

Ejemplo de Modos H-REAP de Configuración de Funcionamiento

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[H-REAP encima COSECHAN](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Preparar el AP con un regulador y una configuración H-REAP](#)

[Teoría de las operaciones de H-REAP](#)

[Estados de la transferencia H-REAP](#)

[Autenticación central, transferencia central](#)

[Verifique la autenticación central, transferencia central](#)

[Autenticación abajo, conmutando abajo](#)

[Autenticación central, Local Switching](#)

[Verifique la autenticación central, Local Switching](#)

[Autenticación abajo, Local Switching](#)

[Autenticación local, Local Switching](#)

[Verifique la autenticación local, Local Switching](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento presenta el concepto de Hybrid Remote Edge Access Point (H-REAP) y explica sus diversos modos de funcionamiento con un ejemplo de configuración.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de los reguladores del Wireless LAN (WLCs) y cómo configurar los parámetros

básicos del WLC

- El conocimiento de COSECHA

Componentes Utilizados

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

- WLC de las Cisco 4400 Series que funciona con la versión de firmware 7.0.116.0
- Lightweight Access Point de Cisco 1131AG (REVESTIMIENTO)
- Cisco 2800 Series Router que funcionan con la versión 12.4(11)T.
- Adaptador del cliente del Cisco Aironet 802.11a/b/g que funciona con la versión de firmware 4.0
- Versión utilidad de escritorio 4.0 del Cisco Aironet
- Cisco Secure ACS que funciona con la versión 4.0

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

Convenciones

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

Antecedentes

H-REAP es una solución de red inalámbrica para las implementaciones de la sucursal y de la oficina remota. Clientes de los permisos H-REAP para configurar y para controlar el (APS) de los Puntos de acceso en una bifurcación o una oficina remota de la oficina corporativa a través de un link PÁLIDO sin desplegar un regulador en cada oficina.

H-Cosechar puede conmutar el tráfico de datos del cliente localmente y realizar la autenticación de cliente localmente cuando la conexión al regulador se pierde. Cuando están conectados con el controlador, los H-REAPs también pueden tunelizar de nuevo el tráfico hacia el controlador. En el modo conectado, el híbrido COSECHA EL AP puede también realizar la autenticación local.

H-REAP se soporta solamente encendido:

- 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040, y AP3550 AP
- Cisco 5500, 4400, 2100, 2500, y reguladores de las 7500 Series de la flexión
- Switch integrado 3750G del regulador del Catalyst
- Módulo de Servicios inalámbricos de las Catalyst 6500 Series (WiSM)
- Módulo del regulador del Wireless LAN (WLCM) para el Routers de los Servicios integrados (ISR)

El tráfico del cliente en H-Cosechar se puede o conmutar localmente en el AP o tunneled de nuevo a un regulador. Esto depende de la configuración de la por-red inalámbrica (WLAN). También, localmente el tráfico conmutado del cliente en el H-REAP puede ser 802.1Q marcado con etiqueta para prever la separación del atar con alambre-lado. Durante la Interrupción WAN, el

servicio en todos localmente conmutados, los WLAN localmente autenticados persiste.

Nota: Si los AP están en el modo H-REAP y localmente se conmutan en el sitio remoto, la asignación dinámica de los usuarios a un VLA N específico basado en la configuración de servidor de RADIUS no se soporta. Sin embargo, usted debe poder asignar a los usuarios a los VLA N específicos basados en el VLA N estático a asociar del Service Set Identifier (SSID) hecho localmente en el AP. Por lo tanto, un usuario que pertenece a un SSID determinado puede ser asignado a un VLA N específico al cual el SSID se asocia localmente en el AP.

Nota: Si la Voz sobre la red inalámbrica (WLAN) es importante, después los AP se deben ejecutar en el modo local de modo que consigan el CCKM y el soporte del Control de admisión de la conexión (CAC), que no se soportan en el modo H-REAP.

[H-REAP encima COSECHAN](#)

Refiera al [Telecontrol-borde AP \(COSECHE\) con los AP ligeros y al ejemplo de configuración de los reguladores del Wireless LAN \(WLCs\)](#) para que más información ayude a entender COSECHAN.

H-REAP fue introducido como resultado de estos defectos REAP:

- REAP no tiene separación del atar con alambre-lado. Esto debe faltar del soporte del 802.1Q. Los datos de los WLAN aterrizan en la misma subred atada con alambre.
- Durante una Falla de WAN, una COSECHA AP cesa el servicio ofrecido en todos los WLAN, a menos que primer especificara en el regulador.

Éste es cómo H-REAP supera estos dos defectos:

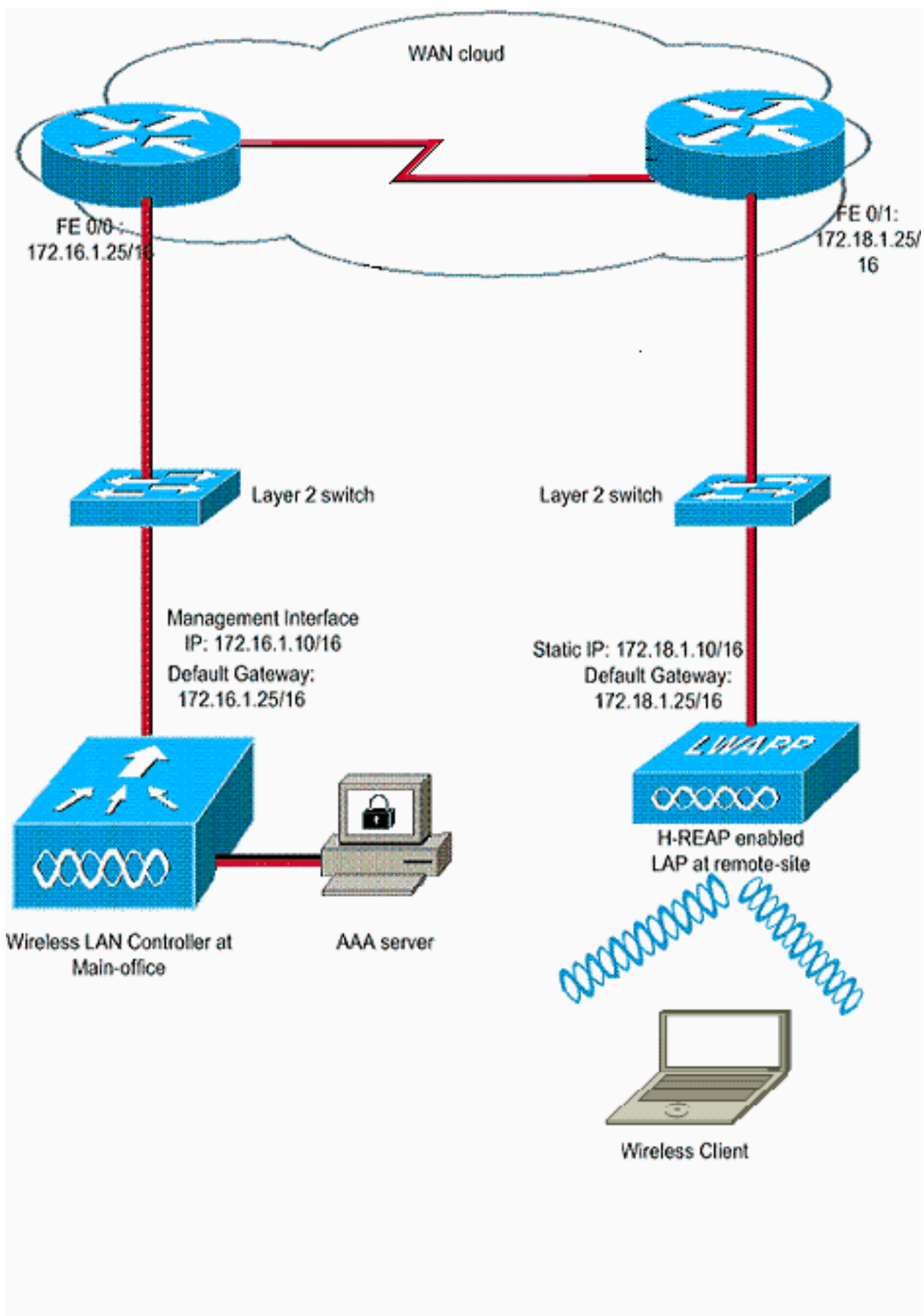
- Proporciona el soporte y el VLA N del dot1q a la asignación SSID. Este VLA N a la asignación SSID necesita ser hecho en H-REAP. Mientras que usted realiza esto, asegúrese de que los VLAN configurados estén permitidos correctamente a través de los puertos en el Switches y el Routers intermedios.
- Proporciona el servicio continuo a todos los WLAN configurados para el Local Switching.

[Configurar](#)

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

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



Configuración

Este ejemplo asume que el regulador está configurado ya con las configuraciones básicas. El regulador utiliza estas configuraciones:

- Dirección IP de la interfaz de administración — 172.16.1.10/16
- Dirección IP de la interfaz del AP manager — 172.16.1.11/16
- IP Address del router del default gateway — 172.16.1.25/16
- Gateway IP Address virtual — 1.1.1.1

Nota: Este documento no muestra las configuraciones WAN y configuración del router y Switches disponibles entre el H-REAP y el regulador. Esto asume que usted es consciente de la encapsulación WAN y de los Routing Protocol se utilizan que. También, este documento asume que usted entiende cómo configurarlos para mantener la Conectividad entre el H-REAP y el regulador a través del link PÁLIDO. En este ejemplo, el encapsulado HDCL se utiliza en el link PÁLIDO.

