Configuración de la Autenticación en Controladores de LAN Inalámbricos

Contenido

Introducción

Este documento proporciona ejemplos de configuración que explican cómo configurar diferentes tipos de métodos de autenticación de capa 1, capa 2 y capa 3 en controladores de LAN inalámbrica (WLC).

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de la configuración de los puntos de acceso ligeros (LAP) y los WLC de Cisco
- Conocimiento de los estándares de seguridad 802.11i

Componentes Utilizados

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

- Cisco 4400 WLC que ejecuta la versión de firmware 6.0.182.0
- Cisco 1000 Series LAP
- Adaptador de cliente inalámbrico Cisco 802.11a/b/g que utiliza firmware versión 2.6
- Servidor Cisco Secure ACS versión 3.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Autenticación en WLC

La solución de seguridad Cisco Unified Wireless Network (UWN) agrupa componentes de seguridad de punto de acceso (AP) 802.11 de capa 1, capa 2 y capa 3 potencialmente complicados en un gestor de políticas sencillo que personaliza las políticas de seguridad de todo el sistema en función de la LAN (WLAN) por conexión inalámbrica. La solución de seguridad Cisco UWN proporciona herramientas de gestión de seguridad sencillas, unificadas y sistemáticas.

Estos mecanismos de seguridad se pueden implementar en los WLC.

Soluciones de capa 1

Restrinja el acceso del cliente en función del número de intentos fallidos consecutivos.

Soluciones de capa 2

Ninguna autenticación : cuando se selecciona esta opción en la lista desplegable Seguridad de Capa 2, no se realiza ninguna autenticación de Capa 2 en la WLAN. Esto es lo mismo que la autenticación abierta del estándar 802.11.

WEP estática : con privacidad equivalente a conexión con cables estática (WEP), todos los puntos de acceso y las tarjetas NIC de radio cliente en una WLAN determinada deben utilizar la misma clave de cifrado. Cada estación de envío cifra el cuerpo de cada trama con una clave WEP antes de la transmisión, y la estación de recepción la descifra usando una clave idéntica en la recepción.

802.1x —Configura la WLAN para utilizar la autenticación basada en 802.1x. El uso de IEEE 802.1X ofrece un marco eficaz para autenticar y controlar el tráfico de los usuarios a una red protegida, así como para modificar dinámicamente las claves de cifrado. 802.1X vincula un protocolo denominado protocolo de autenticación extensible (EAP) a los medios por cable y WLAN y admite varios métodos de autenticación.

WEP estática + 802.1x : esta configuración de seguridad de capa 2 habilita tanto 802.1x como WEP estática. Los clientes pueden utilizar la autenticación estática WEP o 802.1x para conectarse a la red.

Acceso Wi-Fi protegido (WPA) : WPA o WPA1 y WPA2 son soluciones de seguridad basadas en estándares de Wi-Fi Alliance que proporcionan protección de datos y control de acceso para sistemas WLAN. WPA1 es compatible con el estándar IEEE 802.11i pero se implementó antes de la ratificación del estándar. WPA2 es la implementación de Wi-Fi Alliance del estándar IEEE 802.11i ratificado.

De forma predeterminada, WPA1 utiliza el protocolo de integridad de clave temporal (TKIP) y la comprobación de integridad de los mensajes (MIC) para la protección de datos. WPA2 utiliza el algoritmo de cifrado estándar de cifrado avanzado más fiable mediante el modo de contador con el protocolo de código de autenticación de mensajes de encadenamiento de bloques cifrados (AES-CCMP). Tanto WPA1 como WPA2 utilizan 802.1X para la administración de claves autenticadas de forma predeterminada. Sin embargo, estas opciones también están disponibles: PSK, CCKM y CCKM+802.1x. Si selecciona CCKM, Cisco solo permite clientes compatibles con CCKM. Si selecciona CCKM+802.1x, Cisco también permite clientes que no sean CCKM.

CKIP : Cisco Key Integrity Protocol (CKIP) es un protocolo de seguridad propiedad de Cisco para cifrar medios 802.11. CKIP mejora la seguridad 802.11 en el modo de infraestructura mediante la permutación de claves, MIC y el número de secuencia de mensajes. La versión de software 4.0 admite CKIP con clave estática. Para que esta función funcione correctamente, debe activar los elementos de información de Aironet (IE) para la WLAN. La configuración de CKIP especificada en una WLAN es obligatoria para cualquier cliente que intente asociarse. Si la WLAN se configura para la permutación de la clave CKIP y MMH MIC, el cliente debe soportar ambos. Si la WLAN está configurada para sólo una de estas funciones, el cliente debe soportar solamente esta función CKIP. Los WLC sólo admiten CKIP estático (como WEP estático). Los WLC no soportan CKIP con 802.1x (CKIP dinámico).

Soluciones de capa 3

Ninguno: cuando se selecciona esta opción en la lista desplegable de seguridad de Capa 3, no se realiza ninguna autenticación de Capa 3 en la WLAN.

Nota: El ejemplo de configuración para No Layer 3 authentication y No Layer 2 authentication se explica en la sección None Authentication.

Política Web (autenticación Web y paso a través de Web) : la autenticación Web la utilizan normalmente los clientes que desean implementar una red de acceso de invitado. En una red de acceso de invitado, hay autenticación inicial de nombre de usuario y contraseña, pero no se requiere seguridad para el tráfico subsiguiente. Las implementaciones típicas pueden incluir ubicaciones de "puntos de conexión", como T-Mobile o Starbucks.

La autenticación Web para el WLC de Cisco se realiza localmente. Cree una interfaz y, a continuación, asocie un identificador de conjunto de servicios/WLAN (SSID) a esa interfaz.

La autenticación Web proporciona autenticación simple sin un suplicante o cliente. Considere que la autenticación Web no proporciona la cifrado de datos. La autenticación Web se utiliza típicamente como acceso simple de invitados para “hot spot” o ambiente de campus donde la conectividad es la única preocupación.

El paso a través de la Web es una solución a través de la cual los usuarios inalámbricos se redirigen a una página de política de uso aceptable sin tener que autenticarse cuando se conectan a Internet. El propio WLC se encarga de esta redirección. El único requisito es configurar el WLC para el paso a través de la web, que es básicamente la autenticación web sin

tener que ingresar ninguna credencial.

Paso a través de VPN —VPN Passthrough es una función que permite a un cliente establecer un túnel solamente con un servidor VPN específico. Por lo tanto, si necesita acceder de forma segura al servidor VPN configurado así como a otro servidor VPN o a Internet, esto no es posible con el paso a través de VPN habilitado en el controlador.

En las secciones siguientes, se proporcionan ejemplos de configuración para cada uno de los mecanismos de autenticación.

Ejemplos de Configuración

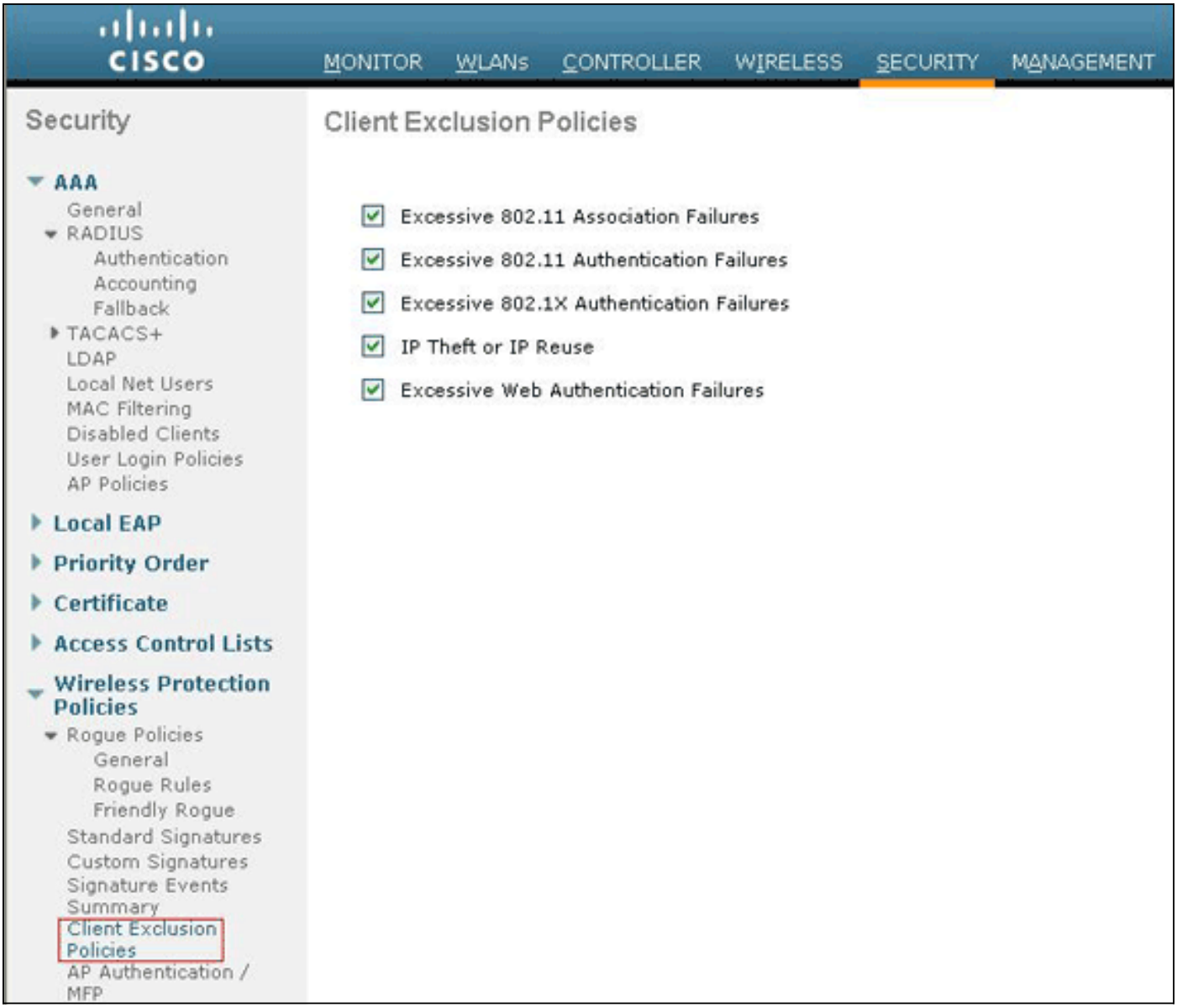
Antes de configurar las WLAN y los tipos de autenticación, debe configurar el WLC para el funcionamiento básico y registrar los LAPs en el WLC. Este documento asume que el WLC está configurado para el funcionamiento básico y que los LAPs están registrados en el WLC. Si es un usuario nuevo que intenta configurar el WLC para el funcionamiento básico con los LAP, consulte Registro de Lightweight AP (LAP) en un controlador de LAN inalámbrica (WLC).

Soluciones de seguridad de capa 1

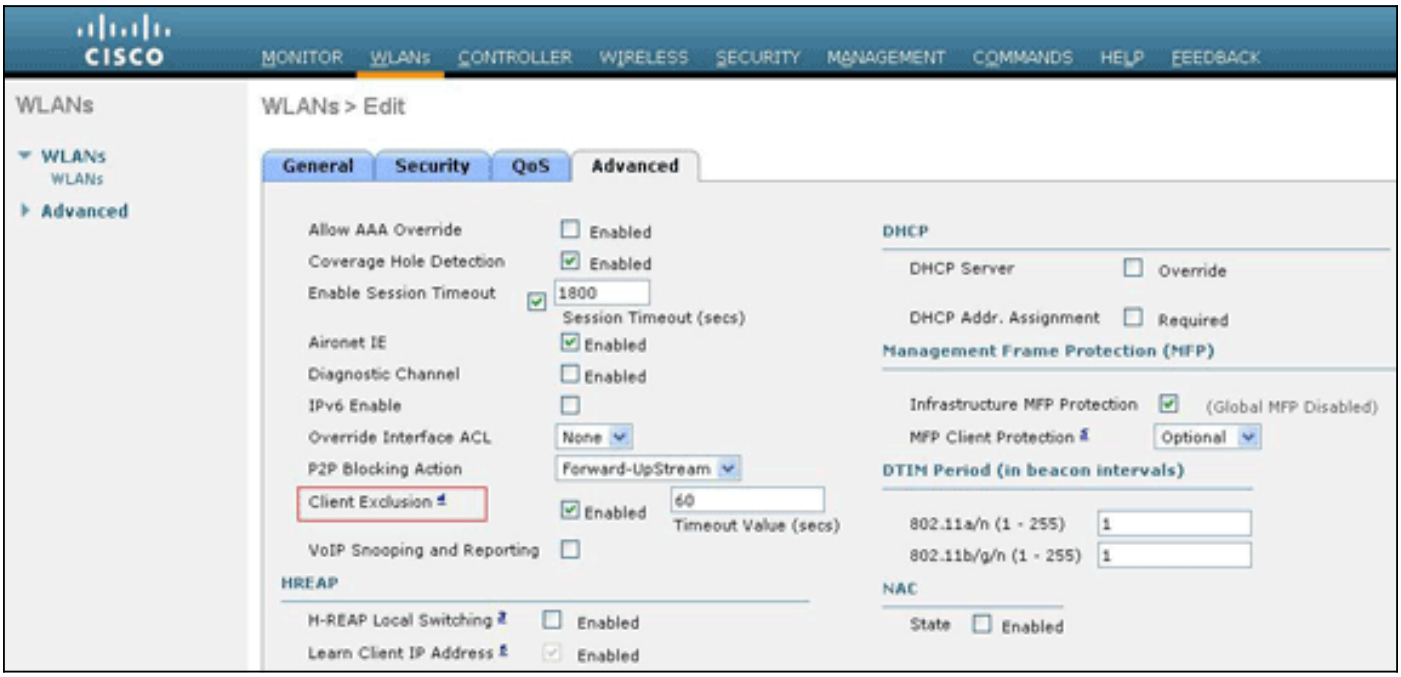
Los clientes inalámbricos pueden restringirse el acceso en función del número de intentos fallidos consecutivos para acceder a la red WLAN. La exclusión del cliente ocurre en estas condiciones de forma predeterminada. Estos valores no se pueden cambiar.

- Fallo de autenticación 802.11 consecutivo (5 veces consecutivas, se excluye el sexto intento)
- Fallas de asociación 802.11 consecutivas (5 veces consecutivas, se excluye el sexto intento)
- Fallas de autenticación 802.1x consecutivas (3 veces consecutivas, se excluye el cuarto intento)
- Falla del servidor de directivas externo
- Intento de utilizar una dirección IP ya asignada a otro dispositivo (robo de IP o reutilización de IP)
- Autenticación web consecutiva (se excluye el cuarto intento de 3 veces consecutivas)

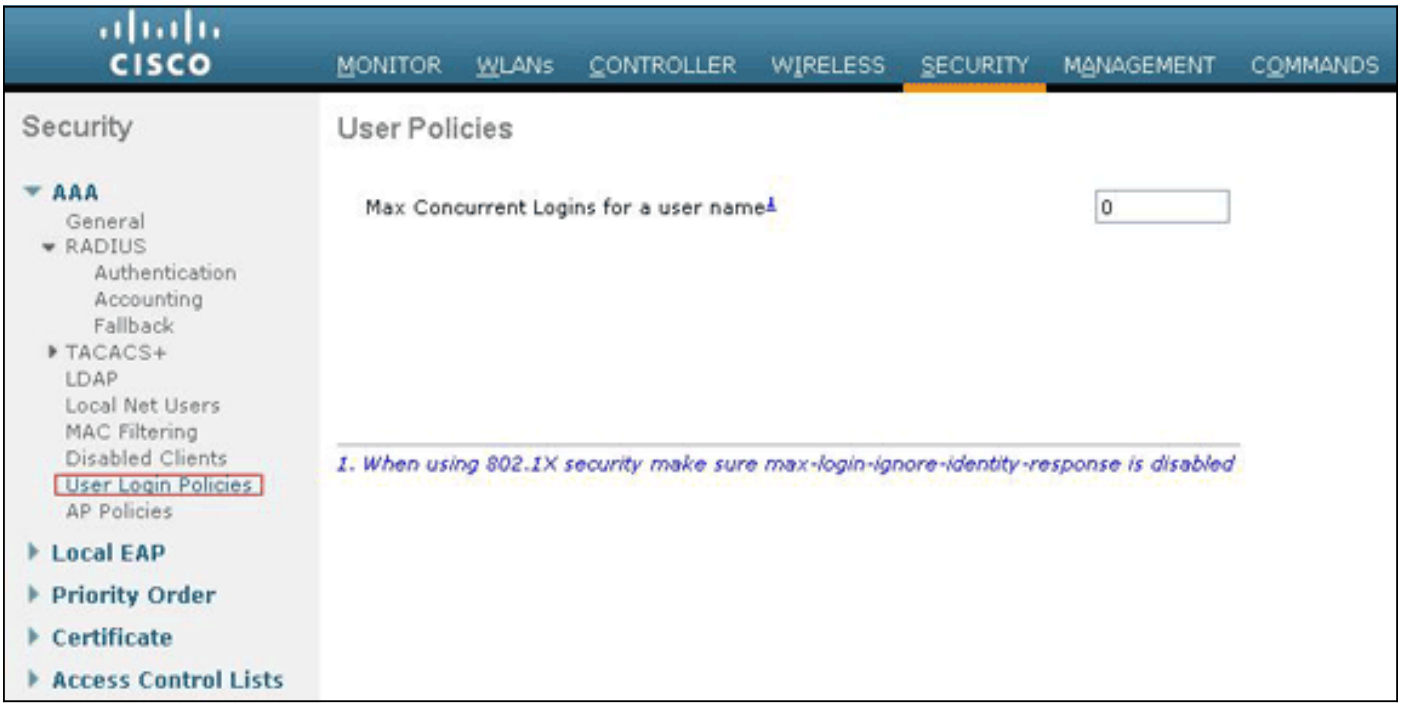
Para localizar las Políticas de Exclusión de Cliente, haga clic en **Seguridad** en el menú superior y luego elija **Políticas de Protección Inalámbrica > Políticas de Exclusión de Cliente** la navegación en el lado izquierdo de la página.



Se puede configurar el temporizador de exclusión. Las opciones de exclusión se pueden activar o desactivar por controlador. El temporizador de exclusión se puede habilitar o inhabilitar por WLAN.



De forma predeterminada, el número máximo de inicios de sesión simultáneos para un único nombre de usuario es 0. Puede introducir cualquier valor entre 0 y 8. Este parámetro se puede establecer en **SECURITY > AAA > User Login Policies** y le permite especificar el número máximo de inicios de sesión simultáneos para un único nombre de cliente, entre uno y ocho, o 0 = ilimitado. Aquí tiene un ejemplo:

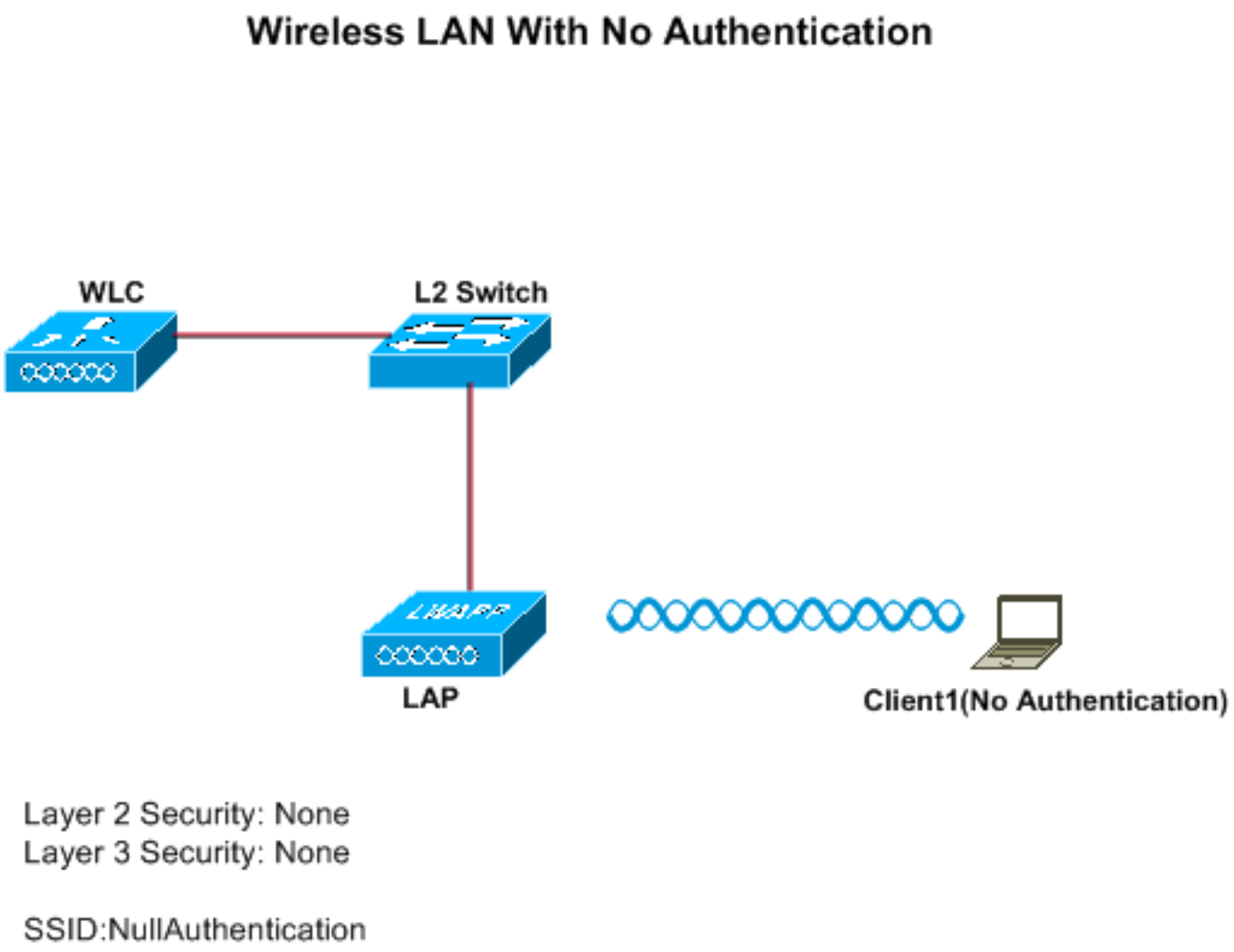


Soluciones de seguridad de capa 2

Ninguna autenticación

Este ejemplo muestra una WLAN configurada sin autenticación.

Nota: Este ejemplo también funciona para Sin autenticación de Capa 3.



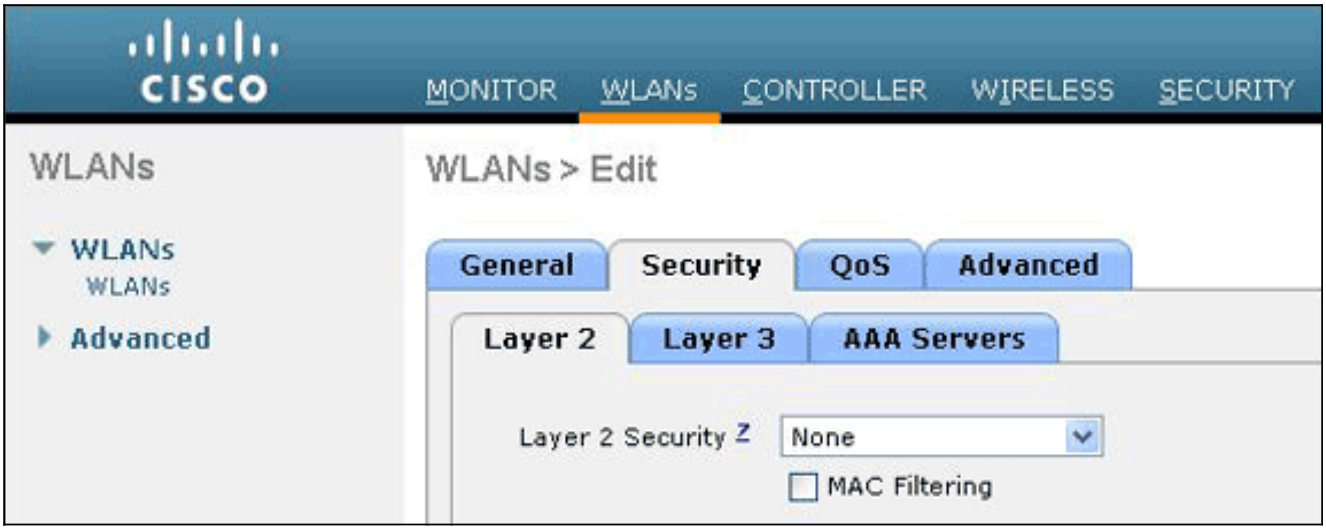
Configuración del WLC para Sin Autenticación

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic en **WLAN en la GUI para crear una WLAN.**Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.
2. Haga clic en **Ir** para configurar una nueva WLAN.
3. Introduzca los parámetros para la WLAN. Este ejemplo muestra la configuración para esta WLAN.

4. Haga clic en Apply (Aplicar).
5. En la ventana WLAN > Edit , defina los parámetros específicos de la WLAN.
6. Haga clic en la pestaña **Seguridad** y elija **Ninguno** para la seguridad de Capa 2 y Capa

3.



Nota: Para que una WLAN se active, el estado debe estar habilitado. Para habilitarlo, marque la casilla de verificación **Estado** en la ficha General.Esto habilita No authentication para esta WLAN.

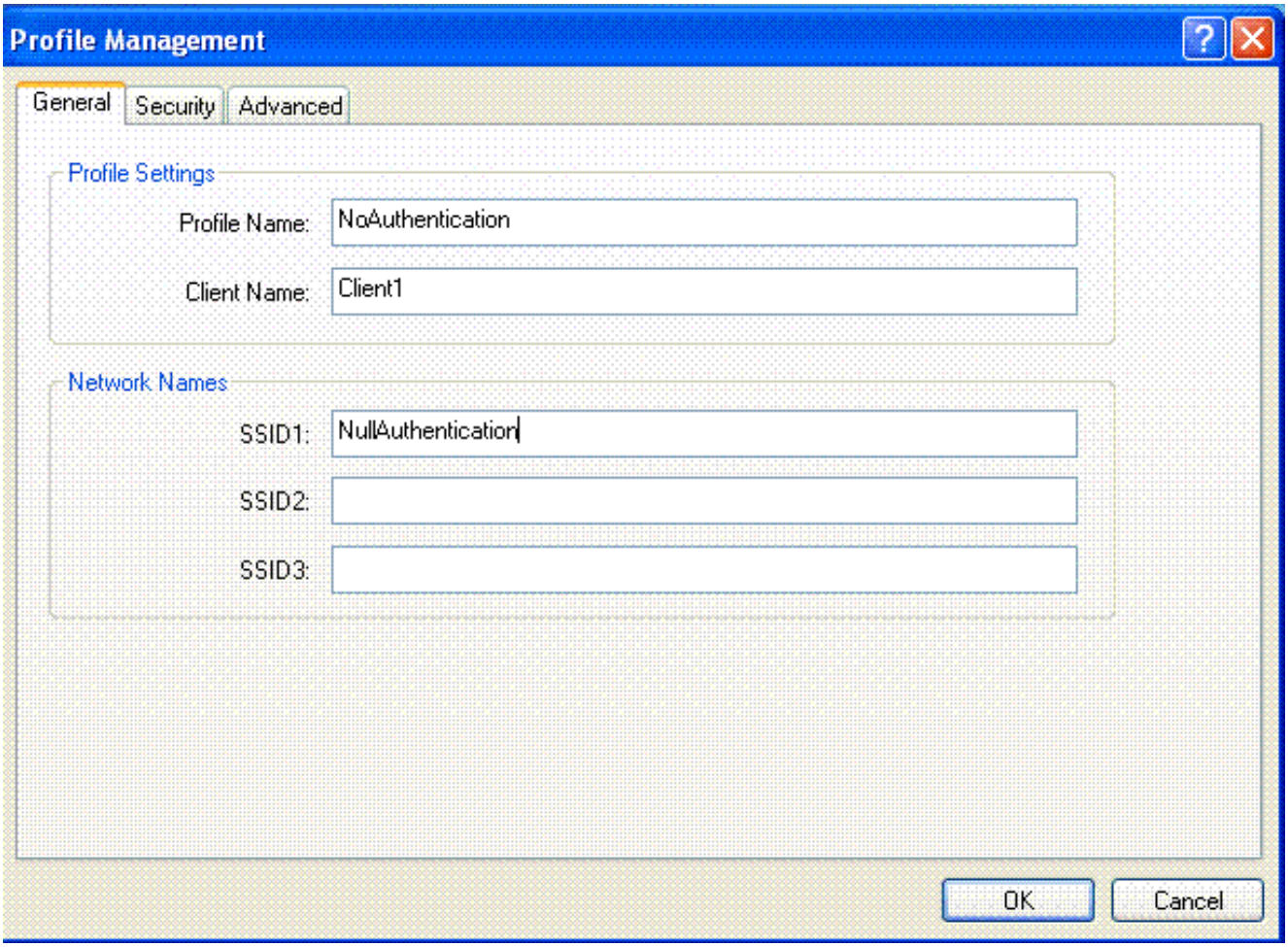
7. Elija otros parámetros en función de sus requisitos de diseño. Este ejemplo utiliza los valores predeterminados.
8. Haga clic en Apply (Aplicar).

Configuración del cliente inalámbrico para ausencia de autenticación

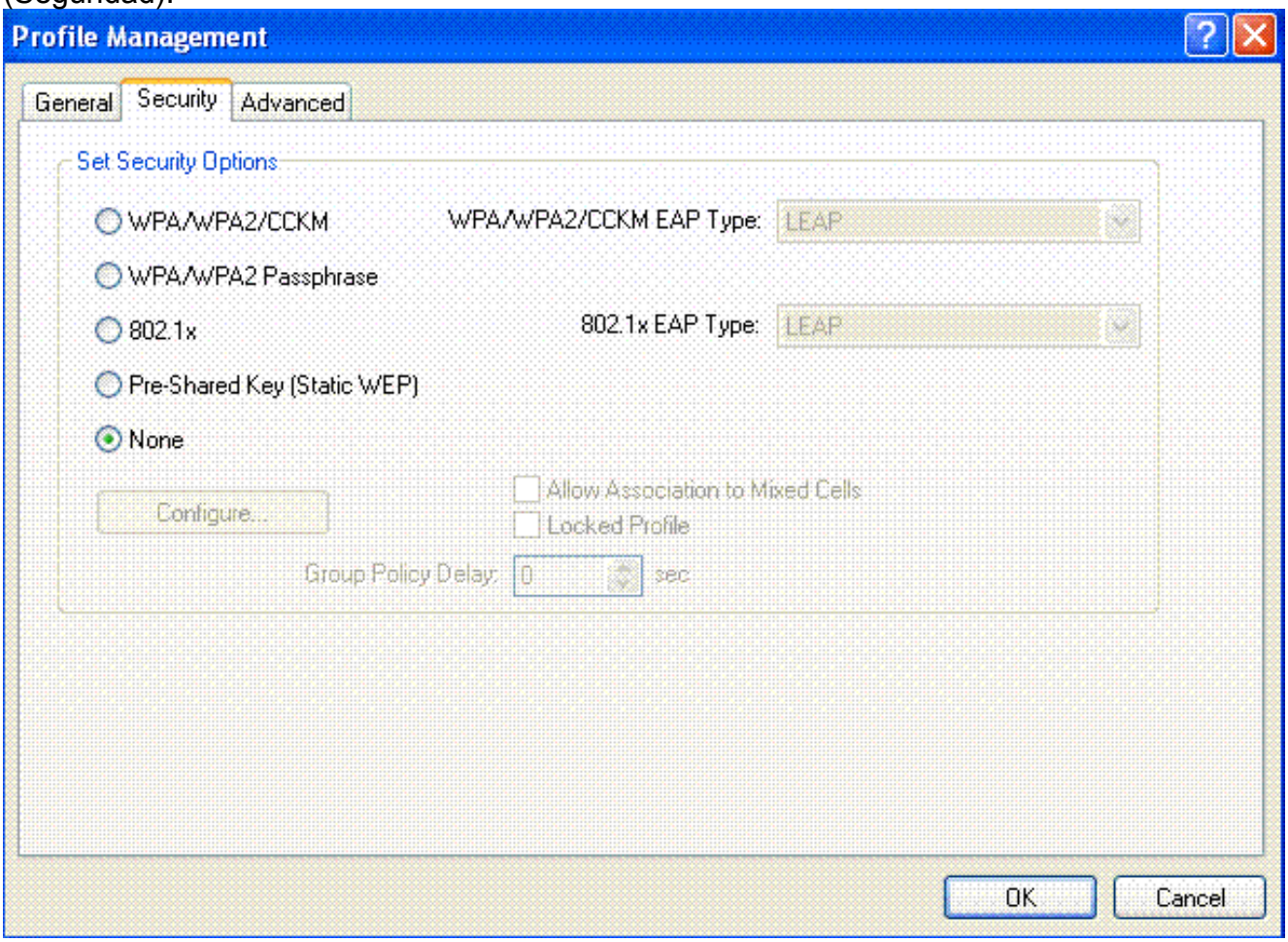
Complete estos pasos para configurar el cliente de LAN inalámbrica para esta configuración:

Nota: Este documento utiliza un Aironet 802.11a/b/g Client Adapter que ejecuta firmware 3.5 y explica la configuración del adaptador del cliente con ADU versión 3.5.

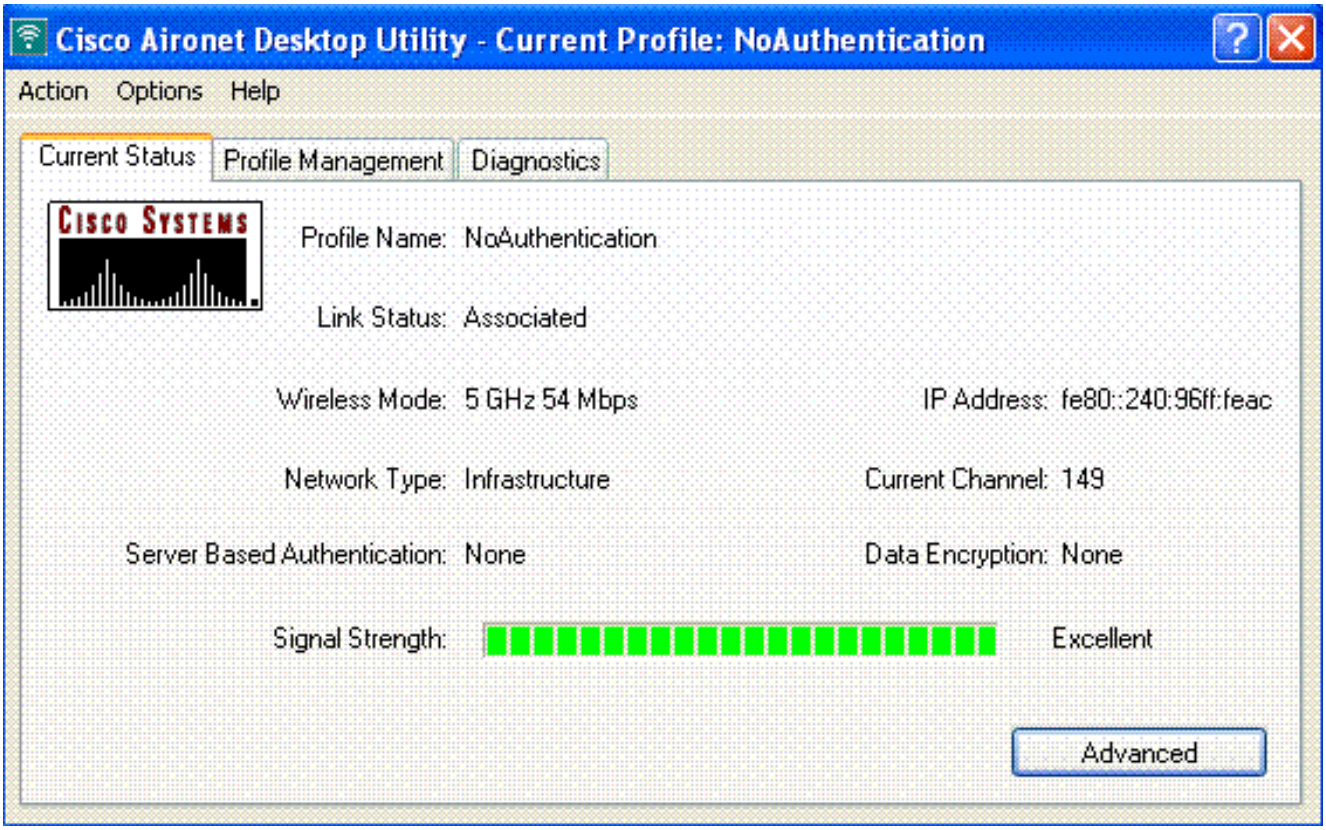
1. Para crear un nuevo perfil, haga clic en la pestaña **Administración de perfiles** en la ADU.
2. Haga clic en **New**.
3. Cuando se muestra la ventana Administración de Perfil (Generales), complete estos pasos para establecer el Nombre de Perfil, Nombre del Cliente, y SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *NoAuthentication* como nombre de perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza *Cliente 1* para el nombre del cliente.En Nombres de Red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es el mismo que el SSID que configuró en el WLC. El SSID en este ejemplo es
NullAuthentication.



4. Haga clic en la ficha Security (Seguridad).

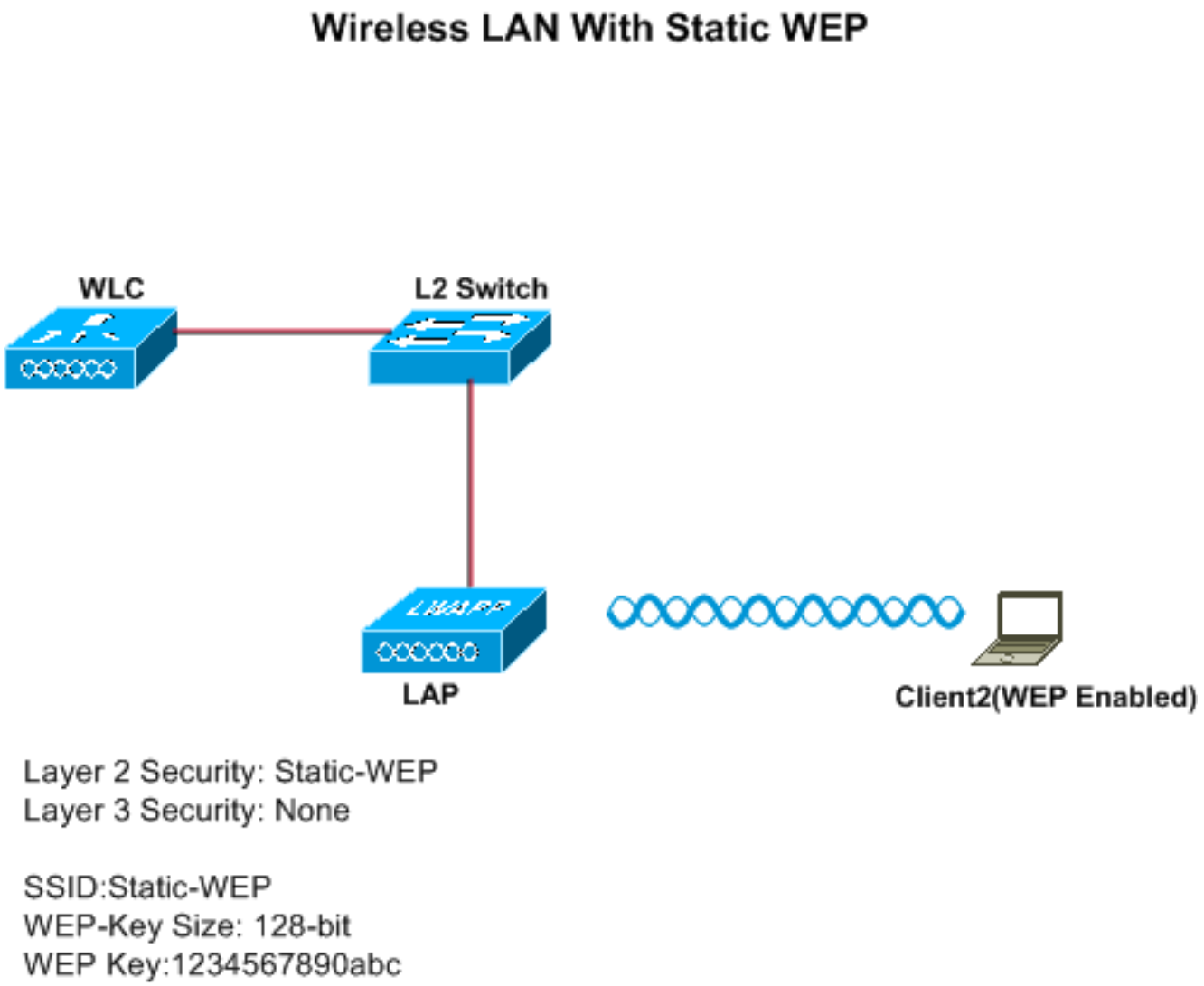


5. Haga clic en el botón de opción **Ninguno** en Establecer opciones de seguridad y, a continuación, haga clic en **Aceptar**.Cuando se activa el SSID, el cliente inalámbrico se conecta a la WLAN sin ninguna autenticación.



WEP estática

Este ejemplo muestra una WLAN configurada con WEP estática.



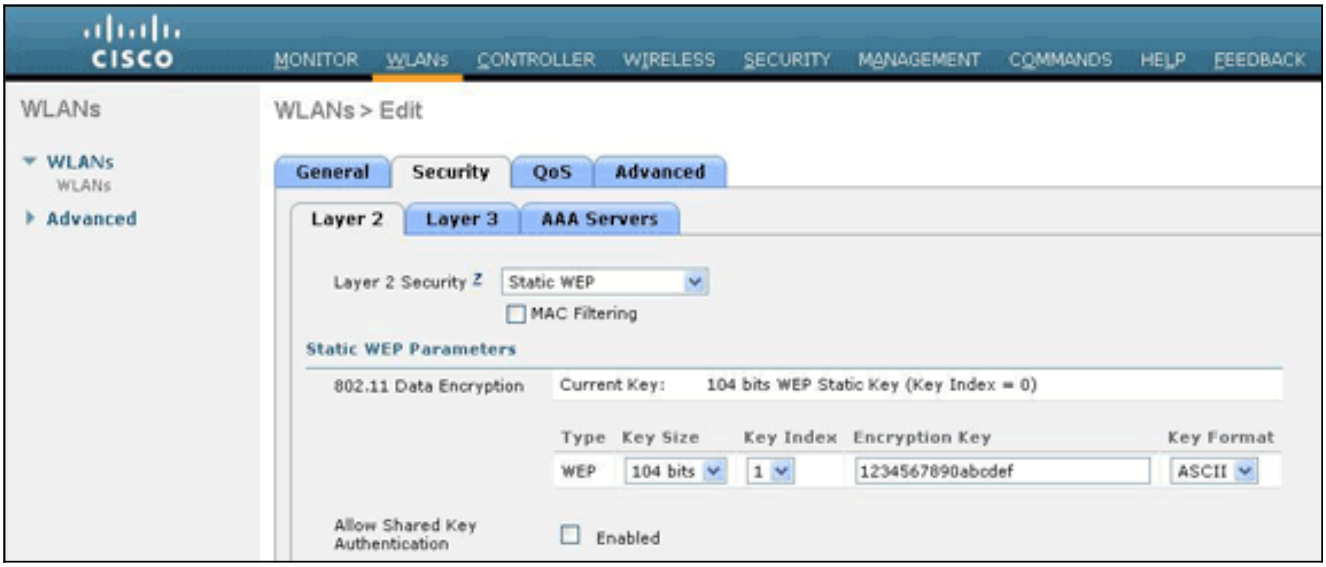
Configuración del WLC para el WEP Estático

Complete estos pasos para configurar el WLC para esta configuración:

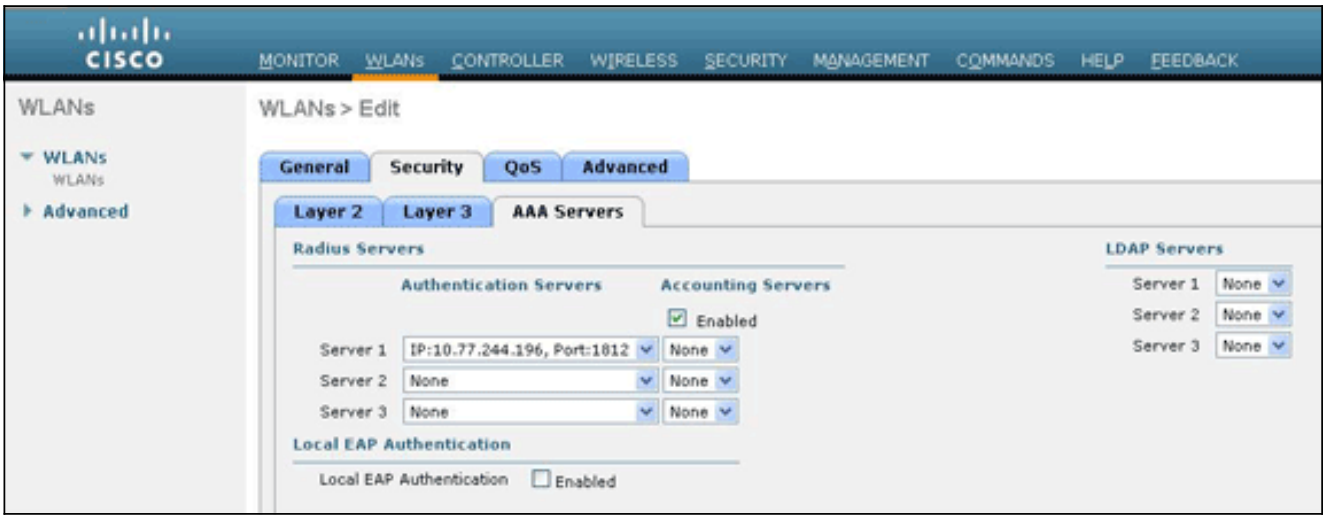
1. Haga clic en **WLAN en la GUI para crear una WLAN.**Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.
2. Haga clic en **Nuevo para configurar una WLAN nueva.**
3. Introduzca el ID de WLAN y el SSID de WLAN.En este ejemplo, la WLAN se denomina *StaticWEP* y el ID de WLAN es *2*.

4. Haga clic en Apply (Aplicar).

5. En la ventana WLAN > Edit , defina los parámetros específicos de la WLAN.En la lista desplegable Capa 2, elija **WEP estática**.Esto habilita el WEP estático para esta WLAN.En Static WEP Parameters (Parámetros WEP estáticos), elija el tamaño de clave WEP y el índice de clave, e introduzca la clave de encriptación WEP estática.El tamaño de la clave puede ser 40 bits o 104 bits. El índice de claves puede estar entre 1 y 4. Se puede aplicar un único índice de clave WEP a cada WLAN. Debido a que sólo hay cuatro índices de clave WEP, sólo se pueden configurar cuatro WLAN para el cifrado estático de capa 2 WEP. En este ejemplo, se utiliza el WEP de 104 bits y la clave WEP utilizada es 1234567890abcdef.



Verifique si el servidor Radius está configurado para la autenticación. El servidor Radius se puede configurar en la pestaña **Seguridad** ubicada en **AAA > Radius > Authentication**. Una vez configurado, el servidor Radius se debe asignar a la WLAN para la autenticación. Vaya a **WLANs > Security > AAA Servers** para asignar el servidor Radius a la WLAN para la autenticación.En este ejemplo, 10.77.244.196 es el servidor Radius.



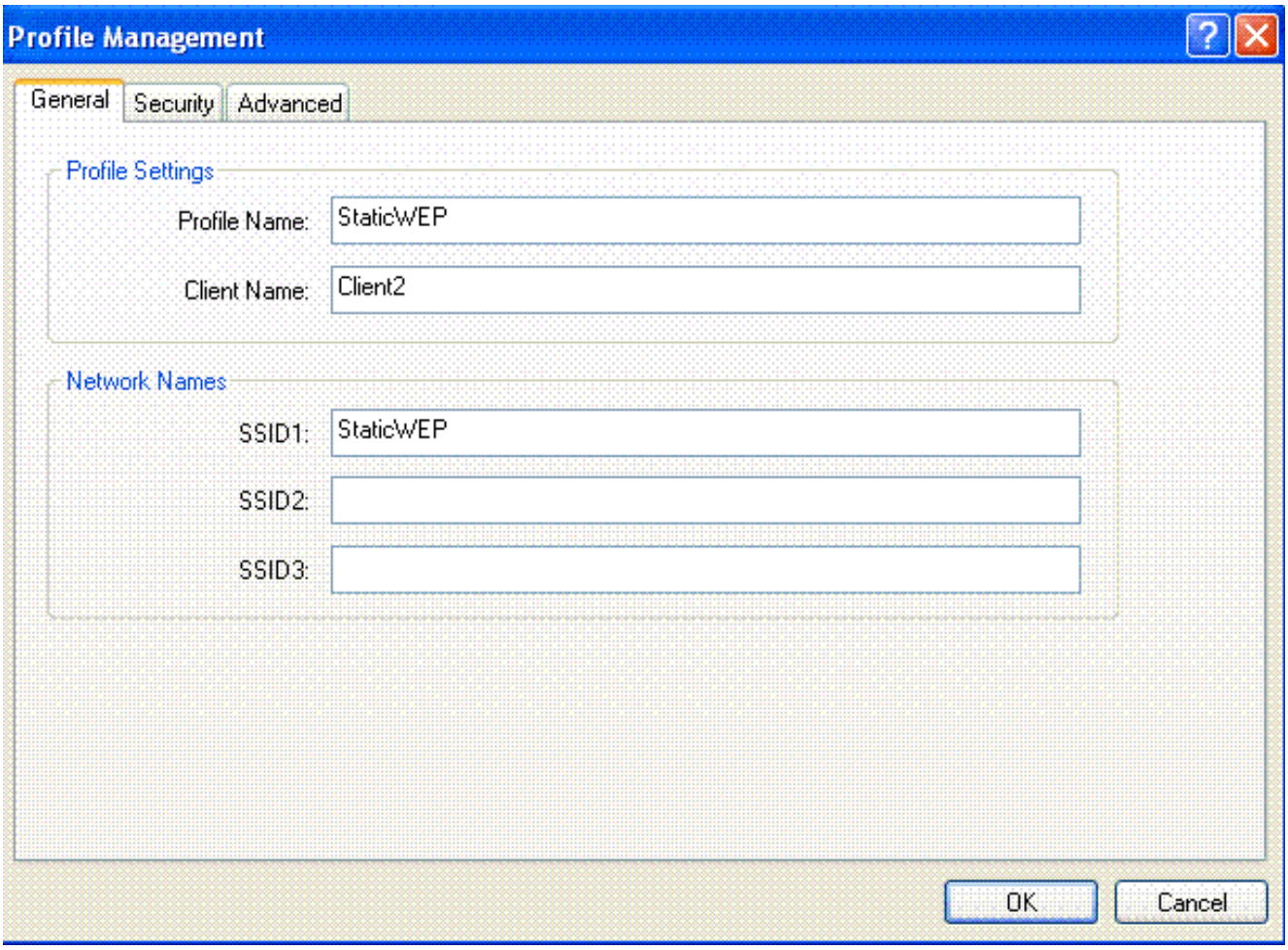
6. Elija otros parámetros en función de sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.
7. Haga clic en Apply (Aplicar).**Nota:** WEP siempre se representa en hexadecimal (hexadecimal). Cuando ingresa la clave WEP en ASCII, la cadena WEP ASCII se convierte en hexadecimal, que se utiliza para cifrar el paquete. No hay un método estándar que los proveedores realicen para convertir el hexadecimal en ASCII, ya que algunos lo harán al relleno mientras que otros no. Por lo tanto, para lograr la máxima compatibilidad entre

proveedores, utilice hex para las claves WEP.**Nota:** Si desea habilitar la autenticación de clave compartida para la WLAN, marque la casilla de verificación **Permitir autenticación de clave compartida** en Parámetros WEP estáticos. De esta manera, si el cliente también está configurado para la autenticación de clave compartida, la autenticación de clave compartida seguida de la encriptación WEP de los paquetes tendrá lugar en la WLAN.

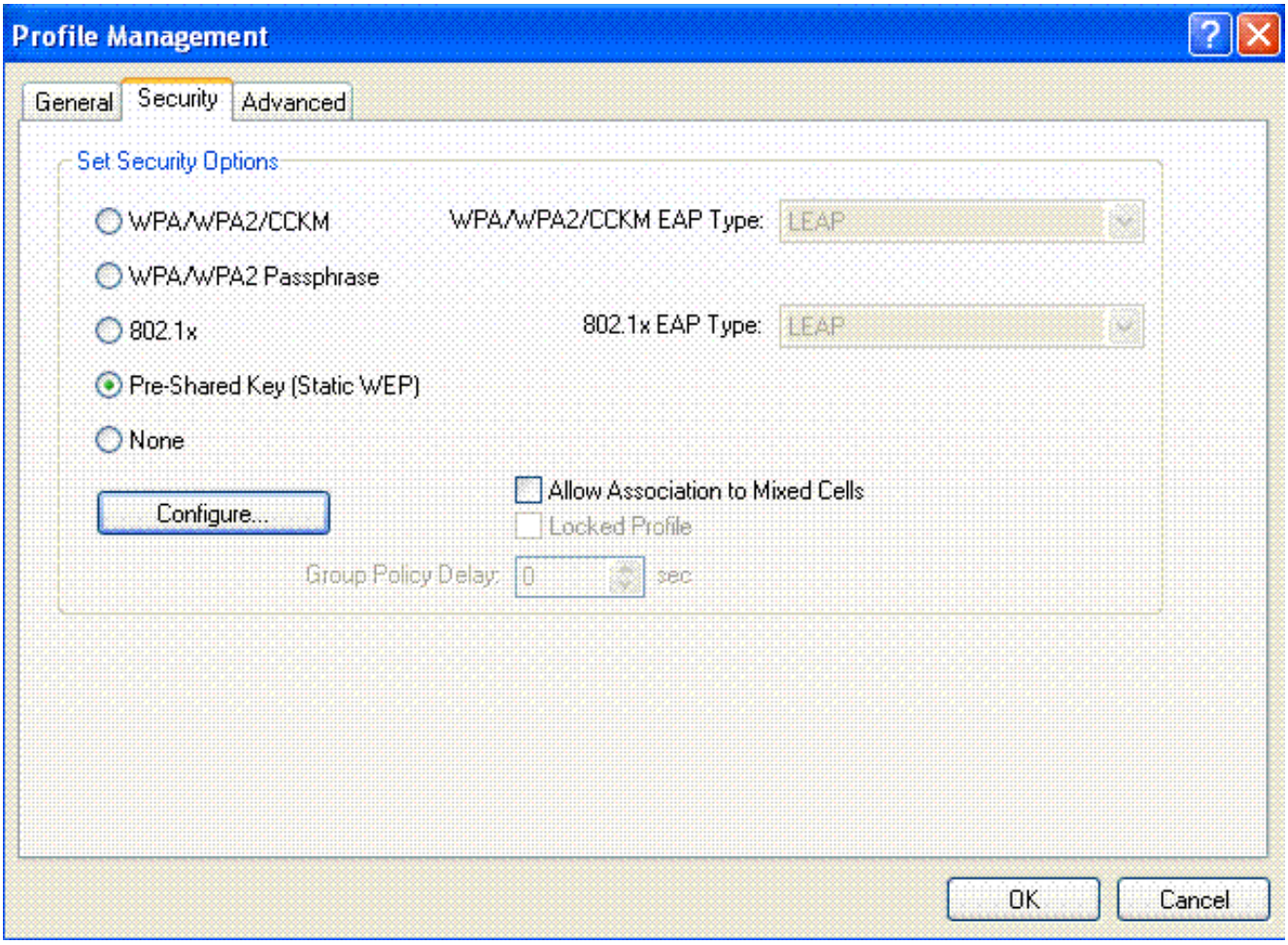
Configuración del cliente inalámbrico para WEP estática

Complete estos pasos para configurar el Wireless LAN Client para esta configuración:

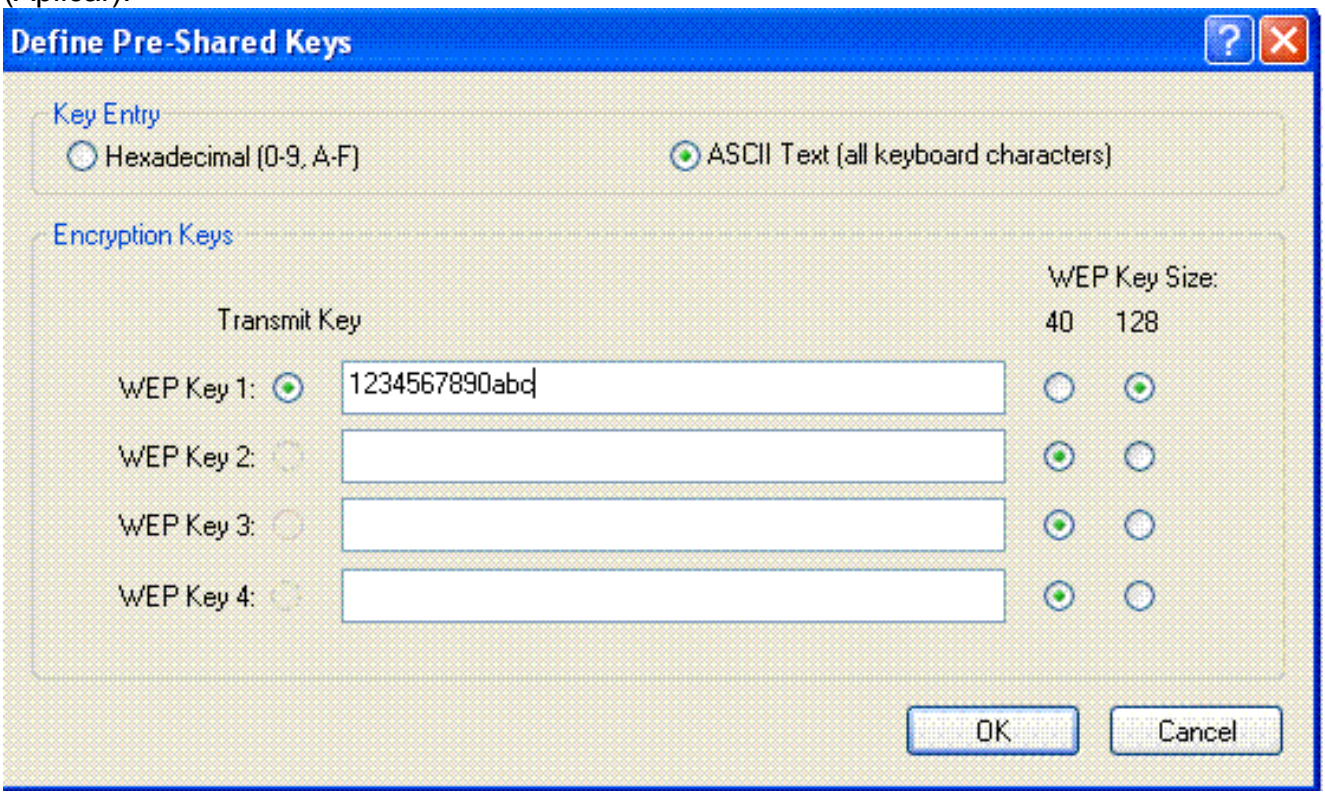
1. Para crear un nuevo perfil, haga clic en la pestaña **Administración de perfiles** en la ADU.
2. Haga clic en **New**.
3. Cuando se muestra la ventana Administración de Perfil (Generales), complete estos pasos para establecer el Nombre de Perfil, Nombre del Cliente, y SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *StaticWEP* como nombre de perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza *Cliente 2* para el nombre del cliente.En Nombres de Red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es el mismo que el SSID que configuró en el WLC. El SSID en este ejemplo es *StaticWEP*.



4. Haga clic en la ficha Security (Seguridad).

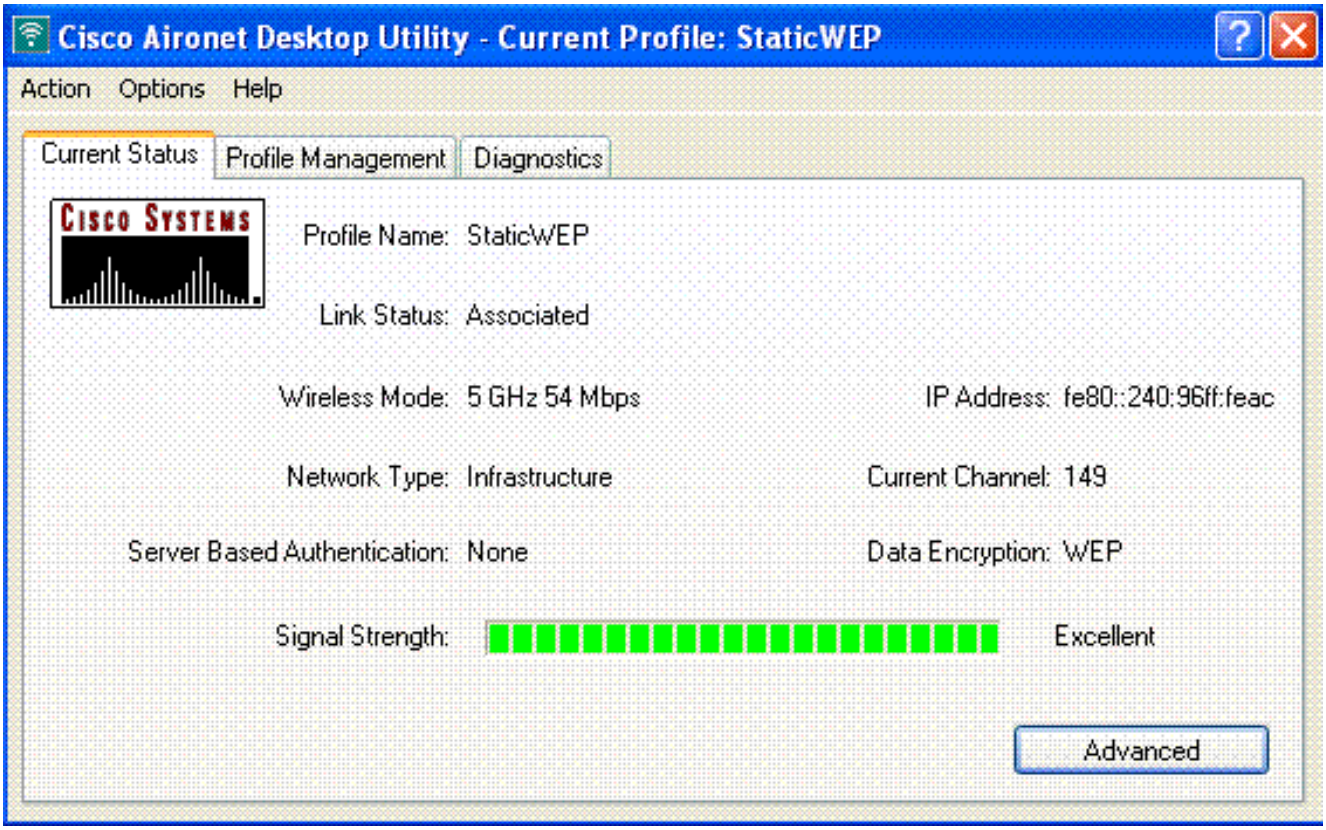


5. Elija **Pre-Shared Key (Static WEP)** en Set Security Options (Establecer opciones de seguridad).
6. Haga clic en **Configure** y defina el tamaño de la clave WEP y la clave WEP.Esto debe coincidir con la clave WEP configurada en el WLC para esta WLAN.
7. Haga clic en Apply (Aplicar).



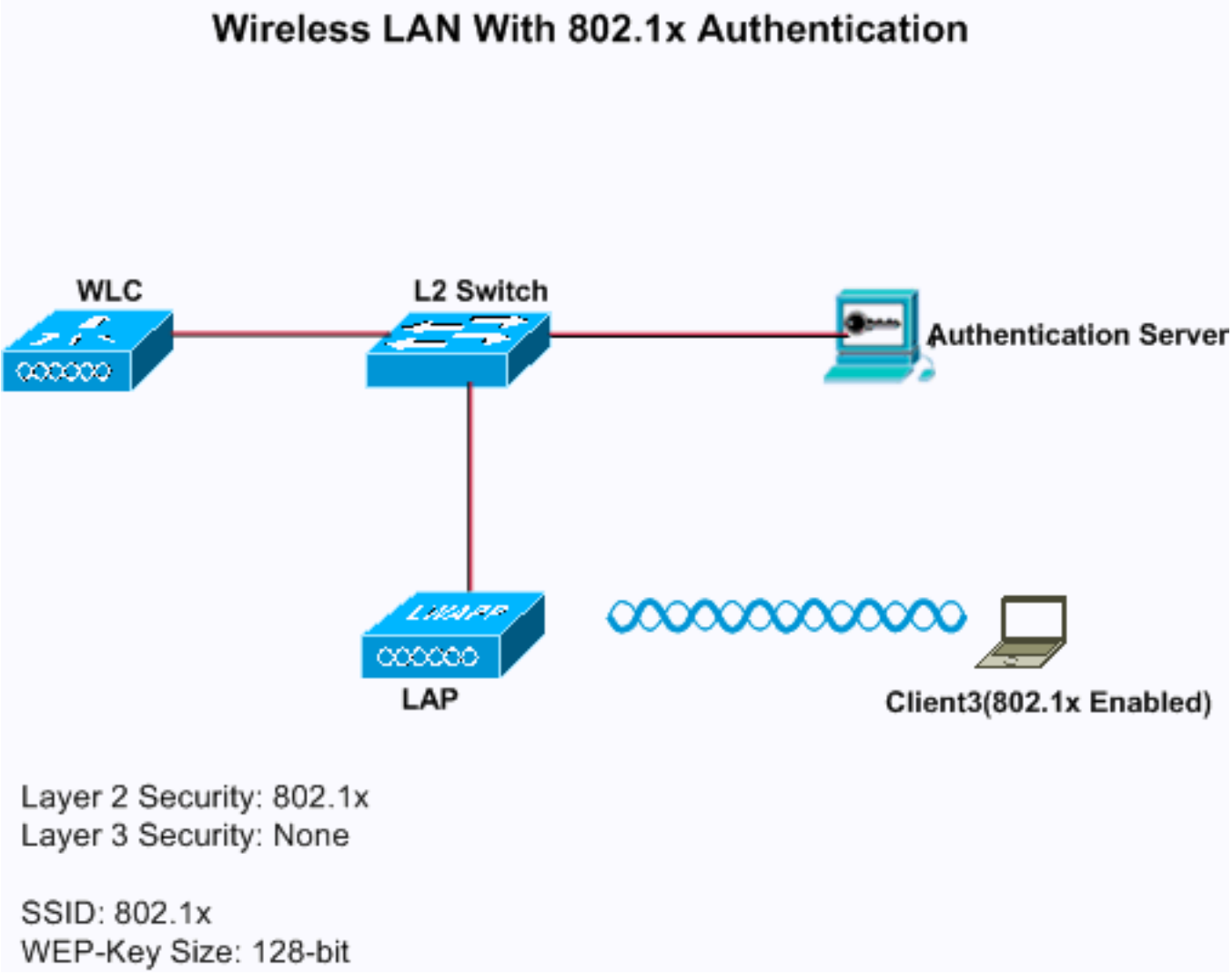
Cuando se activa el SSID, el cliente inalámbrico se conecta a la WLAN y los paquetes se

cifran mediante la clave WEP
estática.



Autenticación 802.1x

Este ejemplo muestra una WLAN configurada con autenticación 802.1x.



Configuración del WLC para la autenticación 802.1x

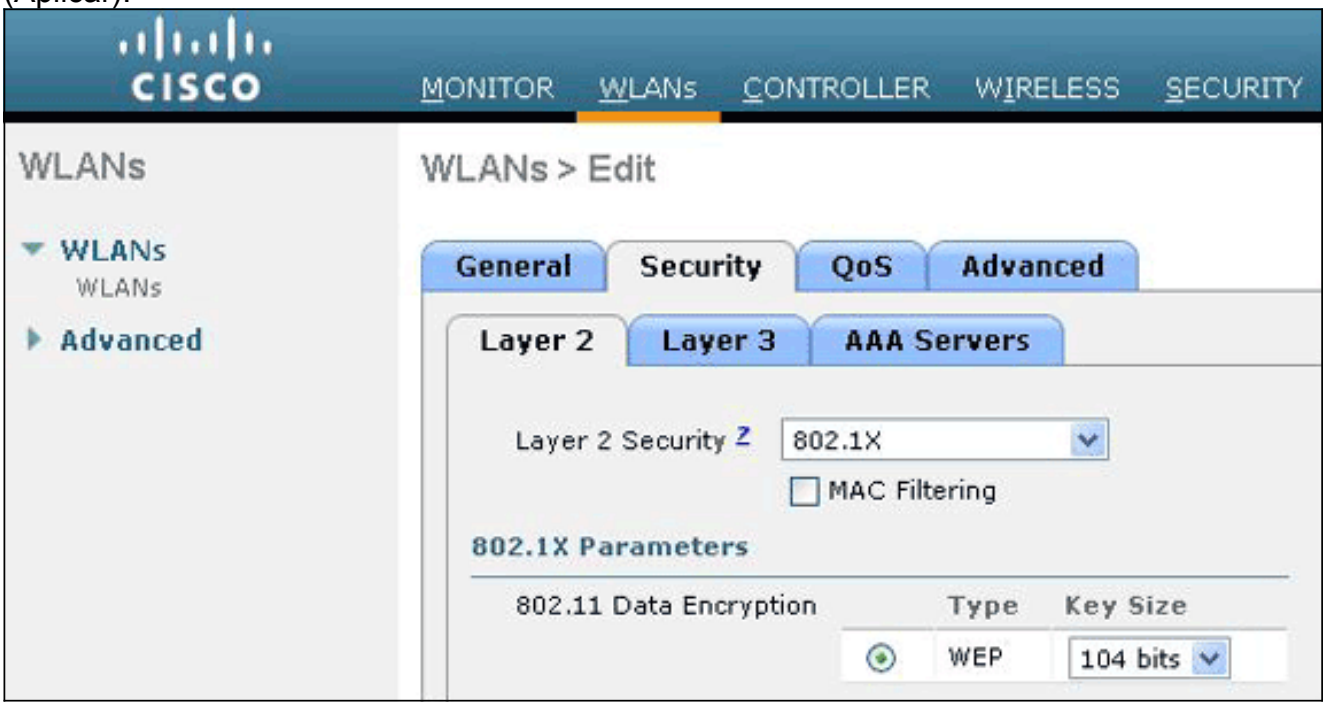
Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic en **WLAN en la GUI para crear una WLAN.**Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.
2. Haga clic en **Nuevo para configurar una WLAN nueva.**En este ejemplo, la WLAN se denomina *802.1x*, y el ID de WLAN es *3*. También se debe agregar un nombre de perfil.

3. Haga clic en Apply (Aplicar).
4. En la ventana WLAN > Edit , defina los parámetros específicos de la WLAN.En la lista desplegable Capa 2, elija **802.1x**.**Nota:** Solo está disponible la encriptación WEP con 802.1x.

Elija 40 bits o 104 bits para el cifrado, y asegúrese de que la seguridad de Capa 3 esté establecida en Ninguno.Esto habilita la autenticación 802.1x para esta WLAN.En Parámetros del servidor RADIUS, seleccione el servidor RADIUS que se utilizará para autenticar las credenciales del cliente.Elija otros parámetros en función de sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.

5. Haga clic en Apply (Aplicar).



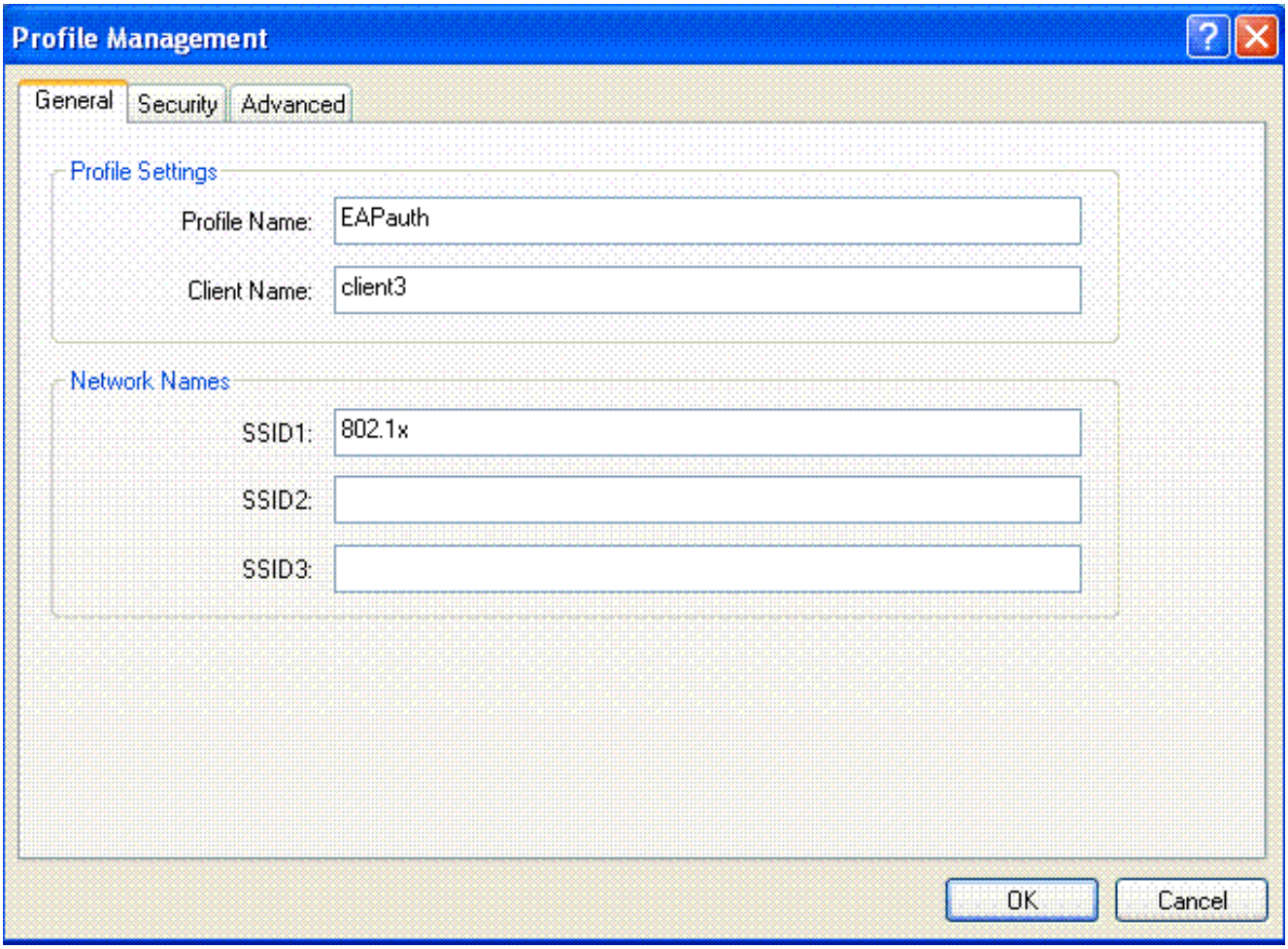
Notas: Si elige *802.1x* para la seguridad de Capa 2, no se puede utilizar CCKM.Si elige *WPA 1* o *WPA 2* para la seguridad de Capa 2, estas opciones aparecen en Administración de claves de autenticación:*802.1x+CCKM*: si elige esta opción, se admiten tanto clientes CCKM como no CCKM (CCKM opcional).*802.1x*: si elige esta opción, sólo se admiten clientes 802.1x.*CCKM*: si elige esta opción, sólo se admiten clientes CCKM, donde los clientes se dirigen a un servidor externo para la autenticación.*PSK* : si elige esta opción, se utiliza una clave previamente compartida para el WLC y el cliente. Además, todos los estándares se han establecido para que se utilicen antes de los estándares previos; por ejemplo, WPA/WPA2 precede a CCKM cuando se utiliza simultáneamente.El tipo de autenticación EAP utilizado para validar los clientes depende del tipo EAP configurado en el servidor RADIUS y en los clientes inalámbricos. Una vez que se habilita 802.1x en el WLC, el WLC permite que todos los tipos de paquetes EAP fluyan entre el LAP, el cliente inalámbrico y el servidor RADIUS.Estos documentos proporcionan ejemplos de configuración en algunos de los tipos de autenticación EAP:PEAP en redes inalámbricas unificadas con ACS 4.0 y Windows 2003EAP-TLS en Unified Wireless Network con ACS 4.0 y Windows 2003Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)

Configuración del cliente inalámbrico para la autenticación 802.1x

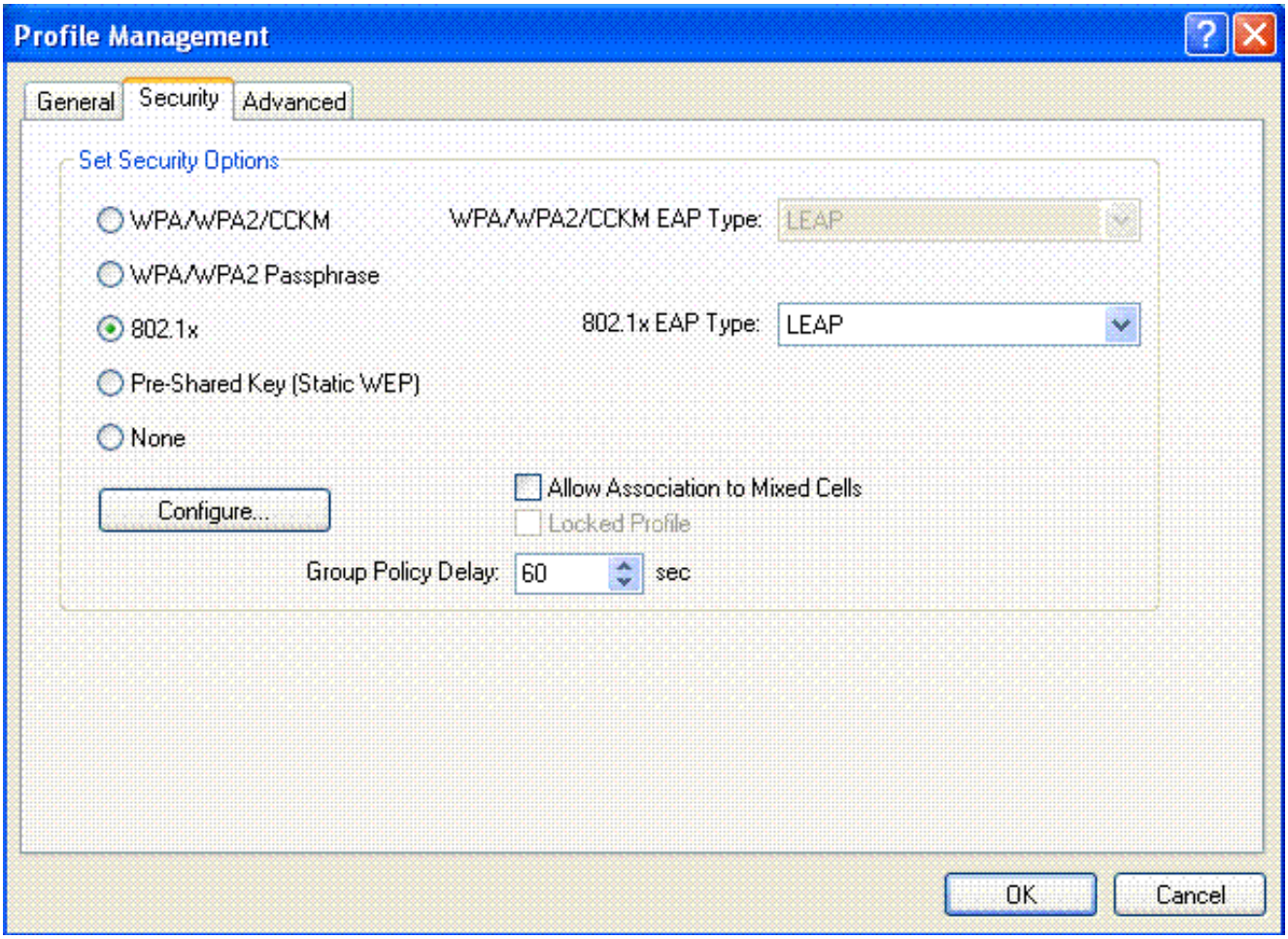
Complete estos pasos para configurar el Wireless LAN Client para esta configuración:

1. Para crear un nuevo perfil, haga clic en la pestaña **Administración de perfiles** en la ADU.
2. Haga clic en **New**.
3. Cuando se muestra la ventana Administración de Perfil (Generales), complete estos pasos

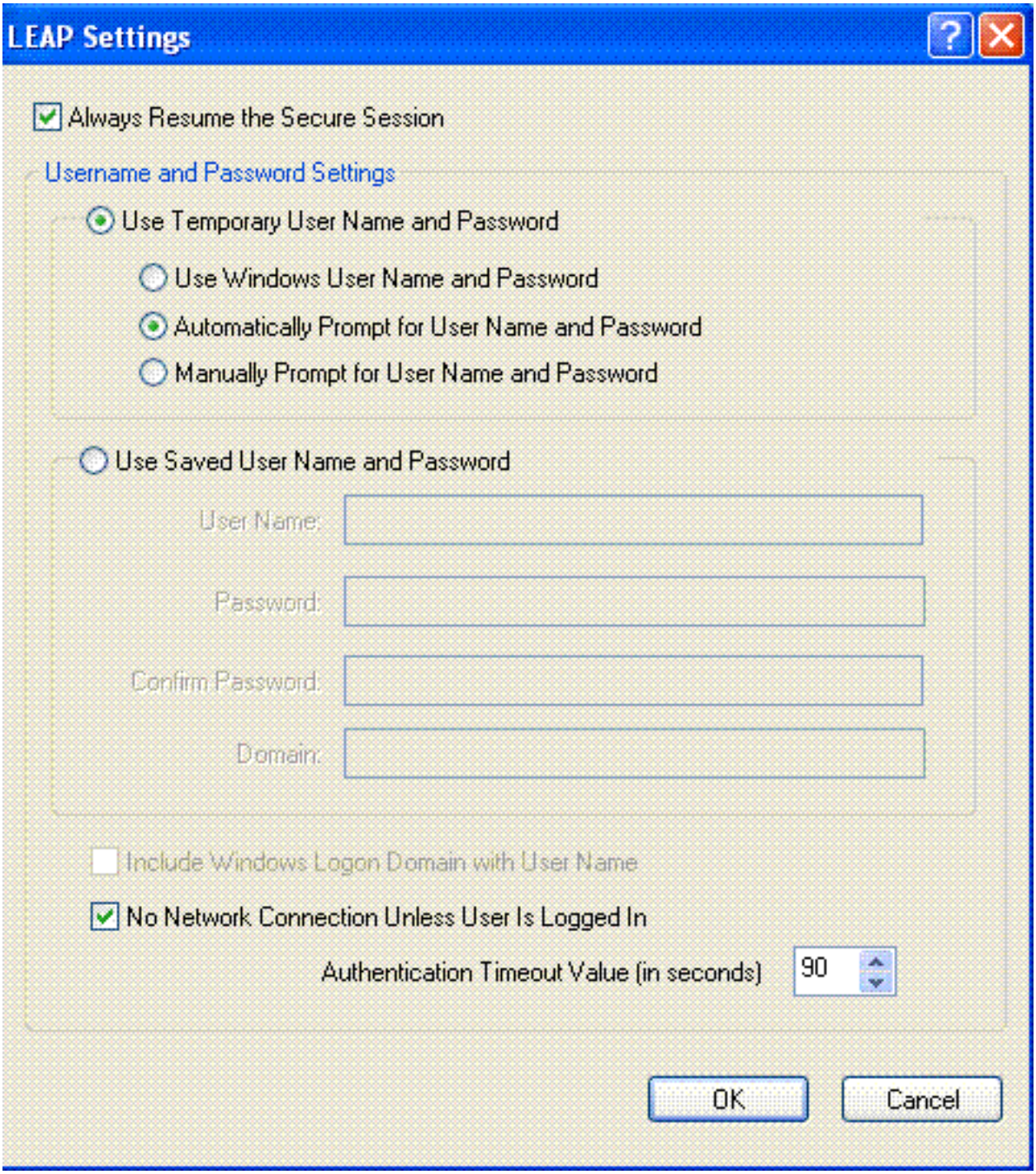
para establecer el Nombre de Perfil, Nombre del Cliente, y SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *EAPAuth* como nombre de perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza *Cliente 3* para el nombre del cliente.En Nombres de Red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es el mismo que el SSID que configuró en el WLC. El SSID en este ejemplo es
802.1x.



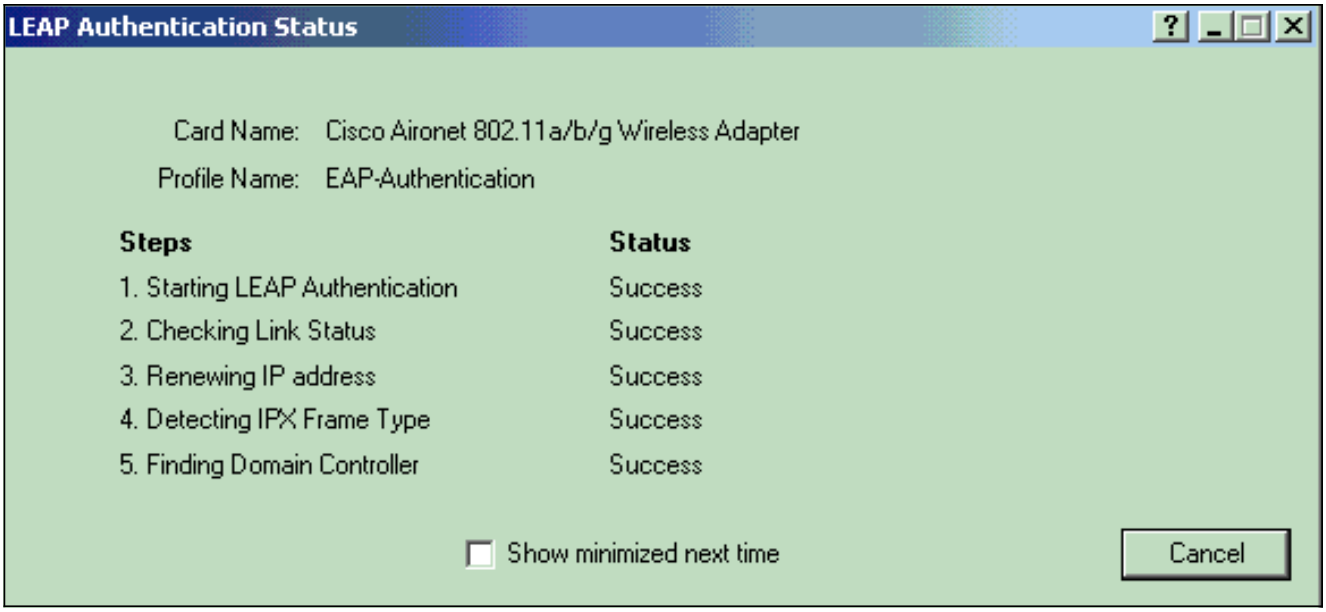
4. Haga clic en la ficha Security
(Seguridad).



5. Haga clic en el botón de opción **802.1x**.
6. En la lista desplegable 802.1x EAP Type , elija el tipo de EAP utilizado.
7. Haga clic en **Configure** para configurar los parámetros específicos del tipo EAP seleccionado.

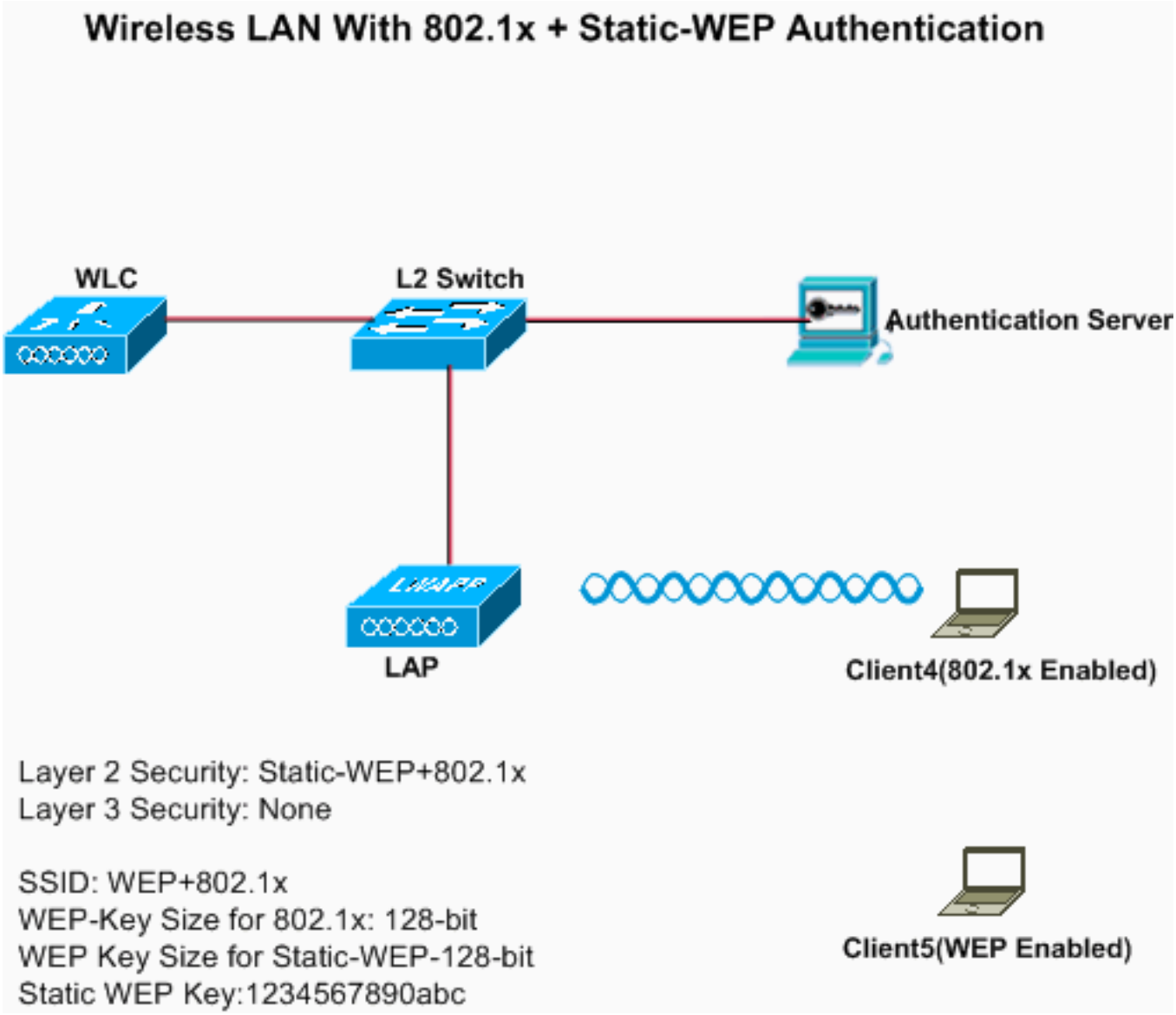


8. Haga clic en Apply (Aplicar).Cuando se activa el SSID, el cliente inalámbrico se conecta a la WLAN mediante la autenticación 802.1x. Las claves WEP dinámicas se utilizan para las sesiones.



WEP estática + autenticación 802.1x

Este ejemplo muestra una WLAN configurada con autenticación estática WEP + 802.1x.



Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic en **WLAN en la GUI para crear una WLAN.**Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.
2. Haga clic en **Nuevo para configurar una WLAN nueva.**
3. Introduzca el ID de WLAN y el SSID de WLAN.En este ejemplo, la WLAN se denomina *WEP+802.1x*, y el ID de WLAN es *4*.

4. Haga clic en Apply (Aplicar).
5. En la ventana WLAN > Edit , defina los parámetros específicos de la WLAN.En la lista desplegable Capa 2, elija **Static-WEP+802.1x**.Esto habilita la autenticación estática WEP y 802.1x para esta WLAN.En Parámetros del servidor RADIUS, seleccione el servidor RADIUS que se utilizará para autenticar las credenciales del cliente mediante 802.1x y configure el servidor RADIUS como se muestra en el ejemplo anterior.En Static WEP Parameters (Parámetros WEP estáticos), seleccione el tamaño de la clave WEP y el índice de clave, e introduzca la clave de encriptación WEP estática, como se muestra en la imagen anterior.Elija otros parámetros en función de sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.

Configuración del cliente inalámbrico para WEP estática y 802.1x

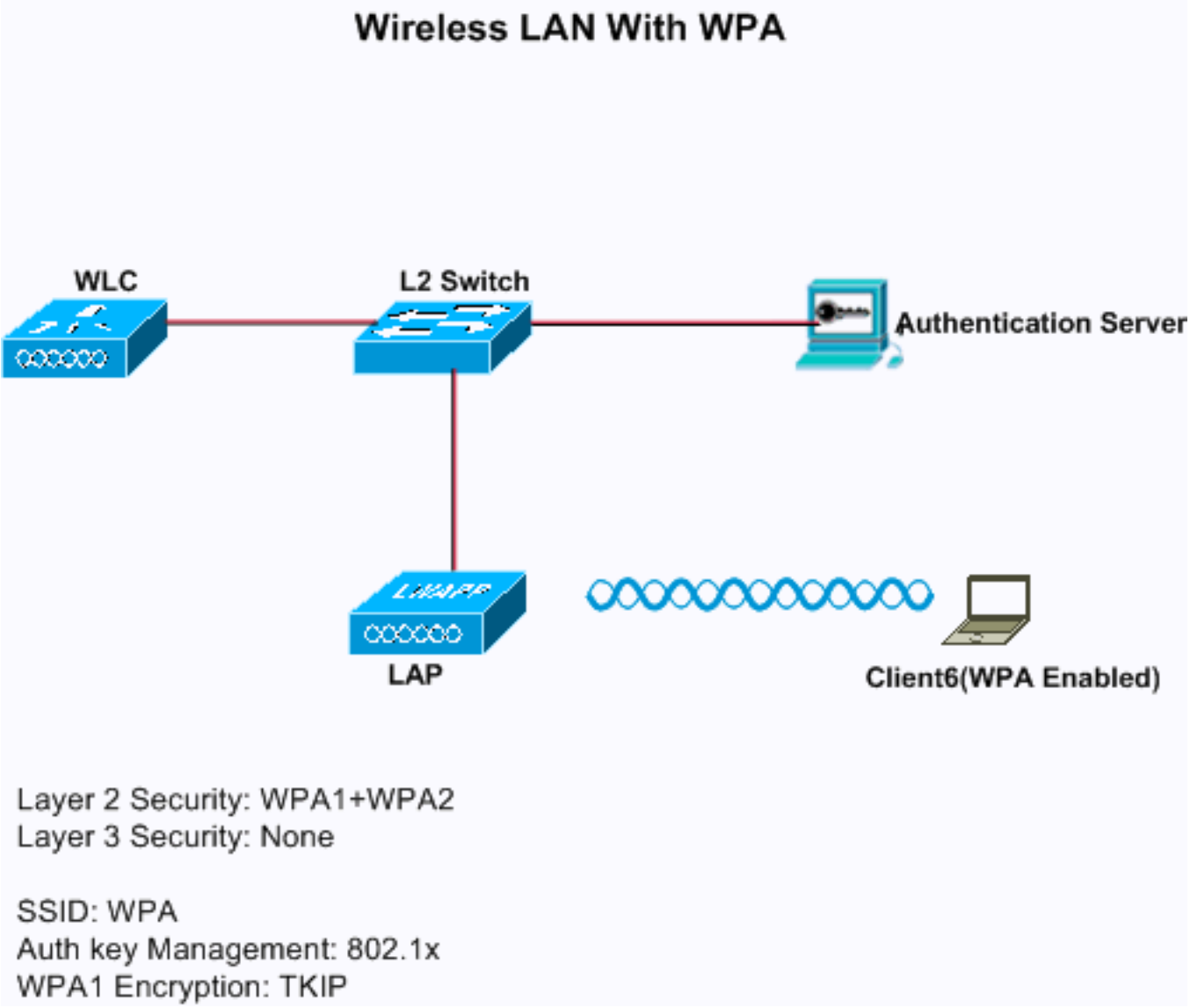
Consulte las secciones Configure Wireless Client for 802.1x Authentication and Configure Wireless Client for Static WEP para obtener información sobre cómo configurar el cliente inalámbrico.

Una vez creados los perfiles de cliente, los clientes configurados para WEP estáticos se asocian con el LAP. Utilice el SSID WEP+802.1x para conectarse a la red.

Del mismo modo, los clientes inalámbricos configurados para utilizar la autenticación 802.1x se autentican mediante EAP y acceden a la red con el mismo SSID WEP+802.1x.

Acceso Wi-Fi protegido

Este ejemplo muestra una WLAN configurada con WPA con 802.1x.



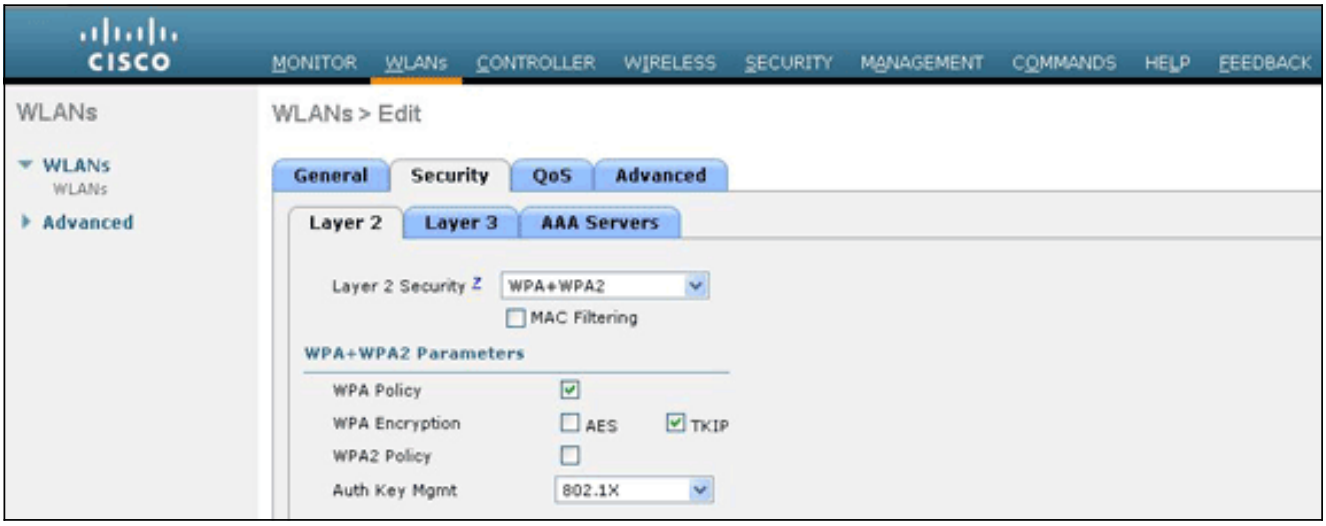
Configuración del WLC para WPA

Complete estos pasos para configurar el WLC para esta configuración:

1. Haga clic en **WLAN en la GUI para crear una WLAN.**Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.
2. Haga clic en **Ir** para configurar una nueva WLAN.Elija el tipo y el nombre del perfil. En este ejemplo, la WLAN se denomina *WPA* y el ID de WLAN es *5*.

3. Haga clic en Apply (Aplicar).
4. En la ventana WLAN > Edit , defina los parámetros específicos de la

WLAN.



Haga clic en la pestaña **Seguridad**, haga clic en la pestaña **Capa 2** y elija **WPA1+WPA2** en la lista desplegable Seguridad de Capa 2.En WPA1+WPA2 Parameters, marque la casilla de verificación **WPA1 Policy** para habilitar WPA1, marque la casilla de verificación **WPA2 Policy** para habilitar WPA2, o marque ambas casillas de verificación para habilitar WPA1 y WPA2.El valor predeterminado está desactivado tanto para WPA1 como para WPA2. Si deja WPA1 y WPA2 desactivados, los puntos de acceso anuncian en sus balizas y elementos de información de respuesta de sonda sólo para el método de administración de claves de autenticación que elija.Marque la casilla de verificación **AES** para habilitar el cifrado de datos AES o la **casilla de verificación TKIP** para habilitar el cifrado de datos TKIP para WPA1, WPA2 o ambos.Los valores predeterminados son TKIP para WPA1 y AES para WPA2.Elija uno de estos métodos de administración clave de la lista desplegable Administración de claves de autenticación:*802.1X*: si elige esta opción, sólo se admiten clientes 802.1x.*CCKM*: si elige esta opción, sólo se admiten clientes CCKM, donde los clientes se dirigen a un servidor externo para la autenticación.*PSK*: si elige esta opción, se utiliza una clave previamente compartida para el WLC y el cliente. Además, todos los estándares se han establecido para que se utilicen antes de los estándares previos; por ejemplo, WPA/WPA2 precede a CCKM cuando se utiliza simultáneamente.*802.1X+CCKM*: si elige esta opción, se admiten tanto clientes CCKM como no CCKM (CCKM opcional).Este ejemplo utiliza 802.1x.

Nota: Si elige PSK, elija **ascii** o **hex** en la lista desplegable Formato PSK y, a continuación, introduzca una clave previamente compartida en el campo en blanco. Las claves

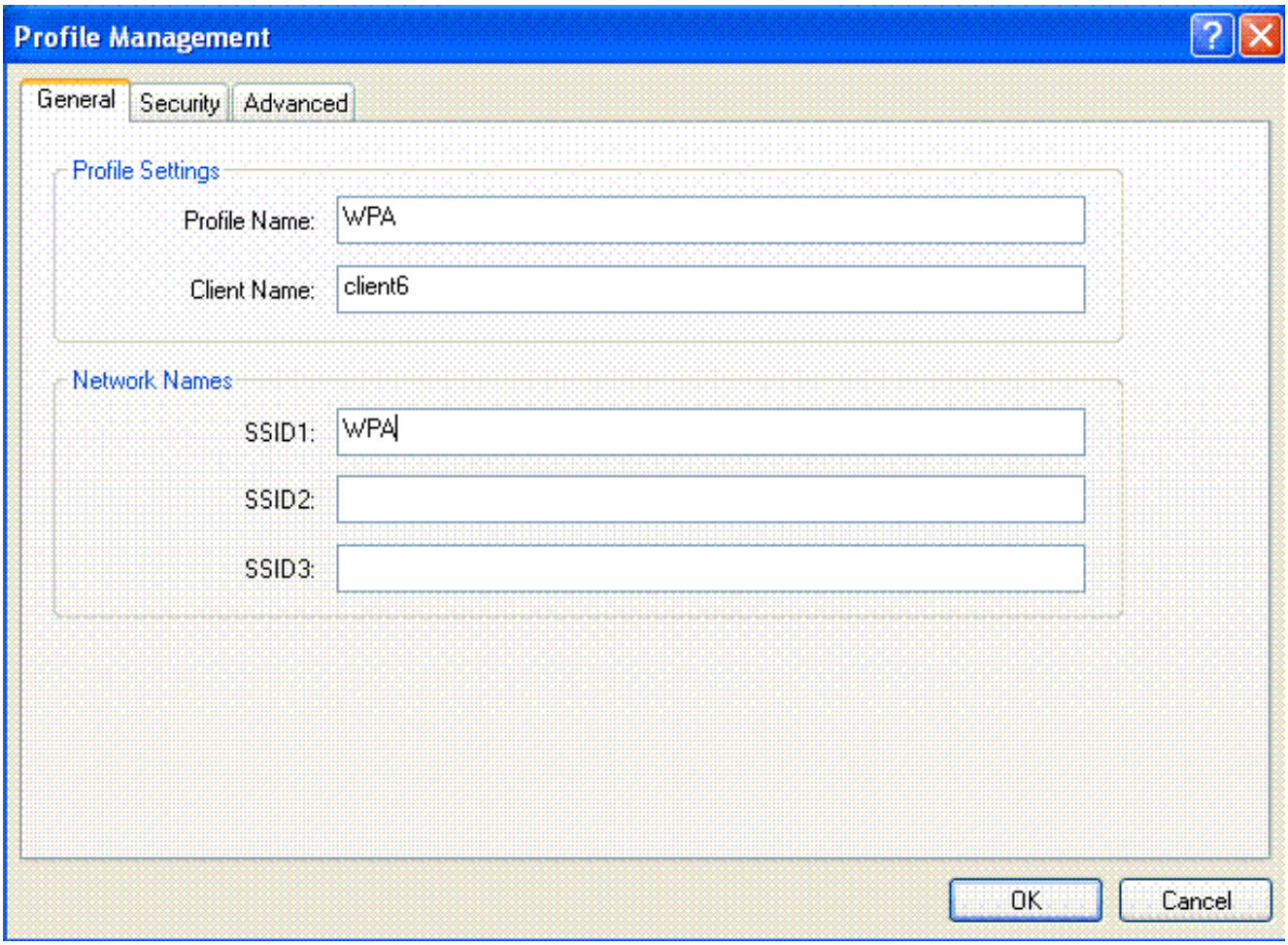
precompartidas WPA deben contener de 8 a 63 caracteres de texto ASCII o 64 caracteres hexadecimales.

5. Haga clic en **Aplicar** para aplicar los cambios.

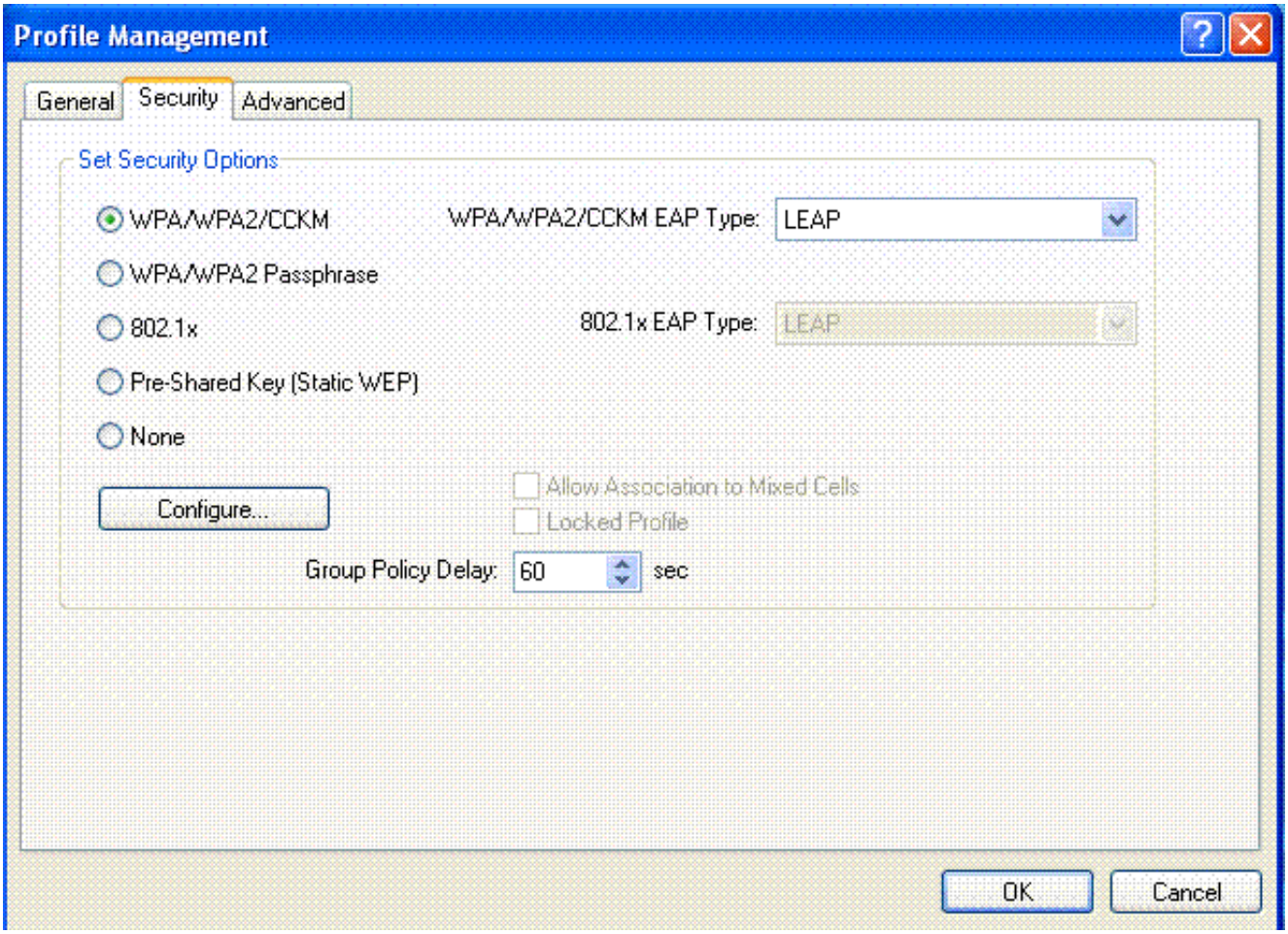
Configuración del cliente inalámbrico para WPA

Complete estos pasos para configurar el cliente de LAN inalámbrica para esta configuración:

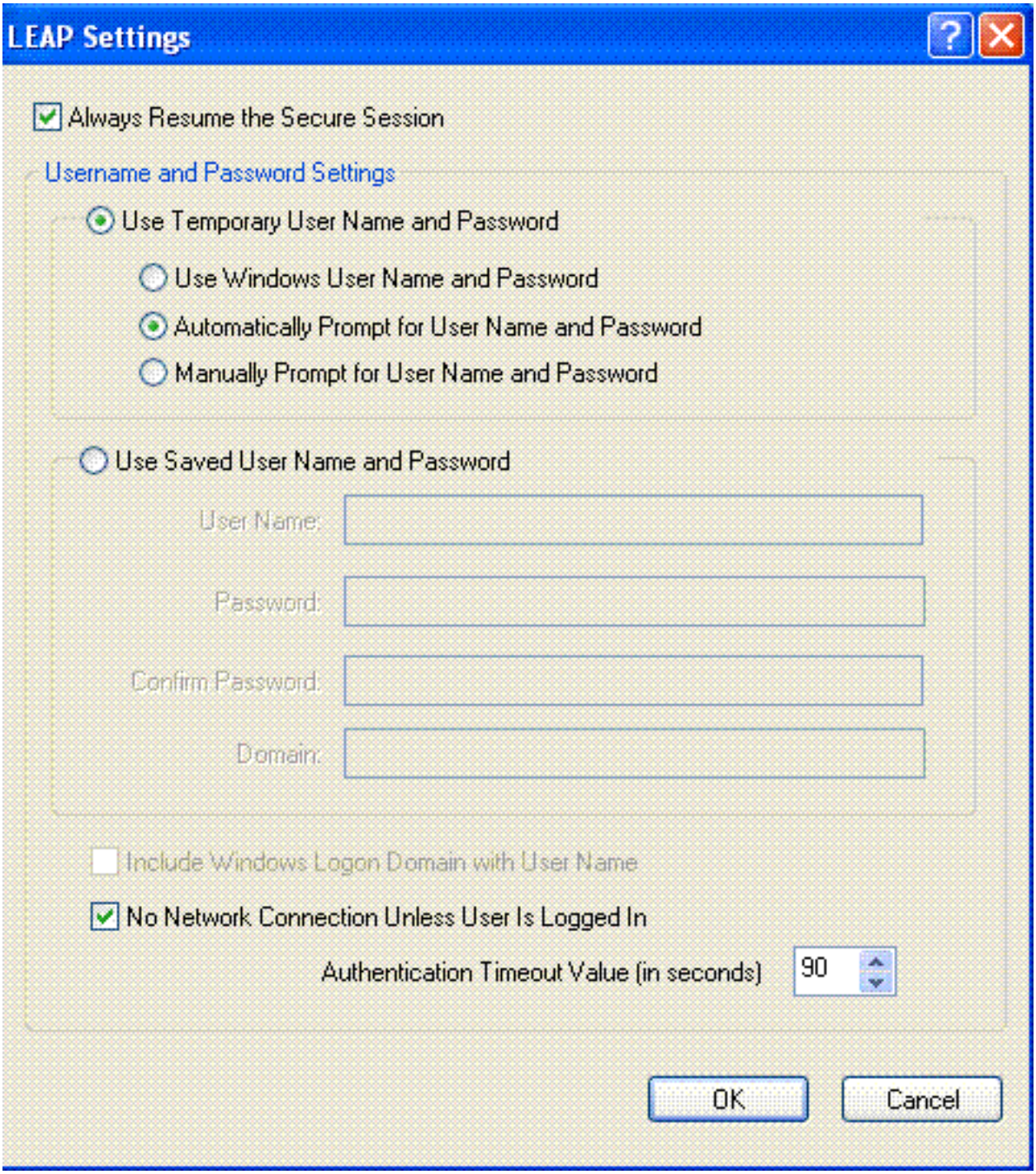
1. En la ventana Profile Management de la ADU, haga clic en **New** para crear un perfil nuevo.
2. Haga clic en la ficha **General** e introduzca el nombre del perfil y el SSID que utilizará el adaptador del cliente.En este ejemplo, el nombre del perfil y el SSID son *WPA*. El SSID debe coincidir con el SSID que configuró en el WLC para WPA.



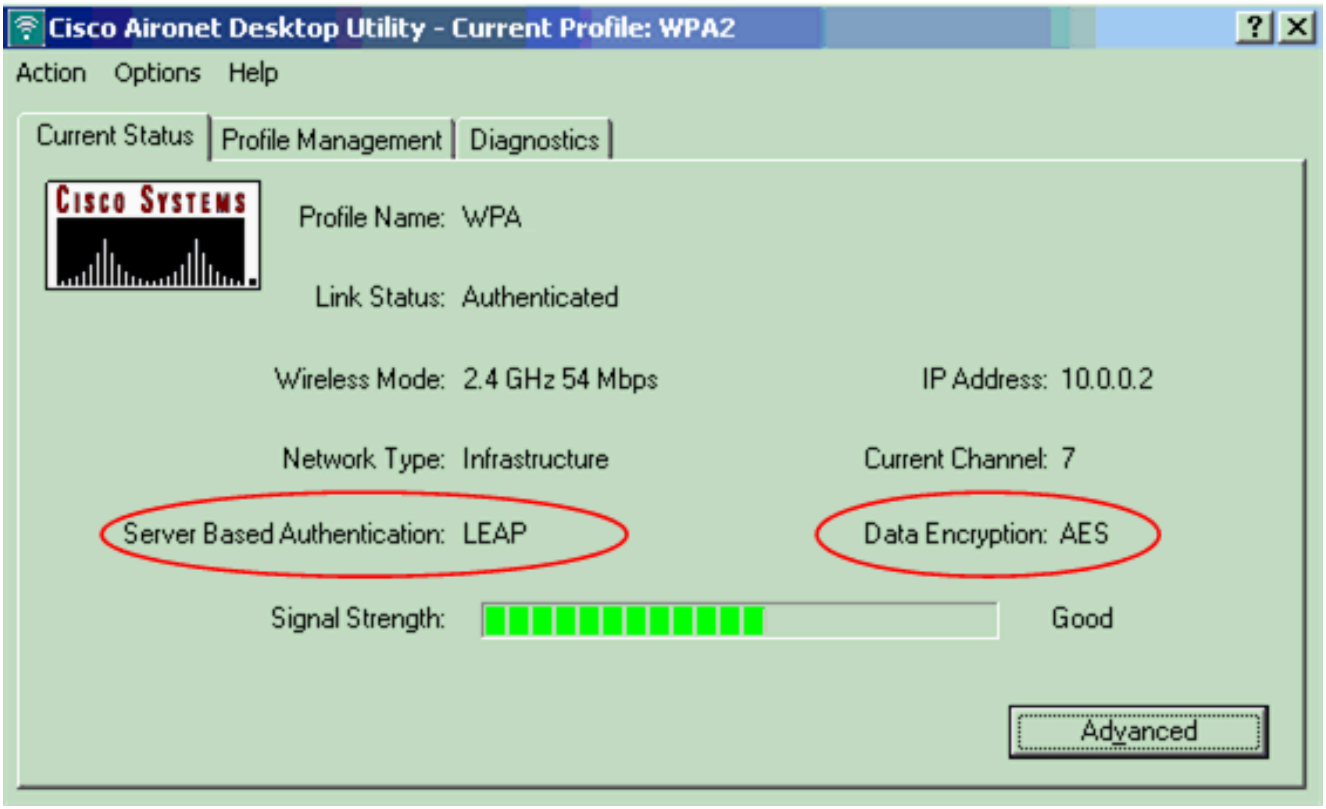
3. En la ficha Security (Seguridad), haga clic en el botón de opción **WPA/WPA2/CCKM** y elija el tipo EAP adecuado en la lista desplegable WPA/WPA2/CCKM EAP Type (Tipo de EAP WPA/WPA2/CCKM). Este paso habilita WPA.



4. Haga clic en **Configurar** para definir la configuración EAP específica del tipo de EAP seleccionado.

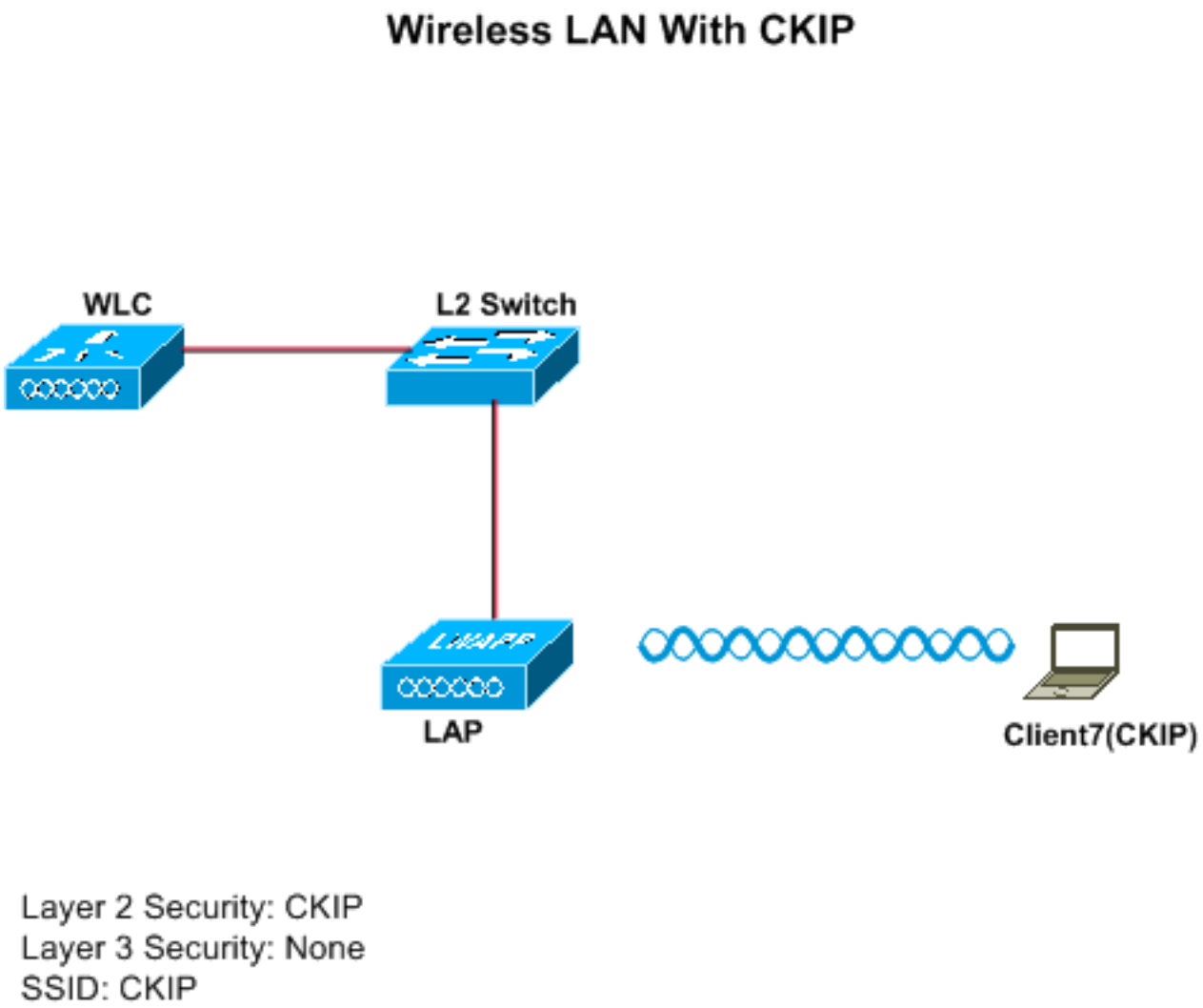


5. Click OK.**Nota:** Cuando se activa este perfil, el cliente se autentica usando 802.1x y cuando la autenticación es exitosa, el cliente se conecta a la WLAN. Verifique el estado actual de ADU para verificar que el cliente utiliza la encriptación TKIP (encriptación predeterminada utilizada por WPA1) y la autenticación
EAP.



CKIP

Este ejemplo muestra una WLAN configurada con CKIP.



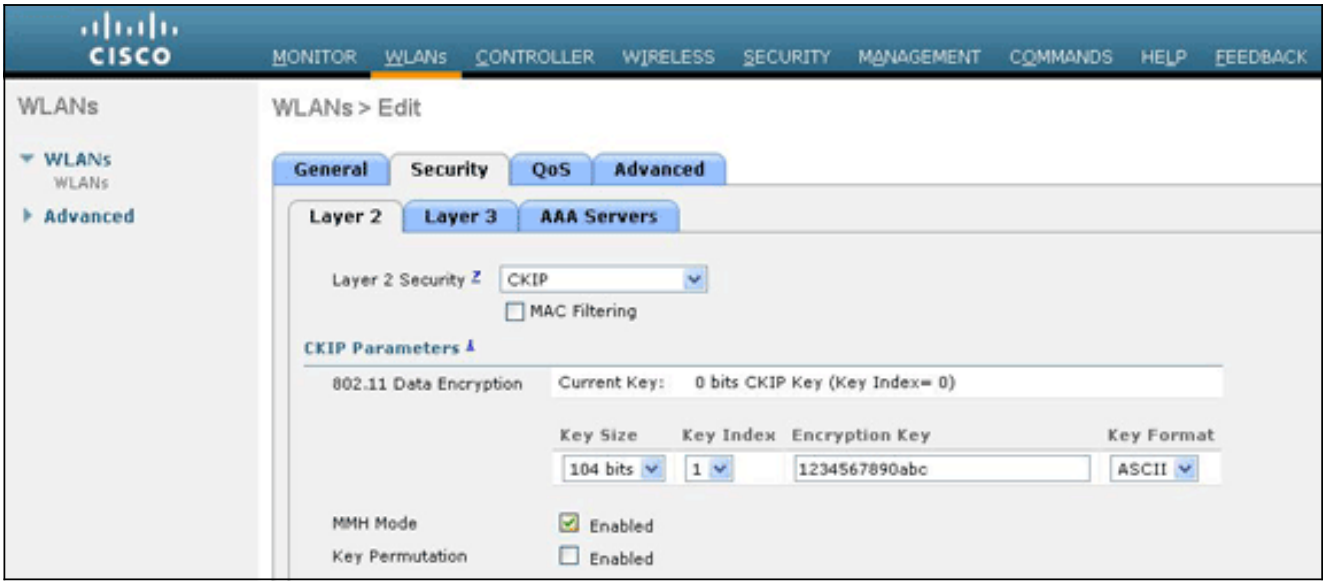
Configuración del WLC para CKIP

Complete estos pasos para configurar el WLC para esta configuración:

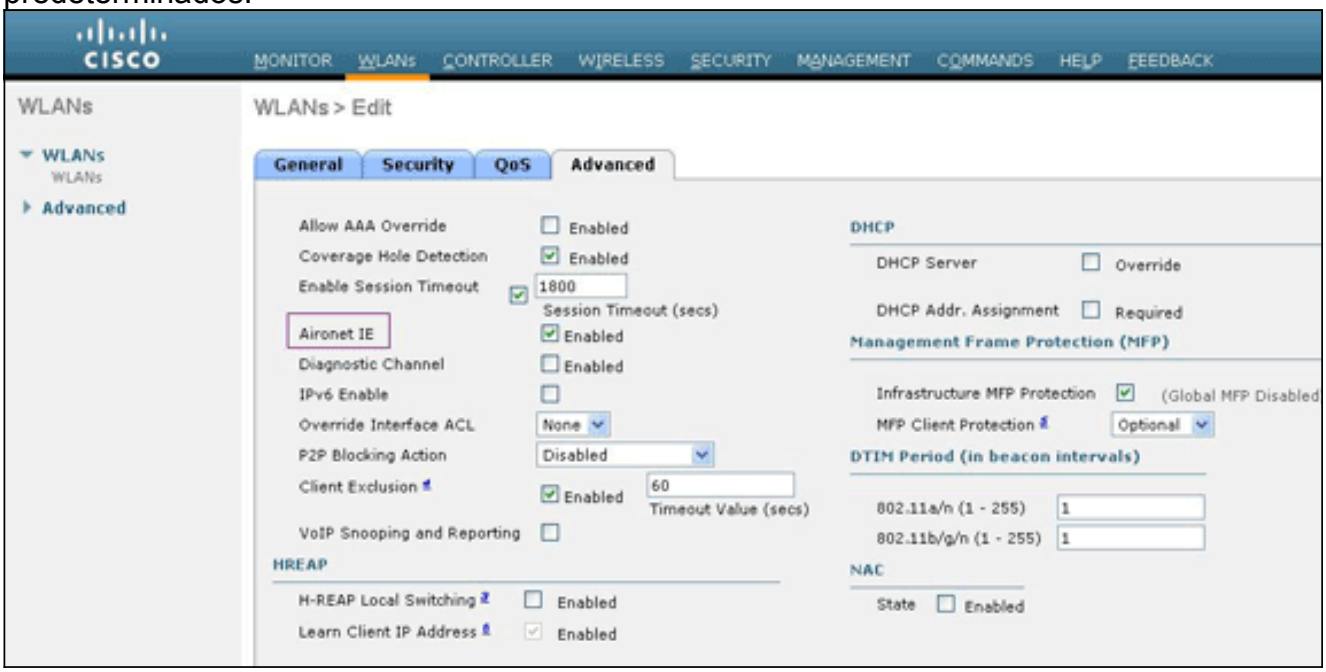
1. Haga clic en **WLAN en la GUI para crear una WLAN.**Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.
2. Haga clic en **Nuevo para configurar una WLAN nueva.**Elija el tipo y el nombre del perfil. En este ejemplo, la WLAN se denomina *CKIP* y el ID de WLAN es *6*.

3. En la ventana WLAN > Edit , defina los parámetros específicos de la WLAN.En la lista desplegable Capa 2, elija **CKIP**.Este paso habilita CKIP para esta WLAN.En los parámetros de CKIP, seleccione el tamaño de clave y el índice de clave, e introduzca la clave de cifrado estática.El tamaño de la clave puede ser de 40 bits, 104 bits o 128 bits. El índice de claves

puede estar entre 1 y 4. Se puede aplicar un índice de clave WEP único a cada WLAN. Debido a que sólo hay cuatro índices de claves WEP, sólo se pueden configurar cuatro WLAN para el cifrado estático de Capa 2 de WEP.Para CKIP, elija la opción **MMH Mode** o la **opción Key Permutation**, o ambas.**Nota:** Se debe seleccionar uno de estos parámetros o ambos para que CKIP funcione según lo esperado. Si no se seleccionan estos parámetros, la WLAN permanece en el estado inhabilitado.En este ejemplo, se utiliza una clave de 104 bits y la clave es 1234567890abc.



4. Elija otros parámetros en función de sus requisitos de diseño.Este ejemplo utiliza los valores predeterminados.

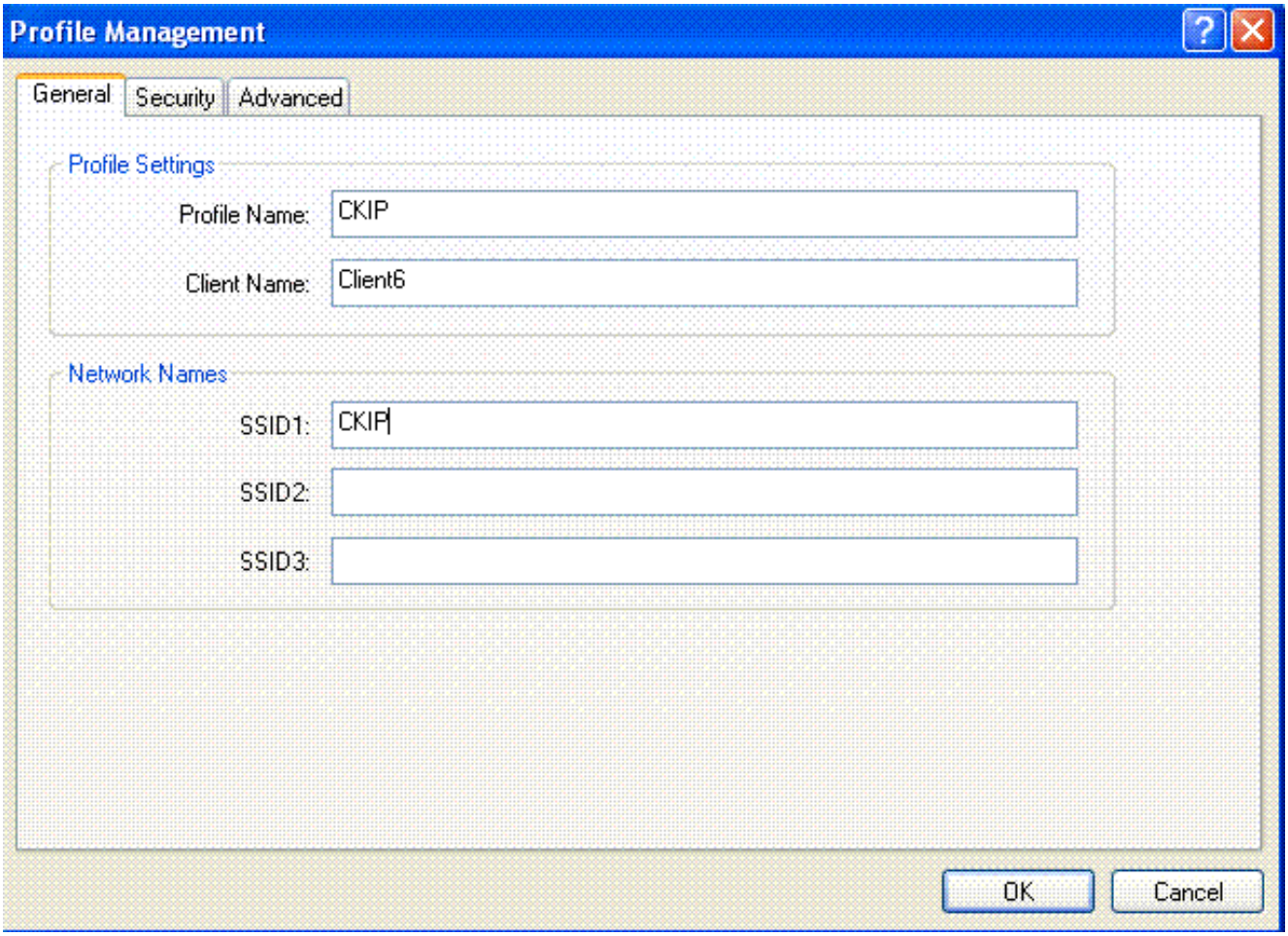


5. Haga clic en Apply (Aplicar).**Nota:** CKIP funciona en los AP 1100, 1130 y 1200, pero no en AP 1000. Aironet IE debe estar habilitado para que esta función funcione. CKIP expande las claves de cifrado a 16 bytes.

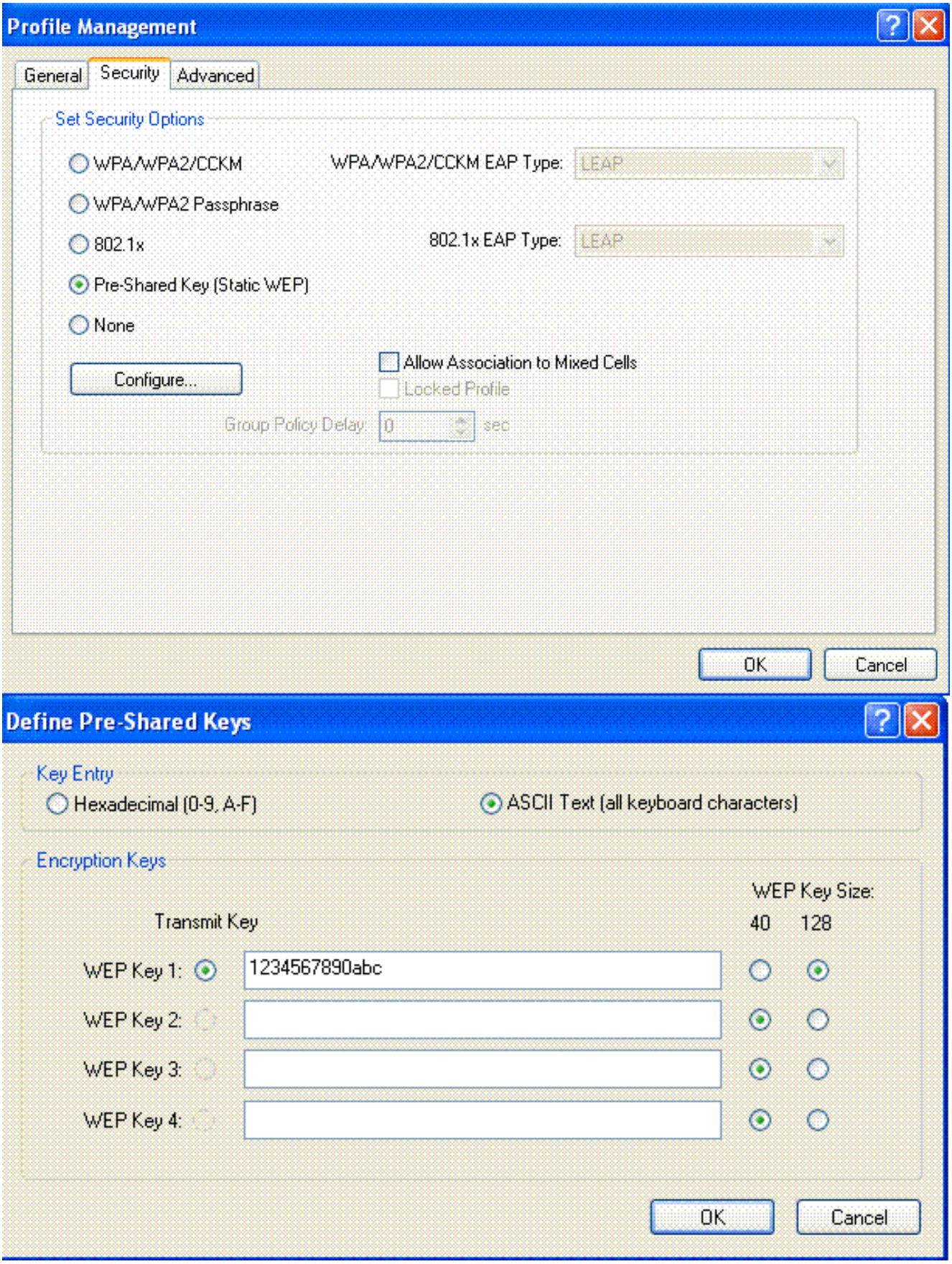
Configuración del cliente inalámbrico para CKIP

Complete estos pasos para configurar el Wireless LAN Client para esta configuración:

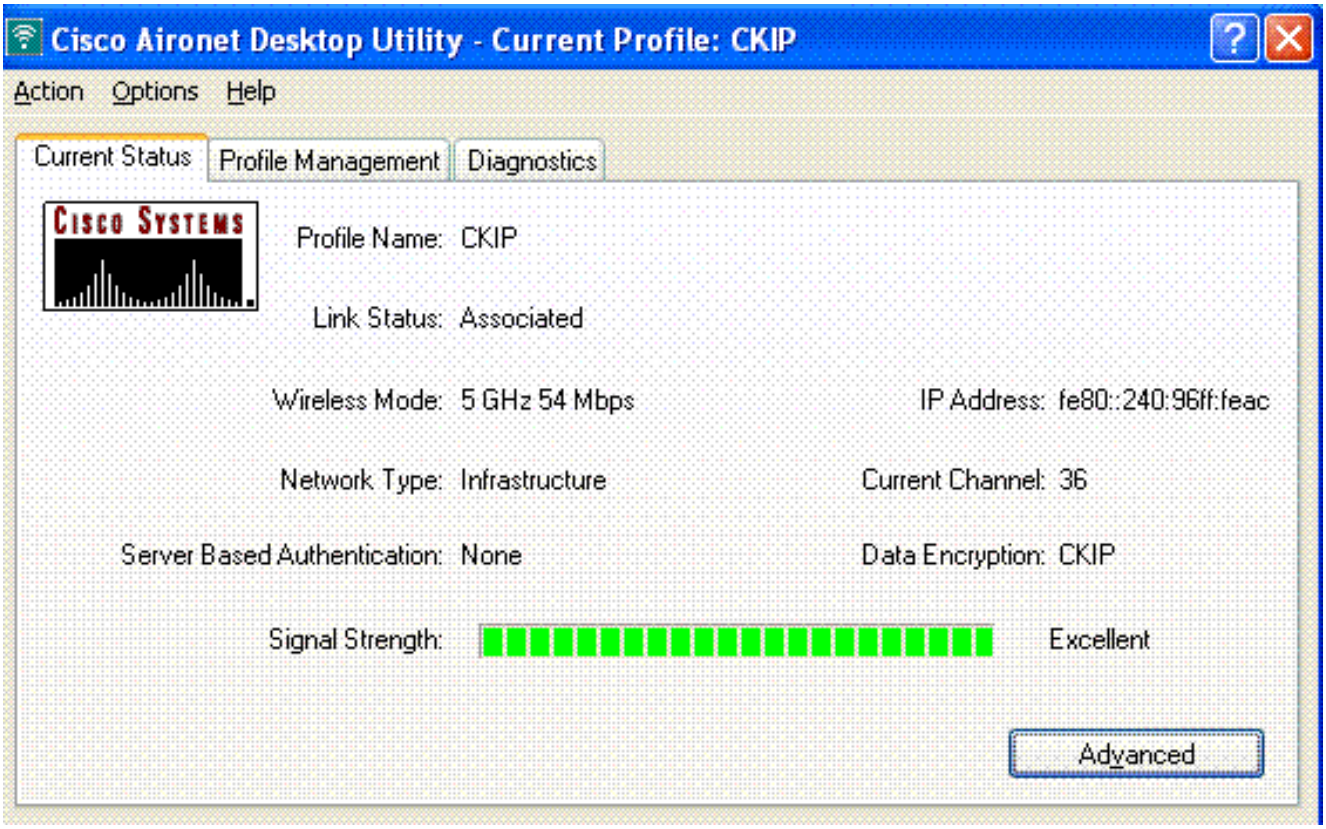
1. Para crear un nuevo perfil, haga clic en la pestaña **Profile Management** en la ADU y luego haga clic en **New**.
2. Cuando se muestra la ventana Administración de Perfil (Generales), complete estos pasos para establecer el Nombre de Perfil, Nombre del Cliente, y SSID:Ingrese el nombre del perfil en el campo de nombre del perfil.Este ejemplo utiliza *CKIP* como nombre de perfil.Ingrese el nombre del cliente en el campo de Nombre del cliente.El Nombre del cliente se utiliza para identificar al cliente de red inalámbrica en la red WLAN. Esta configuración utiliza *Client6* para el nombre del cliente.En Nombres de Red, ingrese el SSID que debe ser utilizado para este perfil.El SSID es el mismo que el SSID que configuró en el WLC. El SSID en este ejemplo es
CKIP.



3. Haga clic en la ficha Security (Seguridad).
4. Elija **Pre-Shared Key (Static WEP)** en Set Security Options, haga clic en **Configure** y defina el tamaño de la clave WEP y la clave WEP.Estos valores deben coincidir con la clave WEP configurada en el WLC para esta
WLAN.



5. Click OK.Cuando se activa el SSID, el cliente inalámbrico negocia con el LAP y el WLC para utilizar CKIP para el cifrado de los
paquetes.



Soluciones de seguridad de capa 3

Política web (autenticación web y paso a través de web)

Consulte Ejemplo de Configuración de Autenticación Web del Controlador de LAN Inalámbrica para obtener información sobre cómo habilitar la autenticación Web en una red WLAN.

Consulte Ejemplo de Configuración de Autenticación Web Externa con Controladores de LAN Inalámbricos para obtener información sobre cómo configurar la autenticación Web externa y la autenticación de paso Web en una WLAN.

Consulte Ejemplo de Configuración de Paso Web del Controlador de LAN Inalámbrica para obtener más información sobre cómo habilitar el paso a través de la Web en una red WLAN.

El mecanismo de la página de bienvenida es un mecanismo de seguridad de Capa 3 introducido en la versión 5.0 del WLC usado para la autenticación del cliente. Refiérase a Ejemplo de Configuración de Redireccionamiento de la Página Splash del Controlador de LAN Inalámbrica para obtener más información.

Paso a través de VPN

Consulte Ejemplo de Configuración de VPN de Cliente sobre LAN Inalámbrica con WLC para obtener información sobre cómo configurar el paso a través de VPN en una WLAN.

Troubleshoot

Comandos para resolución de problemas

Puede utilizar los comandos debug para resolver problemas de configuración.

Depuraciones para la Autenticación Web:

- **debug mac addr** *<client-MAC-address xx:xx:xx:xx:xx:xx>* —Configura la depuración de direcciones MAC para el cliente.
- **debug aaa all enable**: configura la depuración de todos los mensajes AAA.
- **debug pem state enable**: configura la depuración de policy manager State Machine
- **debug pem events enable : configura la depuración de eventos del administrador de políticas.**
- **debug dhcp message enable**: utilice este comando para mostrar información de depuración sobre las actividades del cliente del protocolo de configuración dinámica de host (DHCP) y para supervisar el estado de los paquetes DHCP.
- **debug dhcp packet enable : use este comando para ver la información de nivel de paquete de DHCP.**
- **debug pm ssh-appgw enable : configura la depuración de puertas de enlace de la aplicación.**
- **debug pm ssh-tcp enable** —Configura la depuración del manejo tcp del administrador de políticas

Depuraciones para WEP: No hay depuración para WEP porque se realiza en el AP, active **debug dot11 all enable**.

Depuraciones para almacenamiento en caché 802.1X/WPA/RSN/PMK:

- **debug mac addr** *<client-MAC-address xx:xx:xx:xx:xx>*—Configura la depuración de direcciones MAC para el cliente.
- **debug dot1x all enable**: utilice este comando para mostrar información de depuración 802.1X.
- **debug dot11 all enable**: utilice este comando para habilitar la depuración de las funciones de radio.
- **debug pem events enable : configura la depuración de eventos del administrador de políticas.**
- **debug pem state enable : configura la depuración de la máquina de estado del administrador de políticas.**
- **debug dhcp message enable**: utilice este comando para mostrar información de depuración sobre las actividades del cliente del protocolo de configuración dinámica de host (DHCP) y para supervisar el estado de los paquetes DHCP.
- **debug dhcp packet enable : use este comando para ver la información de nivel de paquete de DHCP.**
- **debug mobility handoff enable (para roaming dentro del switch)**—Configura la depuración de paquetes Mobility.
- **show client detail** *<mac>*—Muestra información detallada para un cliente por dirección mac. Verifique la configuración del tiempo de espera de la sesión WLAN y RADIUS.

Información Relacionada

- Ejemplo de Restringir Acceso WLAN Basado en SSID con WLC y Cisco Secure ACS Configuration
- Ejemplo de Configuración de ACL en el Controlador de LAN Inalámbrica
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems