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

Contenido

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

Nota: El software del Aironet del adaptador del cliente del CB21AG y del PI21AG es incompatible con el otro software del adaptador de cliente Aironet. Usted debe utilizar el ADU con los indicadores luminosos LED amarillo de la placa muestra gravedad menor del CB21AG y del PI21AG, y usted debe utilizar el Aironet Client Utility (ACU) el resto de los adaptadores de cliente 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 del CB21AG y el ADU.

Nota: Este documento utiliza un AP/bridge que tiene una antena integrada. Si usted utiliza un AP/bridge que requiere 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 del AP/bridge vienen con las Antenas integradas, mientras que otros necesitan una antena externa para el funcionamiento general. Para la información sobre los modelos del 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 acerca de la seguridad estándar basada del Wi-Fi Alliance que dirige las vulnerabilidades en los WLAN nativos. El WPA proporciona la protección de datos y el control de acceso aumentados para los sistemas WLAN. El WPA dirige todas las vulnerabilidades sabidas del Wired Equivalent Privacy (WEP) en la instrumentación de seguridad original del IEEE 802.11 y trae una solución acerca de la seguridad inmediata a los WLAN en los entornos de la empresa y del oficina pequeña, oficina en el hogar (SOHO).

El WPA2 es la última generación de Seguridad del Wi-Fi. El WPA2 es la implementación interoperable del Wi-Fi Alliance del estándar ratificado de IEEE 802.11i. El WPA2 implementa el National Institute of Standards and Technology (NIST) - algoritmo de encripción recomendado del Advanced Encryption Standard (AES) con el uso del modo contrario con el protocolo del Message Authentication Code del Cipher Block Chaining (CCMP). El El modo contador AES es un cifrado en bloque que cifra los bloques del 128-bit del en un momento de los datos con una clave de encripción del 128-bit. El algoritmo CCMP produce un código de la Integridad del mensaje (MIC) que proporcione la autenticación del origen de los datos y la integridad de los datos para la trama de red inalámbrica.

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

El WPA2 ofrece un de alto nivel de la Seguridad que el WPA porque el AES ofrece un cifrado más fuerte que el Temporal Key Integrity Protocol (TKIP). El TKIP es el algoritmo de encripción que el WPA utiliza. El WPA2 crea las claves de la sesión frescas en cada asociación. Las claves de encripción 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 encripción porque no hay reutilización dominante. El WPA todavía se considera seguro y el TKIP no ha estado quebrado. Sin embargo, Cisco recomienda esa transición de clientes al WPA2 cuanto antes.

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

- Modo de empresa
- Modo personal

Este documento discute la implementación de estos dos modos con el WPA2.

Soporte WPA2 con el equipo Aironet de Cisco

El WPA2 se soporta en este equipo:

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

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

El WPA2 y el AES también se soportan encendido:

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

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

Nota: Los Wireless Bridge del Cisco Aironet de la serie 1400 no soportan el WPA2 o el AES.

Configuración en el modo de empresa

El modo de empresa del término refiere a los Productos que se prueban para ser interoperables en los modos de operación de la clave previamente compartida (PSK) y del IEEE 802.1X 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 encripción más fuertes. El WPA2 en el modo de 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. El AES proporciona el mecanismo de encripción.

En el modo de empresa, los clientes y los servidores de 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 implementar el WPA2 en el modo de operación de la empresa.

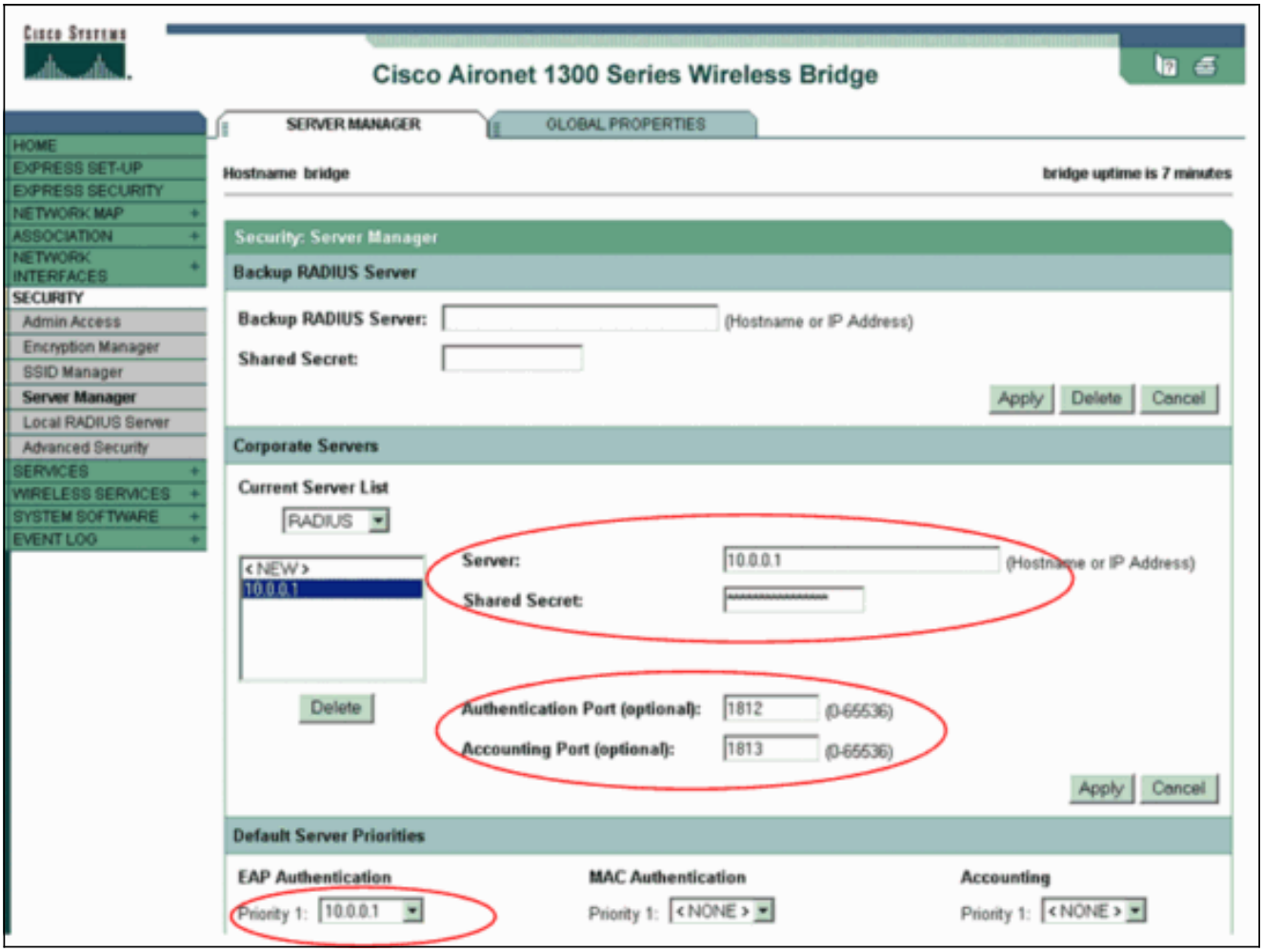
Configuración de la red

En esta configuración, un AP/bridge del Aironet 1310G que se ejecute protocolo extensible authentication de las livianas 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 AES-CCMP el cifrado se configura. 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 implementar esta configuración. Las secciones configuran el AP y configuran la demostración del adaptador del cliente la configuración en el AP y el adaptador del cliente.