[Preparar el AP con un regulador y una configuración H-REAP](#)

Si usted quisiera que el AP descubriera un regulador de una red remota donde no están disponibles los mecanismos de detección CAPWAP, usted puede utilizar el oscurecimiento. Este método le permite para especificar el regulador con el cual el AP debe conectar.

Para preparar un AP H-COSECHAR-capaz, conecte el AP con la red alámbrica en la oficina principal. Durante su arrancar, el AP H-COSECHAR-capaz primero busca una dirección IP para para sí mismo. Una vez que adquiere una dirección IP a través de un servidor DHCP, arranca y busca un regulador para realizar el proceso de inscripción.

Un H-REAP AP puede aprender la dirección IP del regulador de las maneras unas de los explicadas en el [registro ligero AP \(REVESTIMIENTO\) a un regulador del Wireless LAN \(WLC\)](#).

Nota: Usted puede también configurar el REVESTIMIENTO para descubrir el regulador a través de los comandos CLI en el AP. Refiera a la [detección del regulador H-REAP usando los comandos CLI](#) para más información.

El ejemplo en este documento utiliza el procedimiento de la opción DHCP 43 para que el H-REAP aprenda la dirección IP del regulador. Después se une al regulador, descarga la imagen del último software y la configuración del regulador, e inicializa el link de radio. Guarda la configuración descargada en memoria no volátil para el uso en el modo autónomo.

El REVESTIMIENTO se registra una vez con el regulador, completa estos pasos:

1. En el regulador GUI, elija las **puntas de Wireless>Access**. Esto visualiza el REVESTIMIENTO registrado con este regulador.
2. Haga clic en el AP que usted quiere configurar.

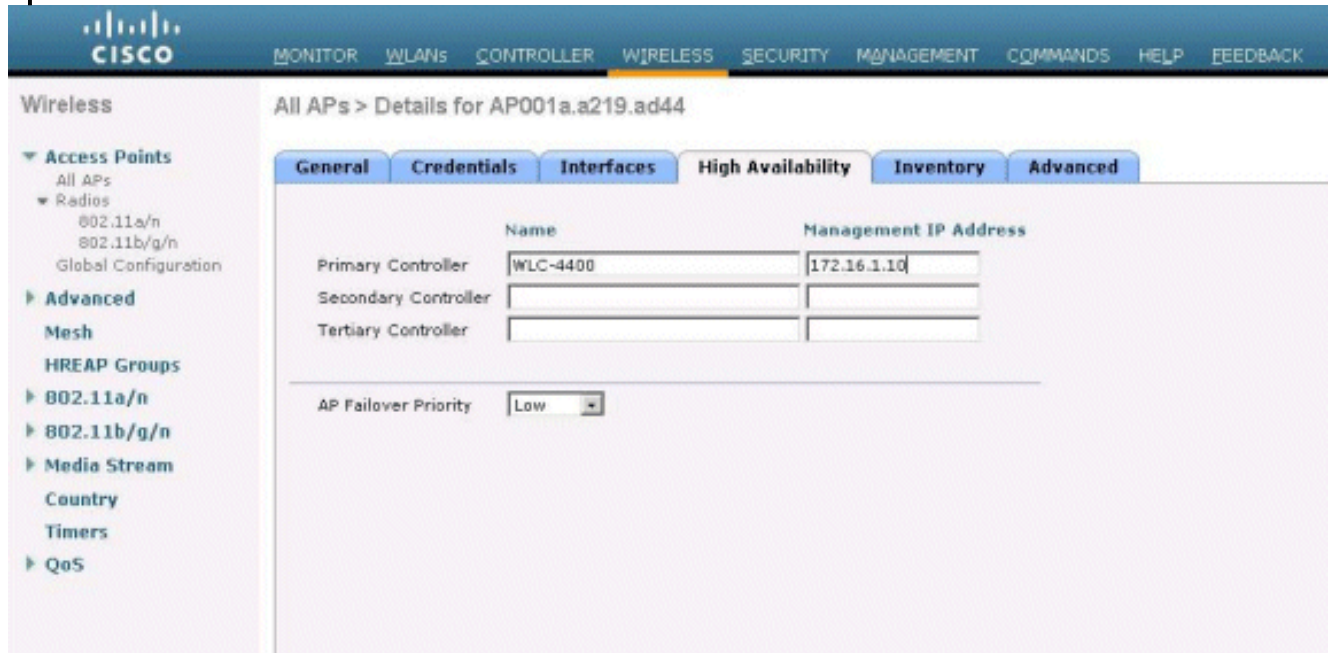


The screenshot shows the Cisco WLC GUI with the 'Wireless' tab selected. The 'All APs' section displays a table with the following data:

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
AP001a.219.a44d	AIR-LAP1131AG-A-K9	001e:1e:21:9a:d4:4d	0 d, 00 h 06 m 12 s	Enabled	REG

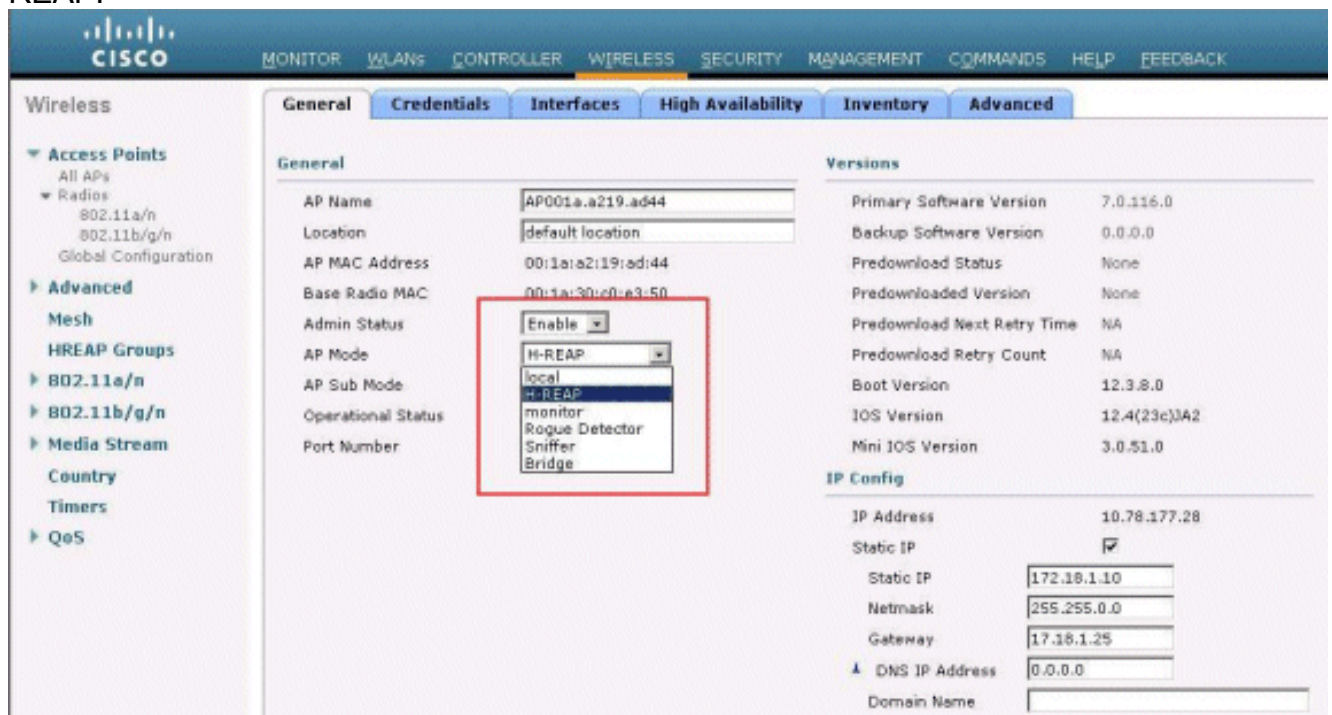
3. En la ventana de APs>Details, haga clic en la lengüeta de gran disponibilidad, y defina los

nombres del regulador que los AP utilizarán para registrar, después hacen clic **se aplican**.



Usted puede definir hasta tres nombres del regulador (primario, secundario, y terciario). Los AP buscan para el regulador en la misma orden que usted proporciona en esta ventana. Porque este ejemplo utiliza solamente un regulador, el ejemplo define el regulador como el controlador primario.

4. REVESTIMIENTO de la configuración para H-REAP. Para configurar el REVESTIMIENTO para actuar en el modo H-REAP, en la ventana de APs>Details, conforme a la ficha general, elige **modo AP** como H-REAP del menú desplegable correspondiente. Esto configura el REVESTIMIENTO para actuar en el modo H-REAP.



Nota: En este ejemplo, usted puede ver que la dirección IP del AP está cambiada al modo estático y se ha asignado el IP Address estático 172.18.1.10. Esta asignación ocurre porque ésta es la subred que se utilizará en la oficina remota. Por lo tanto, usted utiliza la dirección IP del servidor DHCP, pero solamente durante la primera vez a través de la etapa del

registro. Después de que el AP se registre al regulador, usted cambia el direccionamiento a un IP Address estático.

