personal del término refiere a los Productos que se prueban para ser interoperables en el modo de operación de PSK-only para la autenticación. Este modo requiere la configuración



manual de un PSK en el AP y los clientes. PSK autentica los usuarios vía una contraseña, o el código de identificación, en la estación del cliente y el AP. No hay servidor de la autenticación necesario. Un cliente puede acceder a la red solamente si las coincidencias de contraseña del cliente la contraseña AP. La contraseña también proporciona al material de codificación que el TKIP o AES utiliza para generar una clave de encriptación para el cifrado de los paquetes de datos. El modo personal se apunta a los entornos SOHO y no se considera seguro para los entornos de la empresa. Esta sección proporciona a la configuración que usted necesita para ejecutar el WPA2 en el modo de operación personal.

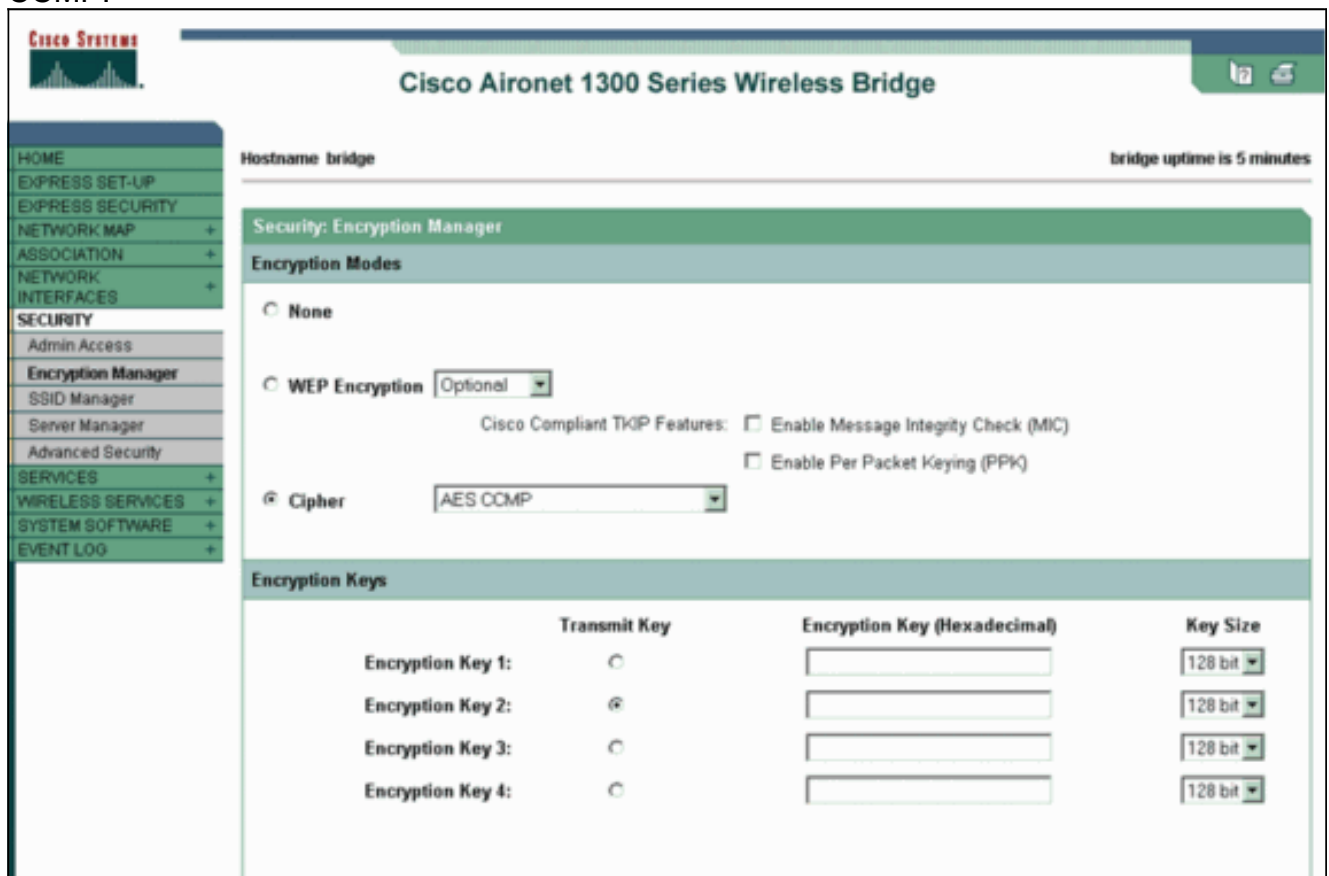
## [Configuración de la red](#)

En esta disposición, un usuario con un adaptador del cliente WPA 2-compatible autentica a un Aironet 1310G AP/Bridge. La administración de claves ocurre con el uso de WPA2PSK, con el cifrado AES-CCMP configurado. Las secciones [configuran el AP](#) y [configuran la demostración del adaptador del cliente la](#) configuración en el AP y el adaptador del cliente.

## [Configure el AP](#)

Complete estos pasos:

1. Elija al **encargado de la Seguridad > del cifrado** en el menú a la izquierda y complete estos pasos: Del menú de la cifra, elija **AES CCMP**. Esta opción activa la encriptación AES con el uso del modo contrario con CCMP.



The screenshot shows the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "bridge" and the uptime is "5 minutes". The left sidebar contains a navigation menu with categories like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Security: Encryption Manager". Under "Encryption Modes", the "Cipher" option is selected, and the dropdown menu shows "AES CCMP". Below this, there are checkboxes for "Cisco Compliant TKIP Features": "Enable Message Integrity Check (MIC)" and "Enable Per Packet Keying (PPK)". The "Encryption Keys" section contains a table with four rows, each representing an encryption key. Each row has a "Transmit Key" radio button, an "Encryption Key (Hexadecimal)" input field, and a "Key Size" dropdown menu set to "128 bit".

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Haga clic en Apply (Aplicar).

2. Elija la **Seguridad > al administrador SSID** y cree un nuevo SSID para el uso con el WPA2. Controle el casilla "Abrir autenticación".

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "bridge" and the uptime is "7 minutes". The left sidebar shows a navigation menu with categories like HOME, EXPRESS SET-UP, SECURITY, SERVICES, and WIRELESS SERVICES. The main content area is titled "Security: SSID Manager" and "SSID Properties". It shows a "Current SSID List" with a table containing a new entry "WPA2PSK" and an existing entry "tsunami". To the right, the "SSID:" field is set to "WPA2PSK", the "VLAN:" is set to "< NONE >", and the "Network ID:" is set to "(0-4096)". Below this, the "Authentication Settings" section shows "Authentication Methods Accepted:" with three options: "Open Authentication" (checked), "Shared Authentication", and "Network EAP". The "Open Authentication" option is highlighted with a red circle.

Enrolle abajo la Seguridad: La ventana del administrador SSID al área autenticada de la administración de claves y completa estos pasos: Del menú de la administración de claves, elija **obligatorio**. Controle la casilla de verificación **WPA** a la derecha.

**Authenticated Key Management**

**Key Management:**
Mandatory
 CCKM
 WPA

**WPA Pre-shared Key:**
[REDACTED]
 ASCII  Hexadecimal

**Accounting Settings**

**Enable Accounting**

**Accounting Server Priorities:**

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

**General Settings**

**Advertise Extended Capabilities of this SSID**

Advertise Wireless Provisioning Services (WPS) Support

Advertise this SSID as a Secondary Broadcast SSID

**Enable IP Redirection on this SSID**

IP Address:

IP Filter (optional):  [Define Filter](#)