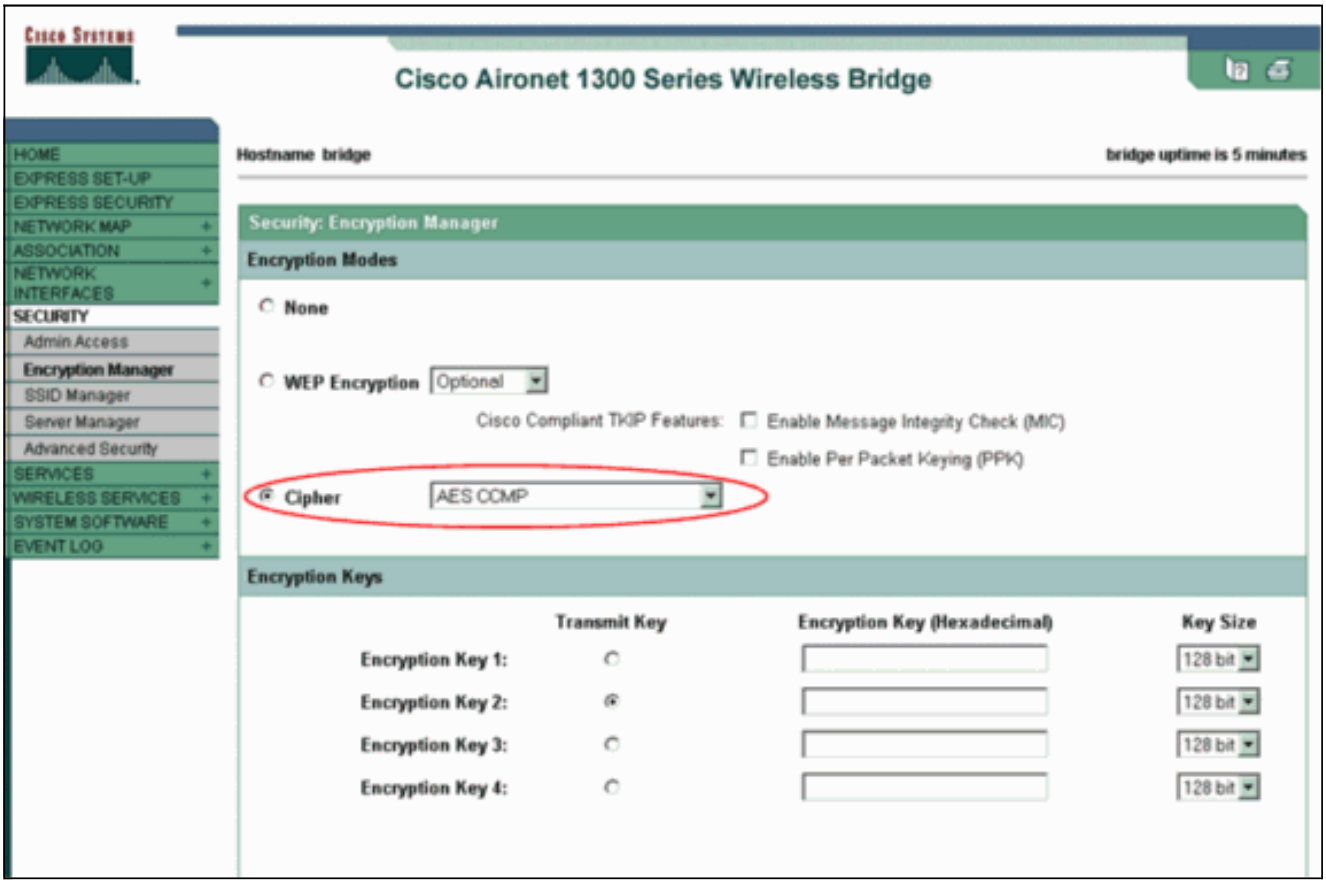
Configure el AP

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 predeterminada del servidor, defina la prioridad predeterminada de la autenticación EAP como 10.0.0.1.**Nota:** 10.0.0.1 es el servidor de RADIUS local.

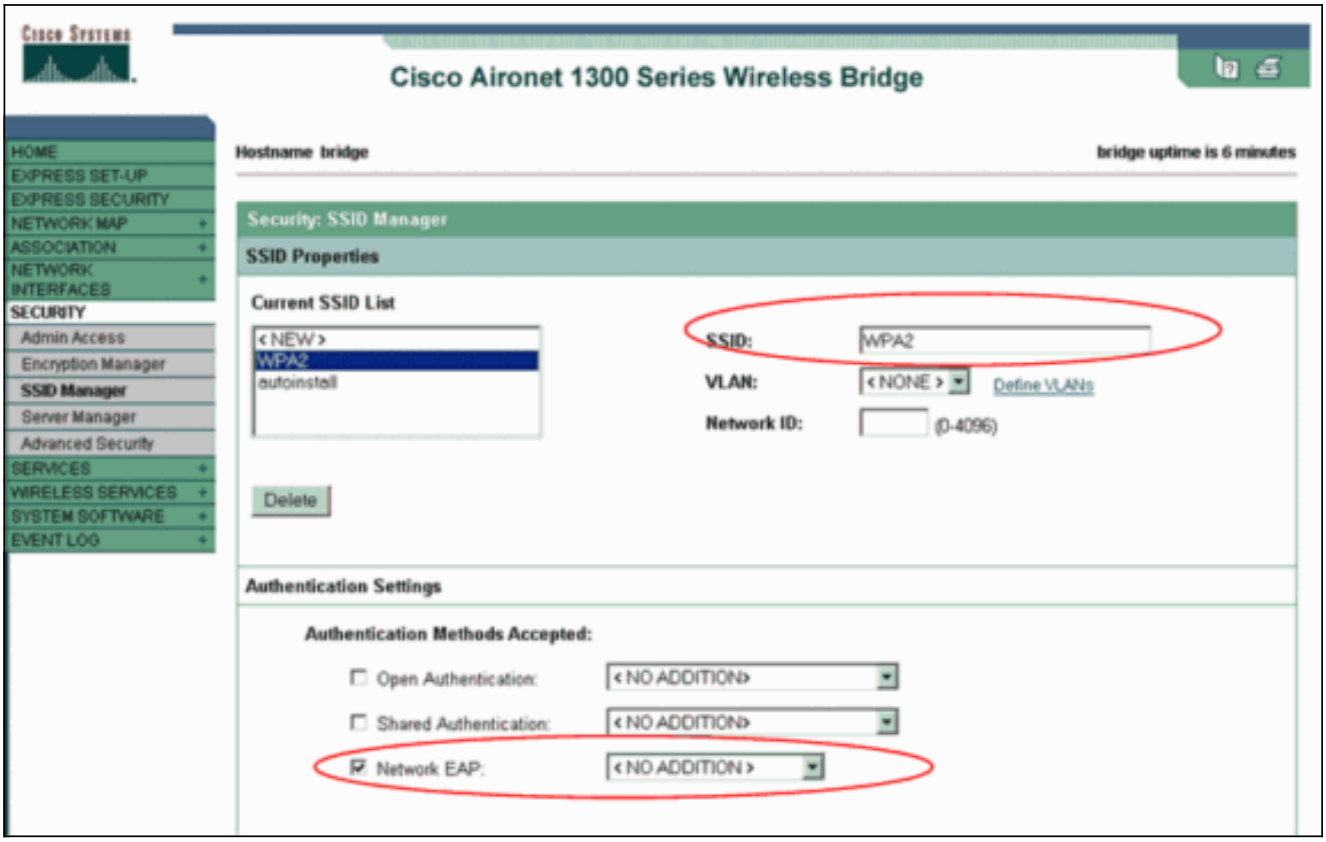


2. Elija al **administrador de la Seguridad > del cifrado del** menú a la izquierda y complete estos pasos:Del menú de la cifra, elija el **CCMP AES**.Esta opción habilita la encripción AES con el uso del modo contrario con CBC-
MAC.



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.Marque **Casilla de verificación EAP de la red.** adentro el área validada los métodos de autentificación.

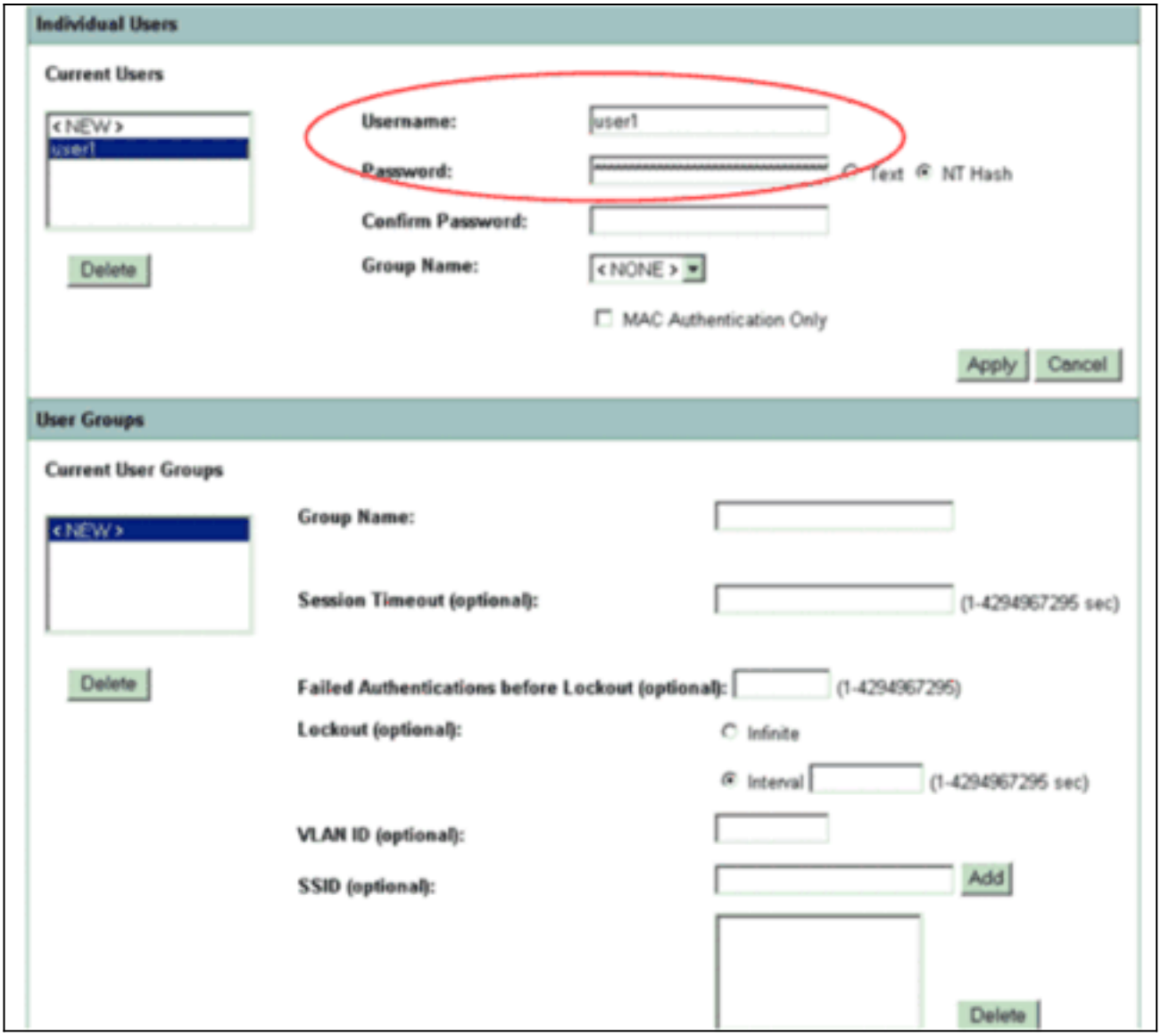


Nota: Utilice estas guías de consulta cuando usted configura el tipo de autenticación en la interfaz radio:Clientes de Cisco — Utilice la red EAP.Clientes de tercera persona (que incluyen los Ciscos Compatibles Extension que el [CCX] - los Productos obedientes) — utiliza la autenticación abierta con el EAP.Una combinación de ambo Cisco y clientes de tercera persona — elija la red EAP y la autenticación abierta con el EAP.Navegue hacia 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**.Marque 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 del 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 implementar los VLA N.

4. Elija la **Seguridad > servidor de RADIUS local** y complete estos pasos:Haga clic la lengueta **general de la configuración** situada en la cima de la ventana.Marque la casilla de verificación del **SALTO** y el tecleo **se aplica**.En el área de los servidores de 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.

Haga clic en Apply (Aplicar).

5. Navegue hacia abajo la ventana general de la configuración 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 los pedidos de 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 nthash password1 group testuser
!--- Individual user user user2 nthash 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
```

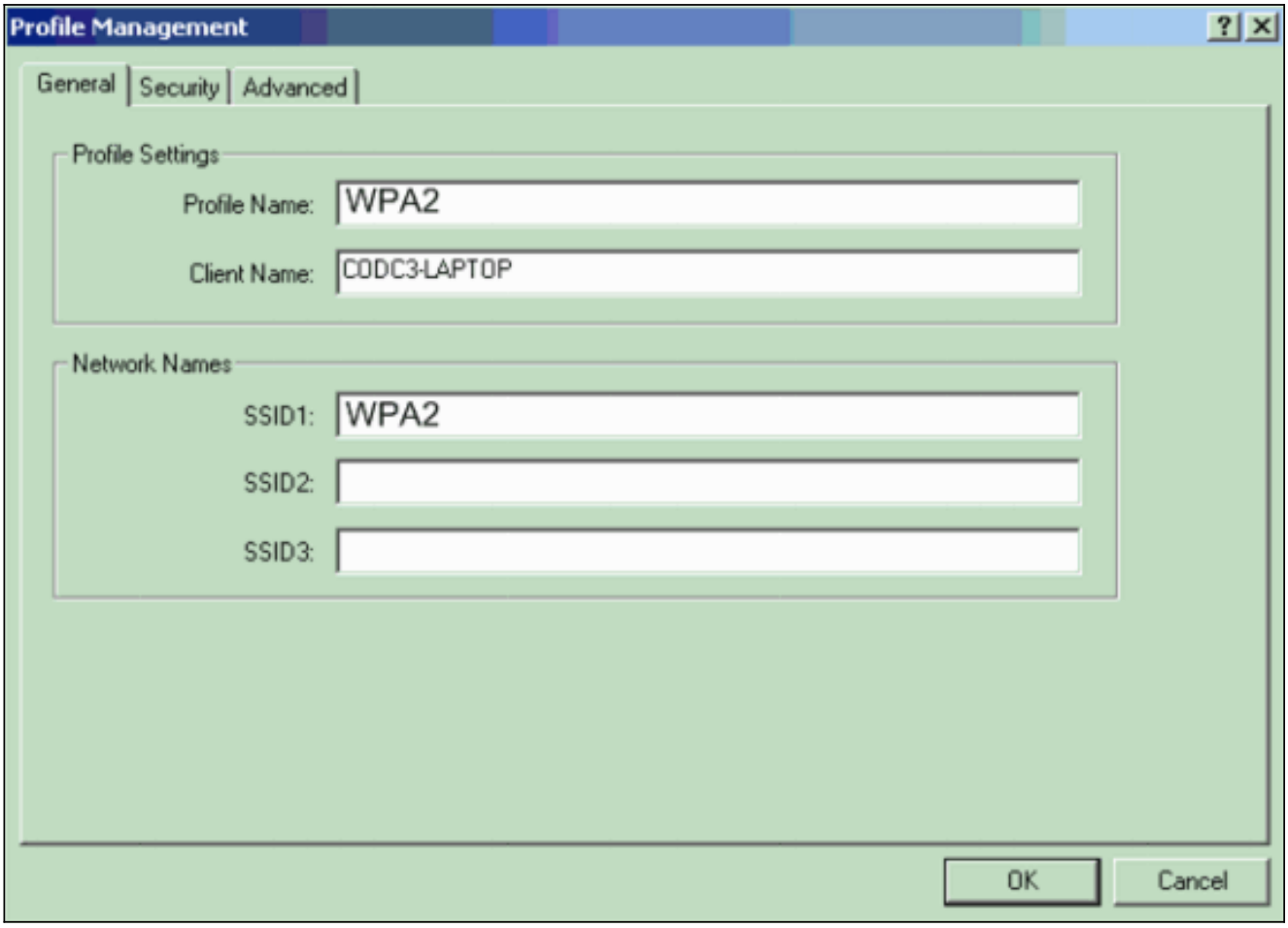
Configure el adaptador del cliente

Complete estos pasos:

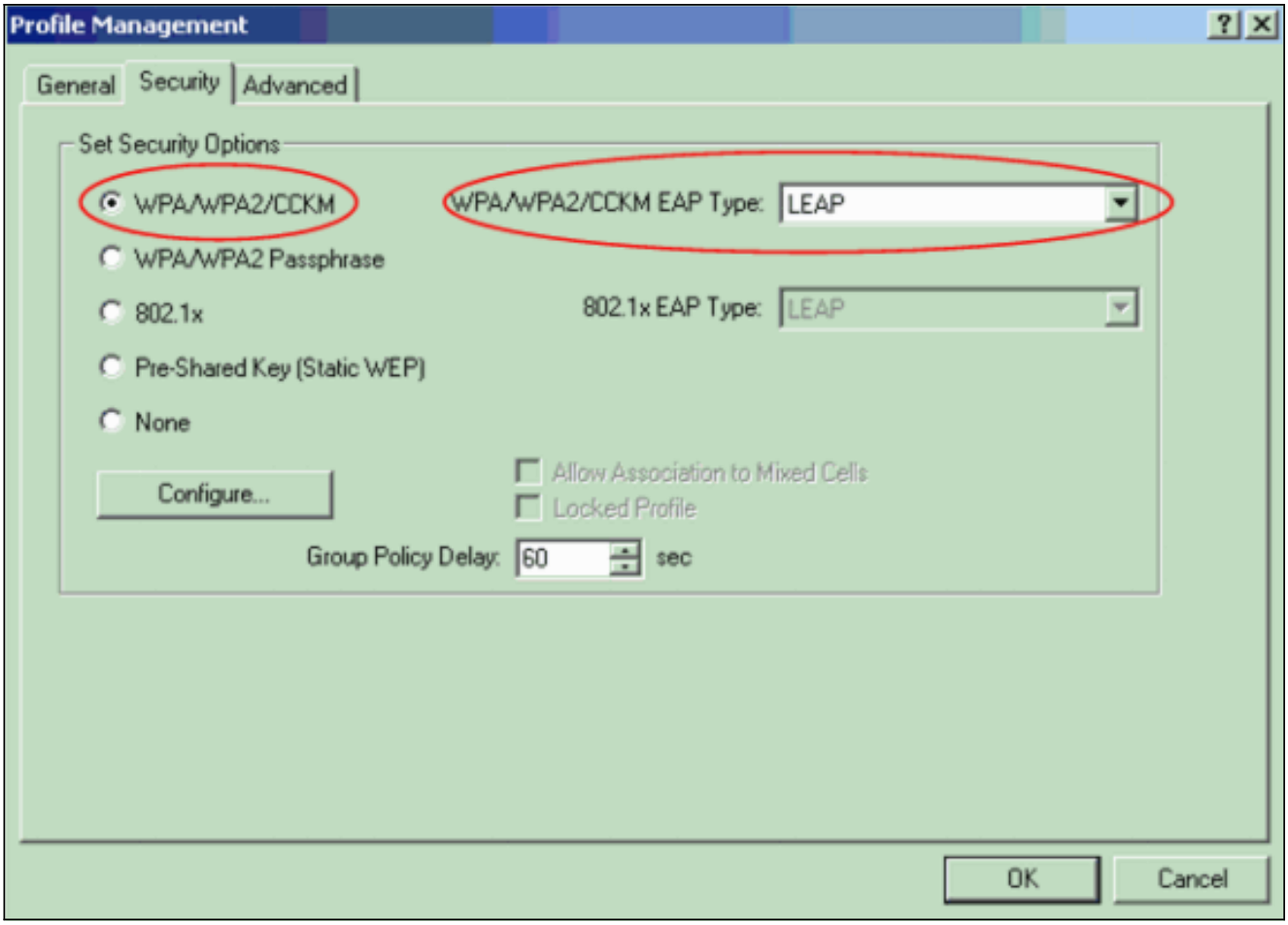
Nota: Este documento utiliza un adaptador del cliente del Aironet 802.11a/b/g que funcione con el firmware 2.5 y explique la configuración del adaptador del cliente con la versión de ADU 2.5.

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 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

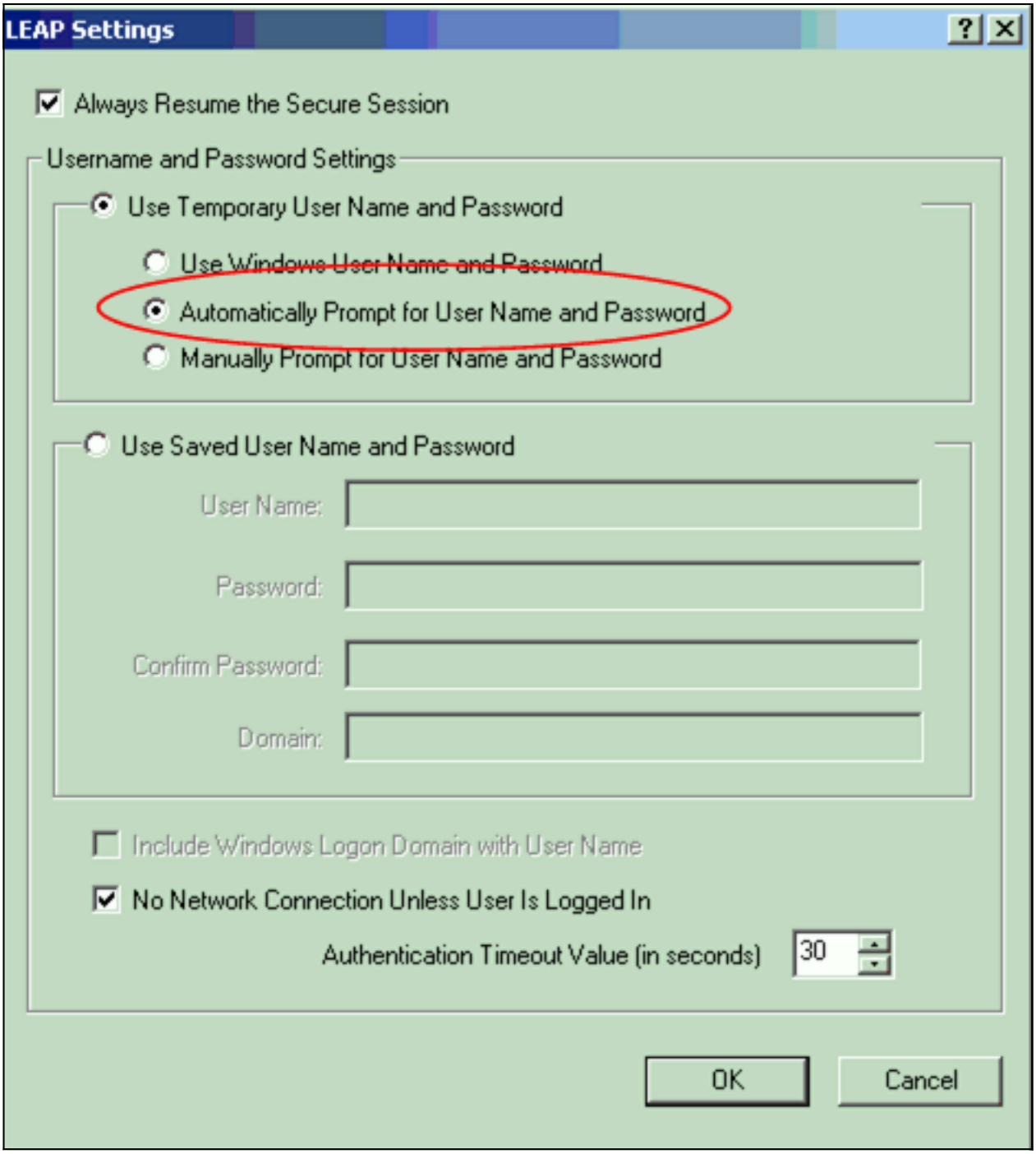
el
WPA2.



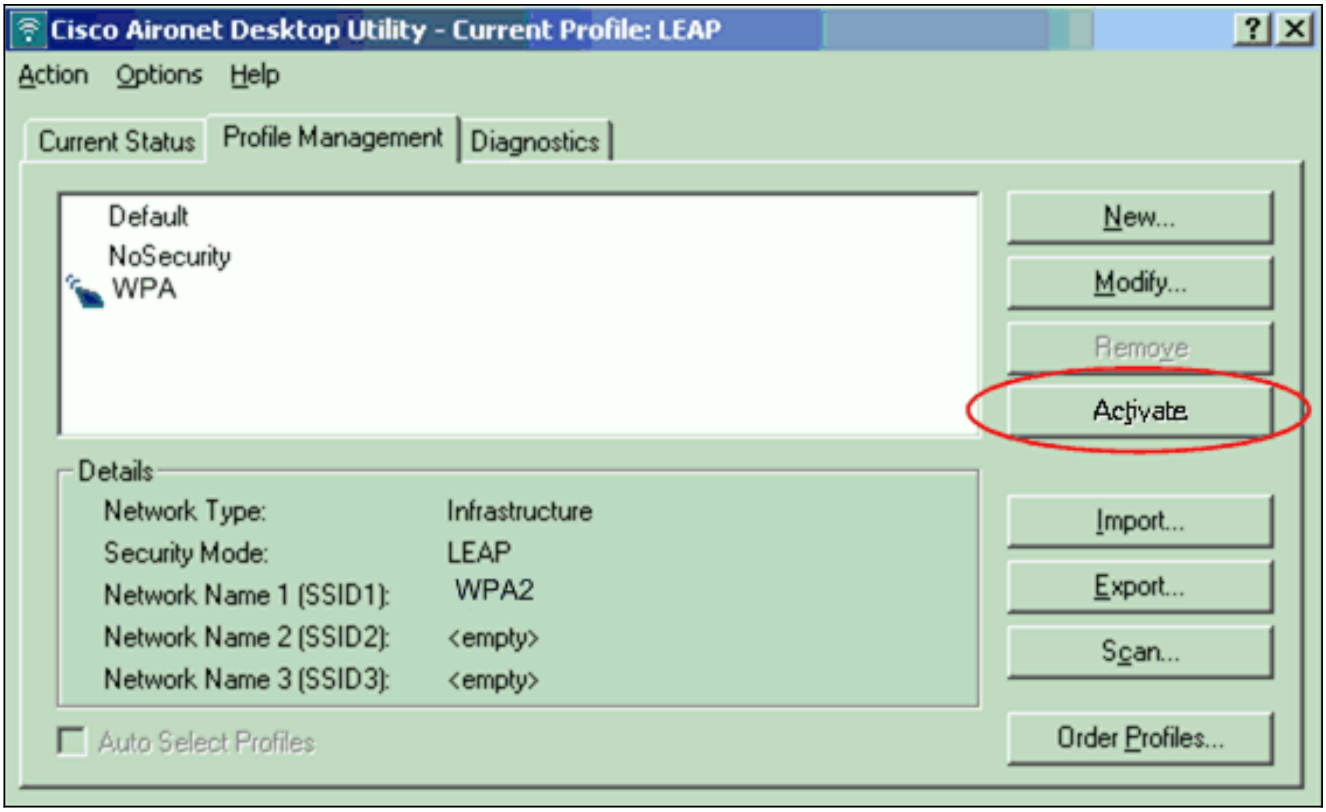
2. Haga clic la **ficha de seguridad**, haga clic **WPA/WPA2/CCKM**, y elija el **SALTO** WPA/WPA2/CCKM del menú EAP Type (Tipo EAP).Esta acción habilita el WPA o el WPA2, cualquiera usted configura en el
AP.