Ahora que su REVESTIMIENTO se prepara con el regulador y se configura para el modo H-REAP, el siguiente paso es configurar H-REAP en el lado del regulador y discutir los estados de la transferencia H-REAP.

[Teoría de las operaciones de H-REAP](#)

El REVESTIMIENTO H-COSECHAR-capaz actúa en estos dos diversos modos:

- **Modo conectado:** Un H-REAP reputa en el modo conectado cuando su link del avión del control CAPWAP al WLC es ascendente y operativo. Esto significa que el link PÁLIDO entre el REVESTIMIENTO y el WLC no está abajo.
- **Modo autónomo:** Un H-REAP reputa en el modo autónomo cuando su link PÁLIDO al WLC está abajo. Por ejemplo, cuando este H-REAP tiene no más Conectividad al WLC conectado a través del link PÁLIDO.

El mecanismo de autenticación usado para autenticar a un cliente se puede definir como la **central** o **Local**.

- **Autenticación central** — Refiere al tipo de autenticación que implica el proceso del WLC del sitio remoto.
- **Autenticación local** — Refiere a los tipos de autenticación que no implican el procesar del WLC para la autenticación.

Nota: Toda la autenticación del 802.11 y proceso de la asociación ocurre en el H-REAP, ninguna materia en la cual el modo el REVESTIMIENTO esté. Mientras que en el modo conectado, los proxys H-REAP entonces estas asociaciones y las autenticaciones al WLC. En el modo autónomo, el REVESTIMIENTO no puede informar al WLC tales eventos.

Cuando un cliente conecta con un H-REAP AP, el AP adelanta todos los mensajes de autenticación al regulador. Después de la autenticación satisfactoria, sus paquetes de datos entonces o se conmutan localmente o tunneled de nuevo al regulador. Esto está de acuerdo a la configuración de la red inalámbrica (WLAN) con la cual está conectada.

Con H-REAP, los WLAN configurados en un regulador se pueden actuar en dos diversos modos:

- **Transferencia central:** Un WLAN en H-REAP se dice para actuar en el Switching Mode central si el tráfico de datos de ese WLAN se configura para ser tunneled al WLC.
- **Local Switching:** Un WLAN en H-REAP se dice para actuar en el modo del Local Switching si el tráfico de datos de ese WLAN termina localmente en la interfaz atada con alambre del REVESTIMIENTO sí mismo, sin conseguir tunneled al WLC. **Nota:** Solamente los WLAN 1 a 8 se pueden configurar para el Local Switching H-REAP porque solamente estos WLAN se pueden aplicar a los 1130, las 1240 y 1250 Series AP que soportan las funciones H-REAP.

[Estados de la transferencia H-REAP](#)

Combinado con los modos de la autenticación y de la transferencia mencionados en la sección anterior, un H-REAP puede actuar en ninguno de estos estados:

- [Autenticación central, transferencia central](#)

- [Autenticación abajo, conmutando abajo](#)
- [Autenticación central, Local Switching](#)
- [Autenticación abajo, Local Switching](#)
- [Autenticación local, Local Switching](#)

Autenticación central, transferencia central

En este estado, para la red inalámbrica (WLAN) dada, el AP adelanta todas las peticiones de la autenticación de cliente al regulador y hace un túnel todos los datos del cliente al WLC. Este estado es válido solamente cuando el H-REAP está en el modo conectado. Cualquier red inalámbrica (WLAN) que se configure para actuar en este modo se pierde durante la Interrupción WAN, no importa qué es el método de autenticación.

Este ejemplo utiliza estos ajustes de la configuración:

- Nombre del WLAN/SSID: **Central**
- Seguridad de la capa 2: **WPA2**
- Local Switching H-REAP: **inhabilitado**

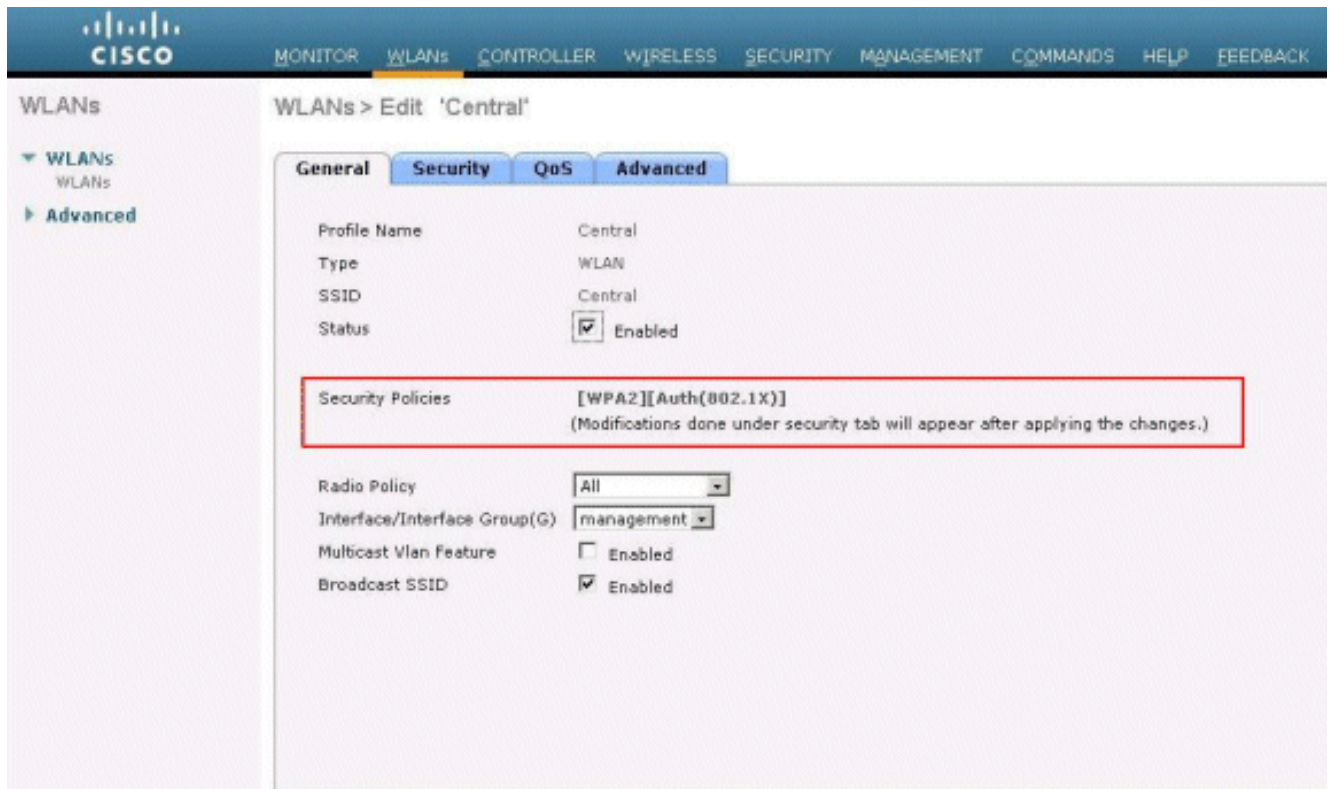
Complete estos pasos para configurar el WLC para la autenticación central, transferencia central usando el GUI:

1. Haga clic los **WLAN** para crear una nueva red inalámbrica (WLAN) nombrada **Central**, después haga clic **se aplican**.

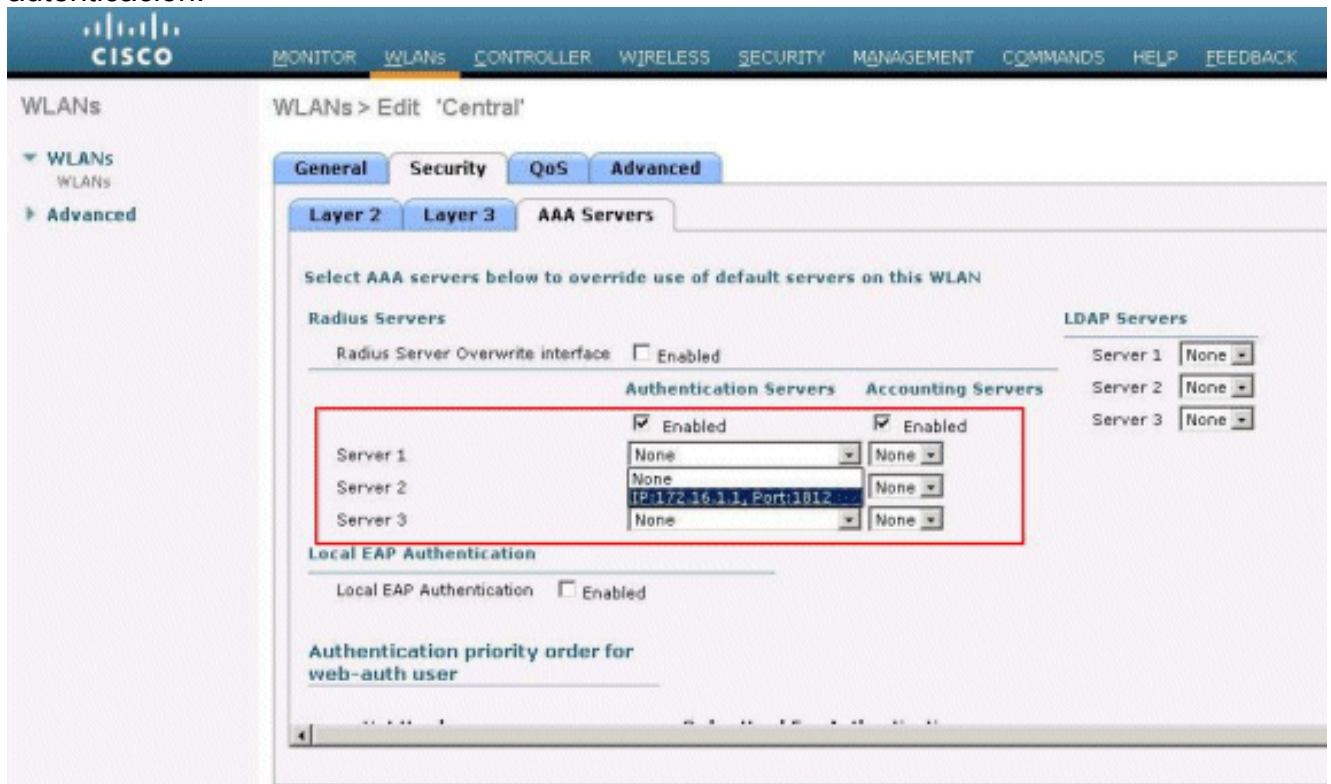
The screenshot shows the Cisco WLC GUI with the 'WLANs > New' configuration page. The 'Type' dropdown is set to 'WLAN', 'Profile Name' is 'Central', 'SSID' is 'Central', and 'ID' is '1'.

