Ejemplo de Configuración de Wi-Fi Protected Access 2 (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: WPA funciona con protocolo de autenticación extensible (EAP).

Prerequisites

Requirements

Asegúrese de tener conocimientos básicos sobre estos temas antes de intentar esta

configuración:

- WPA
- Soluciones de seguridad de WLAN**Nota:** Refiérase a Descripción General de Cisco Aironet Wireless LAN Security para obtener información sobre las soluciones de seguridad Cisco WLAN.

Componentes Utilizados

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

- Punto de acceso (AP) Cisco Aironet 1310G que ejecuta Cisco IOS® Software Release 12.3(2)JA
- Adaptador cliente Aironet 802.11a/b/g CB21AG que ejecuta firmware 2.5
- Aironet Desktop Utility (ADU) que ejecuta firmware 2.5

Nota: El software de adaptador cliente Aironet CB21AG e PI21AG es incompatible con otro software de adaptador de cliente Aironet. Debe utilizar la ADU con tarjetas CB21AG e PI21AG, y debe utilizar la Aironet Client Utility (ACU) todos los demás adaptadores cliente Aironet. Refiérase a Instalación del Adaptador del Cliente para obtener más información sobre cómo instalar la tarjeta CB21AG y ADU.

Nota: Este documento utiliza un AP/bridge que tiene una antena integrada. Si utiliza un AP/bridge que requiere una antena externa, asegúrese de que las antenas estén conectadas al AP/bridge. De lo contrario, el AP/bridge no puede conectarse a la red inalámbrica. Algunos modelos AP/bridge vienen con antenas integradas, mientras que otros necesitan una antena externa para el funcionamiento general. Para obtener información sobre los modelos AP/bridge que vienen con antenas internas o externas, consulte la guía de pedidos/guía de productos del dispositivo apropiado.

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

WPA es una solución de seguridad basada en estándares de Wi-Fi Alliance que aborda las vulnerabilidades de las WLAN nativas. WPA proporciona protección de datos mejorada y control de acceso para los sistemas WLAN. WPA aborda todas las vulnerabilidades de privacidad equivalente a conexión con cables (WEP) conocidas en la implementación de seguridad IEEE 802.11 original y ofrece una solución de seguridad inmediata para las WLAN en entornos empresariales y de oficinas pequeñas, oficinas domésticas (SOHO).

WPA 2 es la última generación de seguridad Wi-Fi. WPA 2 es la implementación interoperable de Wi-Fi Alliance del estándar IEEE 802.11i ratificado. WPA 2 implementa el algoritmo de cifrado

estándar de cifrado avanzado (AES) recomendado por el Instituto Nacional de Normas y Tecnología (NIST) con el uso del modo de contador con el protocolo de código de autenticación de mensajes de encadenamiento de bloques de cifrado (CCMP). AES Counter Mode es un cifrado de bloques que cifra bloques de datos de 128 bits a la vez con una clave de cifrado de 128 bits. El algoritmo CCMP produce un código de integridad de mensaje (MIC) que proporciona autenticación de origen de datos e integridad de datos para la trama inalámbrica.

Nota: CCMP también se conoce como CBC-MAC.

WPA 2 ofrece un mayor nivel de seguridad que WPA porque AES ofrece una encriptación más fiable que el protocolo de integridad de clave temporal (TKIP). TKIP es el algoritmo de encriptación que utiliza WPA. WPA 2 crea nuevas claves de sesión en cada asociación. Las claves de cifrado que se utilizan para cada cliente en la red son únicas y específicas para ese cliente. En última instancia, cada paquete que se envía por el aire se cifra con una clave única. La seguridad se mejora con el uso de una clave de cifrado nueva y única porque no hay reutilización de claves. WPA todavía se considera seguro y TKIP no se ha roto. Sin embargo, Cisco recomienda que los clientes realicen la transición a WPA 2 lo antes posible.

WPA y WPA 2 admiten dos modos de funcionamiento:

- Modo empresarial
- Modo personal

Este documento analiza la implementación de estos dos modos con WPA 2.

Compatibilidad con WPA 2 con equipos Cisco Aironet

WPA 2 es compatible con este equipo:

- Aironet serie 1130AG AP y serie 1230AG AP
- Aironet serie 1100 AP
- Aironet serie 1200 AP
- Aironet serie 1300 AP

Nota: Equipe estos AP con radios 802.11g y use Cisco IOS Software Release 12.3(2)JA o posterior.

WPA 2 y AES también son compatibles con:

- Módulos de radio Aironet serie 1200 con los números de pieza AIR-RM21A y AIR-RM22A**Nota:** El módulo de radio Aironet 1200 con el número de pieza AIR-RM20A no admite WPA 2.
- Aironet 802.11a/b/g Client Adapters con firmware versión 2.5

Nota: Los productos Cisco Aironet serie 350 no admiten WPA 2 porque sus radios carecen de soporte AES.

Nota: Los puentes inalámbricos Cisco Aironet serie 1400 no admiten WPA 2 o AES.

Configuración en modo de empresa

El término **modo empresarial** hace referencia a los productos que se han probado para ser interoperables tanto en los modos de operación Pre-Shared Key (PSK) como IEEE 802.1x para la

autenticación. El estándar 802.1x se considera más seguro que cualquiera de los marcos de autenticación heredados debido a su flexibilidad para admitir una variedad de mecanismos de autenticación y algoritmos de cifrado más fuertes. WPA 2 en modo empresarial realiza la autenticación en dos fases. La configuración de la autenticación abierta ocurre en la primera fase. La segunda fase es la autenticación 802.1x con uno de los métodos EAP. AES proporciona el mecanismo de cifrado.

En el modo empresarial, los clientes y los servidores de autenticación se autentican entre sí con el uso de un método de autenticación EAP, y el cliente y el servidor generan una clave maestra de pares (PMK). Con WPA 2, el servidor genera el PMK dinámicamente y pasa el PMK al AP.

Esta sección trata sobre la configuración necesaria para implementar WPA 2 en el modo de operación empresarial.

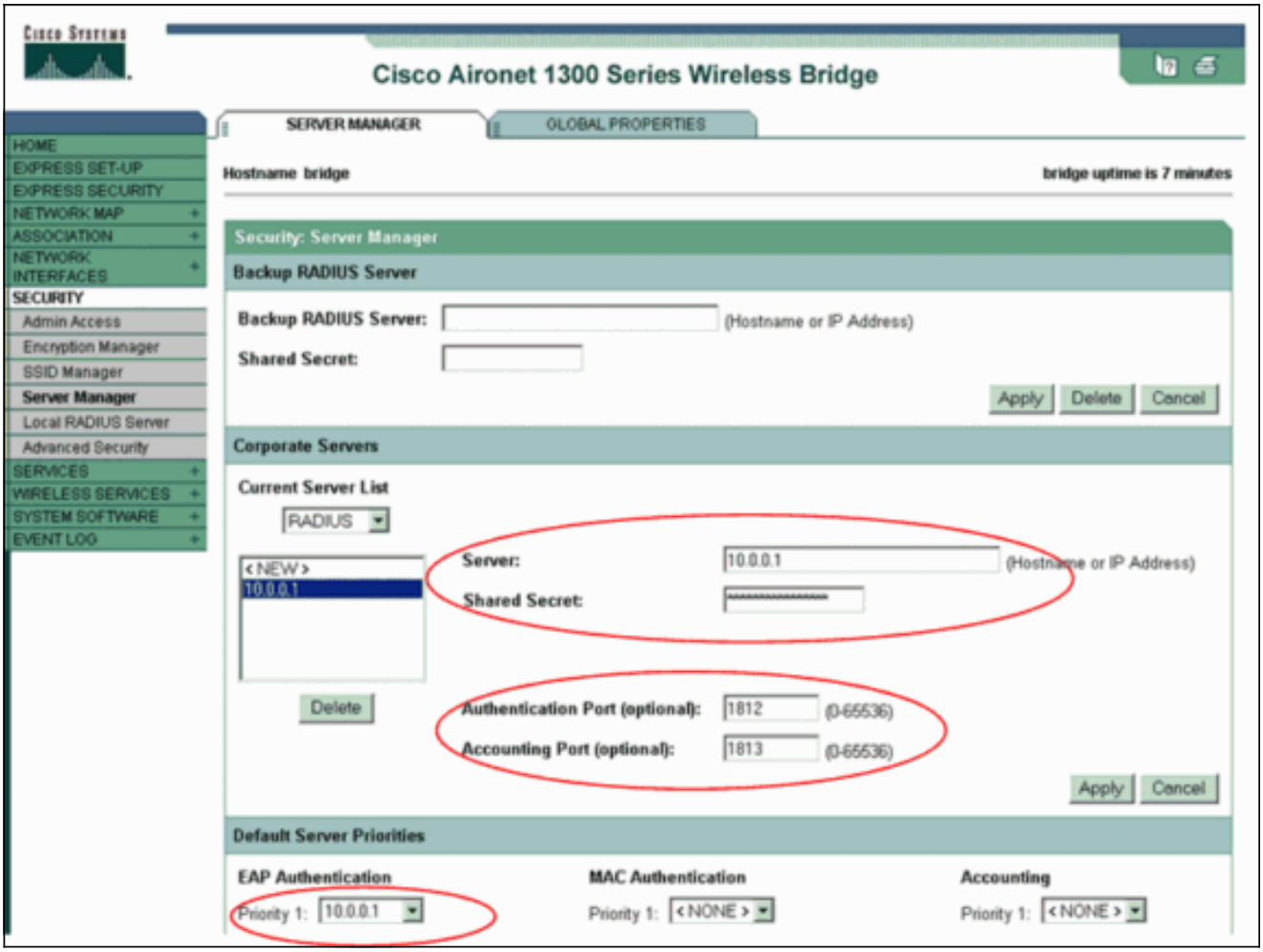
Configuración de la red

En esta configuración, un Aironet 1310G AP/Bridge que ejecuta Cisco Lightweight Extensible Authentication Protocol (LEAP) autentica a un usuario con un adaptador cliente compatible con WPA 2. La administración de claves se produce con el uso de WPA 2, en el que se configura el cifrado AES-CCMP. El AP se configura como un servidor RADIUS local que ejecuta la autenticación LEAP. Debe configurar el adaptador del cliente y el AP para implementar esta configuración. Las secciones Configure el AP y Configure el Adaptador del Cliente muestran la configuración en el AP y el adaptador del cliente.