3. **Configuración del** tecleo 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 indica automáticamente para el Nombre de usuario y la contraseña. Esta opción le permite para ingresar manualmente el Nombre de usuario y la contraseña cuando ocurre la autenticación LEAP.



5. Haga Click en OK para salir la ventana de administración del perfil.
6. El tecleo **activa** para habilitar este perfil en el adaptador del cliente.

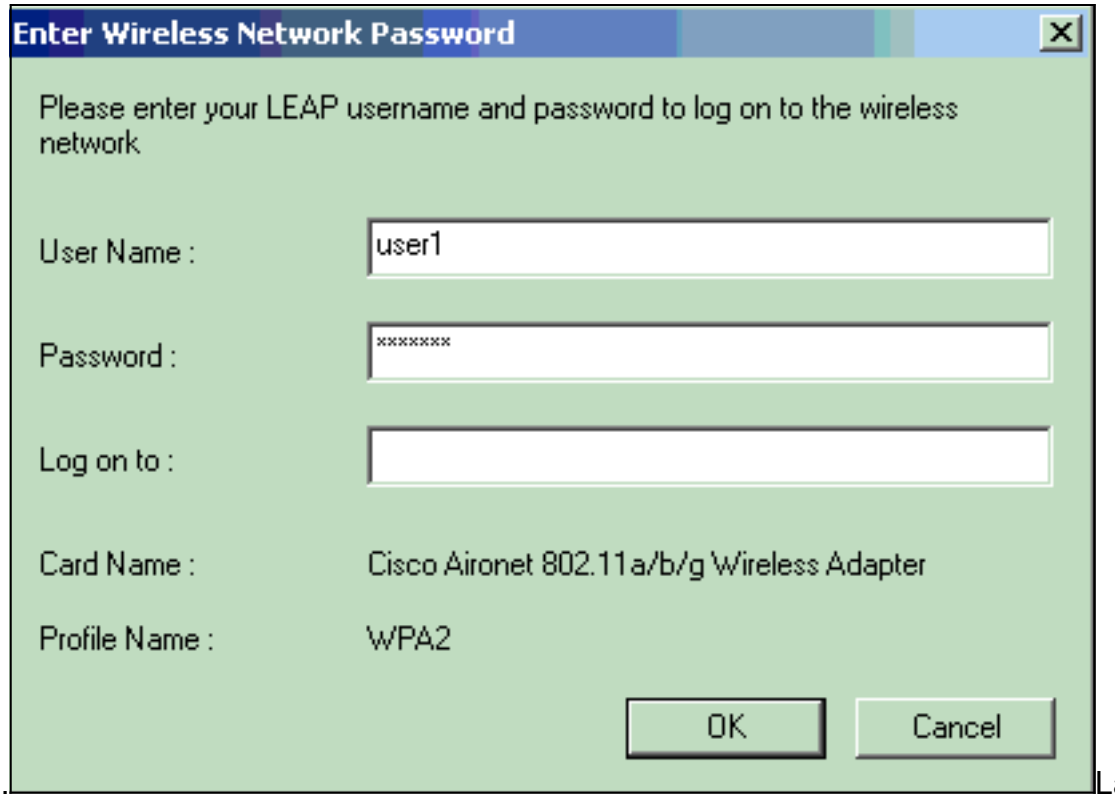


Nota: Si usted utiliza la configuración de la Tecnología inalámbrica cero de Microsoft (WZC) para configurar el adaptador del cliente, por abandono, el WPA2 no está disponible con WZC. Así pues, para permitir que los clientes WZC-habilitados ejecuten el WPA2, usted debe instalar un arreglo caliente para 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

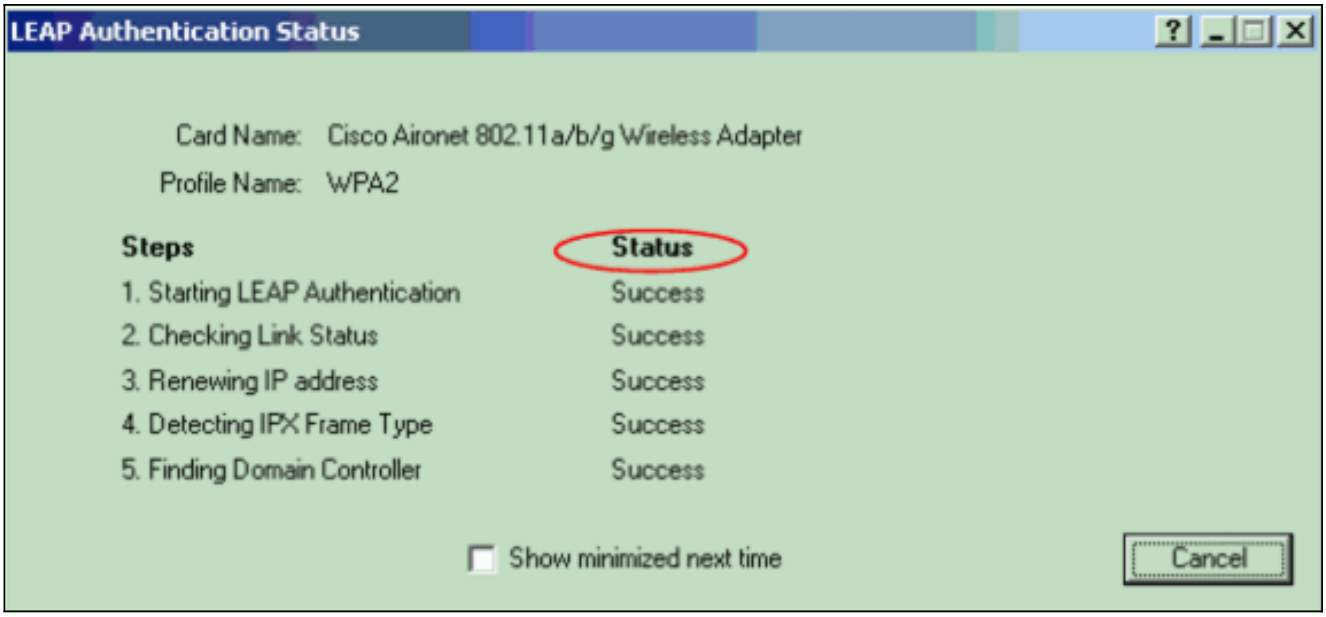
Use esta sección para confirmar que su configuración funciona correctamente.

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



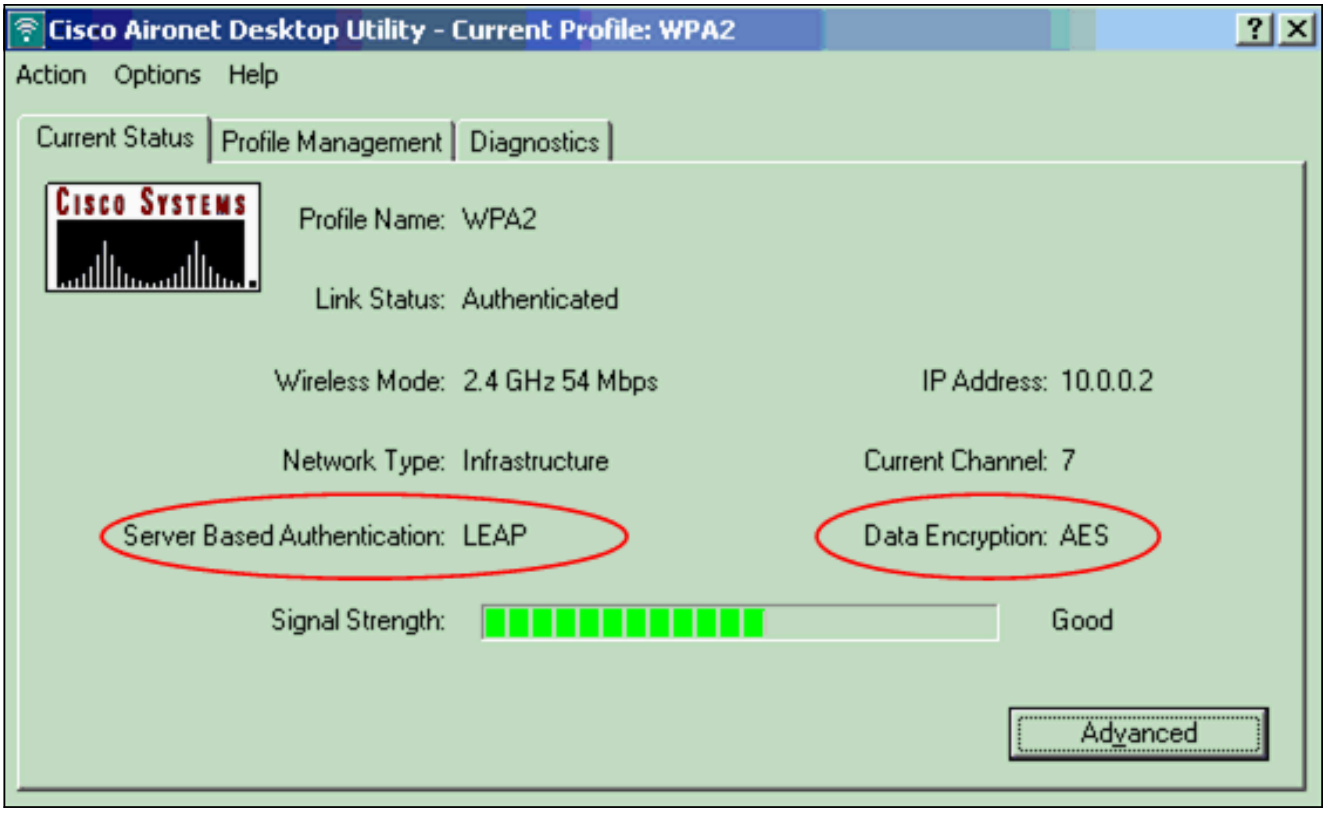
contraseña. La próxima ventana es estatus de la autenticación LEAP. Esta fase verifica los credenciales de usuario contra el servidor de RADIUS local.