Field	Value
Type	WLAN
Profile Name	Central
SSID	Central
ID	1

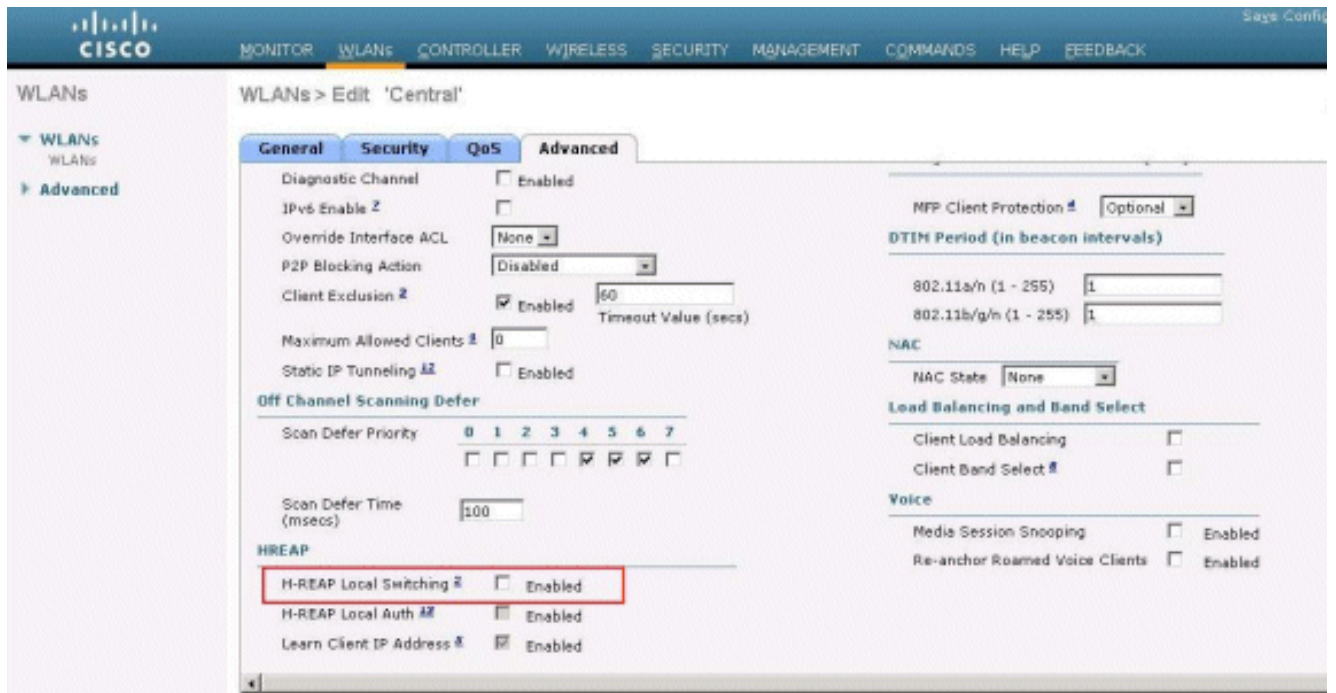
2. Porque esta red inalámbrica (WLAN) utiliza la autenticación central, utilizamos la autenticación WPA2 en el campo de Seguridad de la capa 2. El WPA2 es la Seguridad predeterminada de la capa 2 para una red inalámbrica (WLAN).



3. Elija la lengüeta de los servidores de AAA, y después elija el servidor apropiado configurado para la autenticación.



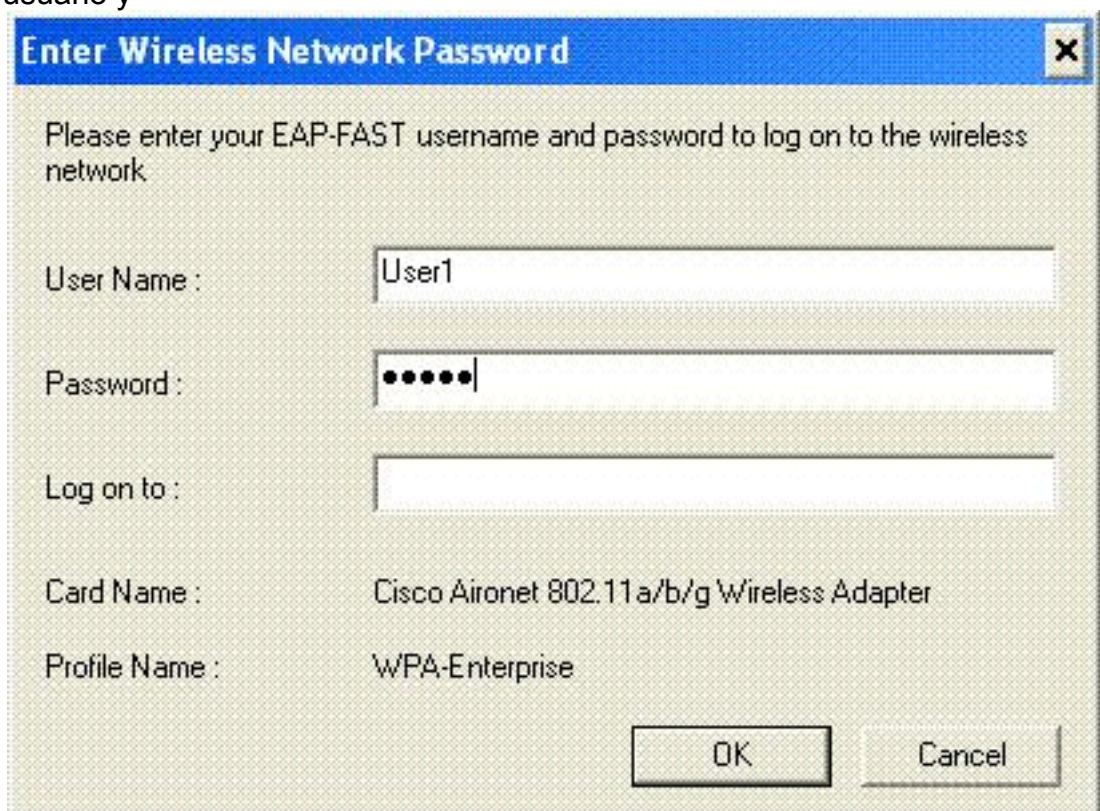
4. Porque esta red inalámbrica (WLAN) utiliza la transferencia central, usted necesita asegurarse de que la casilla de verificación del Local Switching H-REAP esté inhabilitada (es decir la casilla de verificación del Local Switching no se selecciona). Entonces, el teclado se aplica.



[Verifique la autenticación central, transferencia central](#)

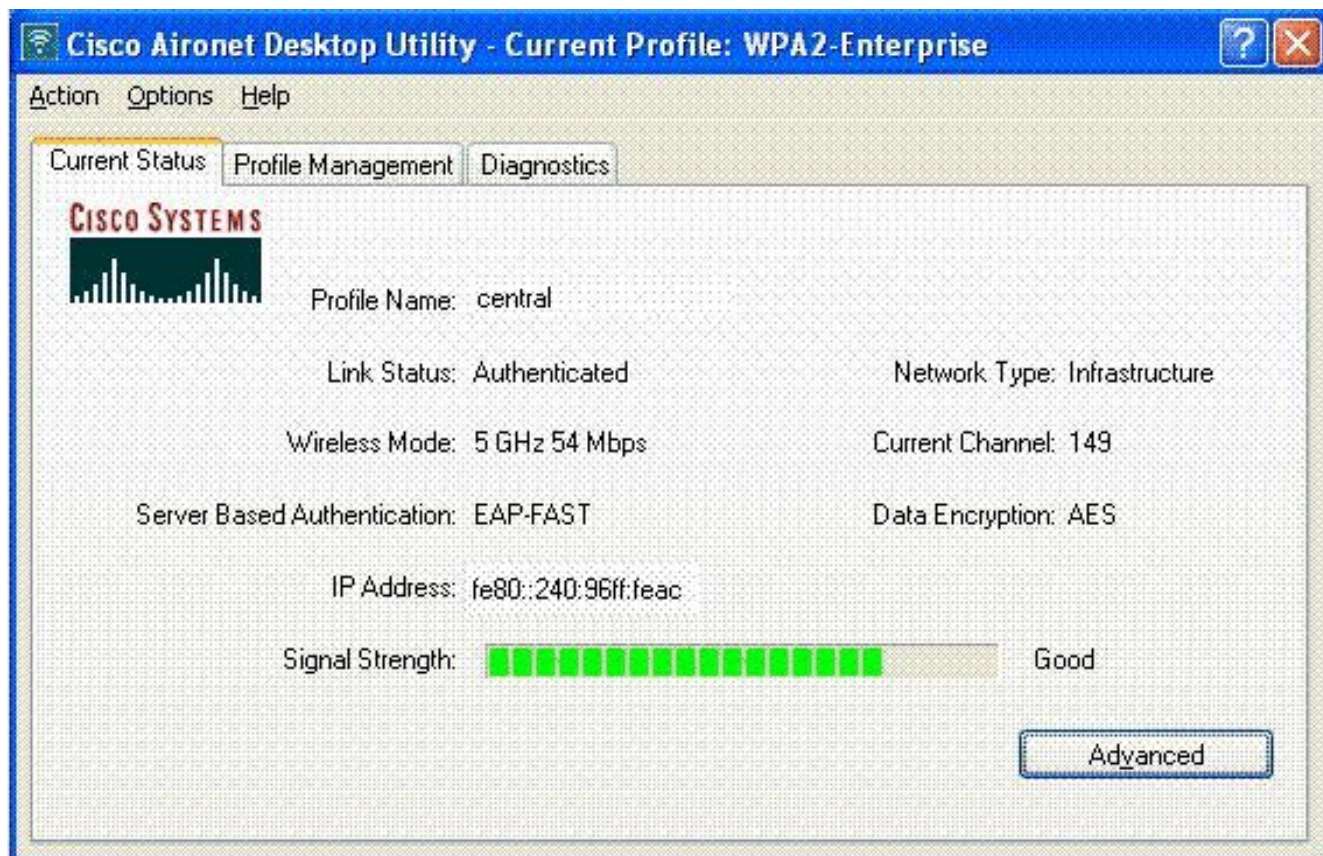
Complete estos pasos:

1. Configure al cliente de red inalámbrica con el mismo SSID y Configuraciones de seguridad. En este ejemplo, el SSID es *central* y el método de seguridad es *WPA2*.
2. Ingrese el nombre de usuario y contraseña como está configurado en el server>User del RADIO puesto para activar el SSID central en el cliente. Este ejemplo utiliza el *user1* como el nombre de usuario y



contraseña.

Al servidor de RADIUS autentica y se asocia al cliente centralmente al H-REAP AP. El H-REAP ahora está en la **autenticación central, transferencia central**.



[Autenticación abajo, conmutando abajo](#)

Con la misma configuración explicada en la [autenticación central](#), la sección de [transferencia central](#), inhabilita el link PÁLIDO que conecta el regulador. Ahora, las esperas del regulador para un latido del corazón contestan del AP. Una contestación del latido del corazón es similar a los mensajes de keepalive. El regulador intenta cinco latidos consecutivos, cada todos en segundo lugar.

Porque no se recibe con una contestación del latido del corazón del H-REAP, el WLC desregistra el REVESTIMIENTO.

Publique el **comando enable de los eventos del capwap del debug del CLI WLC** para verificar el proceso del deregistration. Ésta es la salida de ejemplo de este **comando debug**:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from AP
00:15:c7:ab:55:90 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu
Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister
capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu
Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister
capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 0! Thu Jan 18 03:19:32 2007:
00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 0 Thu Jan 18 03:19:32
2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 1! Thu Jan 18
03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 1
```

El H-REAP entra el modo autónomo.

Porque este WLAN previamente centralmente fue autenticado y centralmente conmutado, controle y el tráfico de datos era tunneled de nuevo al regulador. Por lo tanto, sin el regulador, el cliente no puede mantener la asociación con el H-REAP y es disconnected. Este estado de H-

REAP con la asociación del cliente y la autenticación que están abajo se refiere como autenticación abajo, conmutando abajo.

Autenticación central, Local Switching

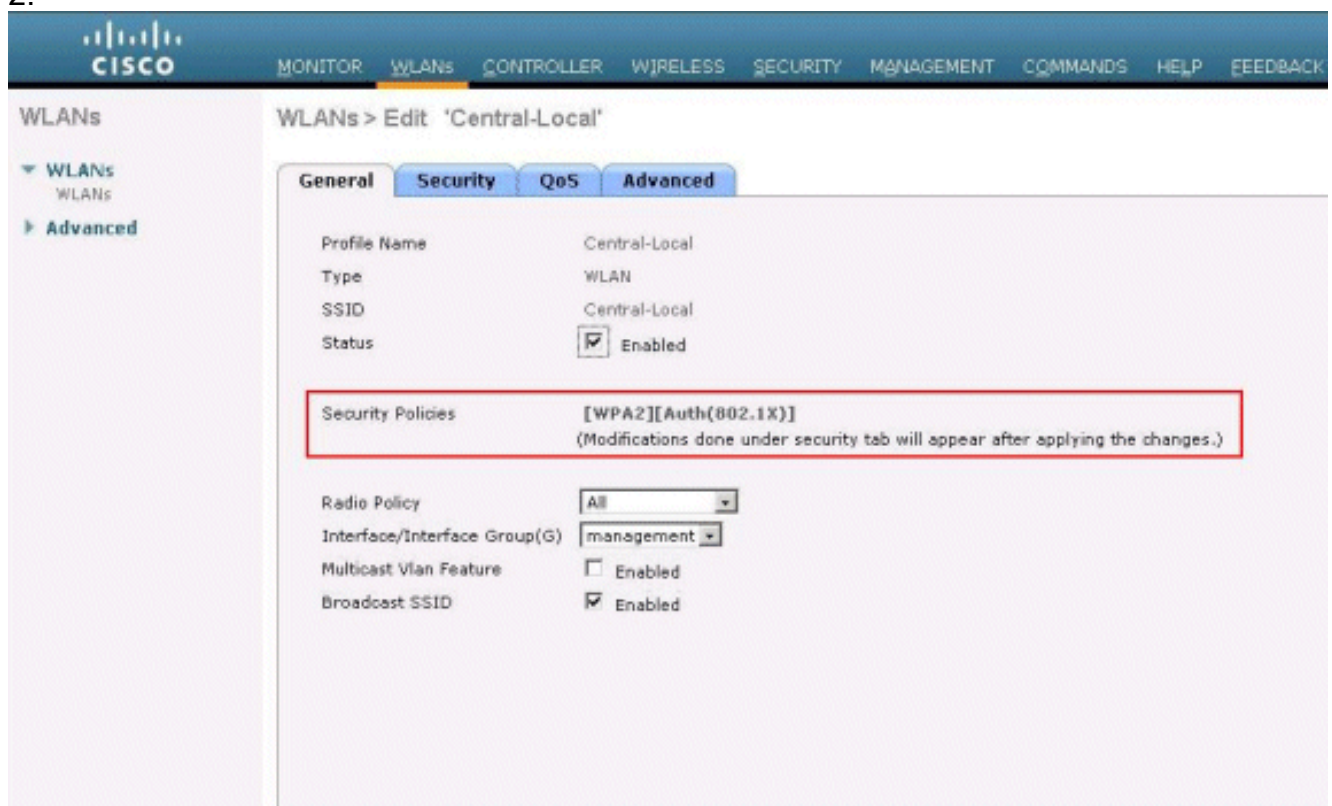
En este estado, para la red inalámbrica (WLAN) dada, el WLC maneja toda la autenticación de cliente, y el REVESTIMIENTO H-REAP conmuta los paquetes de datos localmente. Después de que el cliente autentique con éxito, el regulador envía los comandos de control del capwap al H-REAP y da instrucciones el REVESTIMIENTO para conmutar que los paquetes de datos del cliente dado localmente. Este mensaje se envía por cliente al realizarse satisfactoriamente la autenticación. Este estado es aplicable solamente en el modo conectado.

Este ejemplo utiliza estos ajustes de la configuración:

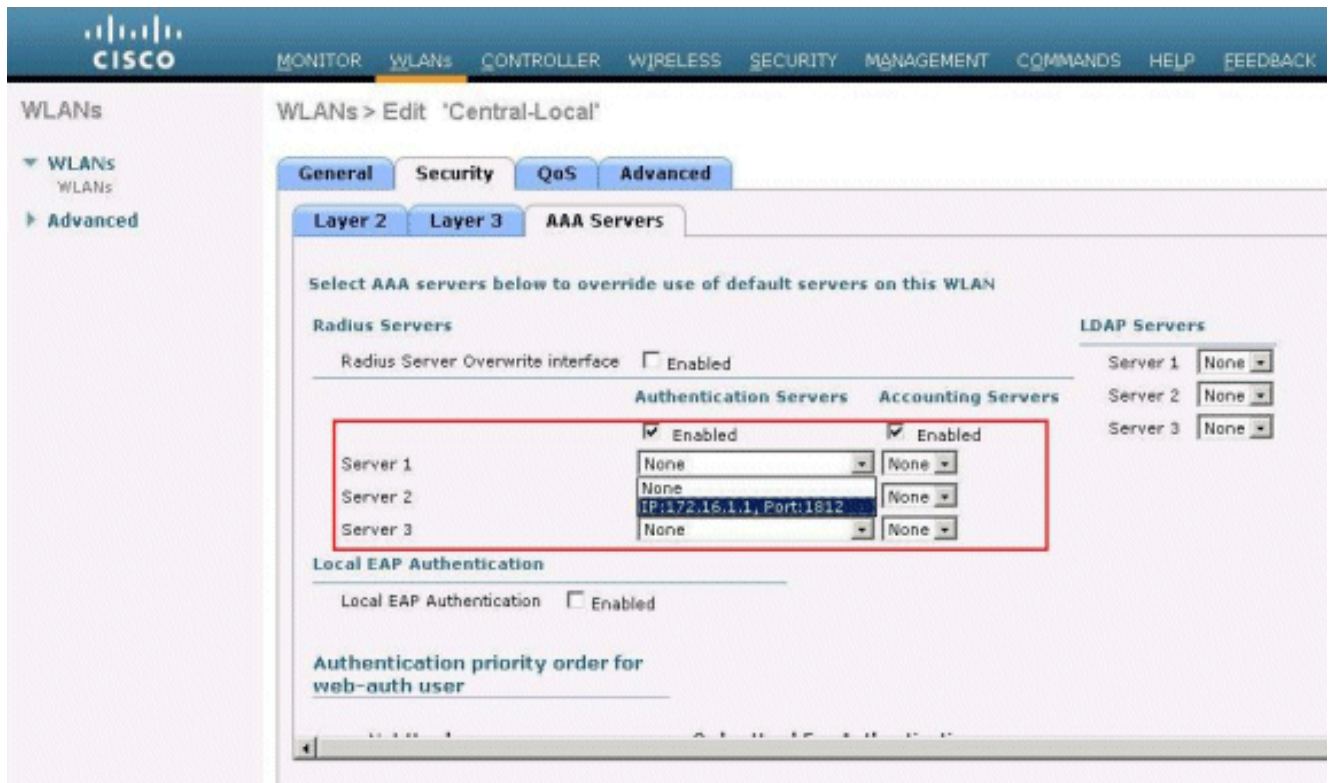
- Nombre del WLAN/SSID: **Central-local**
- Seguridad de la capa 2: **WPA2**.
- Local Switching H-REAP: Habilitado

Del regulador GUI, complete estos pasos:

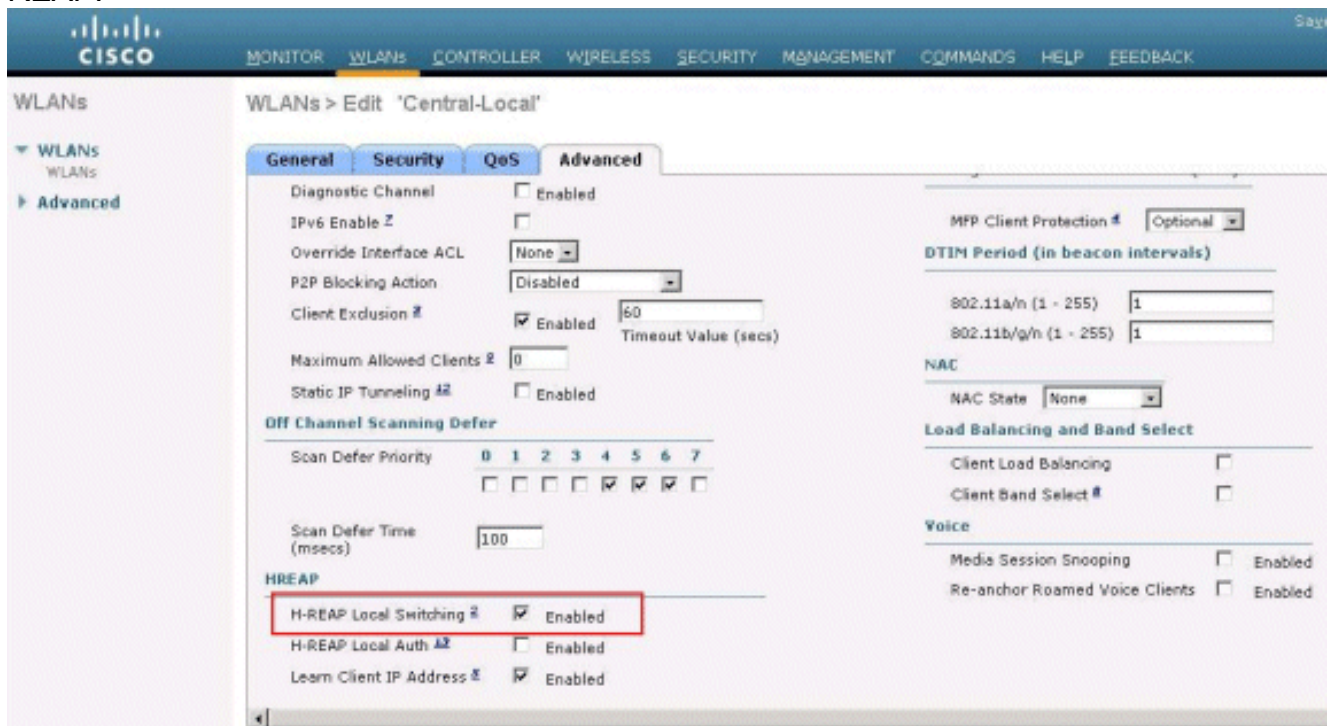
1. Haga clic los **WLAN** para crear una nueva red inalámbrica (WLAN) nombrada Central-Local, después haga clic **se aplican**.
2. Porque esta red inalámbrica (WLAN) utiliza la autenticación central, elija la autenticación **WPA2** en el campo de Seguridad de la capa 2.



3. Bajo los servidores de RADIUS seccione, elija el servidor apropiado configurado para la autenticación.



4. Marque la casilla de verificación del **Local Switching H-REAP** para conmutar el tráfico del cliente que pertenece a esta red inalámbrica (WLAN) localmente en el H-REAP.

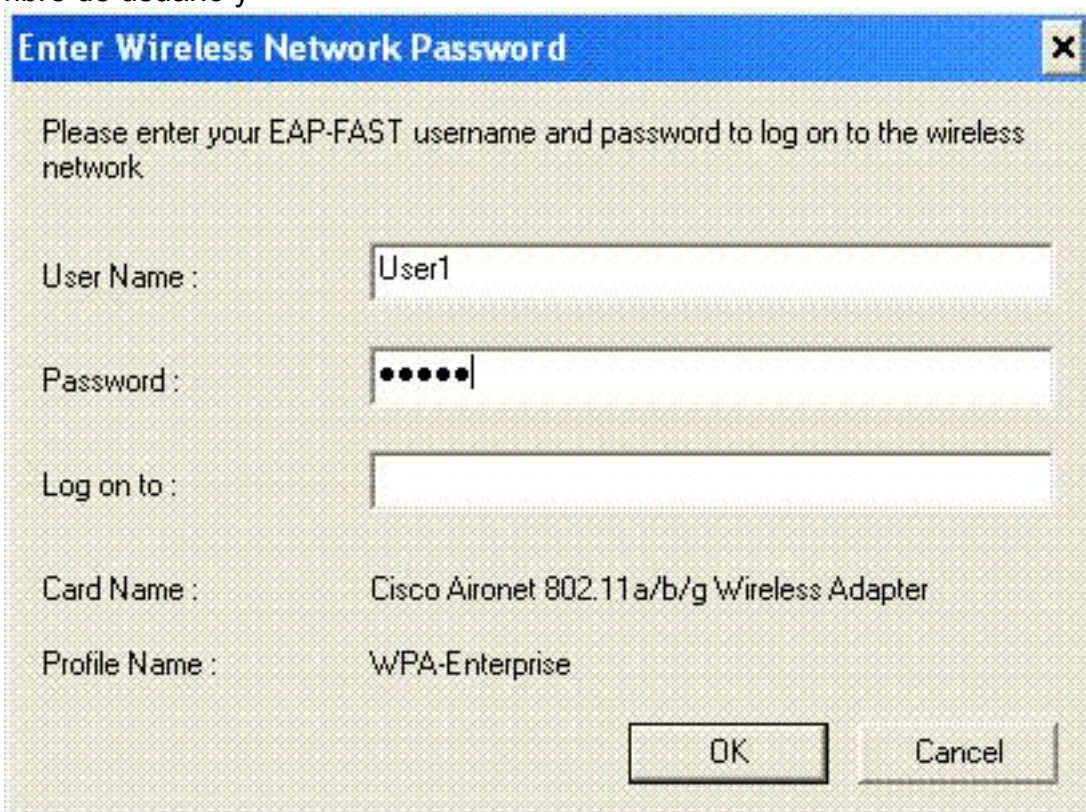


Verifique la autenticación central, Local Switching

Complete estos pasos:

1. Configure al cliente de red inalámbrica con el mismo SSID y Configuraciones de seguridad. En este ejemplo, el SSID es *Central-local* y el método de seguridad es *WPA2*.
2. Ingrese el nombre de usuario y contraseña como está configurado en el `server>User` del RADIO puesto para activar el SSID central-local en el cliente. Este ejemplo utiliza el *user1*

como el nombre de usuario y

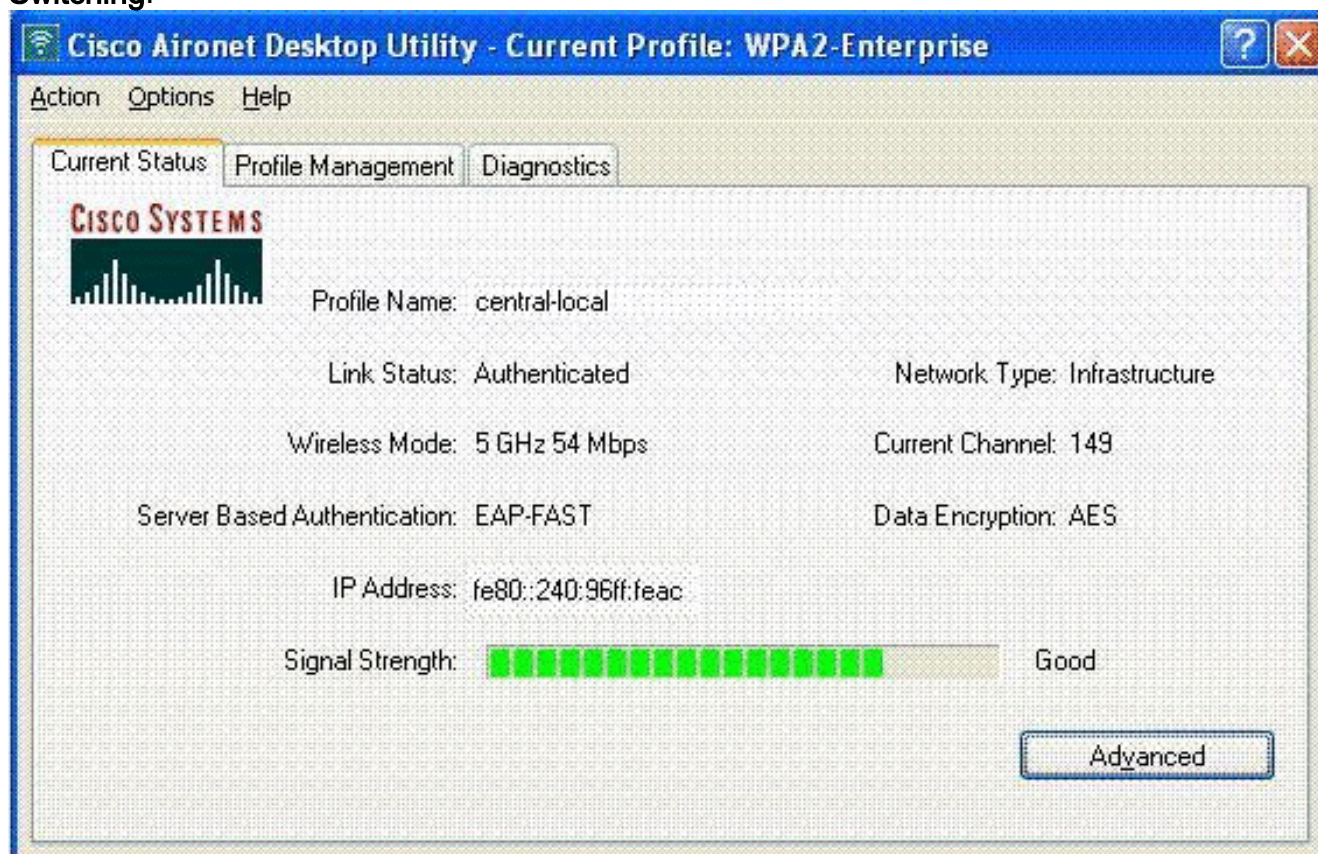


The screenshot shows a dialog box titled "Enter Wireless Network Password". It contains the following fields and information:

- Text: "Please enter your EAP-FAST username and password to log on to the wireless network"
- User Name: "User1"
- Password: "•••••"
- Log on to: (empty field)
- Card Name: "Cisco Aironet 802.11 a/b/g Wireless Adapter"
- Profile Name: "WPA-Enterprise"
- Buttons: "OK" and "Cancel"

contraseña.