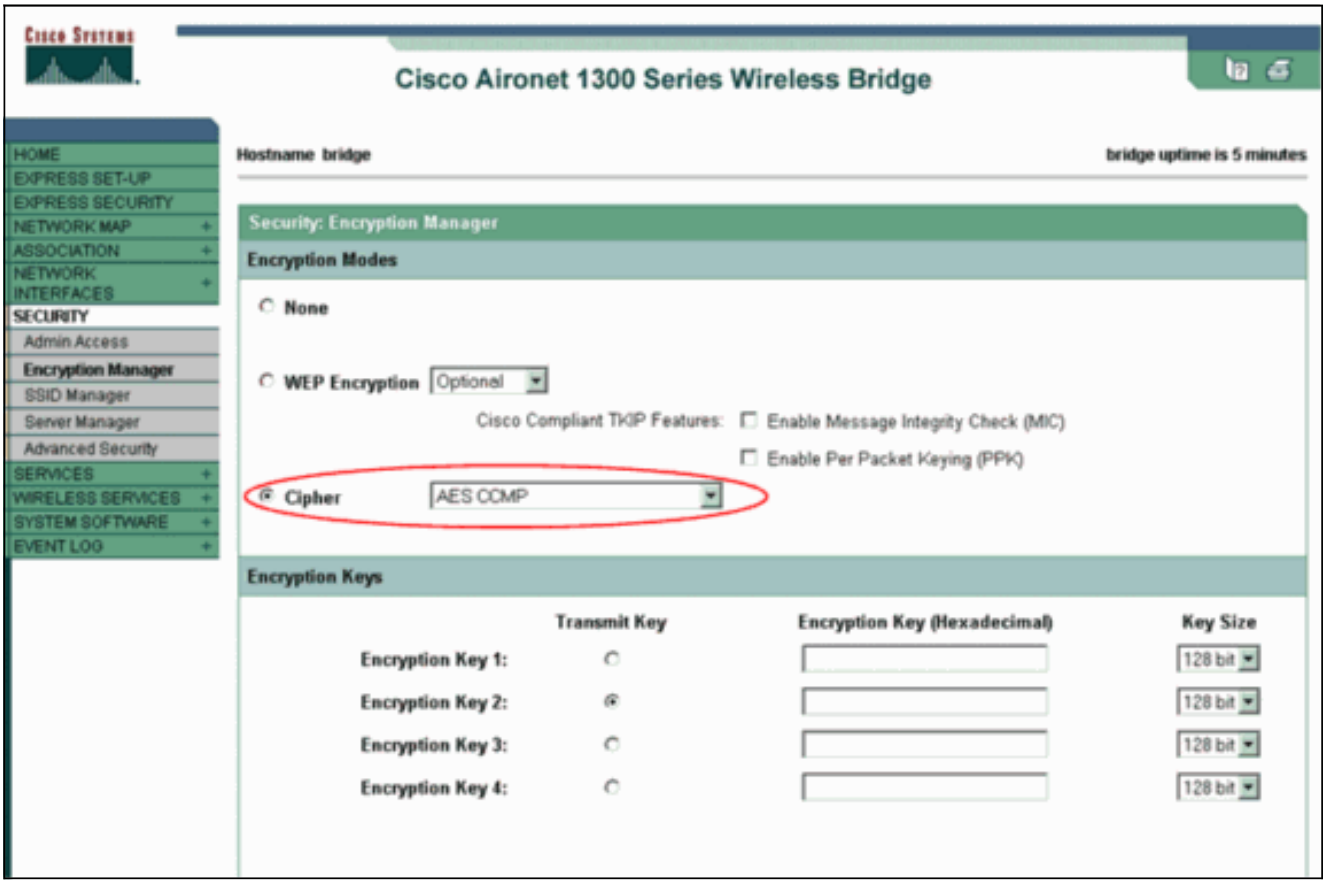
Configure el AP

Complete estos pasos para configurar el AP usando la GUI:

1. Configure el AP como un servidor RADIUS local que ejecuta la autenticación LEAP.Elija **Security > Server Manager** en el menú de la izquierda y defina la dirección IP, los puertos y el secreto compartido del servidor RADIUS.Debido a que esta configuración configura el AP como un servidor RADIUS local, utilice la dirección IP del AP. Utilice los puertos 1812 y 1813 para el funcionamiento del servidor RADIUS local.En el área Prioridades de servidor predeterminadas, defina la prioridad de autenticación EAP predeterminada como 10.0.0.1.**Nota:** 10.0.0.1 es el servidor RADIUS
   local.

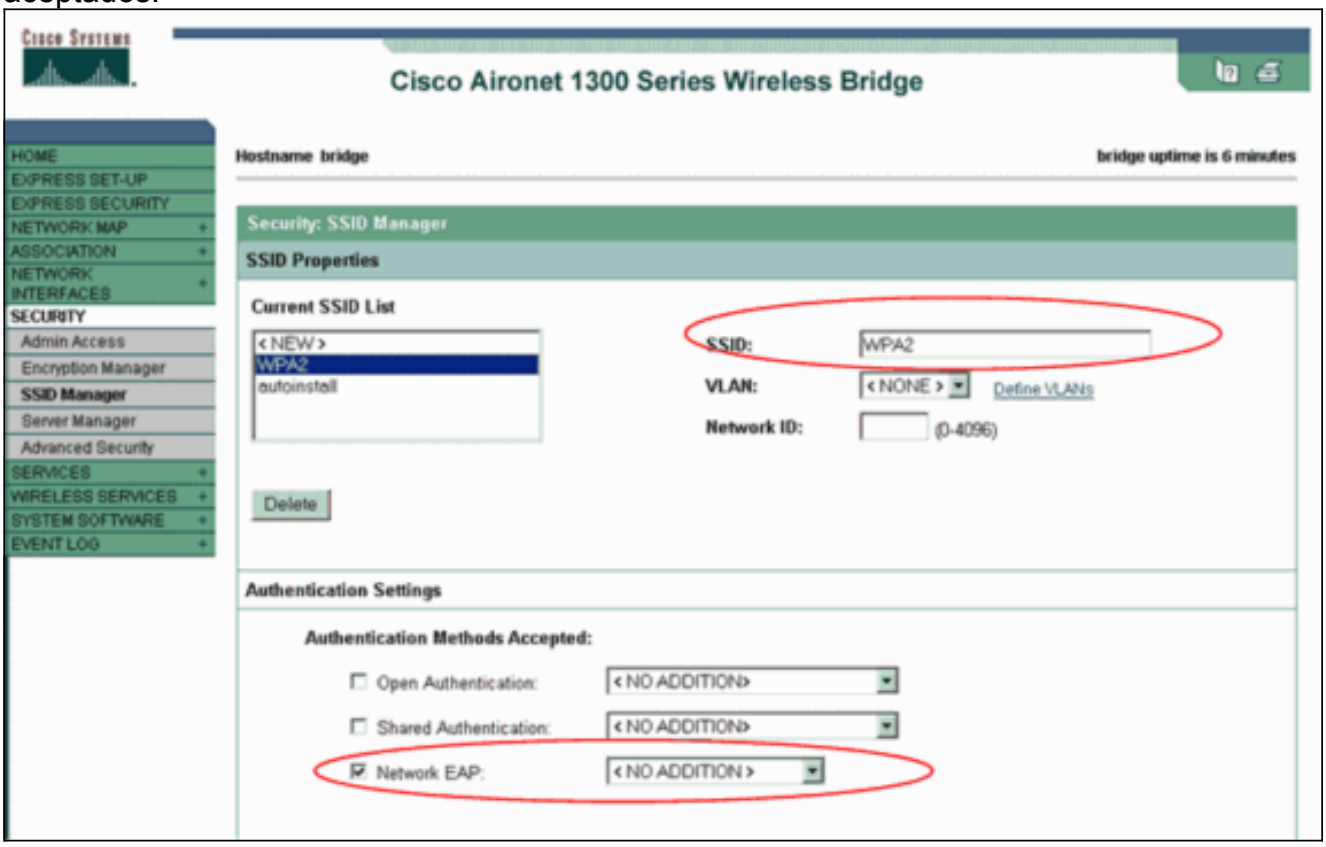


2. Elija **Security > Encryption Manager** en el menú de la izquierda y complete estos pasos:En el menú Cipher, elija **AES CCMP**.Esta opción habilita el cifrado AES con el uso del Modo de contador con CBC-
MAC.



Haga clic en Apply (Aplicar).

3. Elija **Security > SSID Manager** y cree un nuevo Service Set Identifier (SSID) para su uso con WPA 2.Marque la casilla de verificación **EAP de red** en el área Métodos de autenticación aceptados.

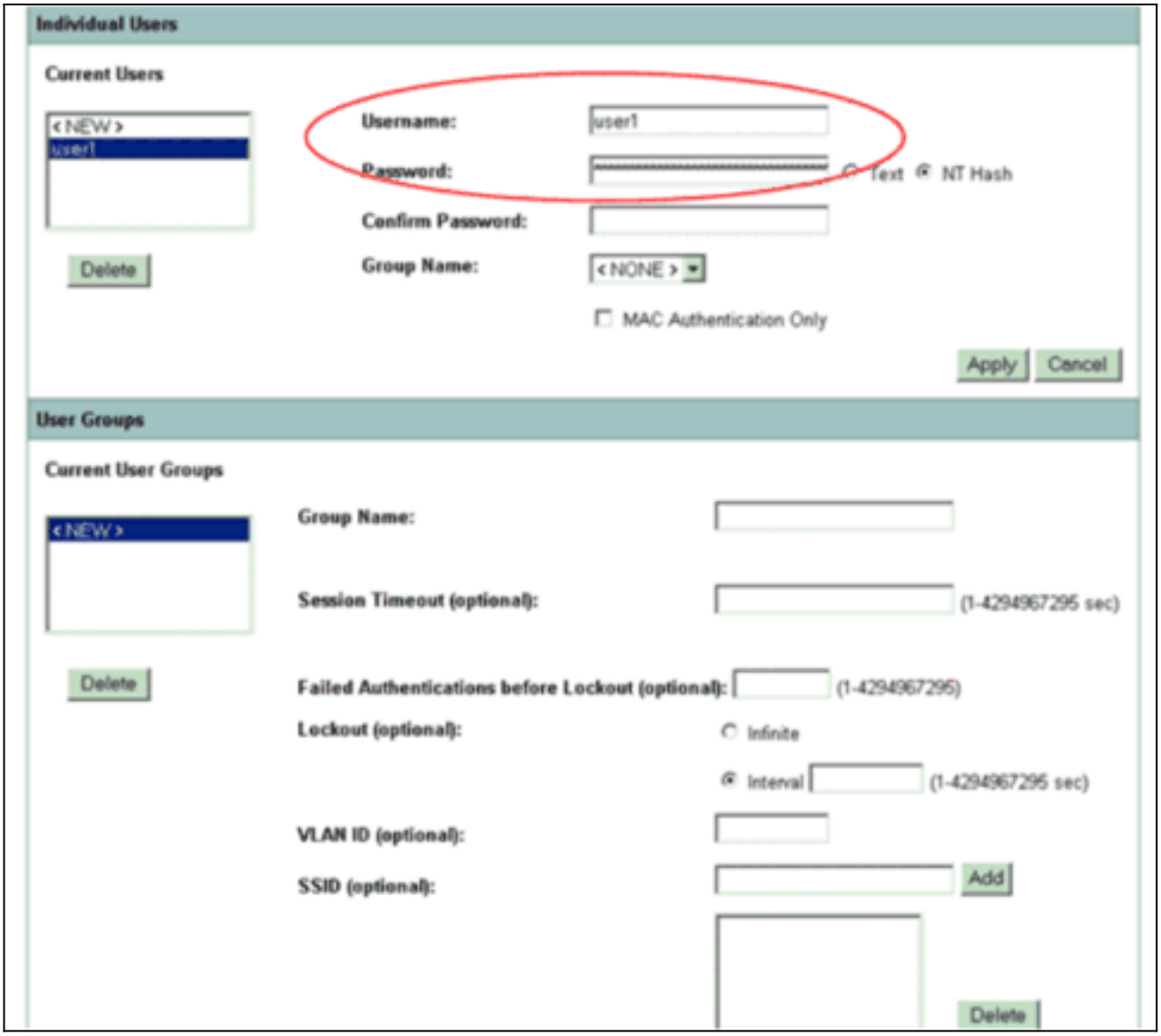


Nota: Utilice estas pautas cuando configure el tipo de autenticación en la interfaz de radio:Clientes de Cisco: utilice EAP de red.Clientes de terceros (que incluyen productos compatibles con Cisco Compatible Extensions [CCX]): utilice la autenticación abierta con EAP.Una combinación de clientes de Cisco y de terceros: elija tanto EAP de red como Autenticación abierta con EAP.Desplácese por la ventana Security SSID Manager (Administrador de SSID de seguridad) hasta el área Authenticated Key Management (Administración de claves autenticadas) y complete estos pasos:En el menú Key Management (Administración de claves), elija **Obligatorio**.Marque la casilla de verificación **WPA** de la derecha.Haga clic en Apply (Aplicar).**Nota:** La definición de VLAN es opcional. Si define VLAN, los dispositivos cliente que se asocian con el uso de este SSID se agrupan en la VLAN. Consulte Configuración de VLAN para obtener más información sobre cómo implementar
VLAN.

4. Elija **Security > Local Radius Server** y complete estos pasos:Haga clic en la pestaña **Configuración general** situada en la parte superior de la ventana.Marque la casilla de verificación **LEAP** y haga clic en **Aplicar**.En el área Network Access Servers (Servidores de acceso a la red), defina la dirección IP y el secreto compartido del servidor RADIUS.Para el servidor RADIUS local, utilice la dirección IP del
AP.

Haga clic en Apply (Aplicar).

5. Desplácese por la ventana Configuración general hasta el área Usuarios individuales y defina los usuarios individuales.La definición de los grupos de usuarios es opcional.



Esta configuración define un usuario con el nombre "user1" y una contraseña. Además, la configuración selecciona el hash NT para la contraseña. Después de completar el procedimiento en esta sección, el AP está listo para aceptar las solicitudes 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
```

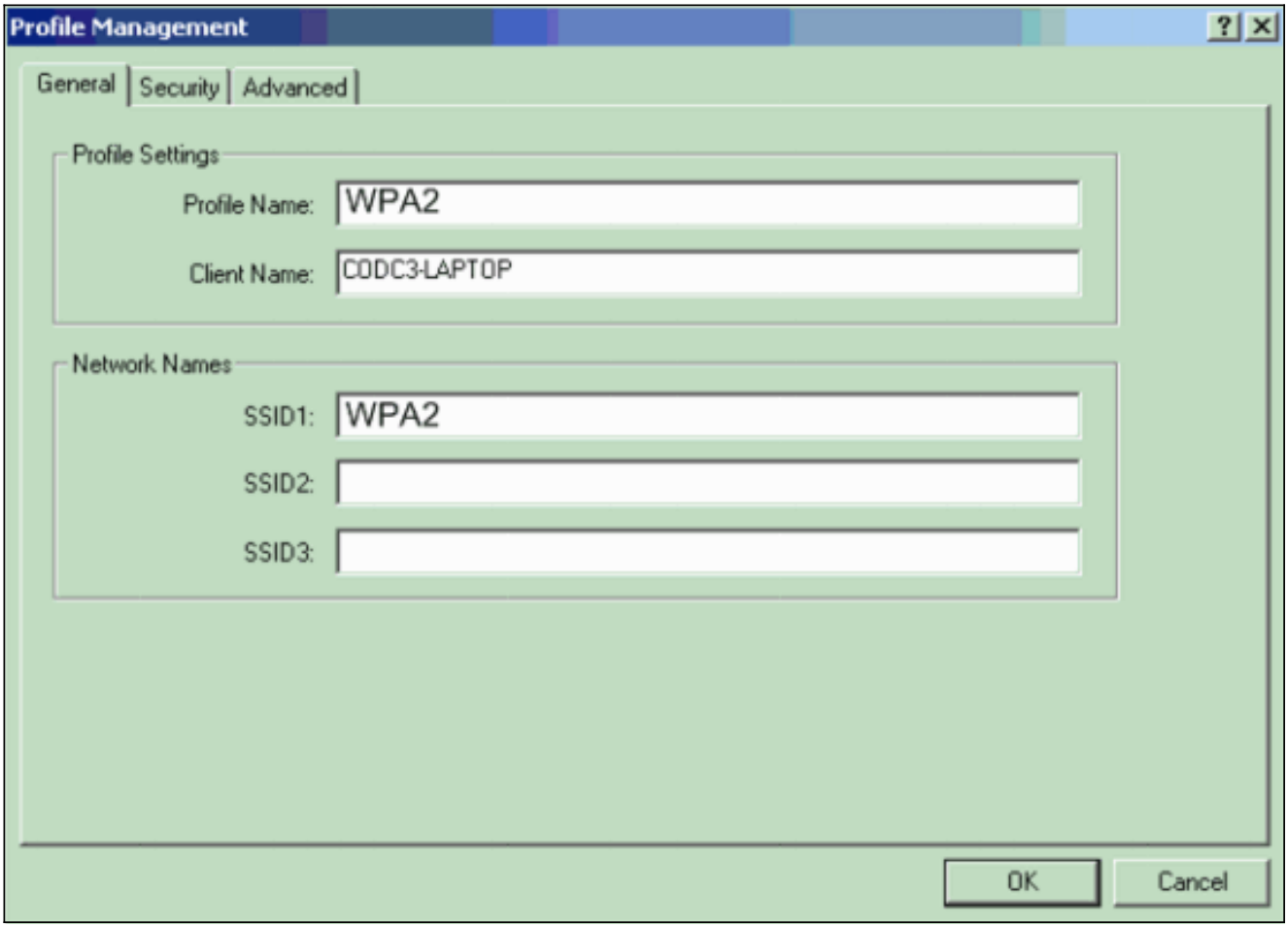
```
Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key
!---This step is optional !--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be 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
```

Configuración del adaptador del cliente

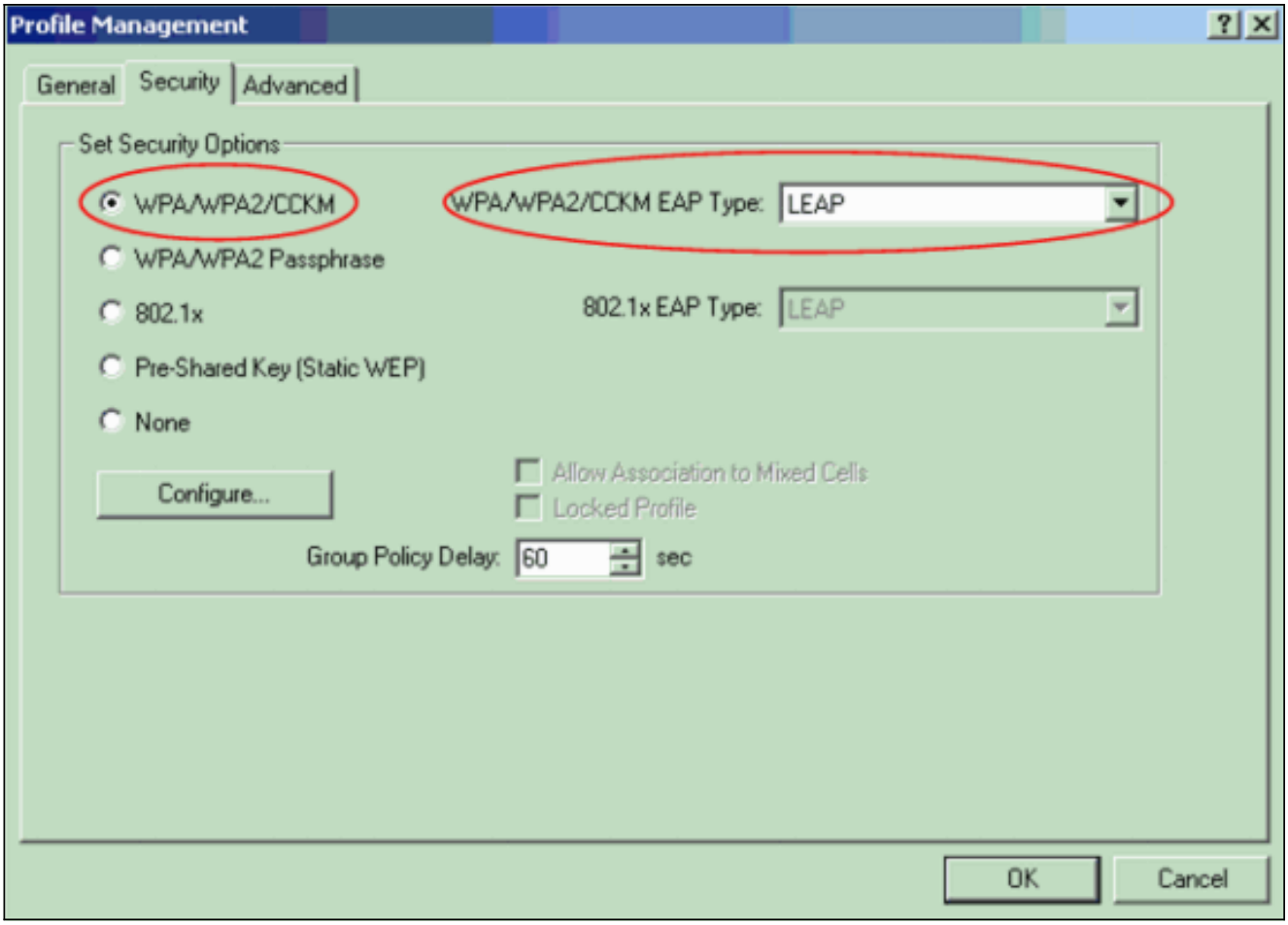
Complete estos pasos:

Nota: Este documento utiliza un Aironet 802.11a/b/g Client Adapter que ejecuta firmware 2.5 y explica la configuración del adaptador del cliente con ADU versión 2.5.

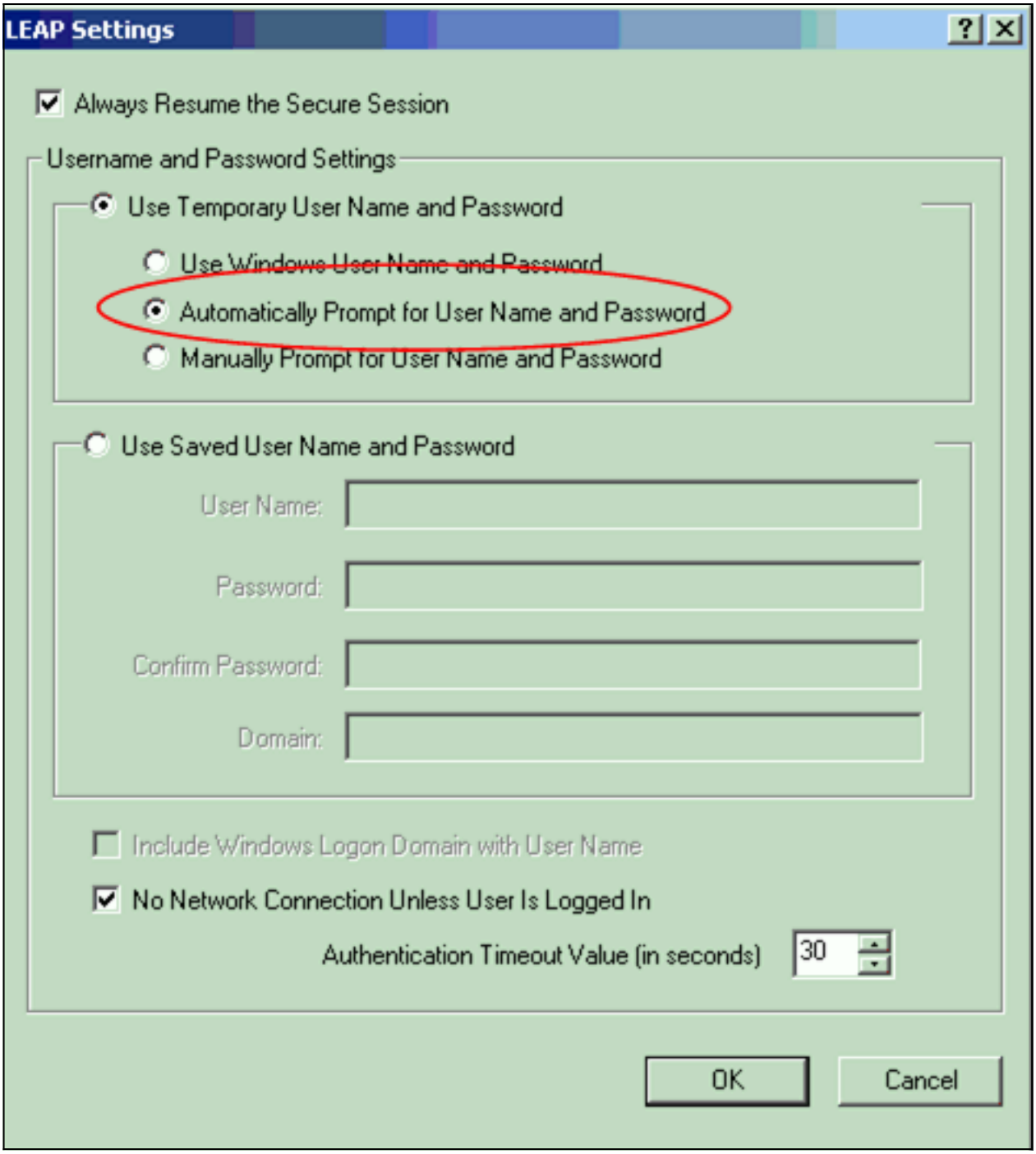
1. En la ventana Profile Management de la ADU, haga clic en **New** para crear un perfil nuevo.Se muestra una nueva ventana en la que puede establecer la configuración para el funcionamiento del modo empresarial WPA 2. En la ficha General, introduzca el nombre del perfil y el SSID que utilizará el adaptador del cliente.En este ejemplo, el nombre del perfil y el SSID son WPA2:**Nota:** El SSID debe coincidir con el SSID que configuró en el AP para WPA 2.



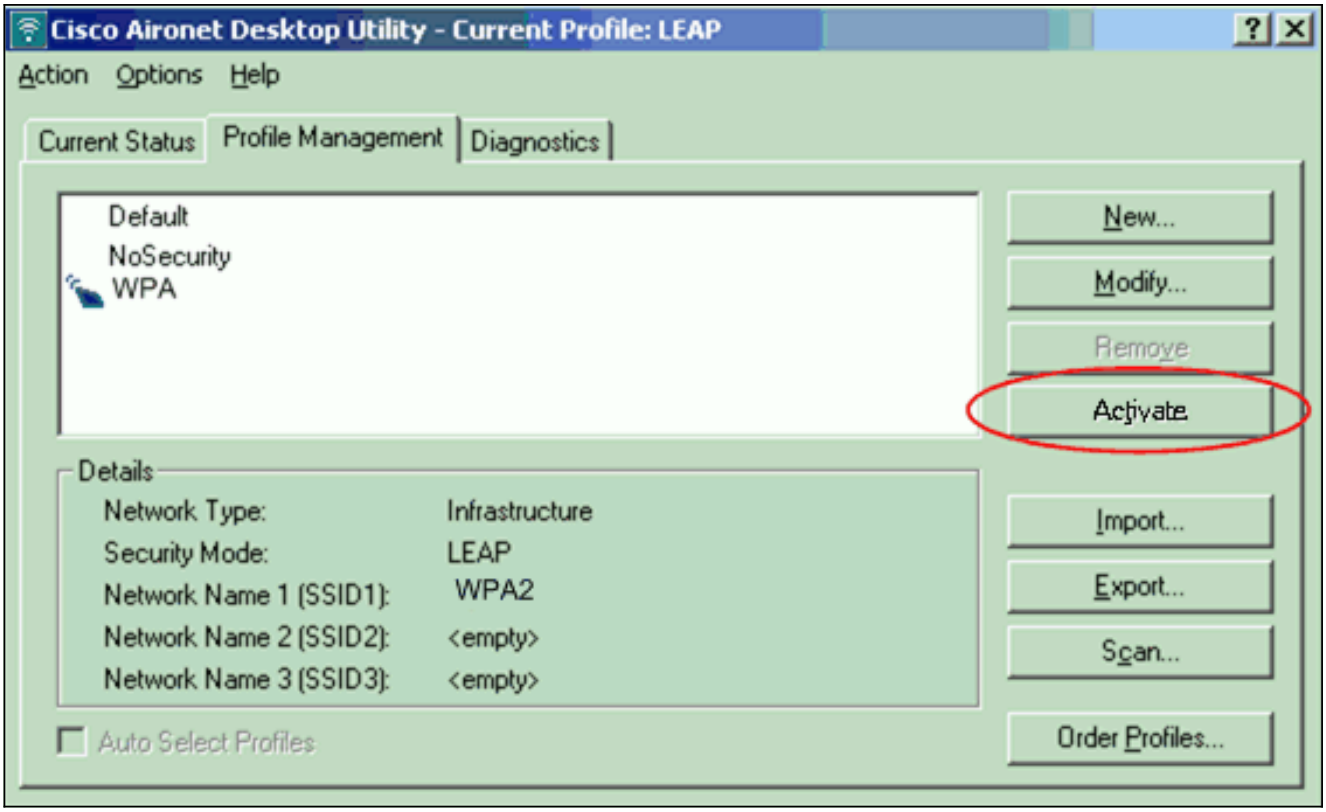
2. Haga clic en la ficha **Seguridad**, haga clic en **WPA/WPA2/CCKM** y elija **LEAP** en el menú WPA/WPA2/CCKM EAP Type .Esta acción habilita WPA o WPA 2, cualquiera que sea la configuración en el
AP.



3. Haga clic en **Configurar** para definir la configuración de LEAP.
4. Elija el nombre de usuario y la configuración de contraseña adecuados, según los requisitos, y haga clic en **Aceptar**.Esta configuración elige la opción Solicitud automática de nombre de usuario y contraseña. Esta opción permite introducir manualmente el nombre de usuario y la contraseña cuando se realiza la autenticación
LEAP.



5. Haga clic en **Aceptar** para salir de la ventana Administración de perfiles.
6. Haga clic en **Activar** para habilitar este perfil en el adaptador del cliente.

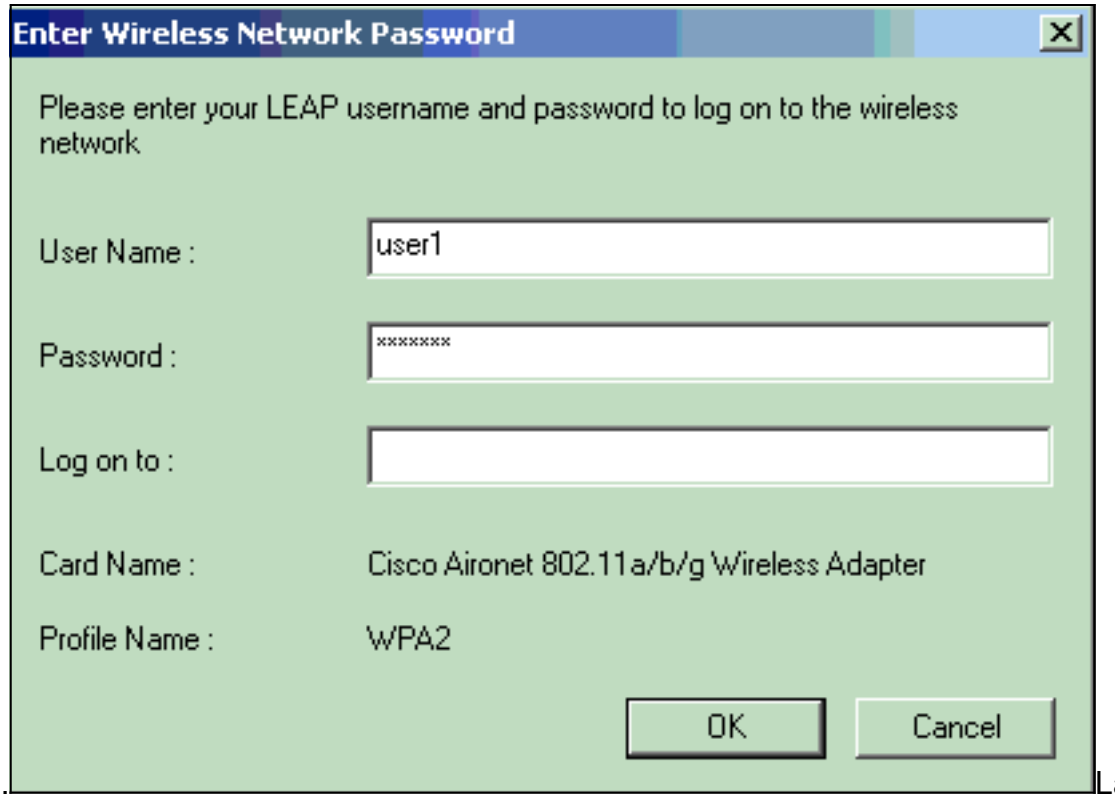


Nota: Si utiliza Microsoft Wireless Zero Configuration (WZC) para configurar el adaptador del cliente, de forma predeterminada, WPA 2 no está disponible con WZC. Por lo tanto, para permitir que los clientes habilitados para WZC ejecuten WPA 2, debe instalar un hot fix para Microsoft Windows XP. Refiérase al Centro de descarga de Microsoft - Actualización para Windows XP (KB893357) para la instalación.Después de instalar el hot fix, puede configurar WPA 2 con WZC.

Verificación

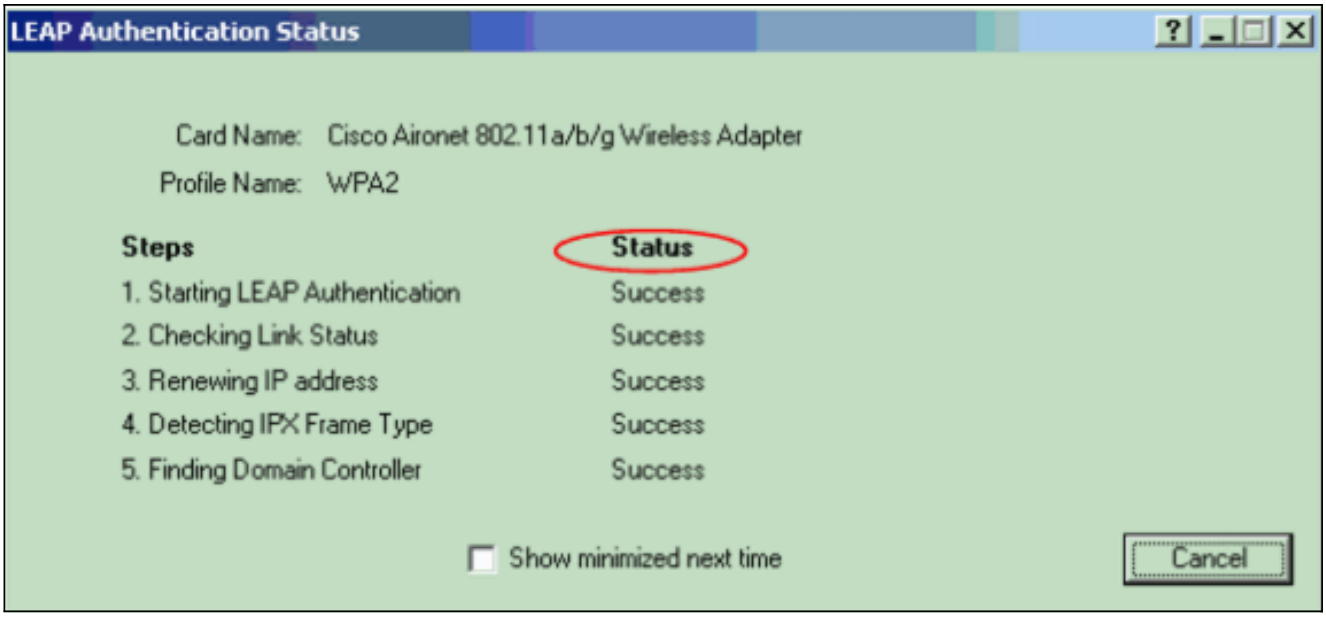
Use esta sección para confirmar que su configuración funciona correctamente.

1. Cuando aparezca la ventana Introducir contraseña de red inalámbrica, introduzca el nombre de usuario y la



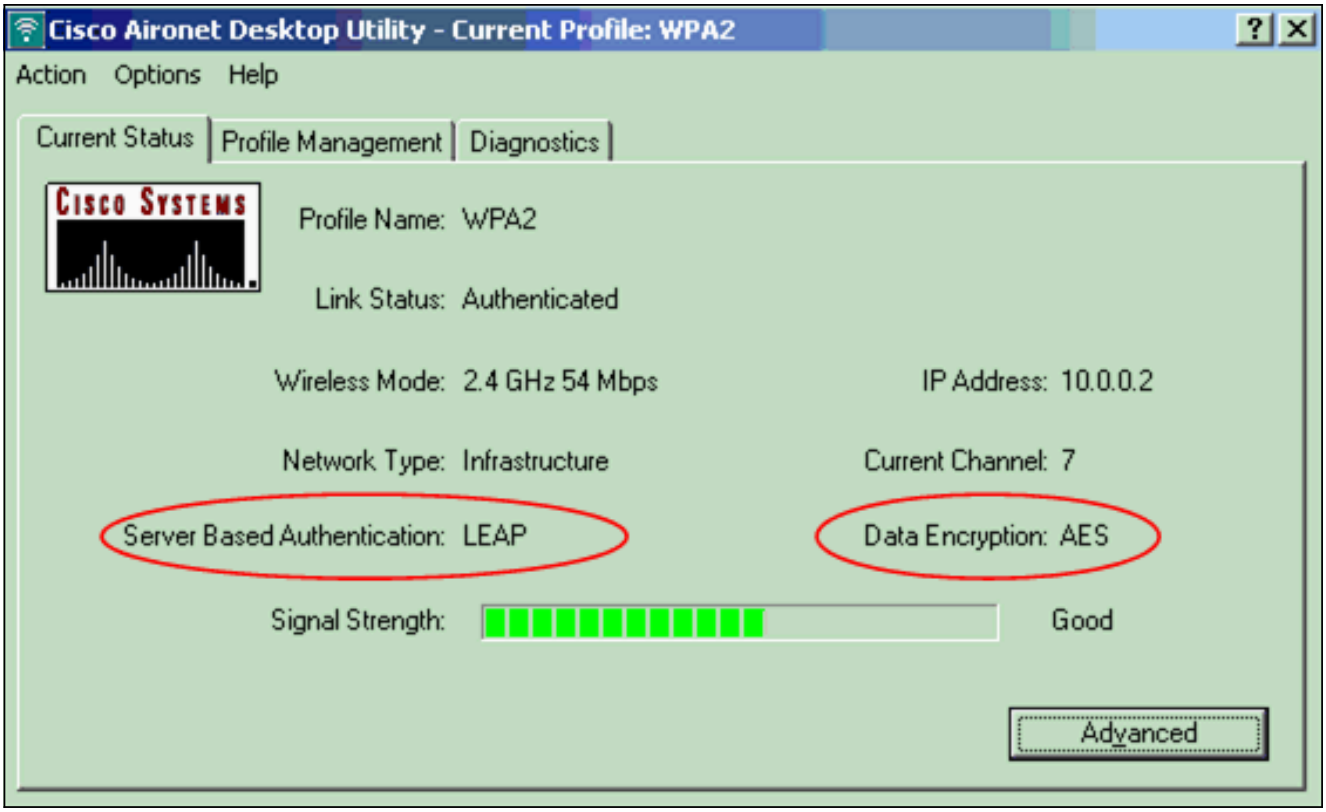
contraseña.La siguiente ventana es LEAP Authentication Status (Estado de autenticación de LEAP). Esta fase verifica las credenciales del usuario en el servidor RADIUS local.

2. Verifique el área Estado para ver el resultado de la autenticación.



Cuando la autenticación se realiza correctamente, el cliente se conecta a la LAN inalámbrica.

3. Verifique el estado actual de ADU para verificar que el cliente utiliza el cifrado AES y la autenticación LEAP.Esto muestra que ha implementado WPA 2 con autenticación LEAP y cifrado AES en la WLAN.



4. Verifique el Registro de Eventos de AP/bridge para verificar que el cliente se ha autenticado exitosamente con WPA
   2.

Troubleshoot

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

Configuración en modo personal

El término **modo personal** hace referencia a los productos que se han probado para ser interoperables en el modo de operación de sólo PSK para la autenticación. Este modo requiere la

configuración manual de un PSK en el AP y los clientes. PSK autentica a los usuarios a través de una contraseña, o código de identificación, tanto en la estación cliente como en el AP. No es necesario un servidor de autenticación. Un cliente puede obtener acceso a la red solamente si la contraseña del cliente coincide con la contraseña AP. La contraseña también proporciona el material de codificación que TKIP o AES utiliza para generar una clave de cifrado para el cifrado de los paquetes de datos. El modo personal está dirigido a entornos SOHO y no se considera seguro para entornos empresariales. Esta sección proporciona la configuración que necesita para implementar WPA 2 en el modo de funcionamiento personal.

Configuración de la red

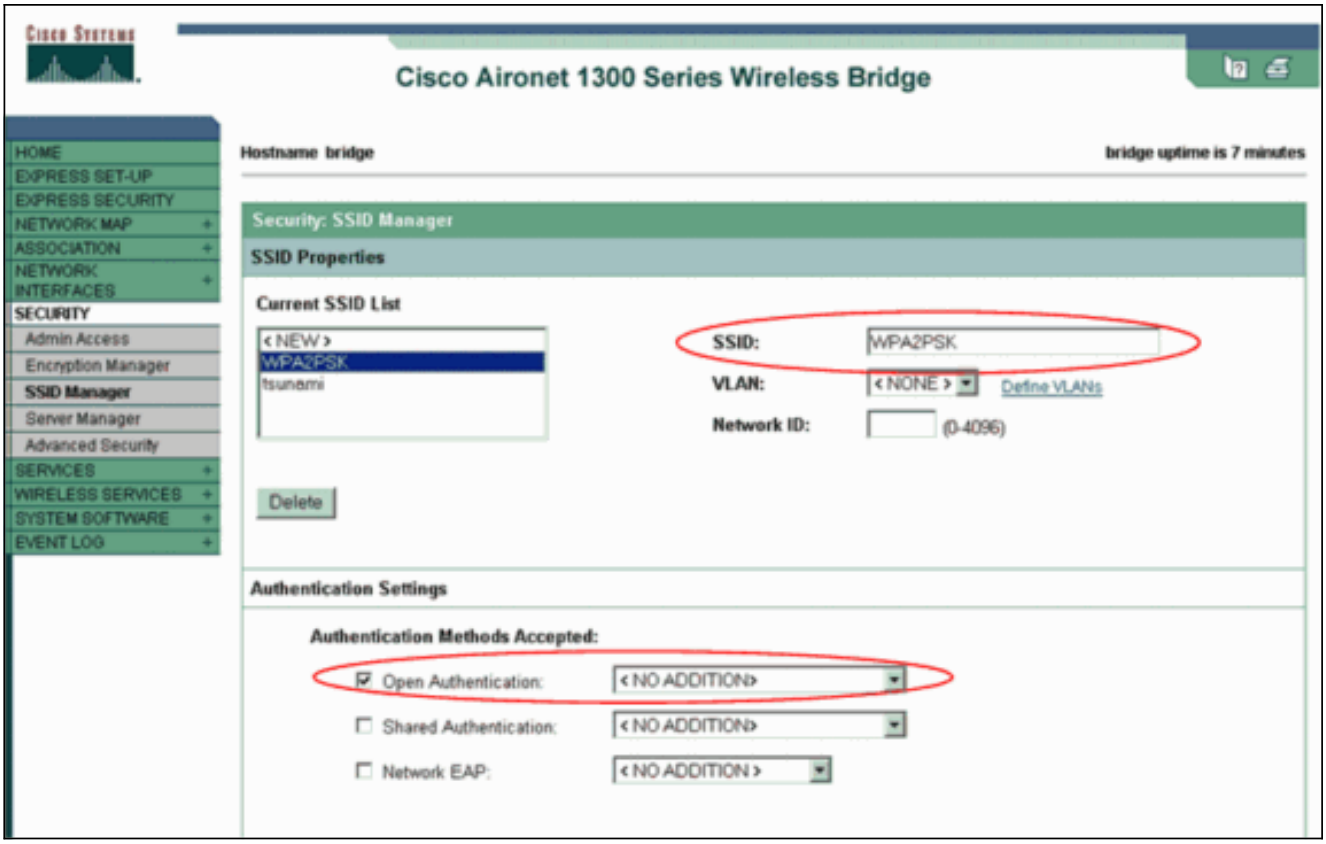
En esta configuración, un usuario con un adaptador cliente compatible con WPA 2 se autentica en un Aironet 1310G AP/Bridge. La administración de claves se produce con el uso de WPA 2 PSK, con el cifrado AES-CCMP configurado. Las secciones Configure el AP y Configure el Adaptador del Cliente muestran la configuración en el AP y el adaptador del cliente.

Configure el AP

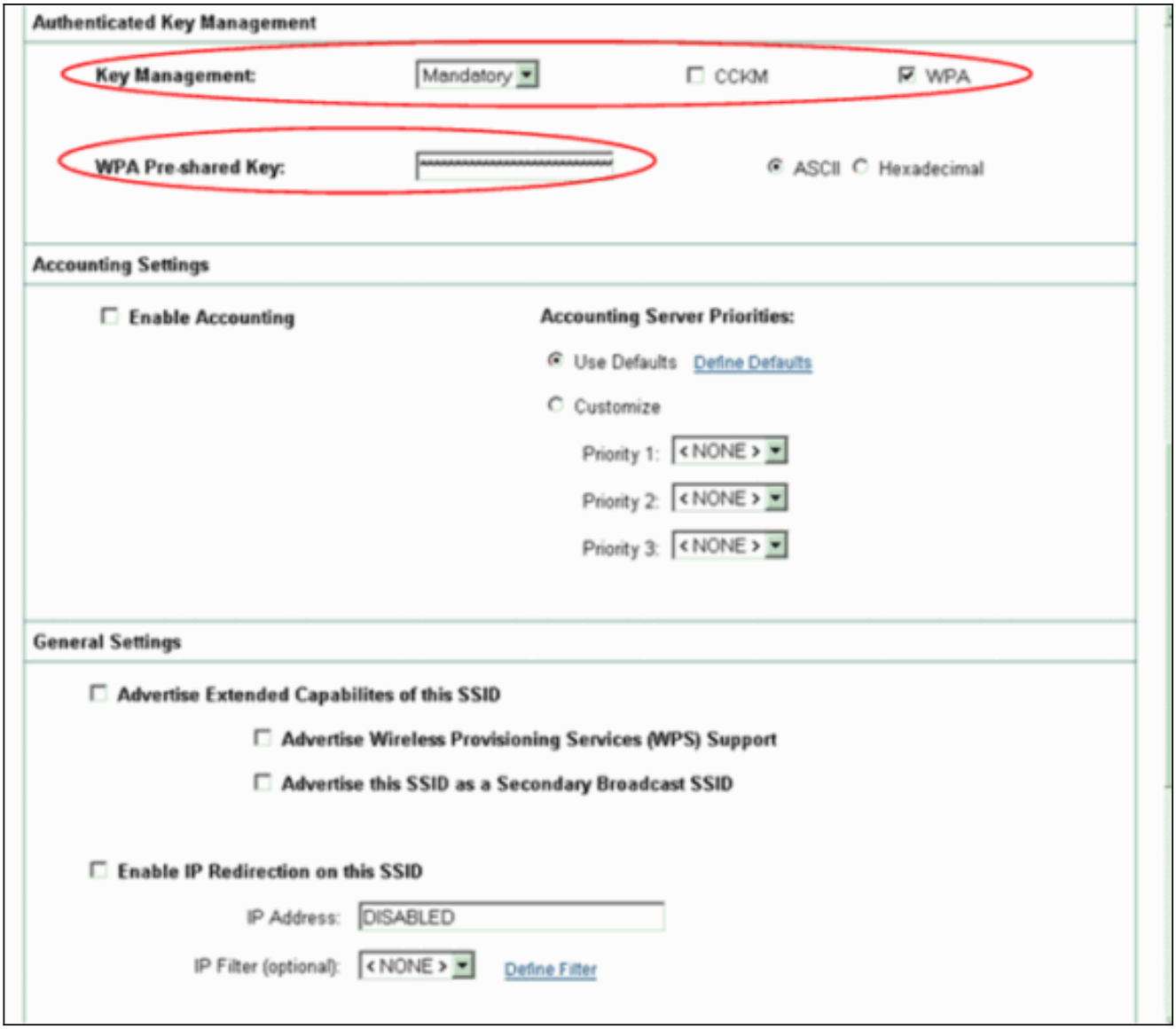
Complete estos pasos:

1. Elija **Security > Encryption Manager** en el menú de la izquierda y complete estos pasos:En el menú Cipher, elija **AES CCMP**.Esta opción habilita el cifrado AES con el uso del modo de contador con
   CCMP.
   

   Haga clic en Apply (Aplicar).
2. Elija **Security > SSID Manager** y cree un nuevo SSID para su uso con WPA 2.Marque la casilla de verificación **Open Authentication**.



Desplácese hacia abajo en Security (Seguridad): Ventana Administrador de SSID al área Administración de claves autenticadas y complete estos pasos:En el menú Key Management (Administración de claves), elija **Obligatorio**.Marque la casilla de verificación **WPA** de la derecha.



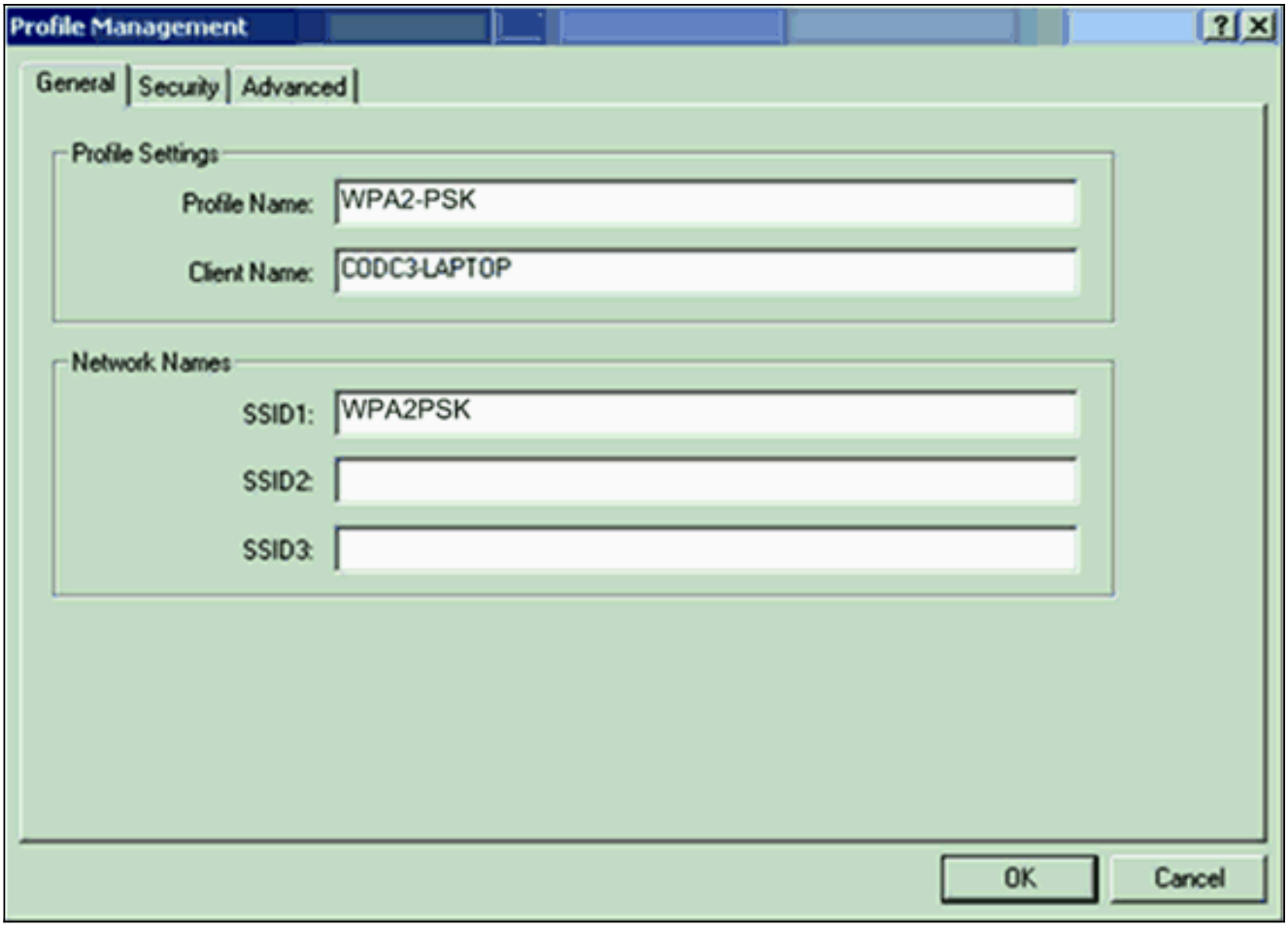
Introduzca la clave secreta compartida WPA PSK o la frase de paso WPA PSK.Esta clave debe coincidir con la clave WPA PSK que configure en el adaptador del cliente.Haga clic en Apply (Aplicar).

El AP ahora puede recibir solicitudes de autenticación de los clientes inalámbricos.

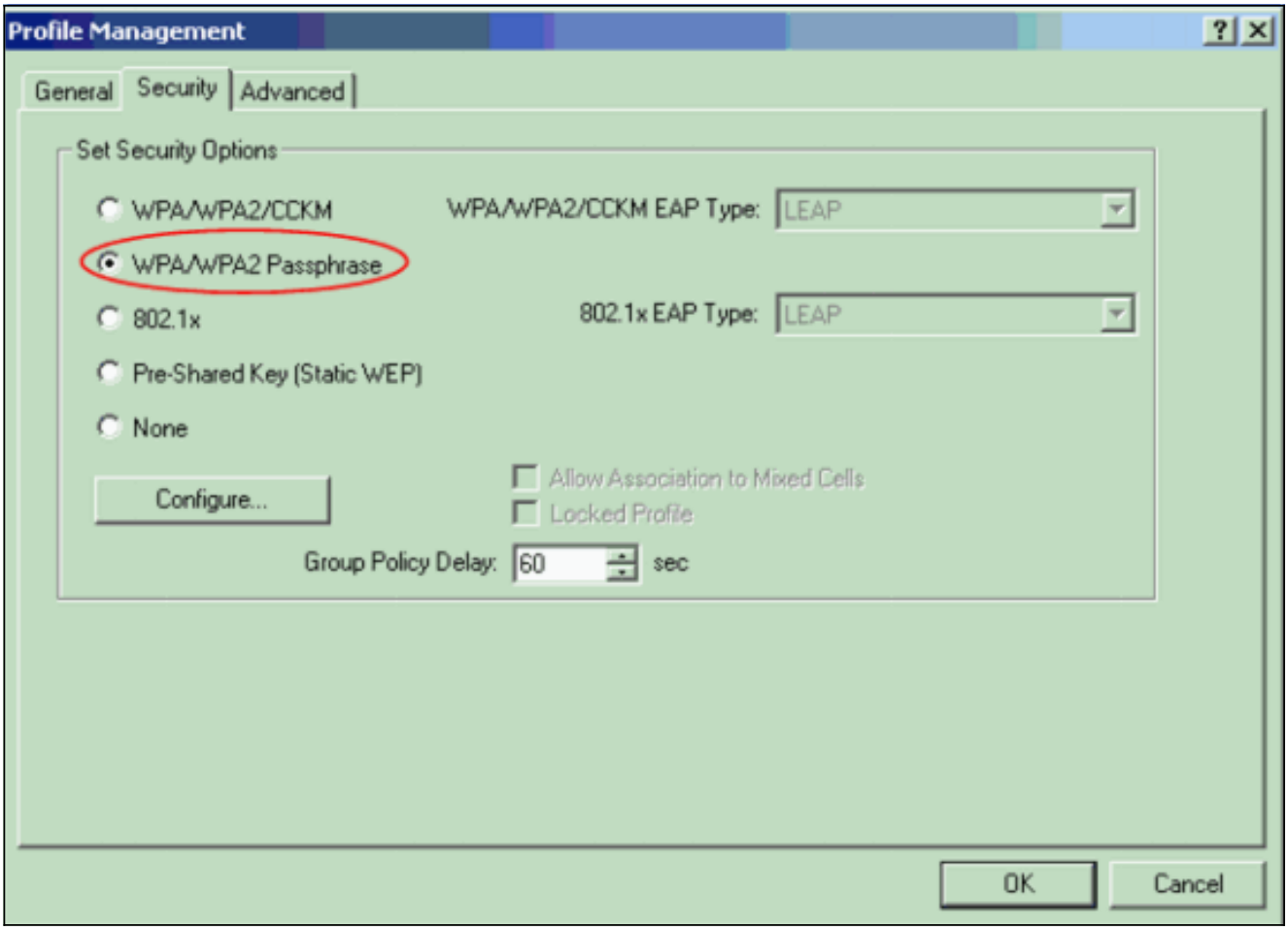
Configuración del adaptador del cliente

Complete estos pasos:

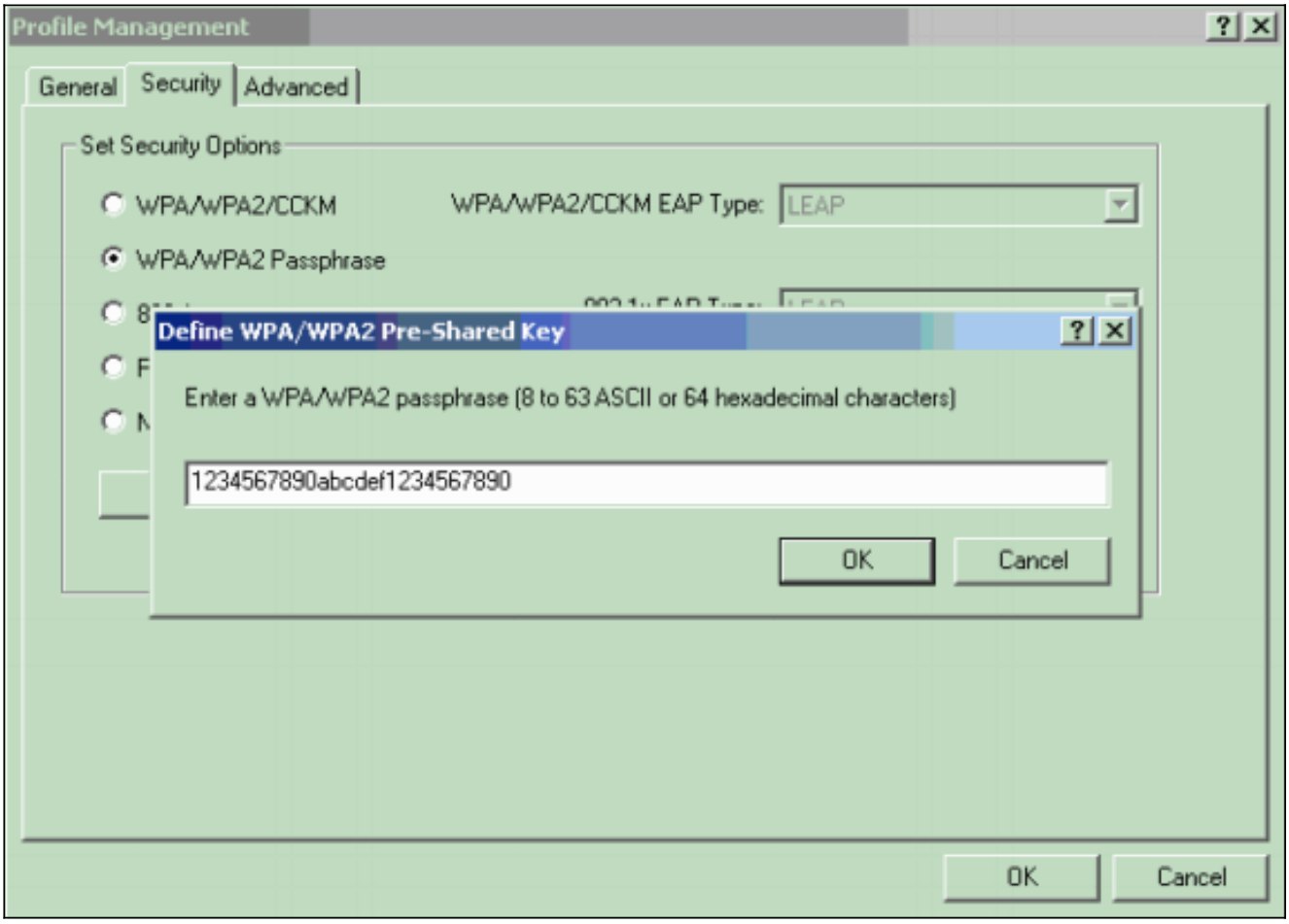
1. En la ventana Profile Management de la ADU, haga clic en **New** para crear un perfil nuevo.Se muestra una nueva ventana en la que se puede establecer la configuración para el modo de funcionamiento WPA 2 PSK. En la ficha General, introduzca el nombre del perfil y el SSID que utilizará el adaptador del cliente.En este ejemplo, el nombre del perfil es WPA2-PSK y el SSID es WPA2PSK:**Nota:** El SSID debe coincidir con el SSID que configuró en el AP para WPA 2
PSK.



2. Haga clic en la ficha **Seguridad** y haga clic en **Frase de paso WPA/WPA2**.Esta acción habilita WPA PSK o WPA 2 PSK, cualquiera que sea la configuración en el AP.



3. Haga clic en Configure (Configurar).Se muestra la ventana Definir clave precompartida WPA/WPA2.
4. Solicite al administrador del sistema la frase de paso WPA/WPA2 e introduzca la frase de paso en el campo Frase de paso WPA/WPA2.Obtenga la frase de paso para el AP en una red de infraestructura o la frase de paso para otros clientes en una red ad hoc.Utilice estas instrucciones para introducir una frase de paso:Las frases de contraseña WPA/WPA2 deben contener entre 8 y 63 caracteres de texto ASCII o 64 caracteres hexadecimales.La frase de paso WPA/WPA2 del adaptador del cliente debe coincidir con la frase de paso del AP con el que planea
comunicarse.



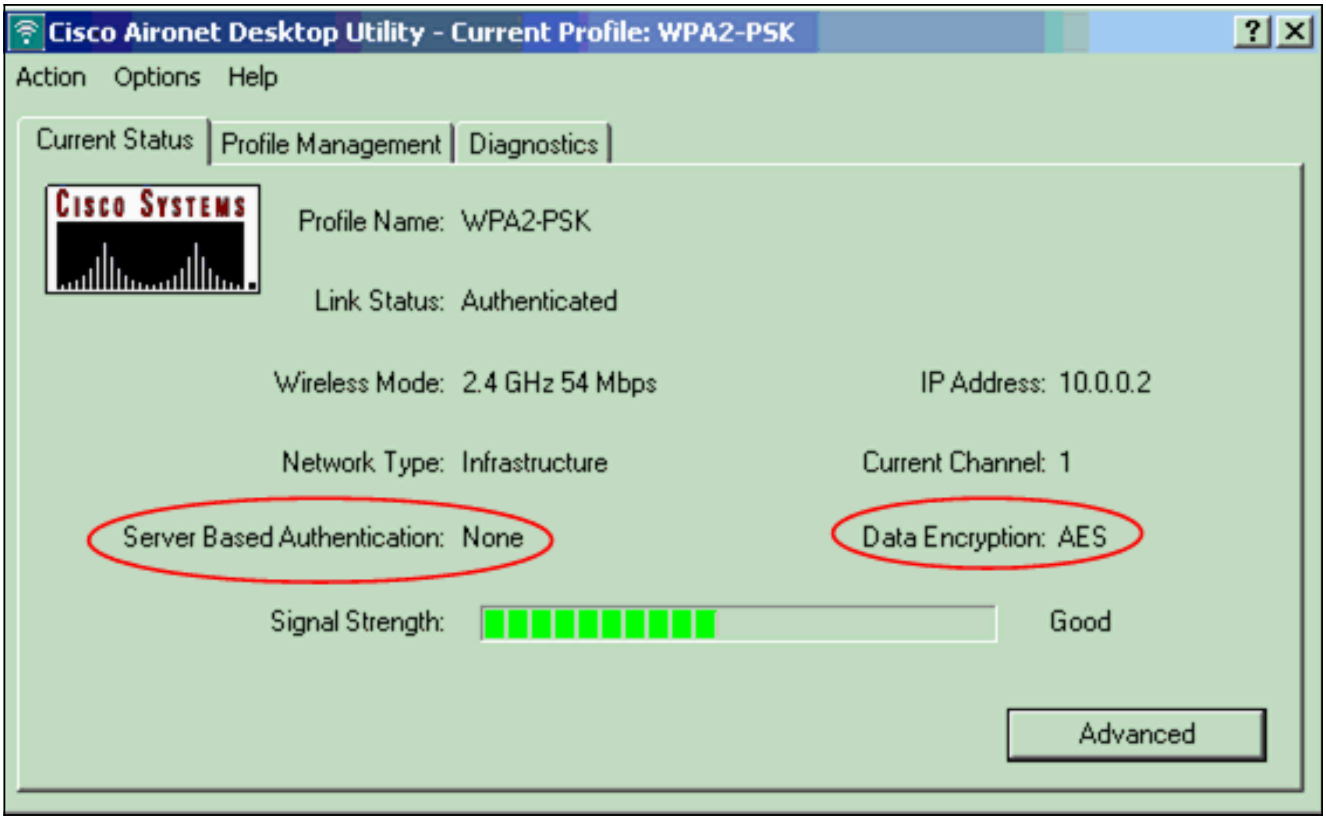
5. Haga clic en **Aceptar** para guardar la frase de paso y volver a la ventana Administración de perfiles.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Después de activar el perfil WPA 2 PSK, el AP autentica el cliente basándose en la frase de paso WPA 2 (PSK) y proporciona acceso a la WLAN.

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



2. Verifique el Registro de Eventos AP/bridge para verificar que el cliente se ha autenticado exitosamente con el modo de autenticación PSK WPA
2.

Troubleshoot

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 Wi-Fi protegido 2
- ¿Qué es la operación de modo mixto WPA y cómo se configura en mi AP?
- Página de Soporte de Red Inalámbrica
- 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).