2. Marque la área de estado para ver el resultado de la autenticación.



Cuando la autenticación es acertada, el cliente conecta con el Wireless LAN.

3. Marque el estado actual ADU para verificar que el cliente utiliza la encripción AES y la autenticación LEAP.Esto muestra que usted ha implementado el WPA2 con la autenticación LEAP y la encripción AES en el WLAN.



4. Marque la orden del login del evento del 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.

Configuración en el modo personal

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

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

Configuración de la red

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

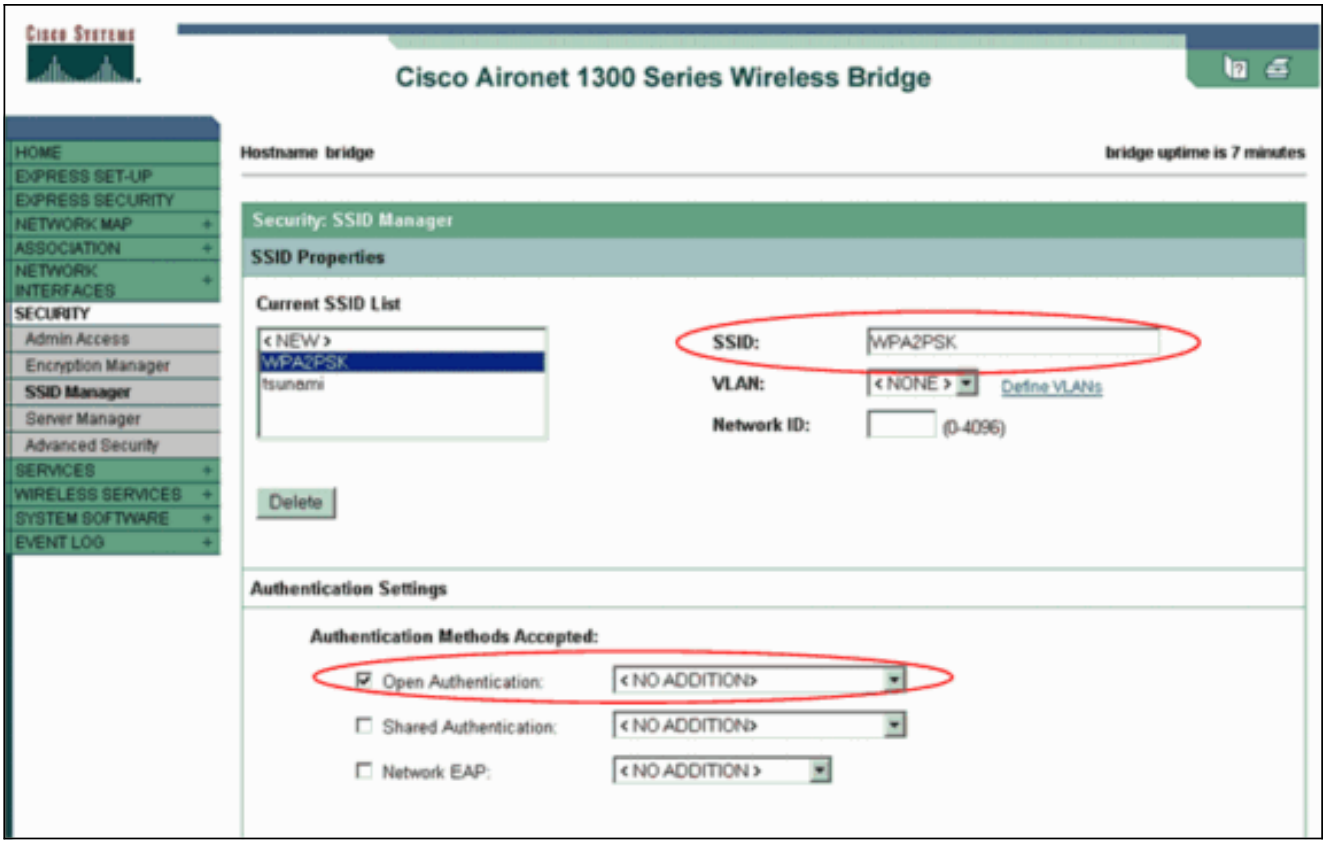
Configure el AP

Complete estos pasos:

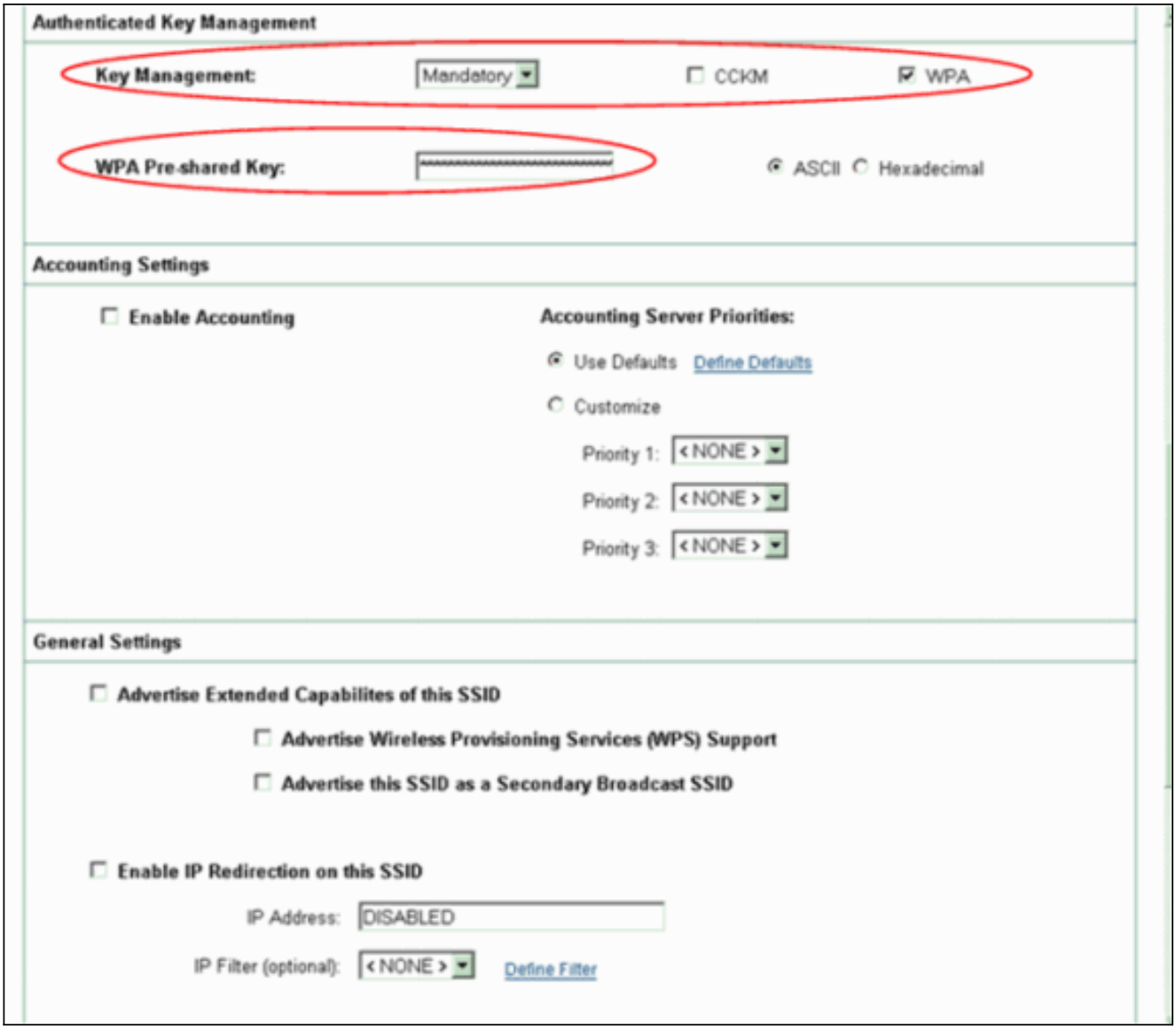
1. Elija al **administrador de la Seguridad > del cifrado** en el menú a la izquierda y complete estos pasos:Del menú de la cifra, elija el **CCMP AES**.Esta opción habilita la encripción AES con el uso del modo contrario con el CCMP.

Haga clic en Apply (Aplicar).