3. Haga clic en OK. Al servidor de RADIUS autentica y consigue asociado al cliente centralmente con el H-REAP AP. El H-REAP ahora está en la **autenticación central, Local Switching**.



The screenshot shows the "Cisco Aironet Desktop Utility" window with the title "Current Profile: WPA2-Enterprise". The "Current Status" tab is active, displaying the following information:

- Profile Name: central-local
- Link Status: Authenticated
- Network Type: Infrastructure
- Wireless Mode: 5 GHz 54 Mbps
- Current Channel: 149
- Server Based Authentication: EAP-FAST
- Data Encryption: AES
- IP Address: fe80::240:96ff:feac
- Signal Strength: (10 green bars) Good
- Button: "Advanced"

[Autenticación abajo, Local Switching](#)

Si un WLAN localmente conmutado se configura para cualquier tipo de autenticación que se

requiera ser procesado en el WLC (tal como autenticación EAP [WEP/WPA/WPA2/802.11i], WebAuth, o NAC dinámico), sobre la Falla de WAN, él ingresa la **autenticación abajo**, estado del **Local Switching**. En este estado, para la red inalámbrica (WLAN) dada, el H-REAP rechaza a cualquier nuevo cliente que intente autenticar. Sin embargo, continúa enviando los faros y las respuestas de la sonda para mantener a los clientes existentes conectados correctamente. Este estado es válido solamente en el modo autónomo.

Para verificar este estado, utilice la misma configuración explicada en la [autenticación central](#), sección del [Local Switching](#).

Si el link PÁLIDO que conecta el WLC está abajo, el WLC pasa con el proceso de desregistrar el H-REAP.

Una vez que el desregistrado, H-REAP entra el modo autónomo.

El cliente asociado con esta red inalámbrica (WLAN) todavía mantiene su Conectividad. Sin embargo, porque el regulador, el authenticator no está disponible, H-REAP no permite ninguna nuevas conexiones de esta red inalámbrica (WLAN).

Esto se puede verificar por la activación de otro cliente de red inalámbrica en la misma red inalámbrica (WLAN). Usted puede encontrar que la autenticación para este cliente falla y que no se permite al cliente asociarse.

Nota: Cuando una cuenta del cliente WLAN iguala cero, el H-REAP cesa todas las funciones asociadas del 802.11 y baliza no más para el SSID dado. Esto baja la red inalámbrica (WLAN) al estado siguiente H-REAP, **autenticación, conmutando abajo**.

[Autenticación local, Local Switching](#)

En este estado, el REVESTIMIENTO H-REAP maneja las autenticaciones de cliente y conmuta los paquetes de datos del cliente localmente. Este estado es válido solamente en el modo autónomo y solamente para los tipos de autenticación que pueden ser manejados localmente en el AP y no implican el proceso del regulador

El H-REAP que estaba previamente en la **autenticación central**, estado del **Local Switching**, los movimientos en este estado, con tal que el tipo de autenticación configurado pueda ser manejado localmente en el AP. Si la autenticación configurada no se puede manejar localmente, por ejemplo la autenticación del 802.1x, después en el modo autónomo, el H-REAP va a la **autenticación abajo**, modo del **Local Switching**.

Éstos son algunos de los mecanismos de autenticación populares que se pueden manejar localmente en el AP en el modo autónomo:

- Abierto
- Compartido
- WPA-PSK
- WPA2-PSK

Nota: Todos los procesos de autenticación son manejados por el WLC cuando el AP está en el modo conectado. Mientras que el H-REAP está en el modo autónomo, abierto, compartido, y las autenticaciones WPA/WPA2-PSK se transfieren a los revestimientos donde ocurre toda la autenticación de cliente.

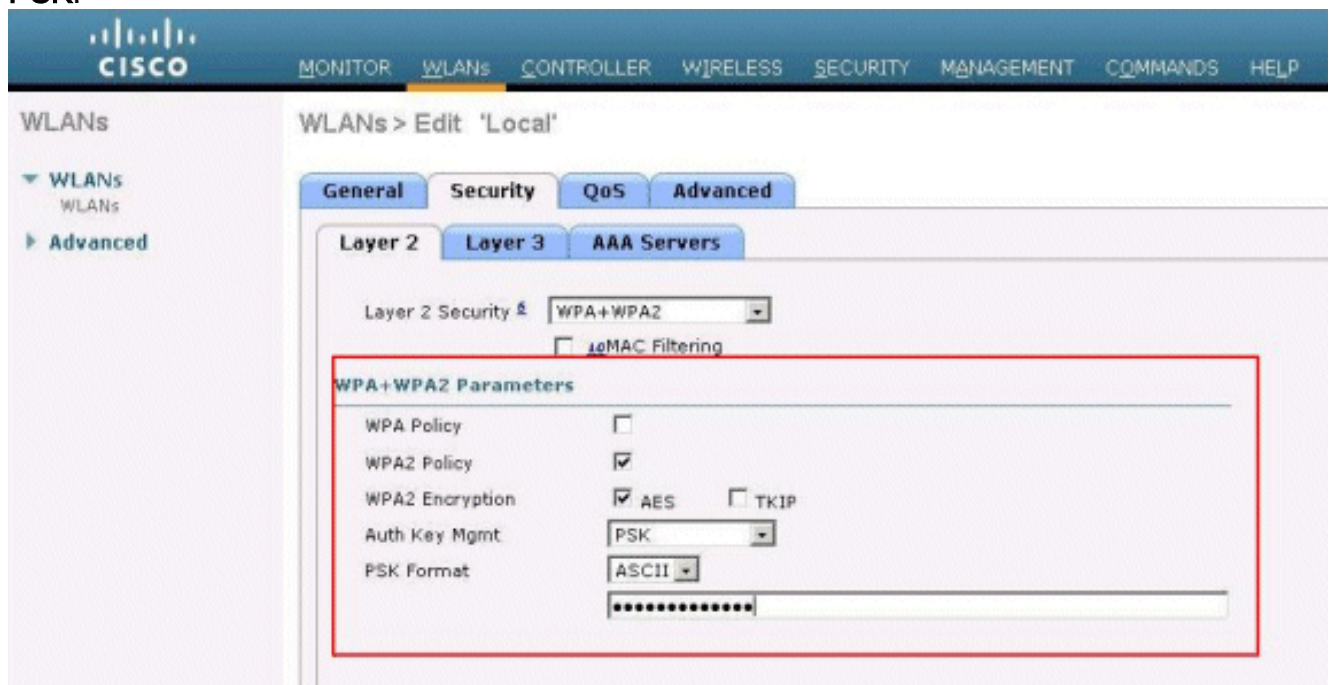
Nota: La autenticación del Web externa no se soporta al usar híbrido-COSECHE con el Local Switching habilitado en la red inalámbrica (WLAN).

Este ejemplo utiliza estos ajustes de la configuración:

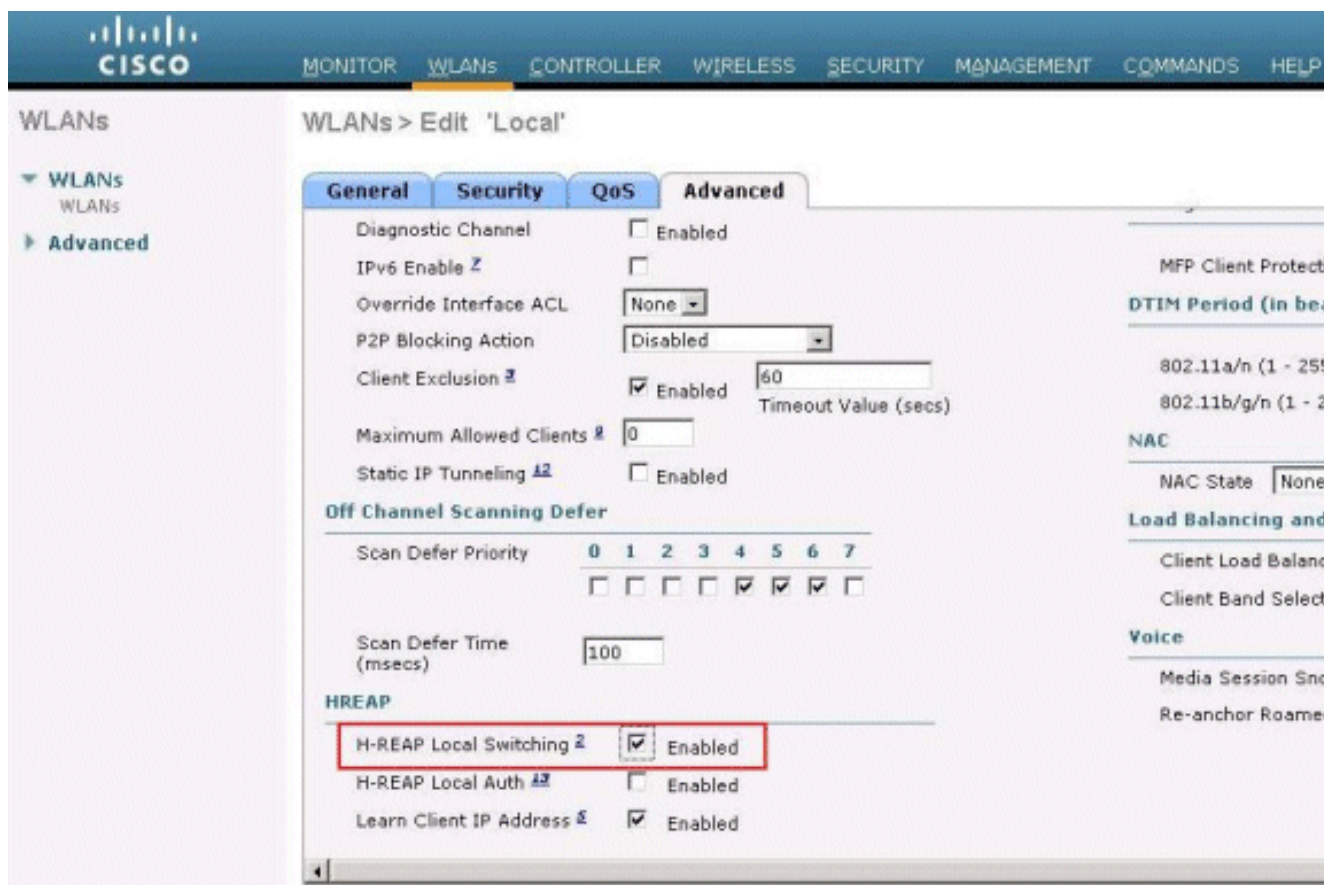
- Nombre del WLAN/SSID: **Local**
- Seguridad de la capa 2: **WPA-PSK**
- Local Switching H-REAP: **habilitado**

Del regulador GUI, complete estos pasos:

1. Haga clic los **WLAN** para crear una nueva red inalámbrica (WLAN) nombrada Local, después haga clic **se aplican**.
2. Porque esta red inalámbrica (WLAN) utiliza la autenticación local, elija el **WPA-PSK** o los mecanismos de seguridad mencionados uces de los que se pueden manejar localmente en el campo de Seguridad de la capa 2. Este ejemplo utiliza el **WPA-PSK**.



3. Una vez que está elegido, usted necesita configurar la clave previamente compartida/la palabra clave que se utilizarán. Éste debe ser lo mismo en el lado del cliente para que la autenticación sea acertada.
4. Marque la casilla de verificación del **Local Switching H-REAP** para conmutar el tráfico del cliente que pertenece a esta red inalámbrica (WLAN) localmente en el H-REAP.



[Verifique la autenticación local, Local Switching](#)

Complete estos pasos:

1. Configure al cliente con el mismo SSID y Configuraciones de seguridad. Aquí, el SSID es *local* y el método de seguridad es *WPA-PSK*.
2. Active el SSID local en el cliente. El cliente consigue autenticado centralmente en el regulador y se asocia al H-REAP. El tráfico del cliente se configura para conmutar localmente. Ahora, el H-REAP está en la autenticación central, estado del Local Switching.
3. Inhabilite el link PÁLIDO que conecta con el regulador. El regulador como de costumbre pasa con el proceso del deregistration. H-REAP se desregistra del regulador. Una vez que el desregistrado, H-REAP entra el modo autónomo. Sin embargo, el cliente que todavía pertenece a esta red inalámbrica (WLAN) mantiene la asociación con H-REAP. También, porque el tipo de autenticación aquí puede ser manejado localmente en el AP sin el regulador, H-REAP permite las asociaciones de cualquier nuevo cliente de red inalámbrica con esta red inalámbrica (WLAN).
4. Para verificar esto, active a cualquier otro cliente de red inalámbrica en la misma red inalámbrica (WLAN). Usted puede ver que autentican y están asociado al cliente con éxito.

[Troubleshooting](#)

- Para resolver problemas más lejos los problemas de la conectividad del cliente en el puerto de la consola del H-REAP, ingrese este comando: `AP_CLI#show capwap reap association`
- Para resolver problemas más lejos los problemas de la conectividad del cliente en el regulador y limitar la salida del debugging adicional, utilice este comando: `AP_CLI#debug mac addr <client's MAC address>`

- Para hacer el debug de los problemas de conectividad del 802.11 de un cliente, utilice este comando:`AP_CLI#debug dot11 state enable`
- Haga el debug del proceso de autenticación y los errores del 802.1x de un cliente con este comando:`AP_CLI#debug dot1x events enable`
- Los mensajes backend controller/RADIUS se pueden hacer el debug de usando este comando:`AP_CLI#debug aaa events enable`
- Alternativamente, habilitar un traje completo de los **comandos debug del cliente**, utilice este comando:`AP_CLI#debug client <client's MAC address>`

[Información Relacionada](#)

- [Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN](#)
- [Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica](#)
- [Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0](#)
- [El híbrido COSECHA el diseño y el Guía de despliegue](#)
- [Troubleshooting Básico de Hybrid Remote Edge Access Point \(H-REAP\)](#)
- [Conmutación por falla del controlador de WLAN para el ejemplo de configuración de los Puntos de acceso ligeros](#)
- [Soporte de Productos de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)