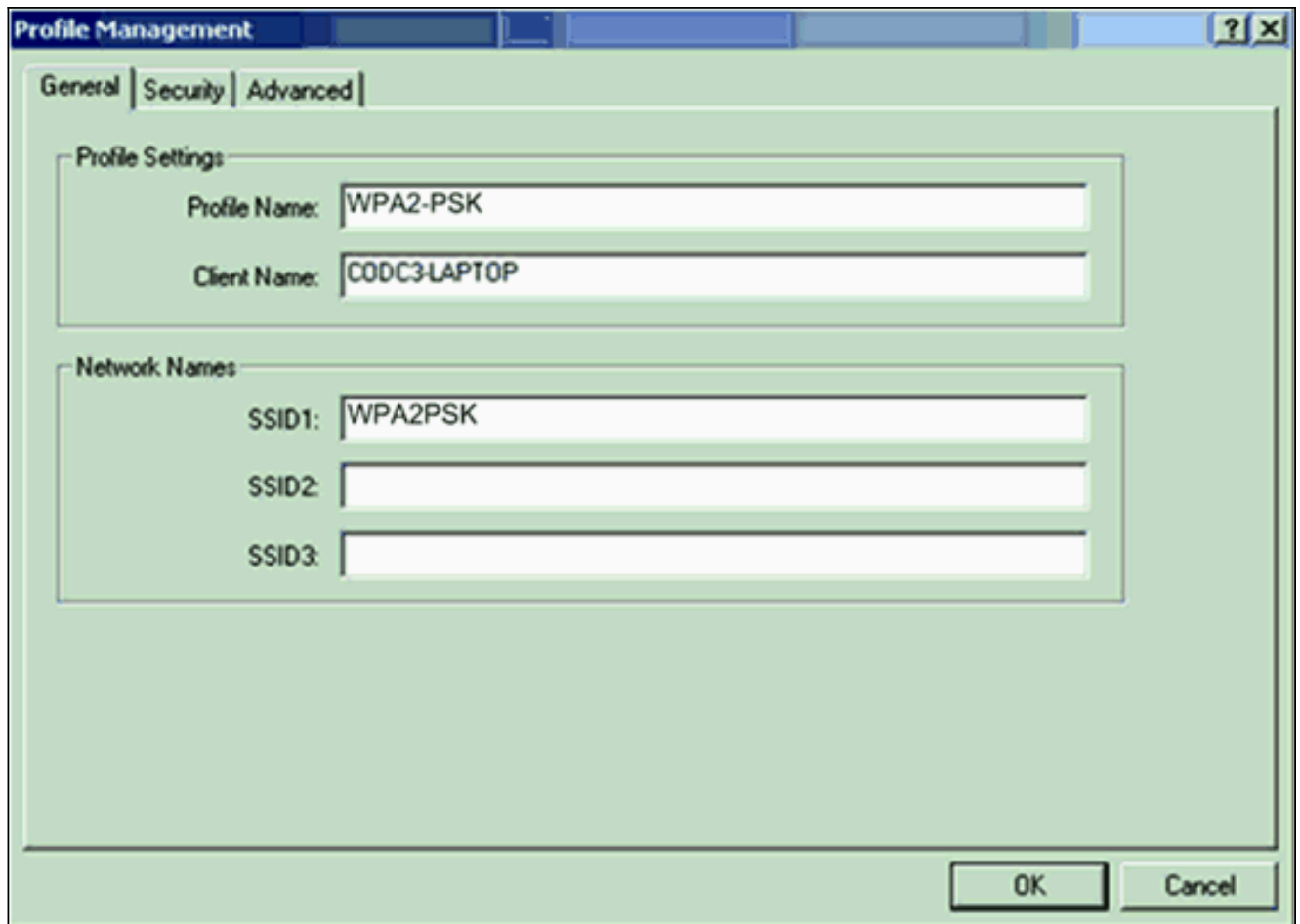
Ingrese la clave secreta compartida PSK WPA o la clave del passphrase WPA PSK. Esta clave debe hacer juego la clave WPA PSK que usted configura en el adaptador del cliente. Haga clic en Apply (Aplicar).

El AP puede ahora recibir las peticiones de la autenticación de los clientes de red inalámbrica.

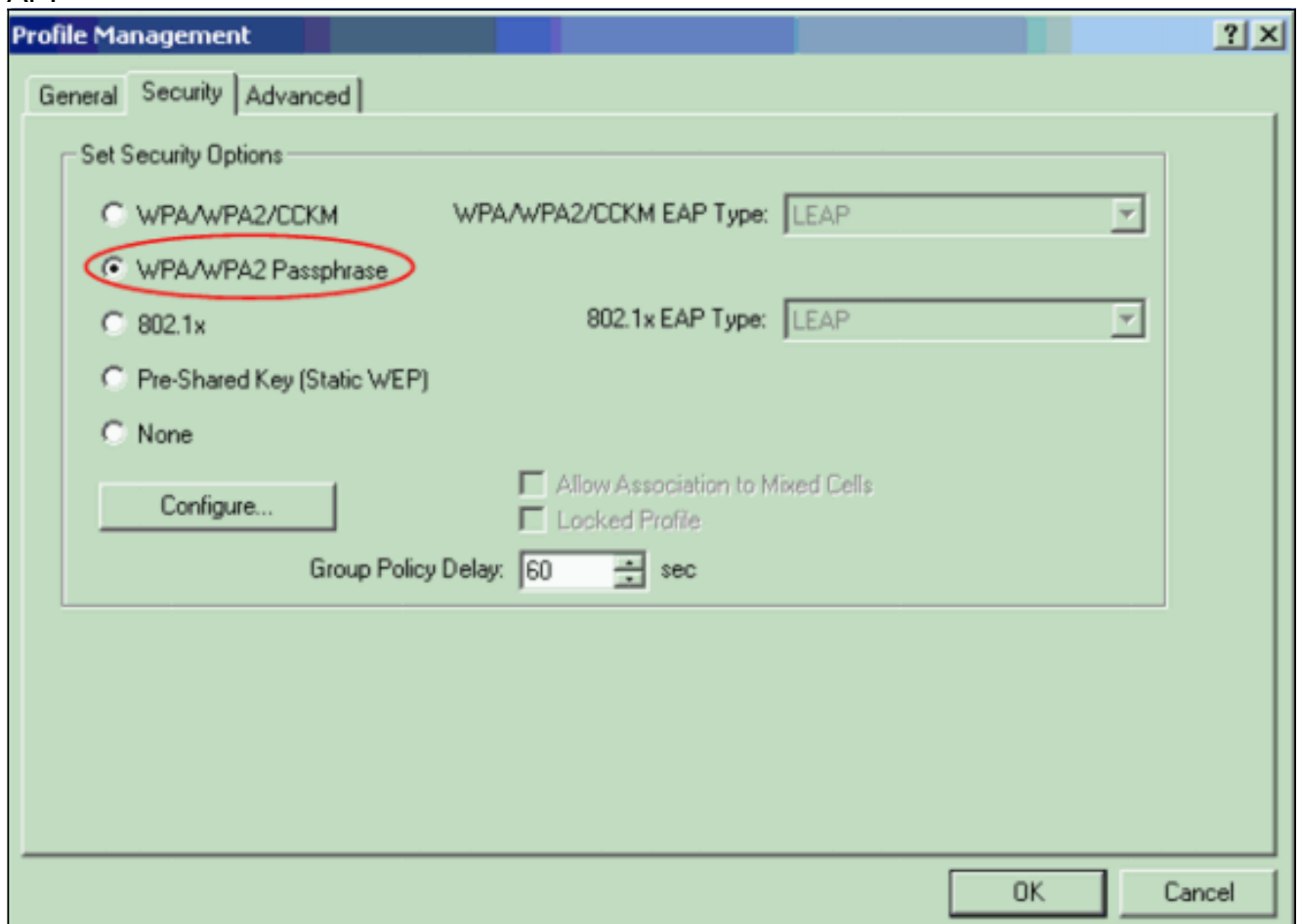
## [Configure el adaptador del cliente](#)

Complete estos pasos:

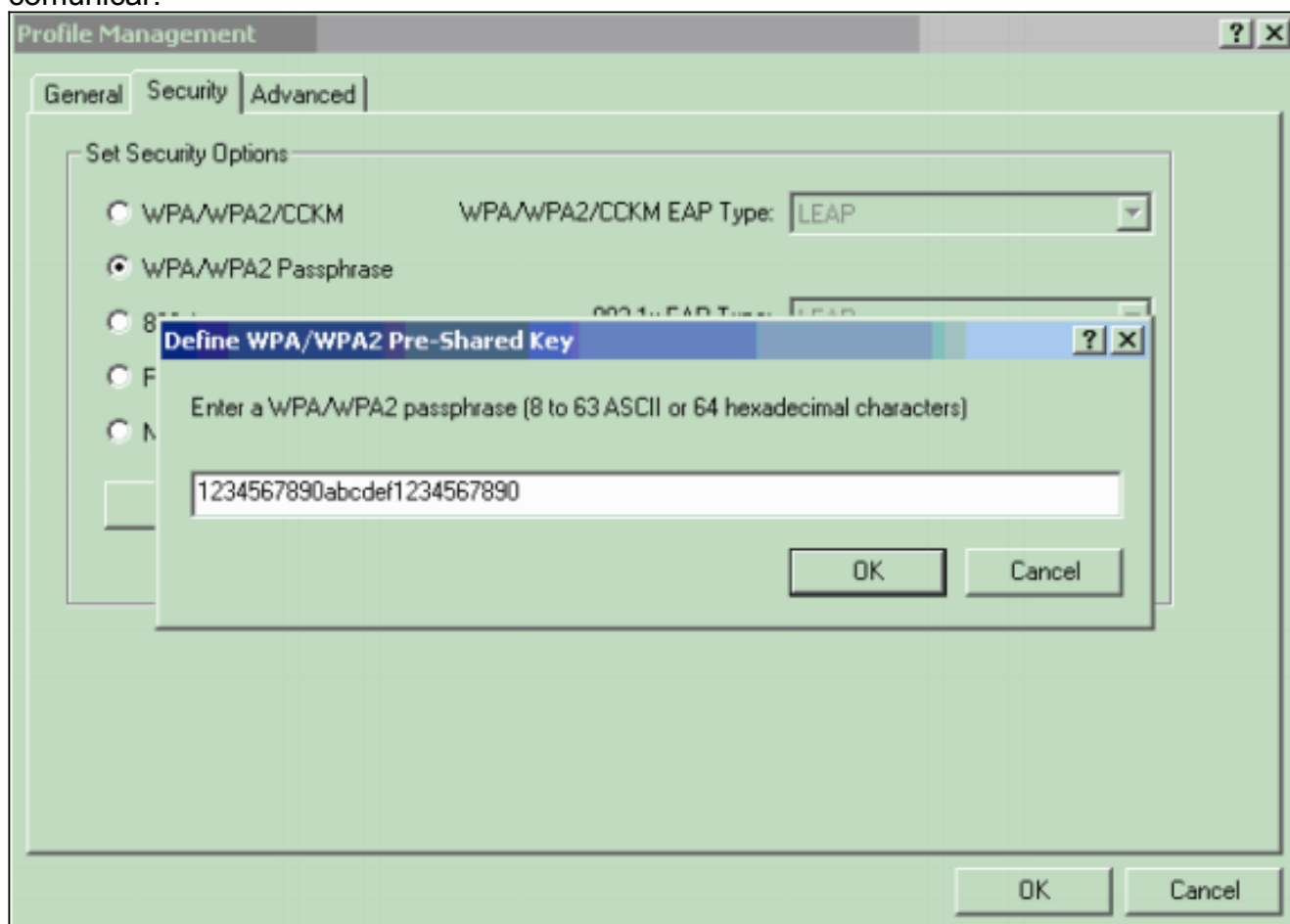
1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil. Visualizaciones de una nueva ventana donde usted puede fijar la configuración para WPA2PSK el modo de operación. Conforme a la ficha general, ingrese el nombre del perfil y el SSID que el adaptador del cliente utilizará. En este ejemplo, el nombre del perfil está WPA2-PSK y el SSID está WPA2PSK: **Nota:** El SSID debe hacer juego el SSID que usted configuró en el AP para WPA2PSK.



2. Haga clic la **ficha de seguridad** y haga clic **WPA/WPA2** la frase de contraseña. Esta acción activa o WPA PSK o WPA2PSK, cualquiera usted configura en el AP.



- Haga clic en Configure (Configurar). De la definición las visualizaciones de la ventana de la clave previamente compartida WPA/WPA2.
- Obtenga WPA/WPA2 el passphrase de su administrador de sistema y ingrese el passphrase en WPA/WPA2 el campo del passphrase. Obtenga la frase de contraseña para el AP en una red de la infraestructura o la frase de contraseña para otros clientes en una red ad-hoc. Utilice estas guías de consulta para ingresar un passphrase: WPA/WPA2 las frases de contraseña deben contener entre 8 y 63 caracteres del texto ASCII o 64 caracteres hexadecimales. Su frase de contraseña del adaptador del cliente WPA/WPA2 debe hacer juego la frase de contraseña del AP con el cual usted planea comunicar.



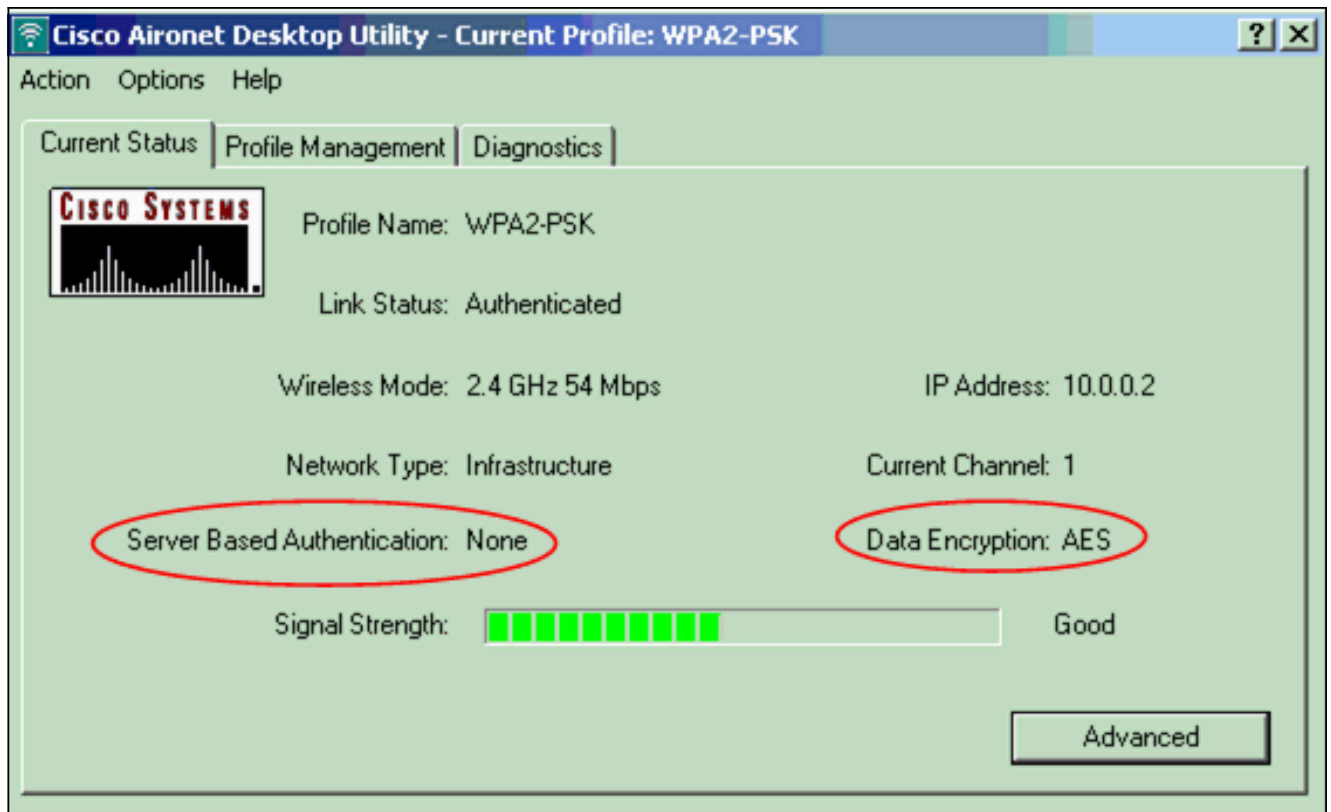
- Haga clic la **AUTORIZACIÓN** para salvar la frase de contraseña y volver a la ventana de administración del perfil.

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Después de que WPA2PSK el perfil se active, el AP autentica al cliente basado en la frase de contraseña WPA2 (PSK) y proporciona al acceso a la red inalámbrica (WLAN).

- Controle el estado actual ADU para verificar la autenticación satisfactoria. Esta ventana proporciona a un ejemplo. La ventana muestra que el cifrado se utiliza que es AES y que no se realiza ninguna autenticación basada en el servidor:



- Controle la orden de la clave del evento AP/bridge para verificar que han autenticado al cliente con éxito con WPA2PSK el modo de autenticación.



## Troubleshooting

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

## Información Relacionada

- [Configuración de conjuntos Cipher y WEP](#)

- [Configuración de los tipos de autenticación](#)
- [Introducción a la configuración de WPA](#)
- [WPA2 - Acceso protegido Wi-Fi 2](#)
- [Cuál es operación de modo mezclada WPA, y cómo yo la configura en mi AP](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)