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



Navegue hacia 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**.Marque la **casilla de verificación WPA** a la derecha.



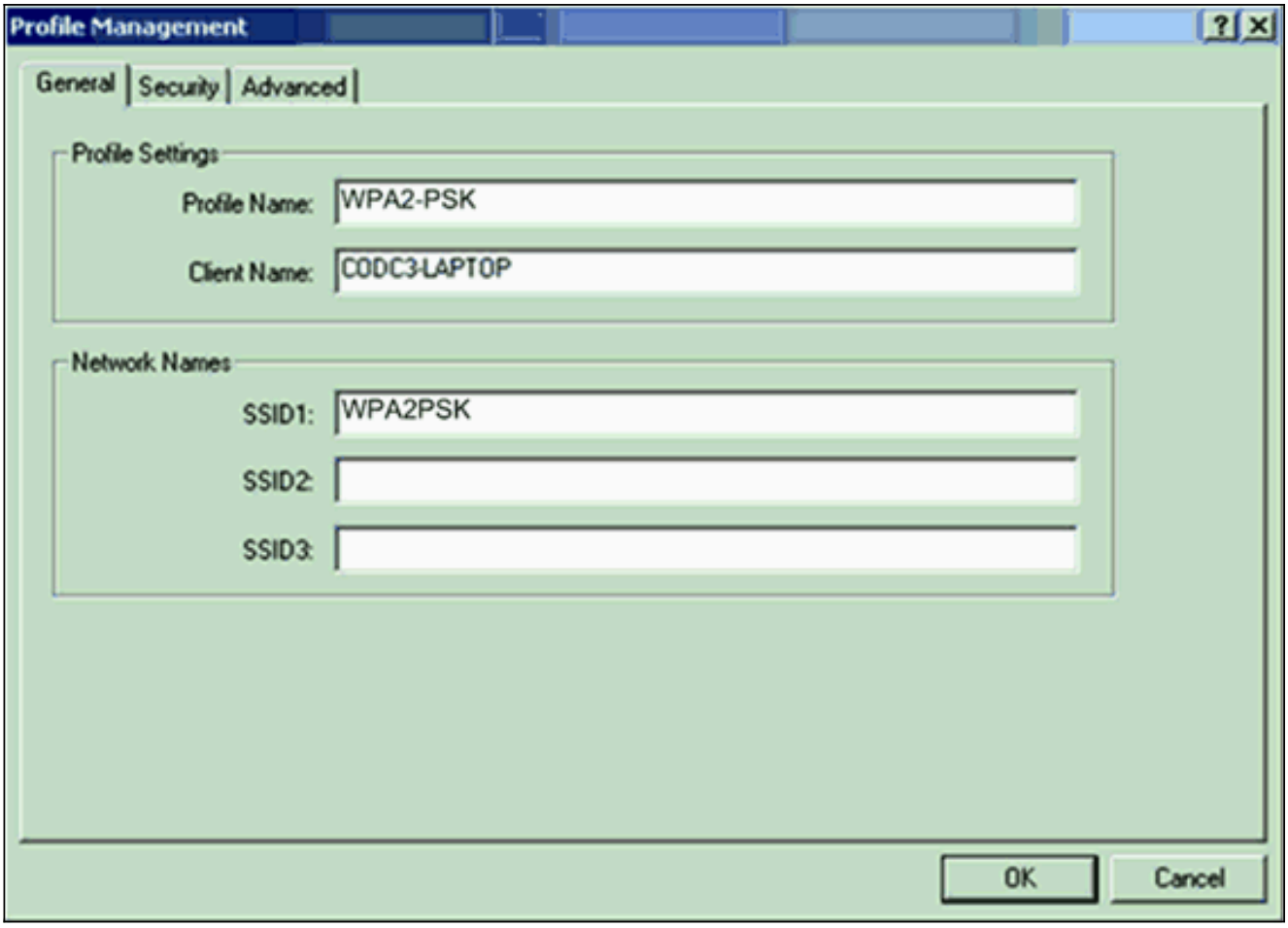
Ingrese la clave secreta compartida PSK WPA o la clave del passphrase del PSK WPA.Esta clave debe hacer juego la clave del PSK WPA que usted configura en el adaptador del cliente.Haga clic en Apply (Aplicar).

El AP puede ahora recibir los pedidos de autenticación de los clientes de red inalámbrica.

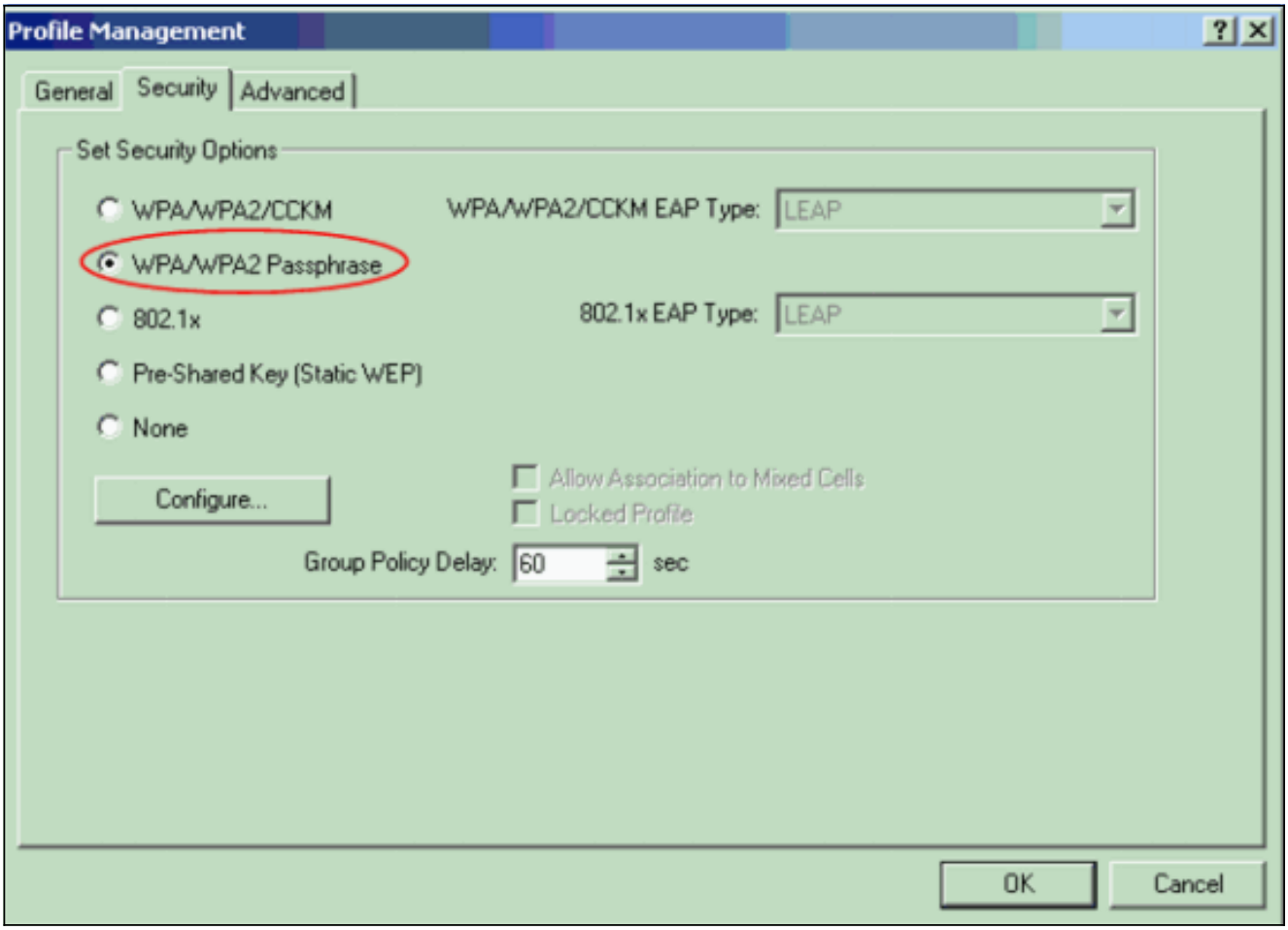
Configure el adaptador del cliente

Complete estos pasos:

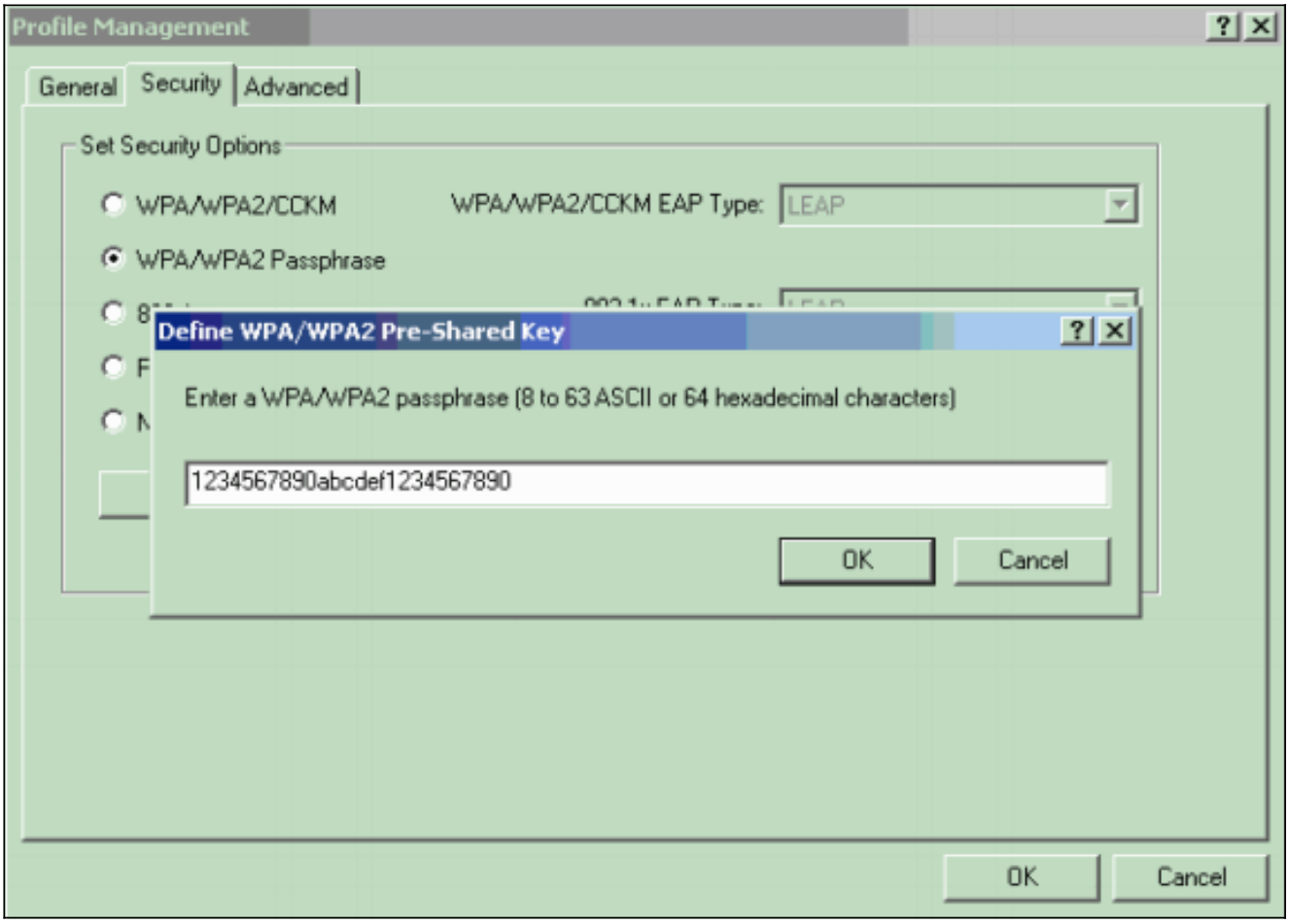
1. En la ventana de administración del perfil en el ADU, haga clic **nuevo** para crear un nuevo perfil.Visualizaciones de una nueva ventana donde usted puede fijar la configuración para WPA2PSK el modo de operación. Conforme a la ficha general, ingrese el nombre del perfil y el SSID que el adaptador 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 el passphrase**.Esta acción habilita o el PSK WPA o WPA2PSK, cualquiera usted configura en el AP.



3. Haga clic en Configure (Configurar).De la definición las visualizaciones de la ventana de la clave previamente compartida WPA/WPA2.
4. Obtenga WPA/WPA2 el passphrase de su administrador de sistema y ingrese el passphrase en WPA/WPA2 el campo del passphrase.Obtenga el passphrase para el AP en una red de infraestructura o el passphrase 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 passphrase del adaptador del cliente WPA/WPA2 debe hacer juego el passphrase del AP con el cual usted planea
comunicar.



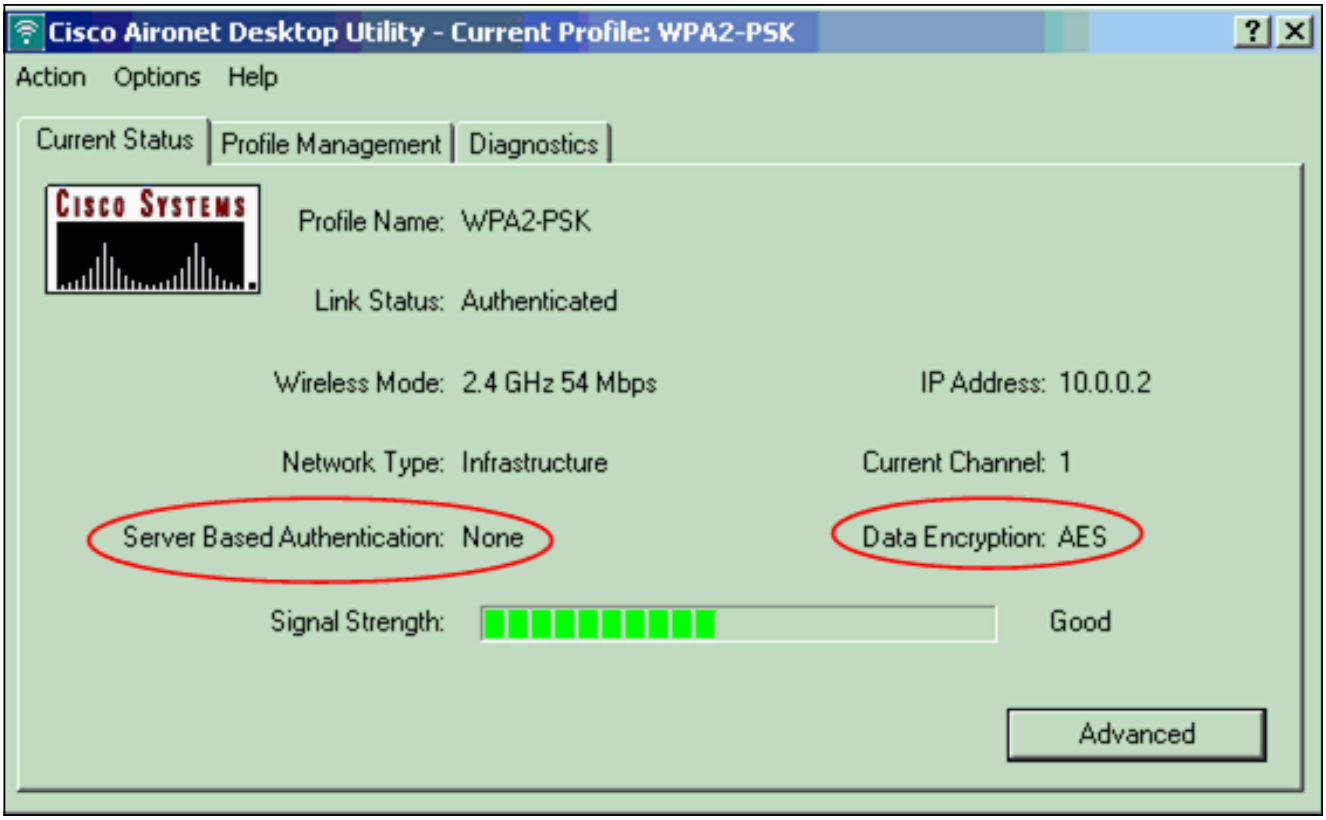
5. Haga Click en OK para salvar el passphrase y volver a la ventana de administración del perfil.

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 el passphrase WPA2 (PSK) y proporciona el acceso a la red inalámbrica (WLAN).

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



2. Marque la orden del login del evento del 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 WPA
- WPA2 - Acceso protegido Wi-Fi 2
- Cuál es operación de modo mezclada WPA, y cómo lo hago configurela en mi AP
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems