Configure los tipos de autenticación inalámbrica en un ISR fijo

Contenido

[Información Relacionada]

Introducción

Este documento brinda un ejemplo de configuración que explica cómo configurar diversos tipos de autenticación de capa 2 en un router inalámbrico integrado de configuración fija de Cisco para conectividad inalámbrica con comandos CLI.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocer cómo se configuran los parámetros básicos de Cisco Integrated Services Router (ISR)
- Conocer cómo se configura el Wireless Client Adapter 802.11a/b/g con Aironet Desktop Utility (ADU)

Componentes Utilizados

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

- ISR Cisco 877W donde se ejecuta el software Cisco IOS® versión 12.3(8)YI1
- Notebook con Aironet Desktop Utility versión 3.6
- Adaptador de cliente 802.11 a/b/g que ejecuta firmware versión 3.6

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Los routers de servicios integrados de configuración fija de Cisco permiten utilizar una solución LAN inalámbrica segura, económica y fácil de utilizar que combina movilidad y flexibilidad con las características de tipo empresarial que los profesionales de redes exigen. Los routers de Cisco, con un sistema de administración basado en Cisco IOS Software, actúan como puntos de acceso

y son transceptores LAN inalámbricos que cumplen con la norma IEEE 802.11a/b/g y poseen certificado Wi-Fi.

Puede configurar y supervisar los routers con la interfaz de línea de comandos (CLI), el sistema de administración basado en el explorador o el Protocolo simple de administración de redes (SNMP). Este documento describe cómo configurar el ISR para conectividad inalámbrica con los comandos CLI.

Configurar

En este ejemplo, se muestra cómo configurar estos tipos de autenticación en un router inalámbrico integrado de configuración fija de Cisco con comandos CLI.

- Autenticación abierta
- Autenticación 802.1x/EAP (Extensible Authentication Protocol)
- Autenticación de acceso Wi-Fi protegido con clave previamente compartida (WPA-PSK)
- Autenticación WPA (con EAP)

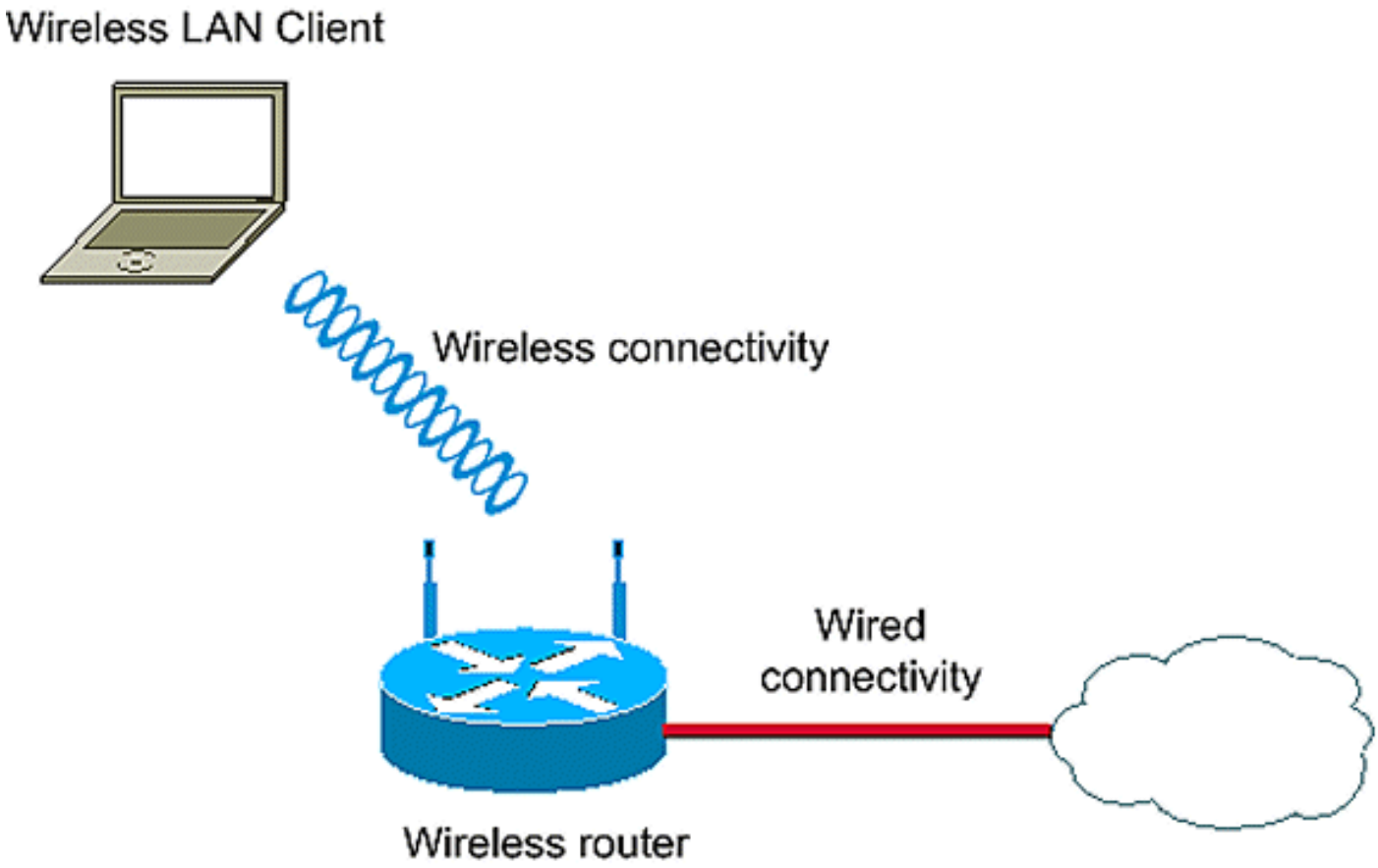
Nota: Este documento no se concentra en la autenticación compartida ya que es un tipo de autenticación menos seguro.

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Esta configuración utiliza el servidor RADIUS local en el ISR inalámbrico para autenticar clientes inalámbricos con autenticación 802.1x.

Configuración de Autenticación Abierta

La autenticación abierta es un algoritmo de autenticación nula. El punto de acceso otorga las peticiones de autenticación. La autenticación abierta permite que cualquier dispositivo acceda a la red. Si el encriptado no está habilitado en la red, cualquier dispositivo que conozca el SSID del punto de acceso puede acceder a la red. Si el encriptado WEP está habilitado en un punto de acceso, la clave WEP se convierte en un medio de control de acceso por sí misma. Si un dispositivo no posee la clave WEP correcta, no puede transmitir datos a través del punto de acceso aunque la autenticación sea correcta. Tampoco puede desencriptar los datos enviados desde el punto de acceso.

Este ejemplo de configuración sólo explica una autenticación abierta simple. La clave WEP puede ser obligatoria u opcional. En este ejemplo, se configura la clave WEP como opcional para que cualquier dispositivo que no utiliza WEP también pueda autenticarse y asociarse con este AP.

Para obtener más información, consulte Autenticación Abierta.

En este ejemplo, se utiliza esta configuración para configurar la autenticación abierta en el ISR.

- Nombre SSID: "open"
- VLAN 1

- Intervalo de servidores DHCP internos: 10.1.0.0/16

Nota: Para simplificar, en este ejemplo no se utiliza ninguna técnica de encriptado para clientes autenticados.

Complete estas acciones en el router:

1. Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group
2. Configuración de la Bridged Virtual Interface (BVI)
3. Configuración del SSID para Autenticación Abierta
4. Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group

Complete estas acciones:

1. Habilite IRB en el router.

   router<configure>#bridge irb

   Nota: Si se deben configurar todos los tipos de seguridad en un solo router, basta con activar IRB sólo una vez de manera global en el router. No es necesario habilitarlo para cada tipo de autenticación individual.

2. Defina un bridge group.

   En este ejemplo, se utiliza el bridge-group número 1.

   router<configure>#bridge 1

3. Elija el Spanning Tree Protocol para el bridge group.

   Aquí el Spanning Tree Protocol IEEE está configurado para este bridge group.

   router<configure>#bridge 1 protocol ieee

4. Habilite una BVI para aceptar y rutear los paquetes ruteables que recibe de su bridge group correspondiente.

   En este ejemplo, se habilita la BVI para aceptar y rutear los paquetes IP.

   router<configure>#bridge 1 route ip

Configuración de la Bridged Virtual Interface (BVI)

Complete estas acciones:

1. Configure la BVI.

   Configure la BVI al asignar el número correspondiente del bridge group a la BVI. Cada bridge group sólo puede tener una BVI correspondiente. En este ejemplo, se asigna el bridge group número 1 a la BVI.

   router<configure>#interface BVI <1>

2. Asigne una dirección IP a la BVI.

   router<config-if>#ip address 10.1.1.1 255.255.0.0

   router<config-if>#no shut

Consulte Configuración de Bridging para obtener más información sobre bridging.

Configuración del SSID para Autenticación Abierta

Complete estas acciones:

1. Habilite la interfaz de radio.

   Para habilitar la interfaz de radio, vaya al modo de configuración de interfaz de radio DOT11 y asigne un SSID a la interfaz.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid open

   El tipo de autenticación abierta puede configurarse en combinación con la autenticación de dirección MAC. En este caso, el access point obliga a que todos los dispositivos clientes realicen una autenticación de dirección MAC antes de poder conectarse a la red.

   La autenticación abierta también puede configurarse junto con la autenticación EAP. El access point obliga a que todos los dispositivos clientes realicen una autenticación EAP antes de poder conectarse a la red. Para el nombre de lista, especifique la lista de métodos de autenticación.

   Un punto de acceso configurado para autenticación EAP obliga a que todos los dispositivos clientes que se asocian realicen autenticación EAP. Los dispositivos clientes que no utilizan EAP no pueden utilizar el punto de acceso.

2. Enlace el SSID a una VLAN.

   Para habilitar el SSID en esta interfaz, enlace el SSID a la VLAN en modo de configuración SSID.

   router<config-ssid>vlan 1

3. Configure el SSID para autenticación abierta.

   router<config-ssid>#authentication open

4. Configure la interfaz de radio para la opción de clave WEP.

   router<config>#encryption vlan 1 mode WEP optional

5. Habilite la VLAN en la interfaz de radio.

   router<config>#interface Dot11Radio 0.1

   router<config-subif>#encapsulation dot1Q 1

   router<config-subif>#bridge-group 1

Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Escriba estos comandos en el modo de configuración global para configurar el servidor DHCP interno para los clientes inalámbricos de esta VLAN:

- ip dhcp excluded-address 10.1.1.1 10.1.1.5
- ip dhcp pool open

Escriba estos comandos en el modo de configuración de agrupación DHCP:

- network 10.1.0.0 255.255.0.0
- default-router 10.1.1.1

Configuración de Autenticación 802.1x/EAP

Este tipo de autenticación proporciona el nivel de seguridad más alto para su red inalámbrica. Con el Extensible Authentication Protocol (EAP), utilizado para interactuar con un servidor RADIUS compatible con EAP, el access point ayuda a un dispositivo de un cliente inalámbrico y al servidor RADIUS a realizar una autenticación mutua y a derivar una clave WEP dinámica de unicast. El servidor RADIUS envía la clave WEP al punto de acceso, que lo utiliza para todas las señales de datos de unicast que envía o recibe del cliente.

Para obtener más información, consulte Autenticación EAP.

En este ejemplo, se utiliza la siguiente configuración:

- Nombre de SSID: leap
- VLAN 2
- Intervalo de servidores DHCP internos: 10.2.0.0/16

En este ejemplo, se utiliza la autenticación LEAP como mecanismo para autenticar al cliente inalámbrico.

Nota: Consulte Cisco Secure ACS para Windows v3.2 con Autenticación de Máquina EAP-TLS para configurar EAP-TLS.

Nota: Consulte Configuración de Cisco Secure ACS para Windows v3.2 con Autenticación de Máquina PEAP-MS-CHAPv2 para configurar PEAP-MS-CHAPv2.

Nota: Debe comprender que toda la configuración de estos tipos de EAP incluye principalmente los cambios de configuración del lado del cliente y del lado del servidor de autenticación. La configuración en el router inalámbrico o el punto de acceso sigue siendo casi la misma para todos estos tipos de autenticación.

Nota: Como se mencionó al principio, esta configuración utiliza el servidor RADIUS local en el ISR inalámbrico para autenticar clientes inalámbricos con autenticación 802.1x.

Complete estas acciones en el router:

1. Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group
2. Configuración de la Bridged Virtual Interface (BVI)
3. Configuración del Servidor RADIUS Local para Autenticación EAP
4. Configuración del SSID para la Autenticación 802.1x/EAP
5. Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group

Complete estas acciones:

1. Habilite IRB en el router.

   router<configure>#bridge irb

   Nota: Si se deben configurar todos los tipos de seguridad en un solo router, basta con activar IRB sólo una vez de manera global en el router. No es necesario habilitarlo para cada tipo de autenticación individual.

2. Defina un bridge group.

   En este ejemplo, se utiliza el bridge-group número 2.

   router<configure>#bridge 2

3. Elija el Spanning Tree Protocol para el bridge group.

Aquí el Spanning Tree Protocol IEEE se configura para este bridge group.

router<configure>#bridge 2 protocol ieee

4. Elija el Spanning Tree Protocol para el bridge group.

   Aquí el Spanning Tree Protocol IEEE se configura para este bridge group.

   router<configure>#bridge 2 protocol ieee

5. Habilite una BVI para aceptar y rutear los paquetes ruteables que recibe de su bridge group correspondiente.

   En este ejemplo, se habilita la BVI para aceptar y rutear los paquetes IP.

   router<configure>#bridge 2 route ip

Configuración de la Bridged Virtual Interface (BVI)

Complete estas acciones:

1. Configure la BVI.

   Configure la BVI al asignar el número correspondiente del bridge group a la BVI. Cada bridge group sólo puede tener una BVI correspondiente. En este ejemplo, se asigna el bridge group número 2 a la BVI.

   router<configure>#interface BVI <2>

2. Asigne una dirección IP a la BVI.

   router<config-if>#ip address 10.2.1.1 255.255.0.0

   router<config-if>#no shut

Configuración del Servidor RADIUS Local para Autenticación EAP

Como se mencionó anteriormente, este documento utiliza el servidor RADIUS local en el router de reconocimiento inalámbrico.

1. Habilite el modelo de control de acceso de autenticación, autorización y contabilidad (AAA).

   router<configure>#aaa new-model

2. Cree un grupo de servidores rad-eap para el servidor RADIUS.

   router<configure>#aaa group server radius rad-eap server 10.2.1.1 auth-port 1812 acct-port 1813

3. Cree una lista de métodos eap_methods que muestra una lista del método de autenticación utilizado para autenticar el usuario de conexión AAA. Asigne la lista de método a este grupo

de servidores.

router<configure>#aaa authentication login eap_methods group rad-eap

4. Habilite el router como un servidor de autenticación local e ingrese en el modo de configuración para el autenticador.

   router<configure>#radius-server local

5. En el modo de configuración del Servidor Radius, agregue el router como un cliente AAA del servidor de autenticación local.

   router<config-radsrv>#nas 10.2.1.1 key Cisco

6. Configure el usuario user1 en el servidor Radius local.

   router<config-radsrv>#user user1 password user1 group rad-eap

7. Especifique el host de servidor RADIUS.

   router<config-radsrv>#radius-server host 10.2.1.1 auth-port 1812 acct-port 1813 key cisco

   Nota: Esta clave debe ser la misma que la que se especificó en el comando nas en el modo de configuración del servidor radius.

Configuración del SSID para la Autenticación 802.1x/EAP

La configuración de la interfaz de radio y del SSID asociada para 802.1x/EAP incluye la configuración de diversos parámetros inalámbricos en el router, entre ellos el SSID, el modo de encriptado y el tipo de autenticación. En este ejemplo, se utiliza el SSID denominado leap.

1. Habilite la interfaz de radio.

   Para habilitar la interfaz de radio, vaya al modo de configuración de interfaz de radio DOT11 y asigne un SSID a la interfaz.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid leap

2. Enlace el SSID a una VLAN.

   Para habilitar el SSID en esta interfaz, enlace el SSID a la VLAN en modo de configuración SSID.

   router<config-ssid>#vlan 2

3. Configure el SSID con autenticación 802.1x/EAP.

router<config-ssid>#authentication network-eap eap_methods

4. Configure la interfaz de radio para administración de claves dinámicas.

   router<config>#encryption vlan 2 mode ciphers wep40

5. Habilite la VLAN en la interfaz de radio.

   router<config>#interface Dot11Radio 0.2

   router<config-subif>#encapsulation dot1Q 2

   router<config-subif>#bridge-group 2

Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Escriba estos comandos en el modo de configuración global para configurar el servidor DHCP interno para los clientes inalámbricos de esta VLAN:

- ip dhcp excluded-address 10.2.1.1 10.2.1.5
- ip dhcp pool leapauth

Escriba estos comandos en el modo de configuración de agrupación DHCP:

- network 10.2.0.0 255.255.0.0
- default-router 10.2.1.1

Administración de Claves WPA

El acceso Wi-Fi protegido es una mejora de seguridad interoperable basada en estándares que mejora en gran medida el nivel de protección de datos y el control de acceso para sistemas LAN inalámbricos actuales y futuros.

Para obtener más información, consulte Administración de Claves WPA.

La gestión de claves WPA admite dos tipos de gestión que se excluyen mutuamente: WPA-Pre-shared key (WPA-PSK) y WPA (con EAP).

Configuración WPA-PSK

WPA-PSK se utiliza como un tipo de administración de claves en una LAN inalámbrica en la que la autenticación basada en 802.1x no está disponible. En dichas redes, se debe configurar una clave previamente compartida en el punto de acceso. Puede ingresar la clave previamente compartida como caracteres ASCII o hexadecimales. Si ingresa la clave como caracteres ASCII, ingresa entre 8 y 63 caracteres y el punto de acceso amplía la clave según el proceso descrito en

el Estándar de Encripción Basado en Contraseñas (RFC2898). Si ingresa la clave como caracteres hexadecimales, debe ingresar 64 caracteres hexadecimales.

En este ejemplo, se utiliza la siguiente configuración:

- Nombre SSID: wpa-shared
- VLAN 3
- Intervalo de servidores DHCP internos: 10.3.0.0/16

Complete estas acciones en el router:

1. Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group
2. Configuración de la Bridged Virtual Interface (BVI)
3. Configuración del SSID para Autenticación WPA-PSK
4. Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group

Complete estas acciones:

1. Habilite IRB en el router.

   router<configure>#bridge irb

   Nota: Si se deben configurar todos los tipos de seguridad en un solo router, basta con activar IRB sólo una vez de manera global en el router. No es necesario habilitarlo para cada tipo de autenticación individual.

2. Defina un bridge group.

   En este ejemplo, se utiliza el bridge-group número 3.

   router<configure>#bridge 3

3. Elija el Spanning Tree Protocol para el bridge group.

   El Spanning Tree Protocol IEEE se configura para este bridge group.

   router<configure>#bridge 3 protocol ieee

4. Habilite una BVI para aceptar y rutear los paquetes ruteables que recibe de su bridge group correspondiente.

   En este ejemplo, se habilita la BVI para aceptar y rutear los paquetes IP.

router<configure>#bridge 3 route ip

Configuración de la Bridged Virtual Interface (BVI)

Complete estas acciones:

1. Configure la BVI.

   Configure la BVI al asignar el número correspondiente del bridge group a la BVI. Cada bridge group sólo puede tener una BVI correspondiente. En este ejemplo, se asigna el bridge group número 3 a la BVI.

   router<configure>#interface BVI <2>

2. Asigne una dirección IP a la BVI.

   router<config-if>#ip address 10.3.1.1 255.255.0.0

   router<config-if>#no shut

Configuración del SSID para Autenticación WPA-PSK

Complete estas acciones:

1. Habilite la interfaz de radio.

   Para habilitar la interfaz de radio, vaya al modo de configuración de interfaz de radio DOT11 y asigne un SSID a la interfaz.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-shared

2. Para habilitar la administración de claves WPA, primero configure la cifra de encripción WPA para la interfaz VLAN. Este ejemplo utiliza tkip como el cifrado de cifrado..

   Escriba este comando para especificar el tipo de administración de claves WPA en la interfaz de radio.

   router<config>#interface dot11radio0

   router(config-if)#encryption vlan 3 mode ciphers tkip

3. Enlace el SSID a una VLAN.

   Para habilitar el SSID en esta interfaz, enlace el SSID a la VLAN en modo de configuración SSID.

   router<config-ssid>vlan 3

4. Configure el SSID con Autenticación WPA-PSK.

   Para habilitar la administración de claves WPA, primero es necesario configurar la autenticación abierta o EAP de red en el modo de configuración SSID. En este ejemplo, se configura la autenticación abierta.

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

   router<config-ssid>#authentication open

   Ahora, habilite la administración de claves WPA en el SSID. La cifra tkip de administración de claves ya está configurada para esta VLAN.

   router(config-if-ssid)#authentication key-management wpa

   Configure la autenticación WPA-PSK en el SSID.

   router(config-if-ssid)#wpa-psk ascii 1234567890 !--- 1234567890 es el valor de la clave previamente compartida para este SSID. Asegúrese de especificar la misma clave para este SSID del lado del cliente.

5. Habilite la VLAN en la interfaz de radio.

   router<config>#interface Dot11Radio 0.3

   router<config-subif>#encapsulation dot1Q 3

   router<config-subif>#bridge-group 3

Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Escriba estos comandos en el modo de configuración global para configurar el servidor DHCP interno para los clientes inalámbricos de esta VLAN:

- ip dhcp excluded-address 10.3.1.1 10.3.1.5
- ip dhcp pool wpa-psk

Escriba estos comandos en el modo de configuración de agrupación DHCP:

- network 10.3.0.0 255.255.0.0
- default-router 10.3.1.1

Configuración de Autenticación WPA (con EAP)

Éste es otro tipo de administración de claves WPA. Aquí, los clientes y el servidor de

autenticación se autentican mutuamente con un método de autenticación EAP. El cliente y el servidor generan una Pairwise Master Key [PMK] (Clave Maestra Pairwise). Con WPA, el servidor genera la PMK de manera dinámica y la transfiere al punto de acceso, pero con WPA-PSK, usted configura una clave previamente compartida tanto del lado del cliente como en el punto de acceso y se utiliza esa clave previamente compartida como PMK.

Para obtener más información, consulte WPA con Autenticación EAP.

En este ejemplo, se utiliza la siguiente configuración:

- Nombre de SSID: wpa-dot1x
- VLAN 4
- Intervalo de servidores DHCP internos: 10.4.0.0/16

Complete estas acciones en el router:

1. Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group
2. Configuración de la Bridged Virtual Interface (BVI)
3. Configuración del Servidor RADIUS Local para Autenticación WPA
4. Configuración del SSID para WPA con Autenticación EAP
5. Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Configuración de Integrated Routing and Bridging (IRB) y Configuración del Bridge Group

Complete estas acciones:

1. Habilite IRB en el router.

   router<configure>#bridge irb

   Nota: Si se deben configurar todos los tipos de seguridad en un solo router, basta con activar IRB sólo una vez de manera global en el router. No es necesario habilitarlo para cada tipo de autenticación individual.

2. Defina un Bridge group.

   En este ejemplo, se utiliza el bridge-group número 4.

   router<configure>#bridge 4

3. Seleccione el Spanning Tree Protocol para el bridge group.

   Aquí el Spanning Tree Protocol IEEE se configura para este bridge group.

router<configure>#bridge 4 protocol ieee

4. Habilite una BVI para aceptar y rutear los paquetes ruteables que recibe de su bridge group correspondiente.

   En este ejemplo, se habilita la BVI para aceptar y rutear los paquetes IP.

   router<configure>#bridge 4 route ip

Configuración de la Bridged Virtual Interface (BVI)

Complete estas acciones:

1. Configure la BVI.

   Configure la BVI al asignar el número correspondiente del bridge group a la BVI. Cada bridge group sólo puede tener una BVI correspondiente. En este ejemplo, se asigna el bridge group número 4 a la BVI.

   router<configure>#interface BVI <4>

2. Asigne una dirección IP a la BVI.

   router<config-if>#ip address 10.4.1.1 255.255.0.0

   router<config-if>#no shut

Configuración del Servidor RADIUS Local para Autenticación WPA

Consulte la sección que aparece en Autenticación 802.1x/EAP para ver el procedimiento detallado.

Configuración del SSID para WPA con Autenticación EAP

Complete estas acciones:

1. Habilite la interfaz de radio.

   Para habilitar la interfaz de radio, vaya al modo de configuración de interfaz de radio DOT11 y asigne un SSID a la interfaz.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-dot1x

2. Para habilitar la administración de claves WPA, primero configure la cifra de encripción WPA para la interfaz VLAN. Este ejemplo utiliza tkip como el cifrado de cifrado..

Escriba este comando para especificar el tipo de administración de claves WPA en la interfaz de radio.

router<config>#interface dot11radio0

router(config-if)#encryption vlan 4 mode ciphers tkip

3. Enlace el SSID a una VLAN.

   Para habilitar el SSID en esta interfaz, enlace el SSID a la VLAN en el modo de configuración SSID.

   vlan 4

4. Configure el SSID con la Autenticación WPA-PSK.

   Para configurar la interfaz de radio para WPA con autenticación EAP, primero configure el SSID asociada para EAP de red.

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

   router<config-ssid>#authentication network eap eap_methods

5. Ahora, habilite la administración de claves WPA en el SSID. La cifra tkip de administración de claves ya está configurada para esta VLAN.

   router(config-if-ssid)#authentication key-management wpa

6. Habilite la VLAN en la interfaz de radio.

   router<config>#interface Dot11Radio 0.4

   router<config-subif>#encapsulation dot1Q 4

   router<config-subif>#bridge-group 4

Configuración del Servidor DHCP Interno para los Clientes Inalámbricos de esta VLAN

Escriba estos comandos en el modo de configuración global para configurar el servidor DHCP interno para los clientes inalámbricos de esta VLAN:

- ip dhcp excluded-address 10.4.1.1 10.4.1.5
- ip dhcp pool wpa-dot1shared

Escriba estos comandos en el modo de configuración de agrupación DHCP:

- network 10.4.0.0 255.255.0.0

- default-router 10.4.1.1

Configuración de Cliente Inalámbrico para Autenticación

Después de configurar el ISR, configure el cliente inalámbrico para diferentes tipos de autenticación según se explica, de modo que el router pueda autenticar estos clientes inalámbricos y proporcionar acceso a la red WLAN. Este documento utiliza Cisco Aironet Desktop Utility (ADU) para configuración del lado del cliente.

Configuración del Cliente Inalámbrico para Autenticación Abierta

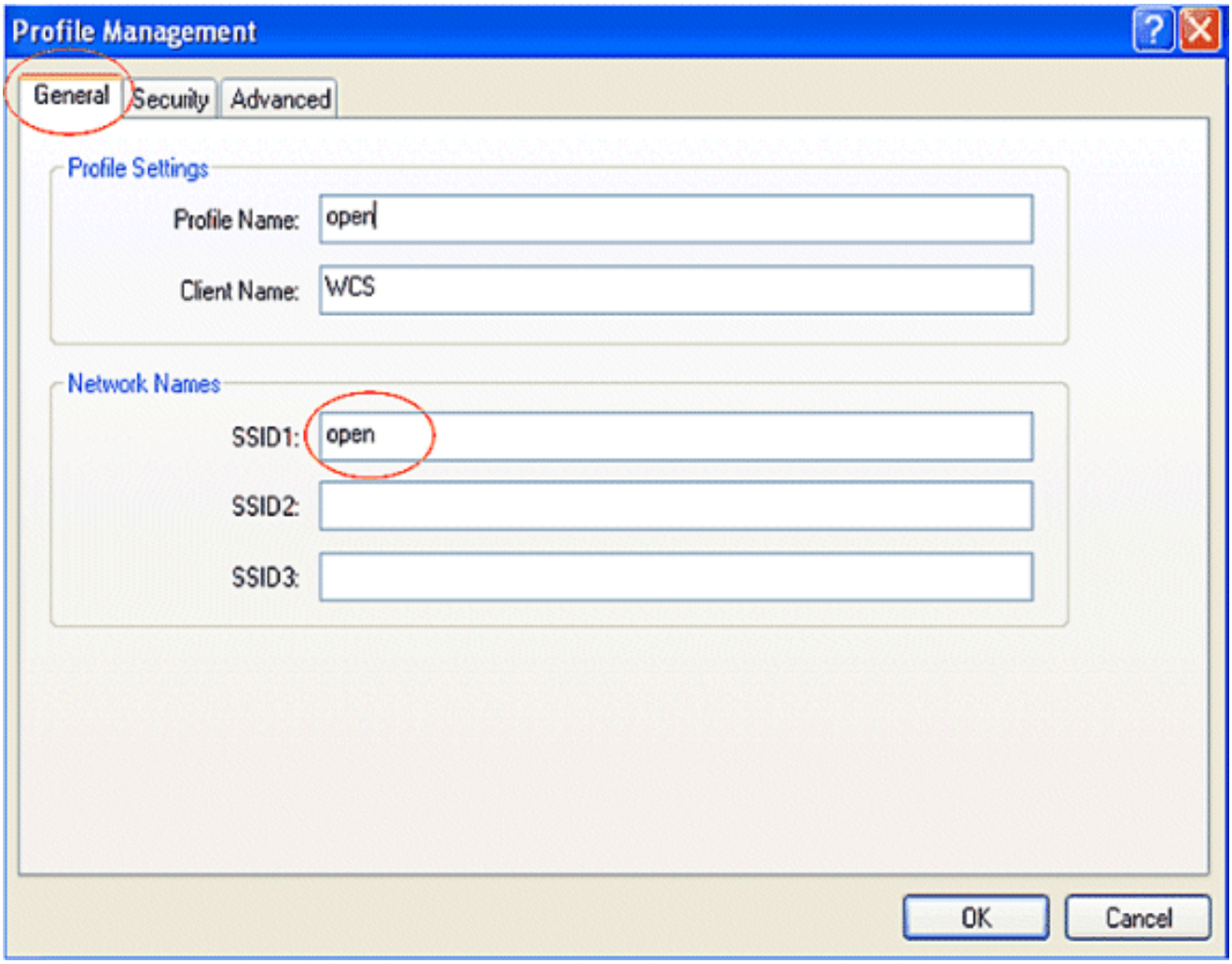
Complete estos pasos:

1. En la ventana Profile Management de la ADU, haga clic en New para crear un perfil nuevo.

   Aparecerá una ventana nueva donde podrá establecer la configuración para autenticación abierta. En la ficha General, ingrese el Profile Name (Nombre del Perfil) y el SSID que utiliza el adaptador del cliente.

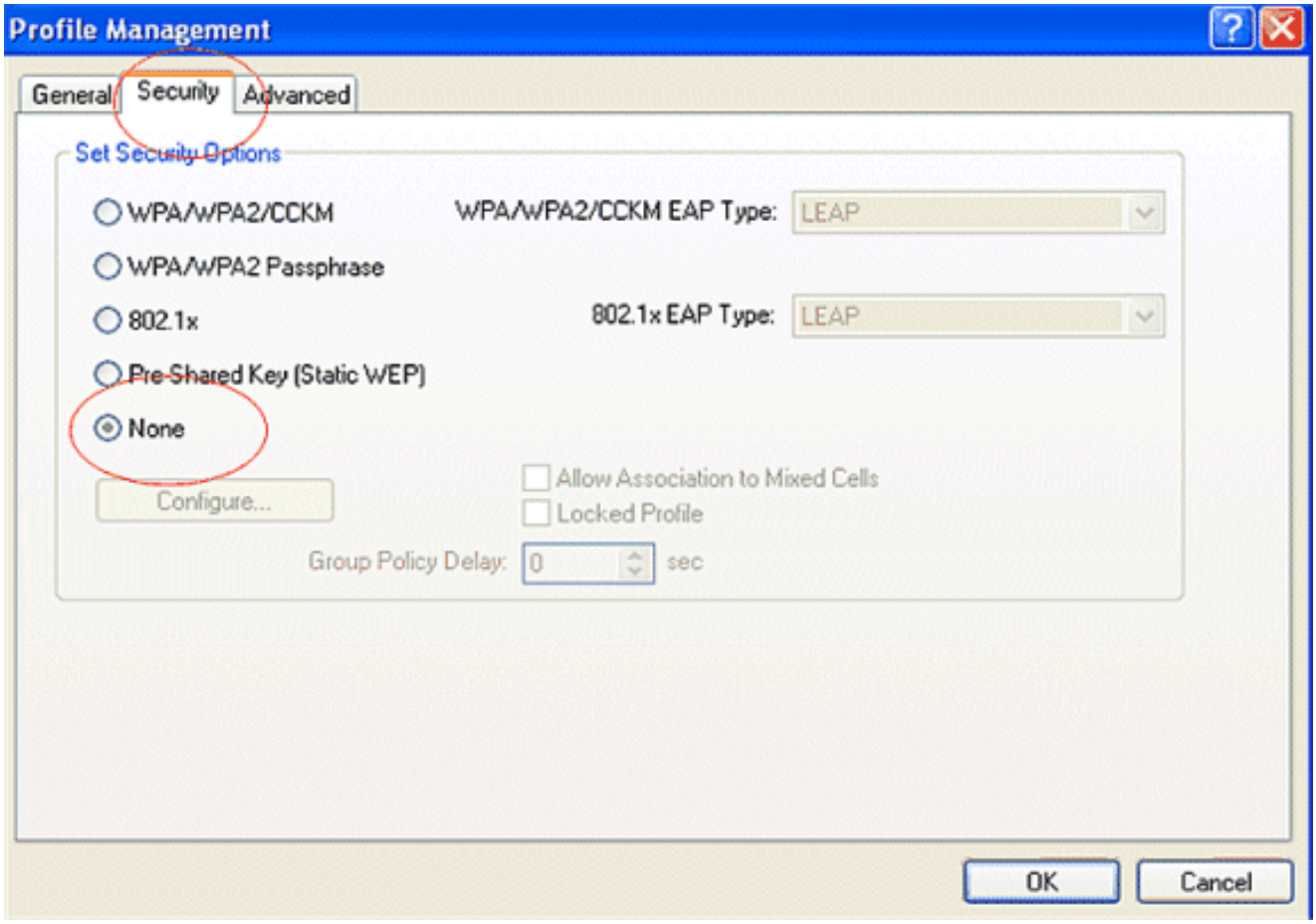
   En este ejemplo, el nombre del perfil y el SSID son open.

   Nota: El SSID debe coincidir con el SSID que configuró en el ISR para autenticación abierta.

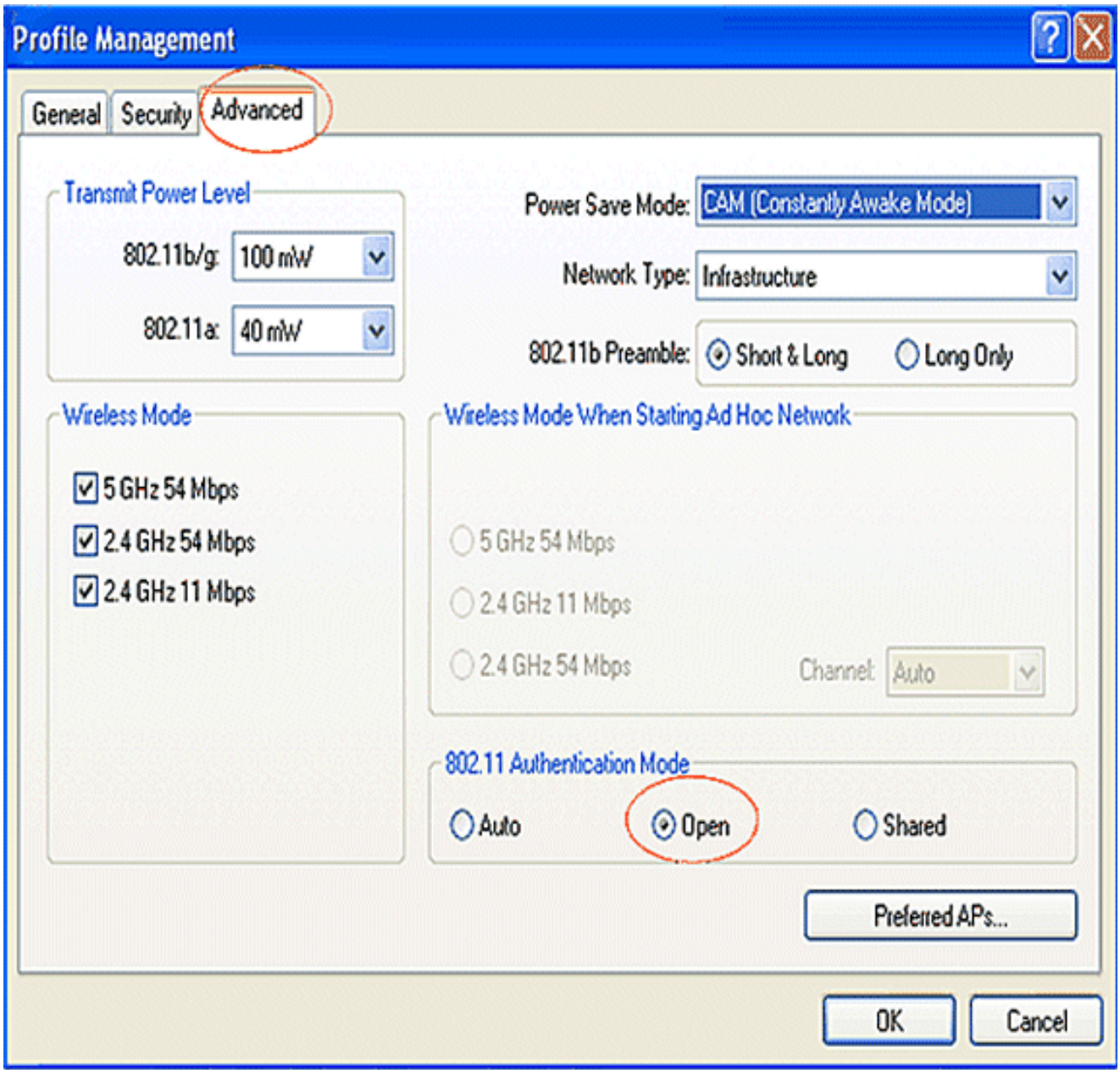


2. Haga clic en la ficha Security y deje la opción de seguridad como None (Ninguna) para la encriptación WEP. Dado que en este ejemplo se utiliza WEP como opcional, al configurar esta opción como None se habilitará al cliente para asociarse y comunicarse satisfactoriamente con la red WLAN.

   Haga clic en OK (Aceptar).

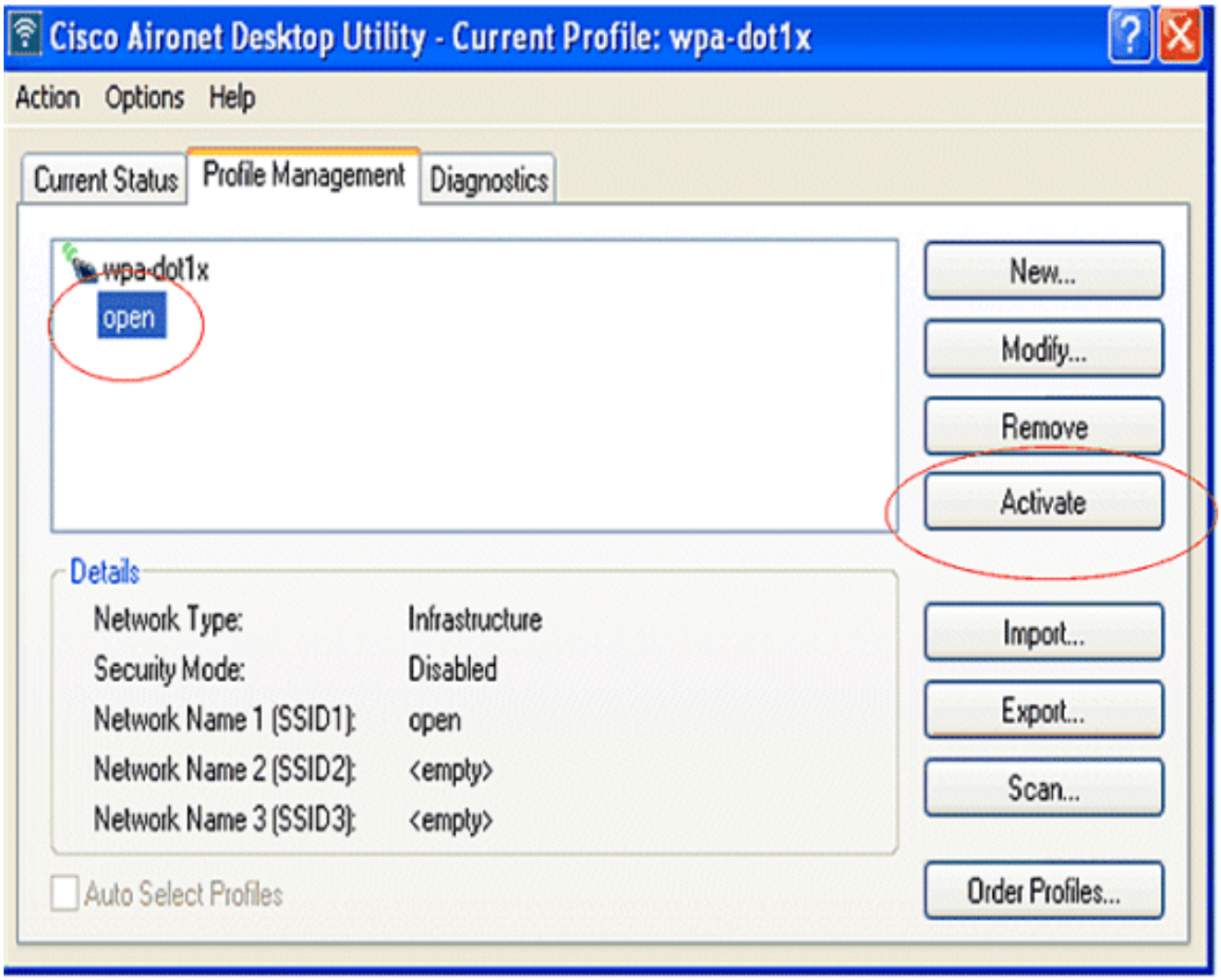


3. Seleccione Advanced en la ficha Profile Management y, en 802.11 Authentication Mode seleccione la opción Open para configurar la autenticación abierta.

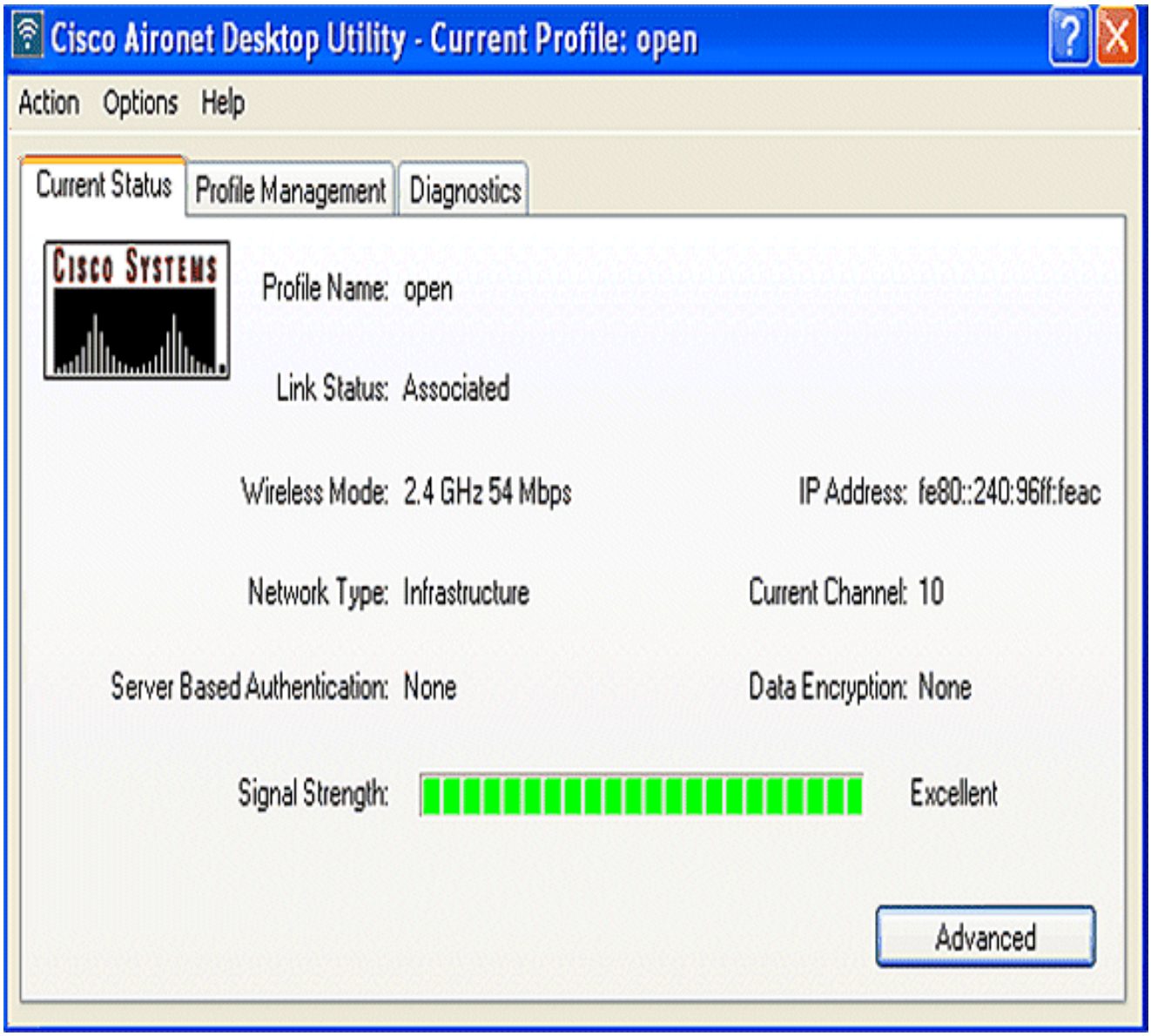


Use esta sección para confirmar que su configuración funciona correctamente.

1. Luego de crear el perfil del cliente, haga clic en Activate en la ficha Profile Management para activar el perfil.



2. Controle el estado ADU para lograr una autenticación satisfactoria.



Configuración del Cliente Inalámbrico para la Autenticación 802.1x/EAP

Complete estos pasos:

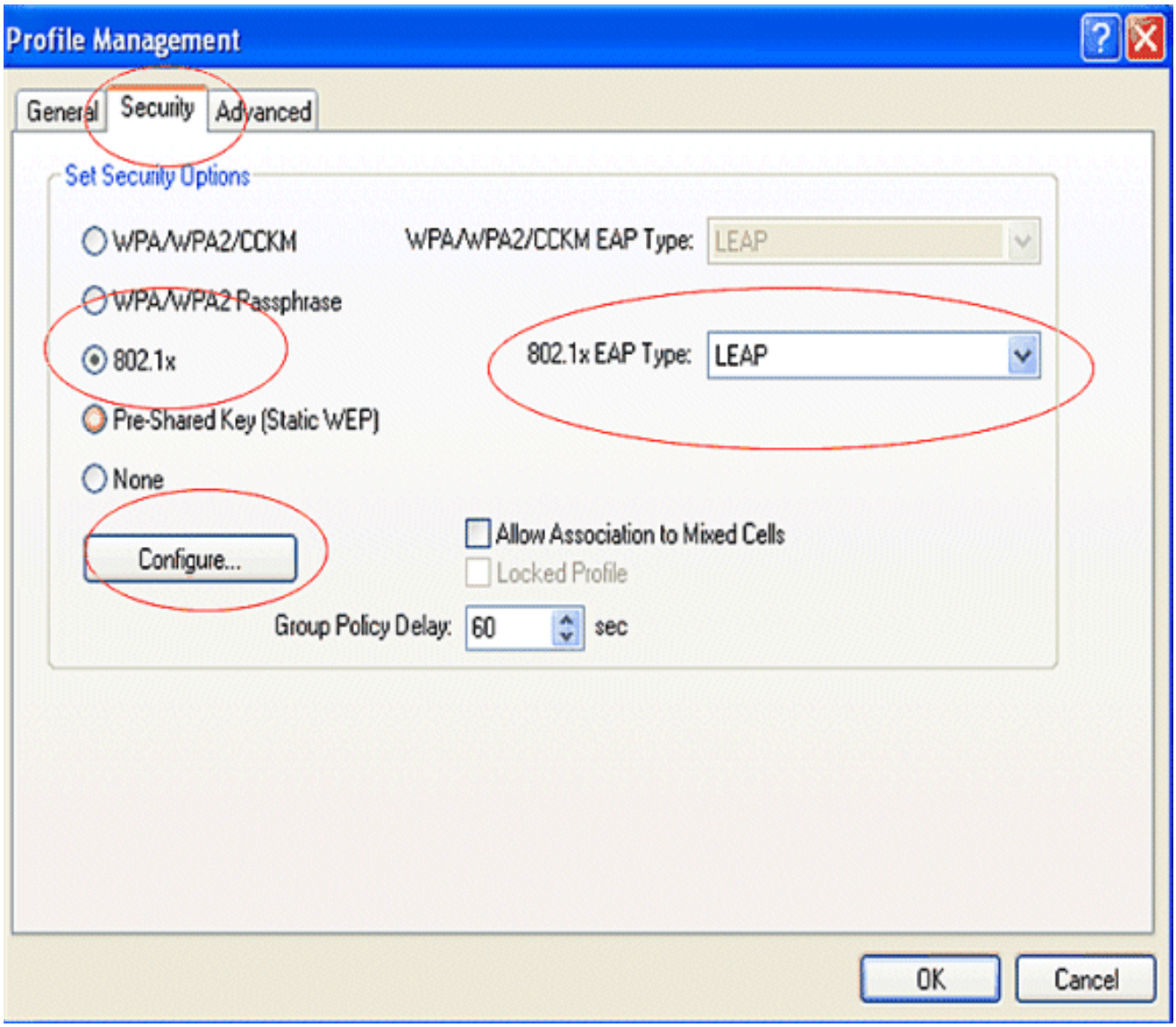
1. En la ventana Profile Management de la ADU, haga clic en New para crear un perfil nuevo.

   Aparecerá una ventana nueva donde podrá establecer la configuración para autenticación abierta. En la ficha General, ingrese el Profile Name (Nombre del Perfil) y el SSID que utiliza el adaptador del cliente.

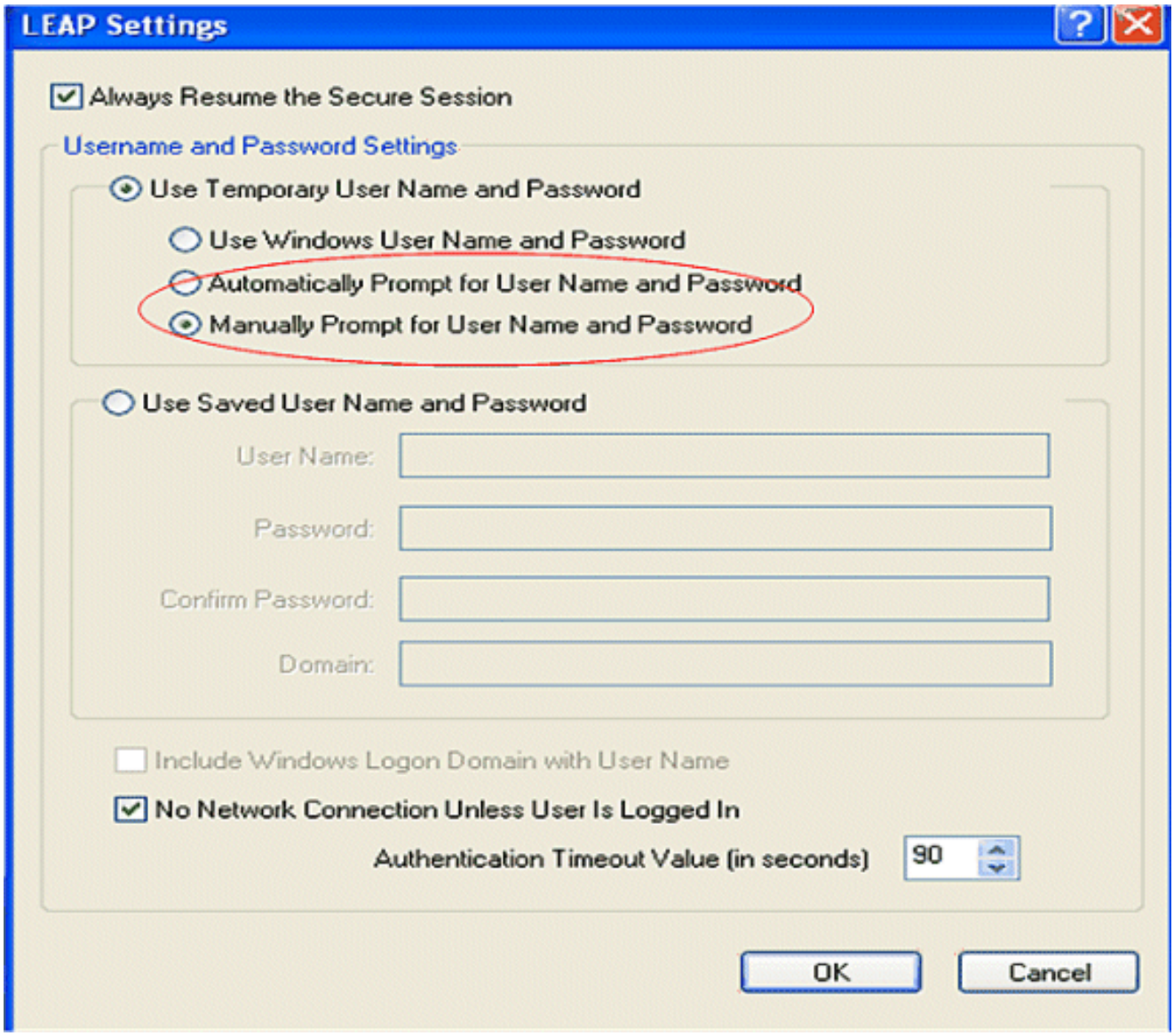
   En este ejemplo, el nombre del perfil y el SSID son leap.

2. En Profile Management, haga clic en la ficha Security, configure la opción de seguridad como 802.1x y elija el tipo de EAP adecuado. Este documento utiliza LEAP como el tipo EAP para autenticación. Ahora, haga clic en Configure para configurar el nombre de usuario y la contraseña de LEAP.

   Nota: Nota: El SSID debe coincidir con el SSID configurado en el ISR para la autenticación 802.1x/EAP.

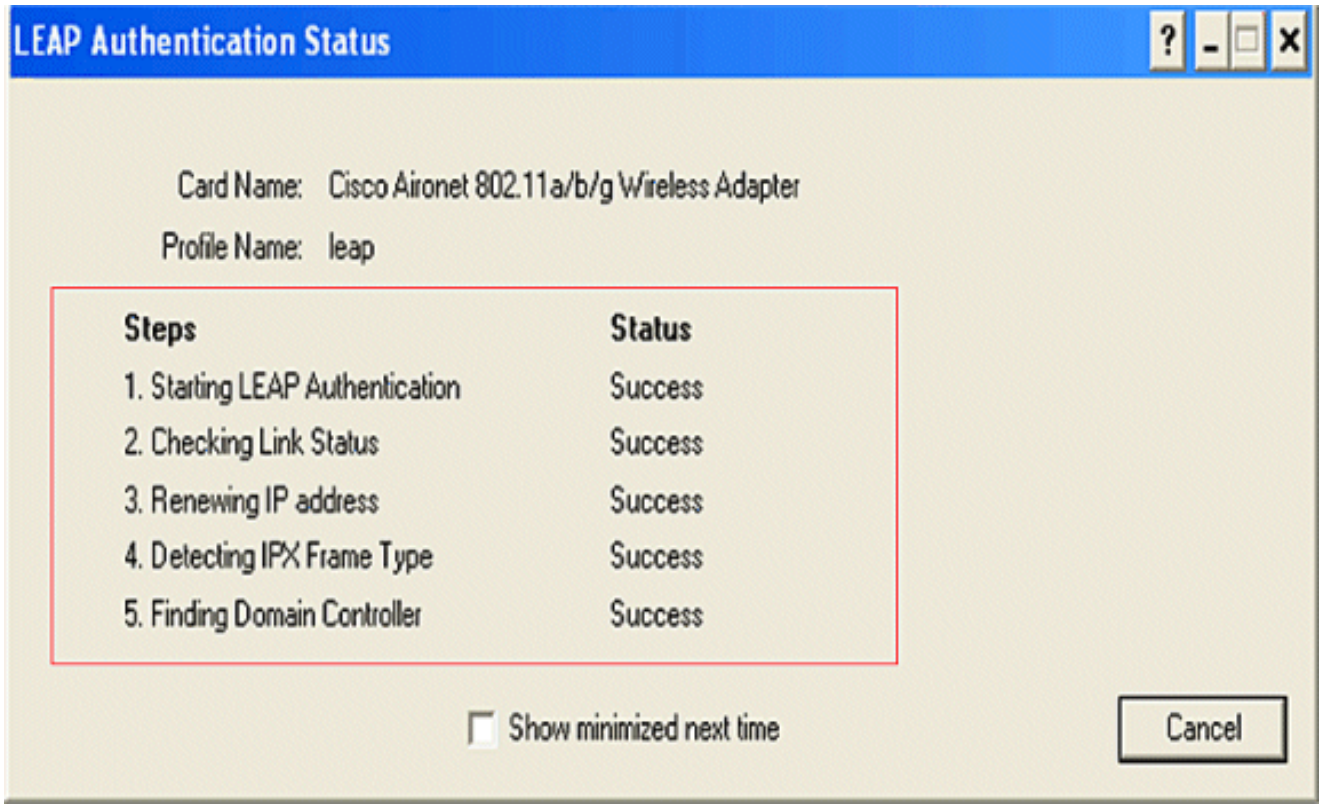


3. En este ejemplo, se elige Manually Prompt for User Name and Password en las configuraciones de nombre de usuario y contraseña para que se le solicite al cliente que ingrese el nombre de usuario y la contraseña correctos cuando intenta conectarse a la red. Click OK.



Use esta sección para confirmar que su configuración funciona correctamente.

- Luego de crear el perfil del cliente, haga clic en Activate en la ficha Profile Management para activar el perfil leap. Se le solicitará que ingrese el nombre de usuario y la contraseña de leap. En este ejemplo, se utiliza el nombre de usuario y la contraseña user1. Click OK.
- Puede observar si el cliente se autentica satisfactoriamente y puede obtener una IP address del servidor DHCP configurado en el router.



Configuración del Cliente Inalámbrico para Autenticación WPA-PSK

Complete estos pasos:

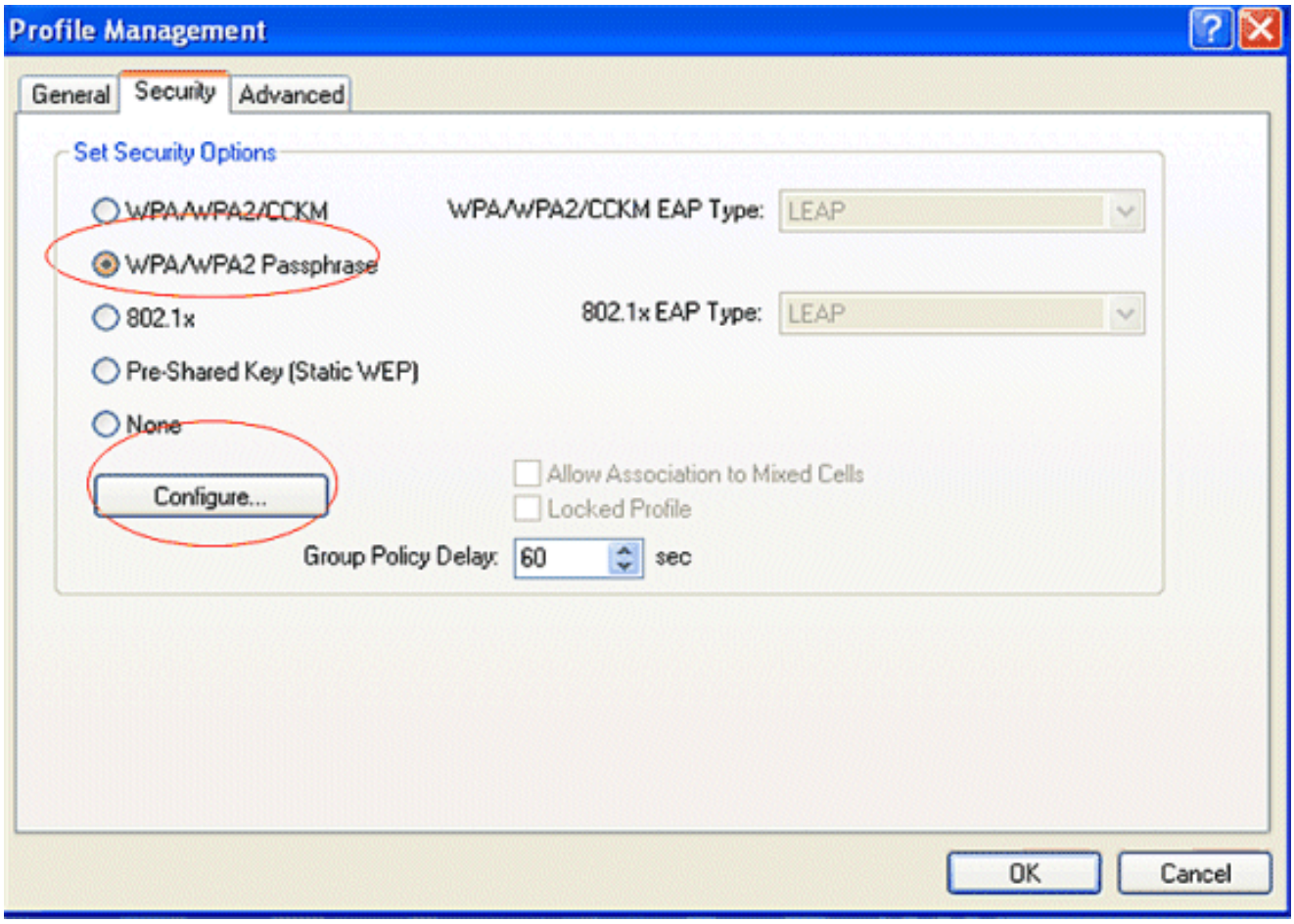
1. En la ventana Profile Management de la ADU, haga clic en New para crear un perfil nuevo.

   Aparecerá una ventana nueva donde podrá establecer la configuración para autenticación abierta. En la ficha General, ingrese el Profile Name y el SSID que utiliza el adaptador de clientes.

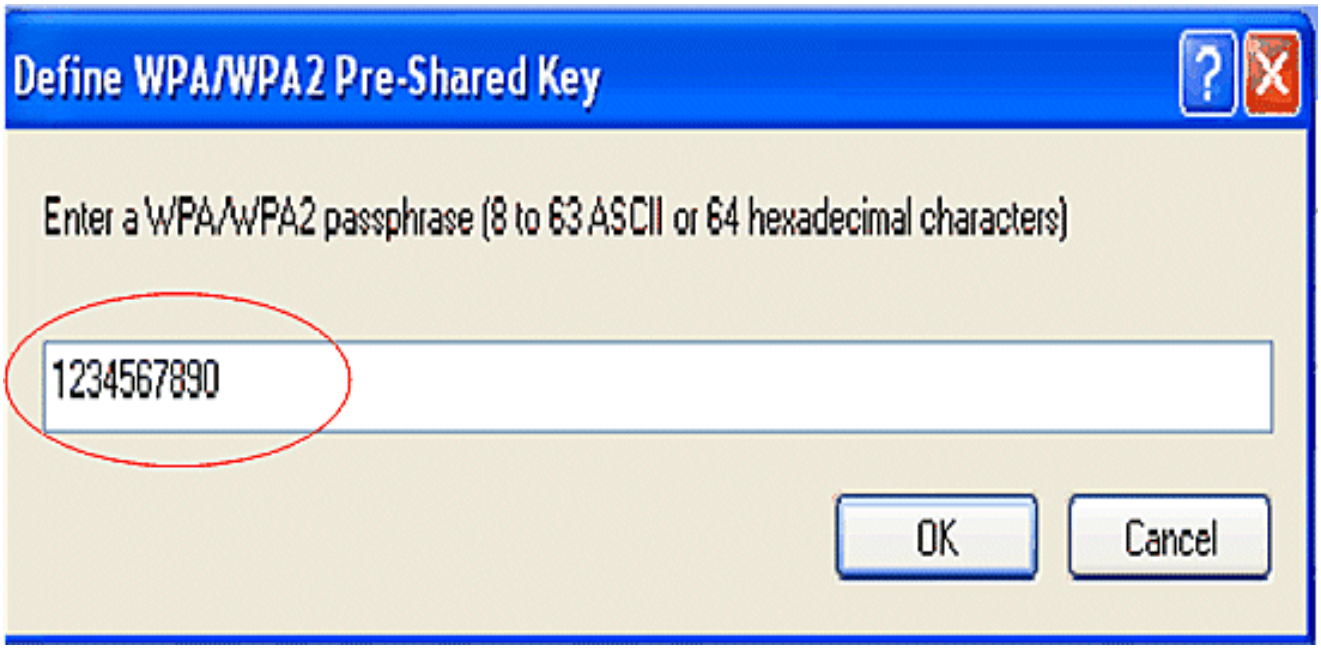
   En este ejemplo, el nombre del perfil y el SSID son wpa-shared.

   Nota: El SSID debe coincidir con el SSID que configuró en el ISR para autenticación WPA-PSK.

2. En Profile Management, haga clic en la ficha Security y configure la opción de seguridad como WPA/WPA2 Passphrase. Ahora, haga clic en Configure para configurar la WPA Passphrase (Palabra Clave WPA).



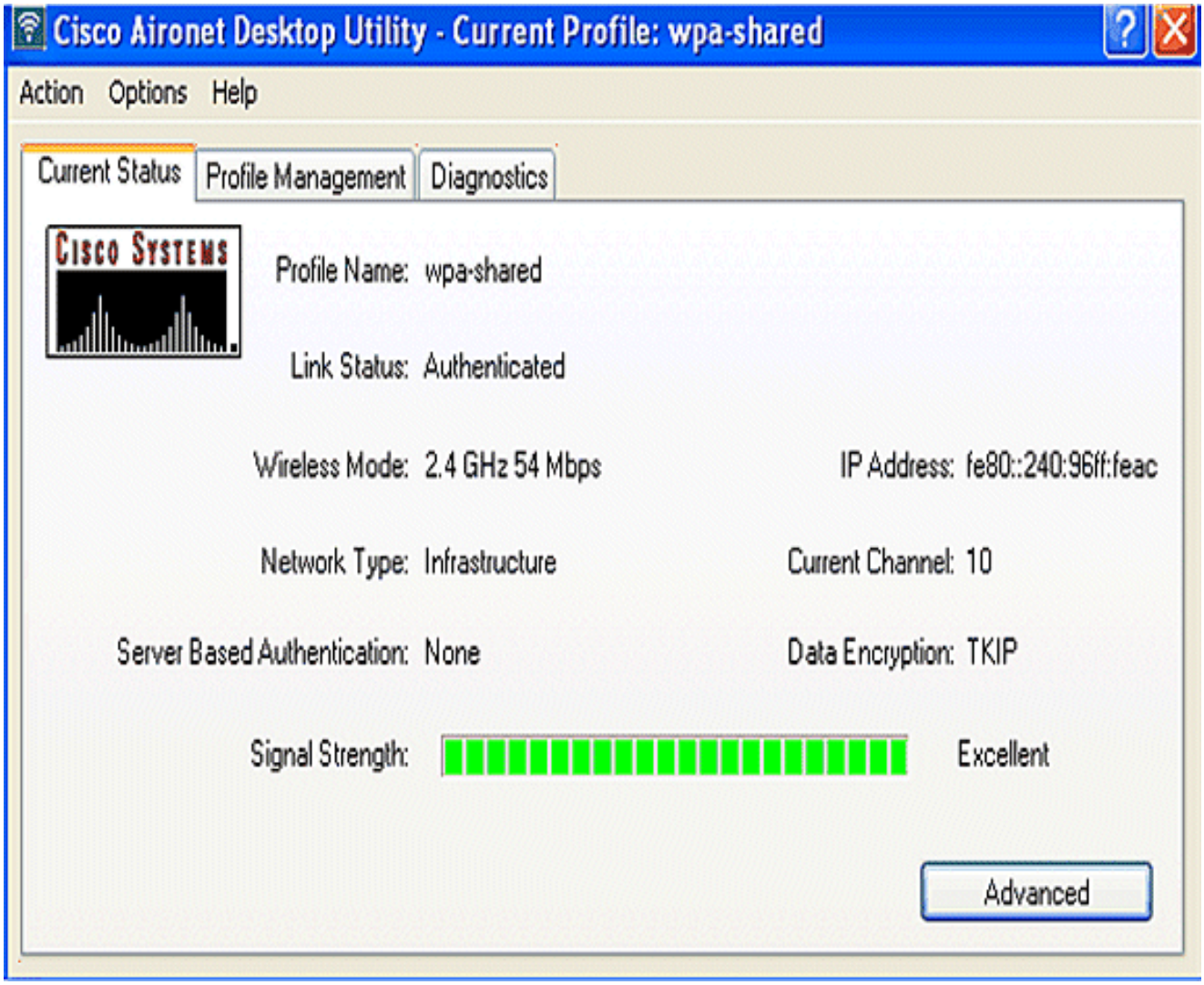
3. Defina una clave WPA previamente compartida. La clave debe tener entre 8 y 63 caracteres ASCII. Click OK.



Use esta sección para confirmar que su configuración funciona correctamente.

- Luego de crear el perfil del cliente, haga clic en Activate en la ficha Profile Management para activar el perfil wpa-shared.

- Controle el ADU para lograr una autenticación satisfactoria.



Configuración del Cliente Inalámbrico para Autenticación WPA (con EAP)

Complete estos pasos:

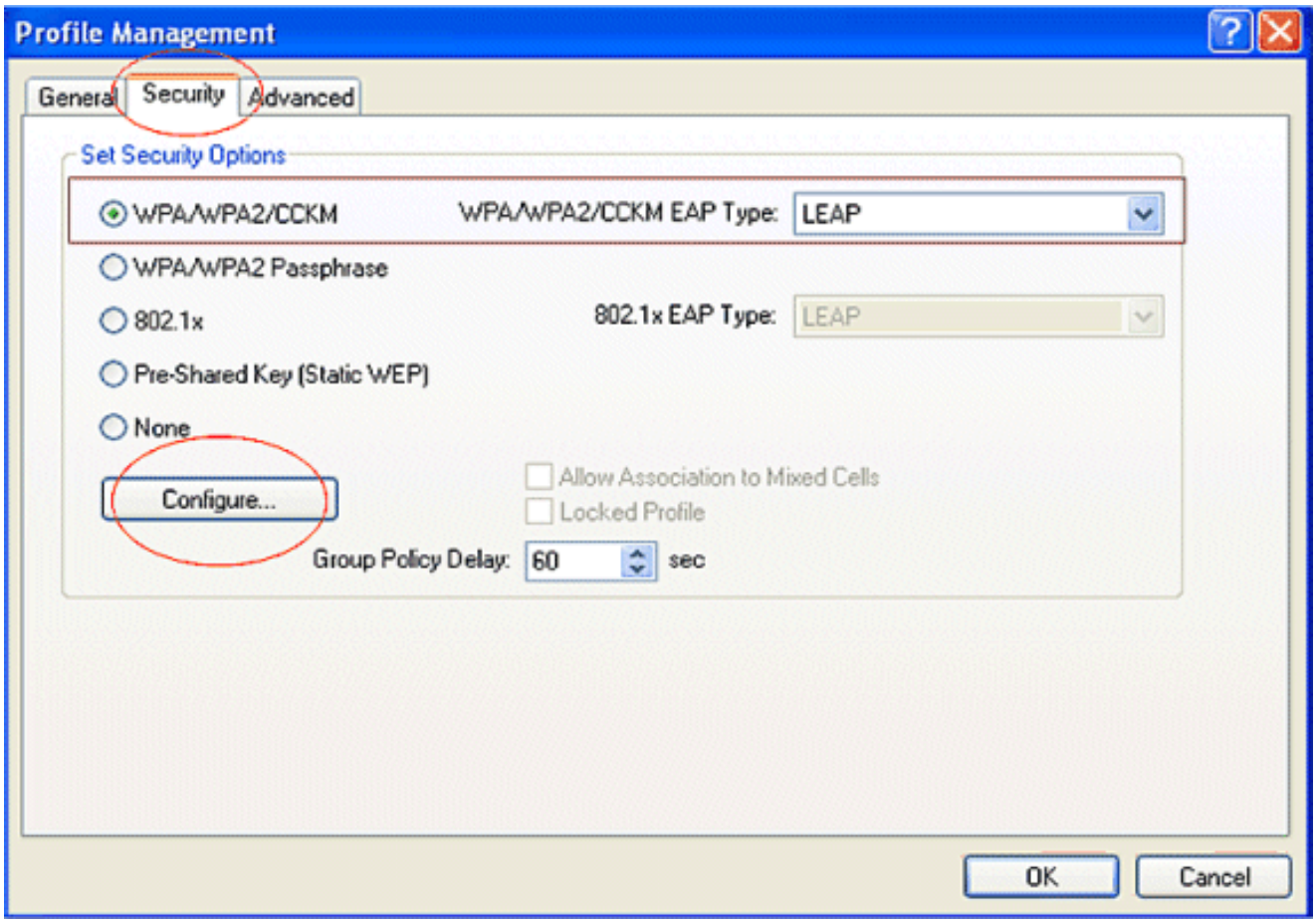
1. En la ventana Profile Management de la ADU, haga clic en New para crear un perfil nuevo.

   Aparecerá una ventana nueva donde podrá establecer la configuración para autenticación abierta. En la ficha General, ingrese el Profile Name y el SSID que utiliza el adaptador de clientes.

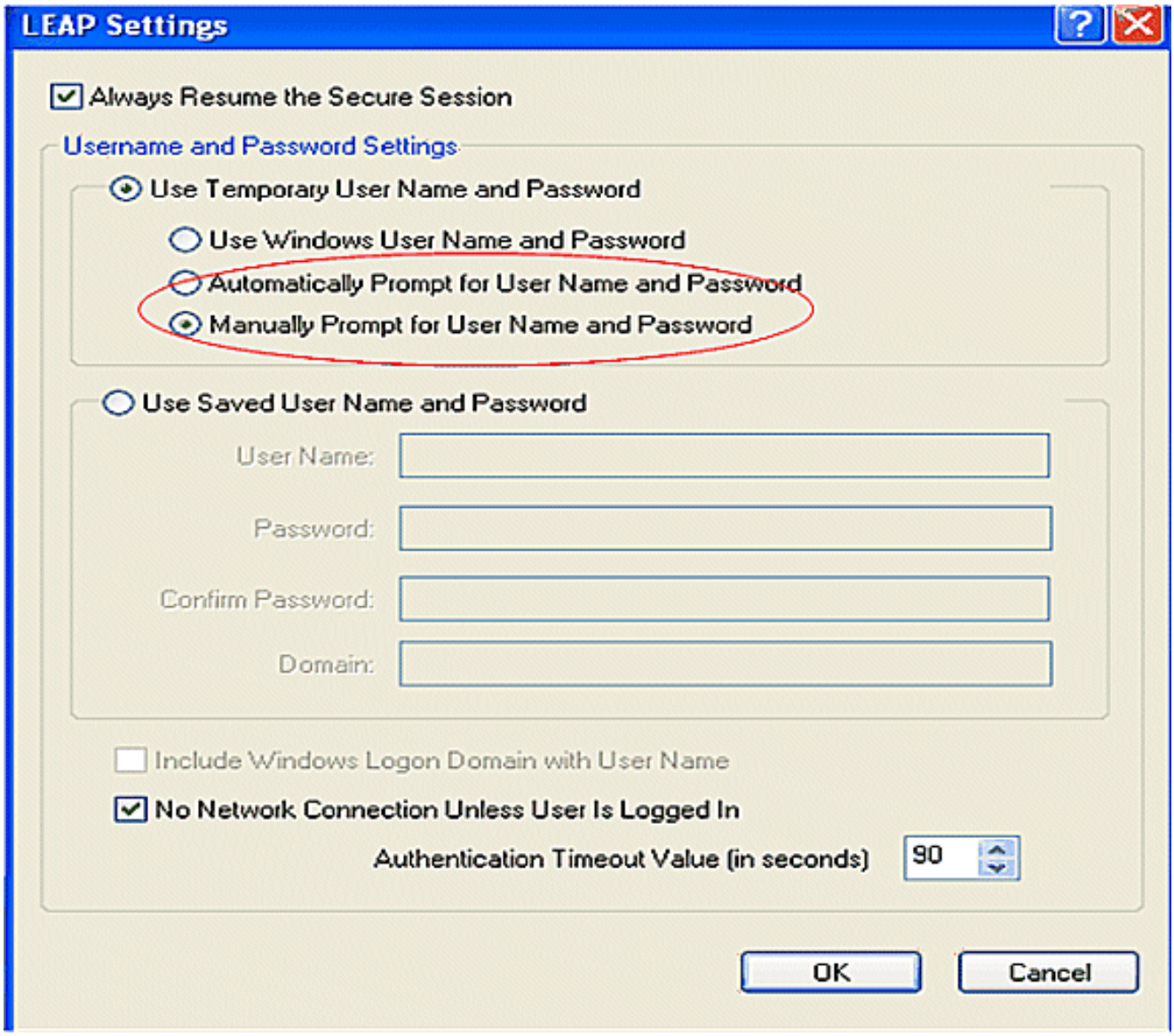
   En este ejemplo, el nombre del perfil y el SSID son wpa-dot1x.

   Nota: El SSID debe coincidir con el SSID que configuró en el ISR para autenticación WPA (con EAP).

2. En Profile Management, haga clic en la ficha Security, configure la opción de seguridad como WPA/WPA2/CCKM y elija el tipo de EAP WPA/WPA2/CCKM adecuado. Este documento utiliza LEAP como el tipo EAP para autenticación. Ahora, haga clic en Configure para configurar el nombre de usuario y la contraseña de LEAP.

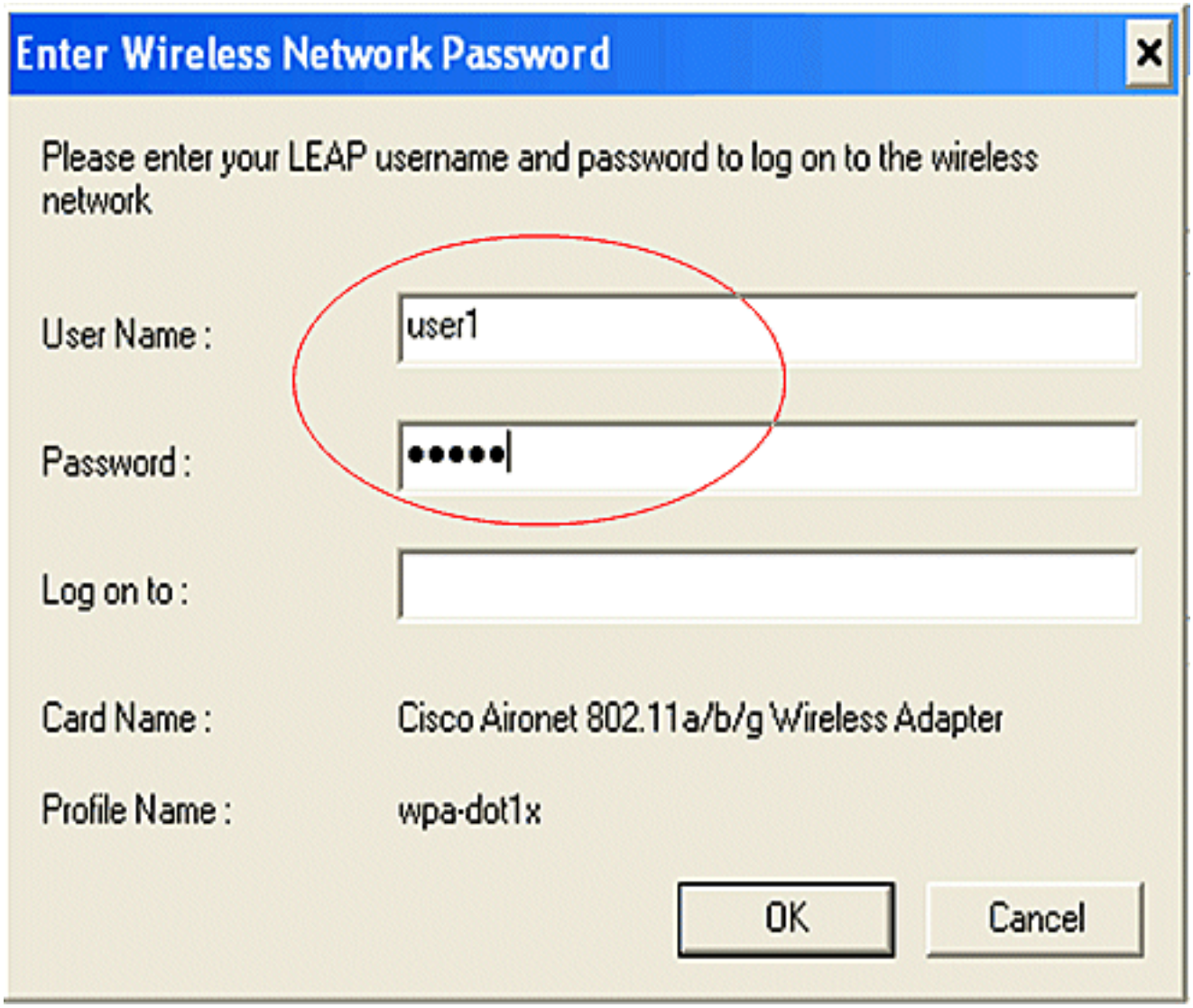


3. En este ejemplo, se elige Manually Prompt for User Name and Password en el área de configuraciones de nombre de usuario y contraseña para que se le solicite al cliente que ingrese el nombre de usuario y contraseña correctos cuando intenta conectarse a la red. Click OK.

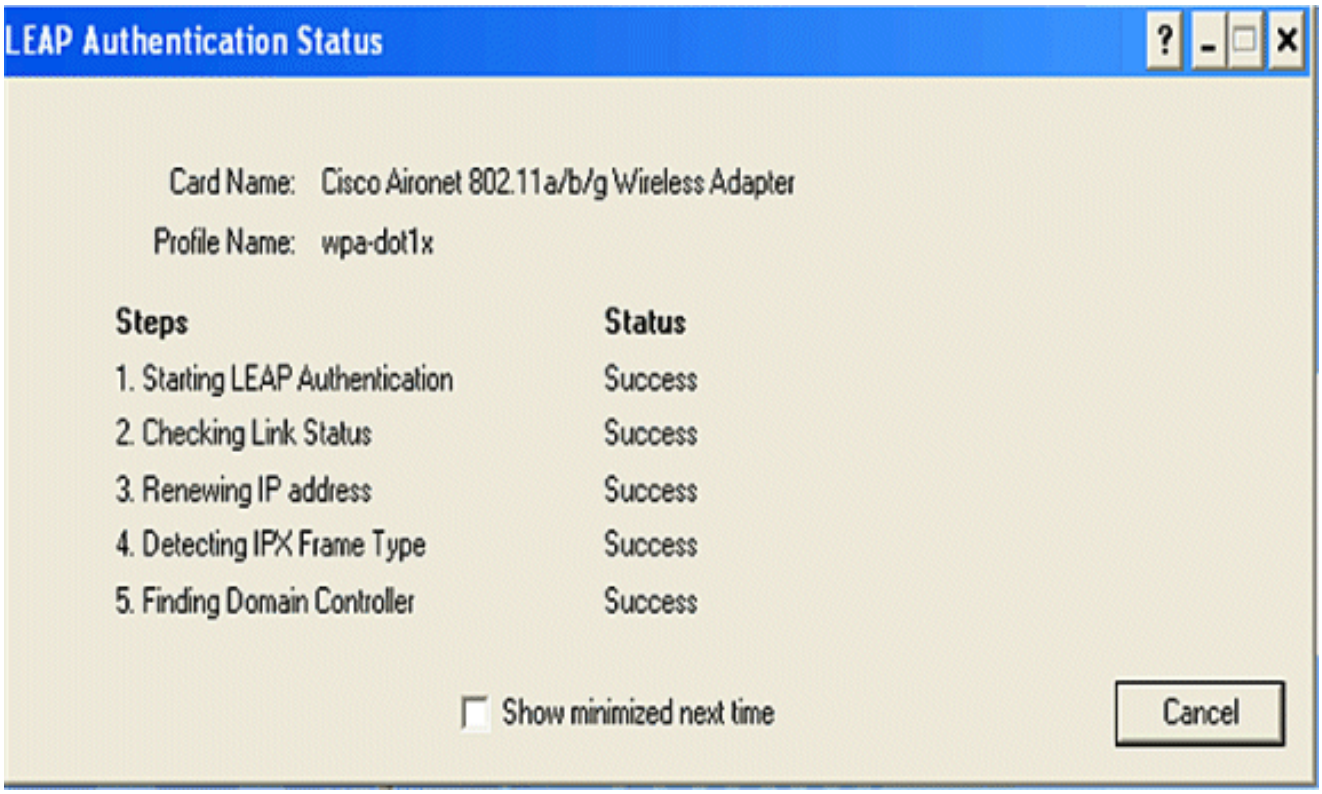


Use esta sección para confirmar que su configuración funciona correctamente.

1. Luego de crear el perfil del cliente, haga clic en Activate en la ficha Profile Management para activar el perfil wpa-dot1x. Se le solicita que ingrese el nombre de usuario y la contraseña LEAP. En este ejemplo, se utiliza el nombre de usuario y la contraseña user1. Click OK.



2. Puede observar si el cliente se autentica satisfactoriamente.



El comando show dot11 associations de la CLI del router muestra todos los detalles del estado de asociación del cliente. Aquí está un ejemplo.

Router#show dot11 associations

<#root>

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.3.0.2        CB21AG/PI21AG WCS             self         EAP-Assoc


SSID [open] :

SSID [pre-shared] : DISABLED, not associated with a configured VLAN

SSID [wpa-dot1x] :

SSID [wpa-shared] :


Others:  (not related to any ssid)
```

Troubleshoot

Comandos para resolución de problemas

Puede utilizar los comandos debug para resolver problemas de configuración.

- debug dot11 aaa authenticator all: Activa la depuración de los paquetes de autenticación MAC y EAP.
- debug radius authentication: Muestra las negociaciones de RADIUS entre el servidor y el cliente.
- debug radius local-server packets: Muestra el contenido de los paquetes RADIUS que se envían y se reciben.
- debug radius local-server client: Muestra los mensajes de error de las autenticaciones fallidas del cliente.

Información Relacionada

- Ejemplos de configuración de autenticación de controladores para redes LAN inalámbricas
- Configuración de VLAN en puntos de acceso
- Ejemplo de configuración de router inalámbrico ISR 1800 con DHCP interno y autenticación abierta
- Guía de configuración de puntos de acceso HWIC e ISR inalámbricos Cisco
- Ejemplo de configuración de conectividad de LAN inalámbrica mediante un ISR con encriptación WEP y autenticación LEAP
- Soporte Técnico y Documentación - Cisco Systems
- Configuración de los tipos de autenticación
- Ejemplo de configuración de conectividad de LAN inalámbrica mediante un ISR con encriptación WEP y autenticación LEAP

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).