

Configuración del punto de acceso OfficeExtend Aironet serie 600

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Antecedentes](#)
[Pautas de configuración](#)
[Descripción general de la solución Office Extend](#)
[Directrices de configuración del firewall](#)
[Pasos de configuración de Office Extend AP-600](#)
[Parámetros de configuración de WLAN y LAN remota](#)
[Parámetros de seguridad WLAN](#)
[Filtrado de MAC](#)
[Recuento de usuarios admitidos](#)
[Gestión y configuración de canales](#)
[Advertencias adicionales](#)
[Configuración del punto de acceso OEAP-600](#)
[Instalación del hardware del punto de acceso OEAP-600](#)
[Resolución de problemas de OEAP-600](#)
[Cómo depurar problemas de asociación de cliente](#)
[Cómo interpretar el registro de eventos](#)
[Cuando la conexión a Internet no es fiable](#)
[Comandos debug adicionales](#)
[Problemas conocidos/Advertencias](#)
[Información Relacionada](#)

Introducción

Este documento proporciona información sobre los requisitos para configurar un controlador de LAN inalámbrica (WLAN) de Cisco para su uso con el punto de acceso OfficeExtend Access Point (OEAP) de la serie Cisco Aironet® 600. El OEAP Cisco Aironet serie 600 admite el funcionamiento en modo dividido y cuenta con instalaciones que requieren configuración a través del controlador WLAN y funciones que el usuario final puede configurar localmente. Este documento también proporciona información sobre las configuraciones necesarias para una conexión adecuada y los conjuntos de funciones soportadas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el punto de acceso OfficeExtend (OEAP) de Cisco Aironet

serie 600.

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 Cisco para obtener más información sobre las convenciones del documento.](#)

Antecedentes

Pautas de configuración

- El OEAP Cisco Aironet serie 600 es compatible con estos controladores: Cisco 5508, WiSM-2 y Cisco 2504.
- La primera versión del controlador que soporta Cisco Aironet 600 Series OEAP es 7.0.116.0
- Las interfaces de gestión del controlador deben encontrarse en una red IP enrutable.
- Es necesario cambiar la configuración del firewall corporativo para permitir el tráfico con los números de puerto UDP **5246** y **5247**.

Descripción general de la solución Office Extend

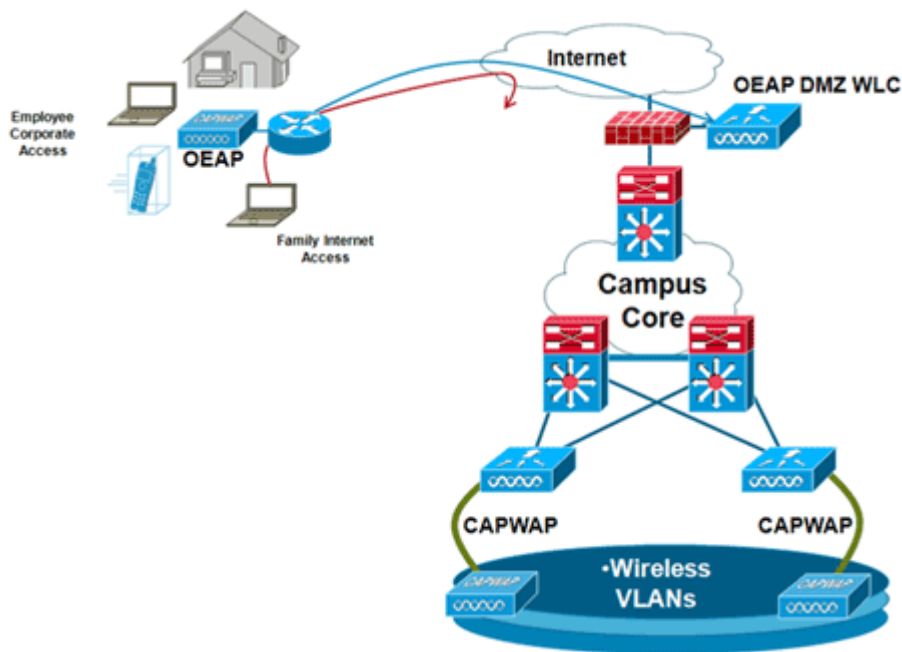
- Un usuario recibe un punto de acceso (AP) preparado con la dirección IP del controlador corporativo, o el usuario puede introducir la dirección IP del controlador desde la pantalla de configuración (páginas HTML de configuración).
- El usuario conecta el AP a su router doméstico.
- El AP obtiene una dirección IP de su router doméstico, se une al controlador preparado y crea un túnel seguro.
- A continuación, el OEAP Cisco Aironet serie 600 anuncia el SSID corporativo, que extiende los mismos métodos y servicios de seguridad a través de la WAN hasta el hogar del usuario.
- Si se configura la LAN remota, un puerto cableado en el AP se tuneliza de nuevo al controlador.
- A continuación, el usuario puede activar adicionalmente un SSID local para uso personal.

Directrices de configuración del firewall

La configuración general del firewall consiste en permitir el control CAPWAP y los números de puerto de administración CAPWAP a través del firewall. El controlador OEAP Cisco Aironet serie 600 se puede colocar en la zona DMZ.

Nota: Los puertos UDP **5246** y **5247** deben abrirse en el firewall entre el controlador WLAN y el Cisco Aironet 600 Series OEAP.

Este diagrama muestra un controlador OEAP Cisco Aironet serie 600 en la DMZ:



A continuación se muestra una configuración de ejemplo del firewall:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address X.X.X.X 255.255.255.224

!--- X.X.X.X represents a public IP address

!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host X.X.X.Y eq 5246

!--- Public reachable IP of corporate controller

access-list Outside extended permit udp any host X.X.X.Y eq 5247

!--- Public reachable IP of corporate controller

access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

Para transmitir la dirección IP interna del administrador de AP al AP OfficeExtend como parte del paquete de respuesta de detección CAPWAPP, el administrador del controlador debe asegurarse de que NAT esté habilitado en la interfaz del administrador de AP y de que se envíe la dirección IP NATed correcta al AP.

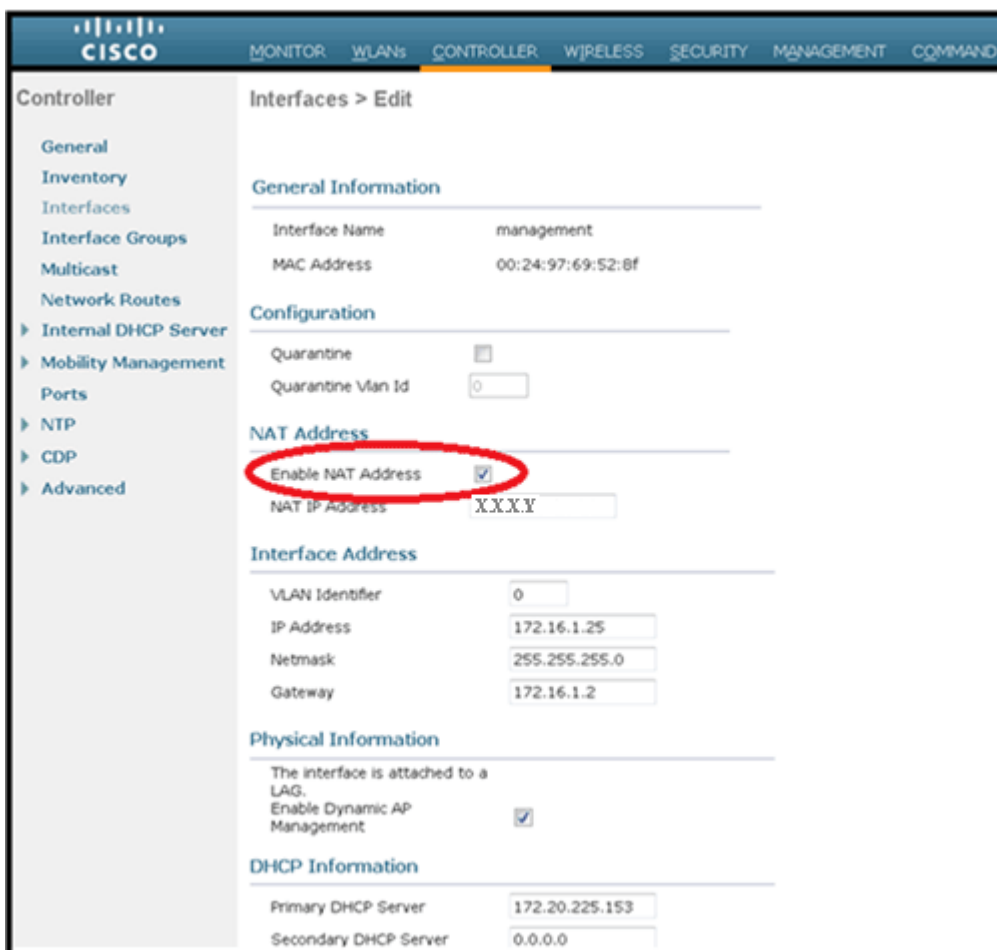
Nota: De forma predeterminada, el WLC solo responderá con la dirección IP NAT durante la detección de AP cuando NAT esté habilitado. Si existen AP en el interior y el exterior del gateway NAT, ejecute este comando para configurar el WLC para responder con la dirección IP NAT y la dirección IP de administración no NAT (interna):

```
<#root>
```

```
config network ap-discovery nat-ip-only disable
```

Nota: Esto solamente se requiere si el WLC tiene una dirección IP NAT.

Este diagrama muestra que NAT está habilitada, suponiendo que el WLC tiene una dirección IP NAT:



Nota: Esta configuración no es necesaria en el controlador siempre que se configure con la dirección IP enrutable de Internet y no detrás de un firewall.

Pasos de configuración de Office Extend AP-600

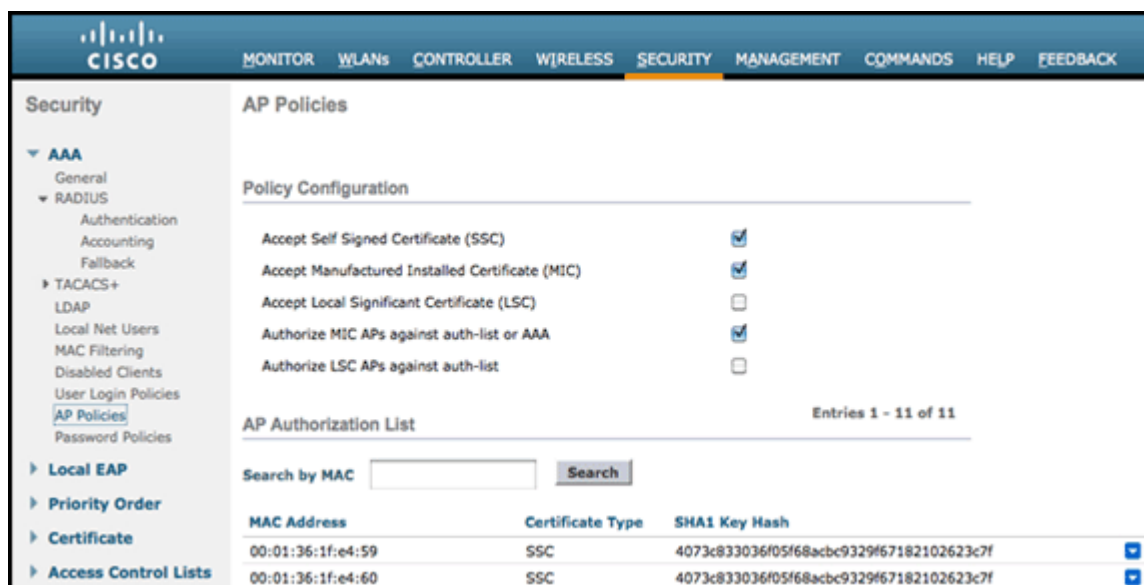
El Cisco Aironet 600 Series OEAP se conectará al WLC como un punto de acceso de modo local.

Nota: Los modos Monitor, H-REAP, Sniffer, Rogue Detection, Bridge y SE-Connect no son compatibles con la serie 600 y no se pueden configurar.

Nota: La funcionalidad de Cisco Aironet 600 Series OEAP en los puntos de acceso 1040, 1130, 1140 y 3502i Series requiere la configuración de los AP para Hybrid REAP (H-REAP) y la configuración del

submodo para el AP para Cisco Aironet 600 Series OEAP. Esto no se hace con la serie 600 porque utiliza el modo local y no se puede alterar.

El filtrado de MAC se puede utilizar en la autenticación de AP durante el proceso de unión inicial para evitar que las unidades OEAP Cisco Aironet serie 600 no autorizadas se unan al controlador. Esta imagen muestra dónde se habilita el filtrado de MAC y se configuran las políticas de seguridad de AP:



Aquí se introduce la dirección MAC de Ethernet (no la dirección MAC de radio). Además, si introduce la dirección MAC en un servidor Radius, debe utilizar minúsculas. Puede examinar el registro de eventos del punto de acceso para obtener información sobre cómo detectar la dirección MAC de Ethernet (más adelante encontrará más información al respecto).

Parámetros de configuración de WLAN y LAN remota

Hay un puerto LAN remoto físico (puerto amarillo #4) en el Cisco Aironet 600 Series EAP. Es muy similar a una WLAN en su configuración. Sin embargo, debido a que no es inalámbrico y un puerto LAN cableado en la parte posterior del AP, se lo llama y se lo administra como un puerto LAN remoto.

Aunque solo hay un puerto físico en el dispositivo, se pueden conectar hasta cuatro clientes con cables si se utiliza un concentrador o un switch.

Nota: El límite de clientes de LAN remota admite la conexión de un switch o concentrador al puerto LAN remoto para varios dispositivos o la conexión directa a un teléfono IP de Cisco que esté conectado a ese puerto.

Nota: solo los primeros cuatro dispositivos pueden conectarse hasta que uno de ellos esté inactivo durante más de un minuto. Si utiliza la autenticación 802.1x, puede haber problemas al intentar utilizar más de un cliente en el puerto cableado.

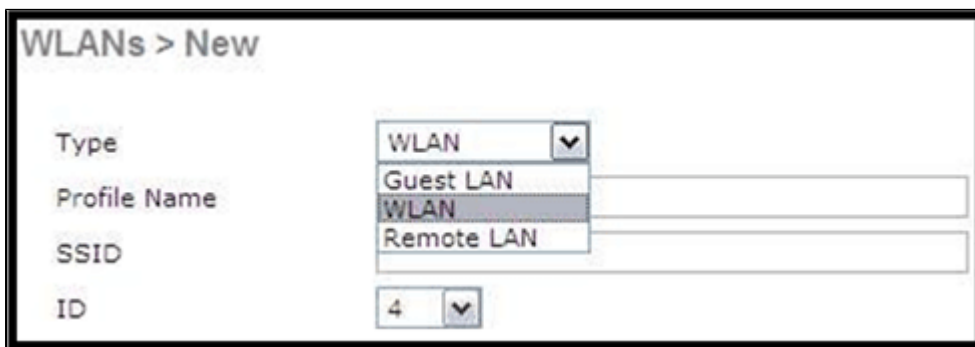
Nota: Este número no afecta el límite de quince impuesto para las WLAN del controlador.

Una LAN remota se configura de manera similar a una WLAN y a una LAN de invitado configurada en el controlador.

Las WLAN son perfiles de seguridad inalámbrica. Estos son los perfiles que utiliza su red corporativa. El OEAP Cisco Aironet serie 600 admite como máximo dos WLAN y una LAN remota.

Una LAN remota es similar a una WLAN excepto que está asignada al puerto cableado en la parte posterior

del punto de acceso (puerto #4 en amarillo) como se muestra en esta imagen:

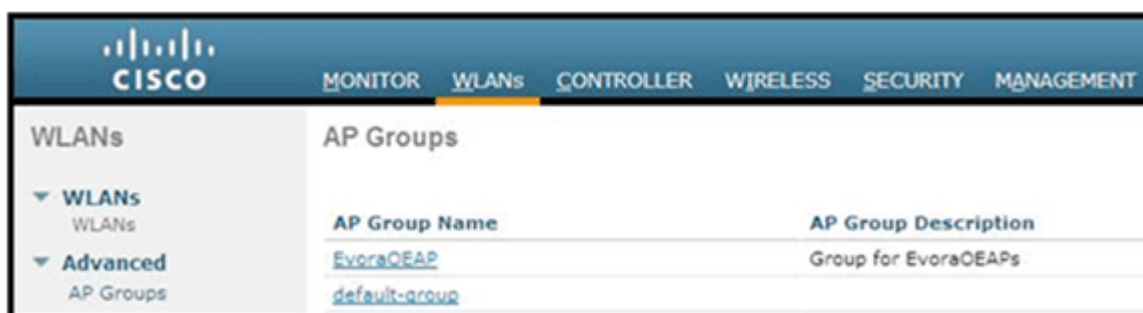


Nota: Si tiene más de dos WLANs o más de una LAN remota, todos deben ubicarse en un grupo de AP.

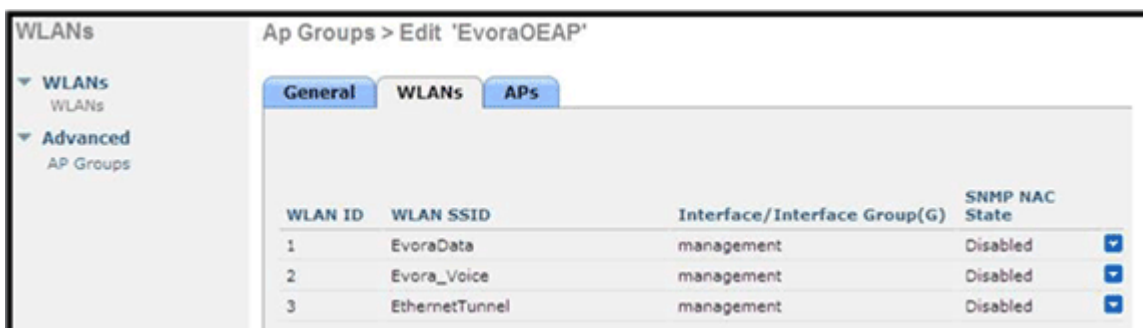
Esta imagen muestra dónde se configuran las WLAN y la LAN remota:



Esta imagen muestra un ejemplo de nombre de grupo OEAP:

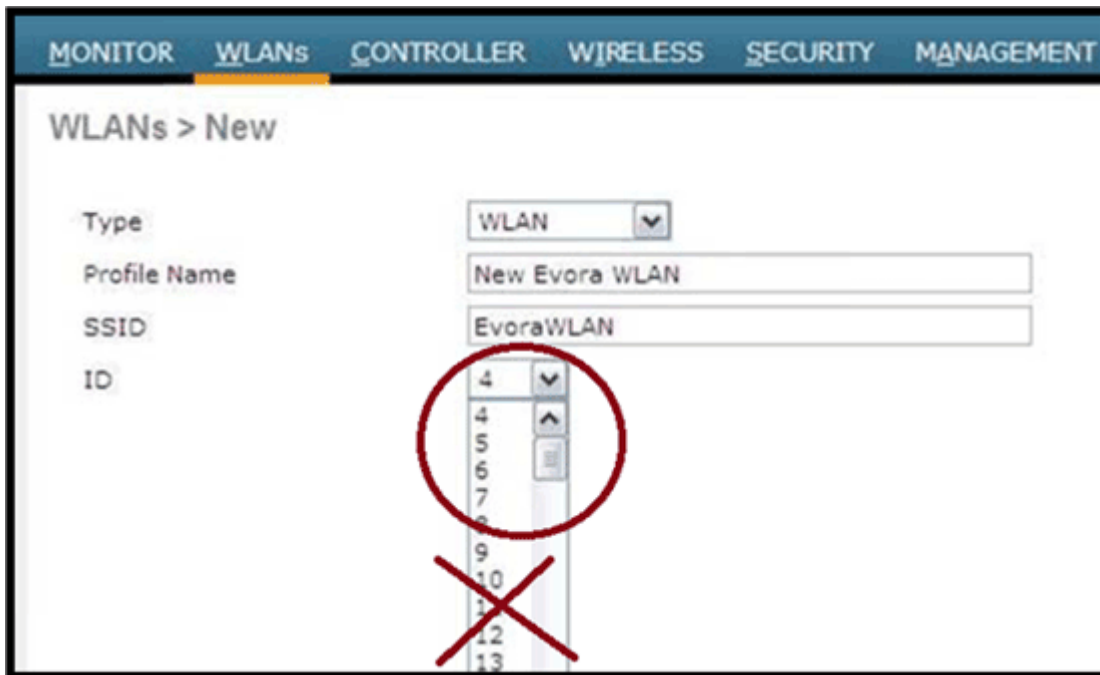


Esta imagen muestra una configuración WLAN SSID y RLAN:



Si el OEAP Cisco Aironet 600 Series se ingresa en un grupo de AP, se aplican los mismos límites de dos WLAN y una LAN remota para la configuración del grupo de AP. Además, si el OEAP Cisco Aironet serie 600 está en el grupo predeterminado, lo que significa que no está en un grupo de AP definido, los ID de LAN remota/WLAN deben establecerse en menos que el ID 8 porque este producto no admite los conjuntos de ID más altos.

Mantenga los conjuntos de ID en menos de 8, como se muestra en esta imagen:



Nota: Si se crean WLAN o LAN remotas adicionales con la intención de cambiar las WLAN o la LAN remota que utiliza el OEAP Cisco Aironet serie 600, desactive las WLAN o LAN remotas actuales que está quitando antes de activar las nuevas WLAN o LAN remota en la serie 600. Si hay más de una LAN remota habilitada para un grupo de AP, inhabilite todas las LAN remotas y luego habilite solamente una.

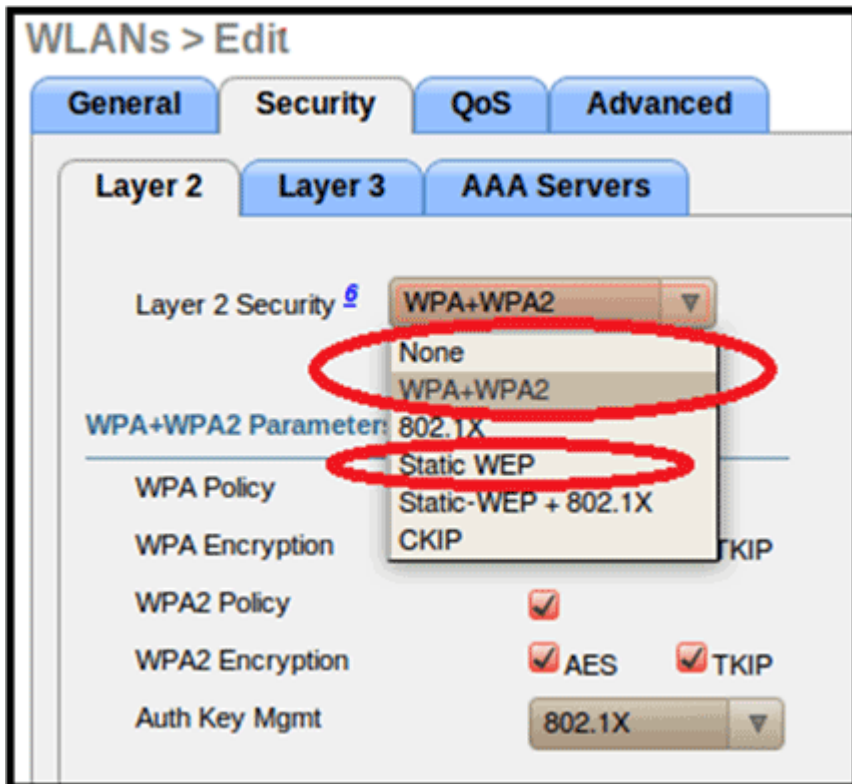
Si hay más de dos WLANs habilitadas para un grupo AP, inhabilite todas las WLANs y luego habilite solamente dos.

Parámetros de seguridad WLAN

Al establecer la configuración de seguridad en la WLAN, hay elementos específicos que no se soportan en la serie 600.

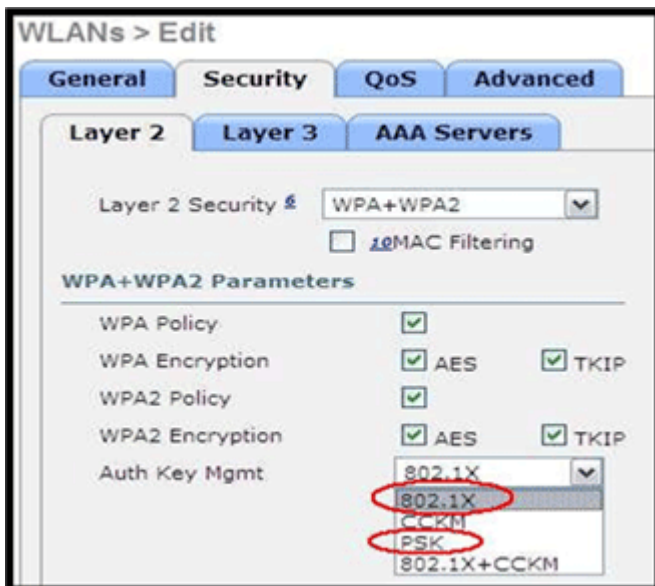
En el caso de la seguridad de capa 2, solo estas opciones son compatibles con Cisco Aironet 600 Series EAP:

- Ninguno
- WPA+WPA2
- También se puede utilizar WEP estática, pero no para velocidades de datos .11n.

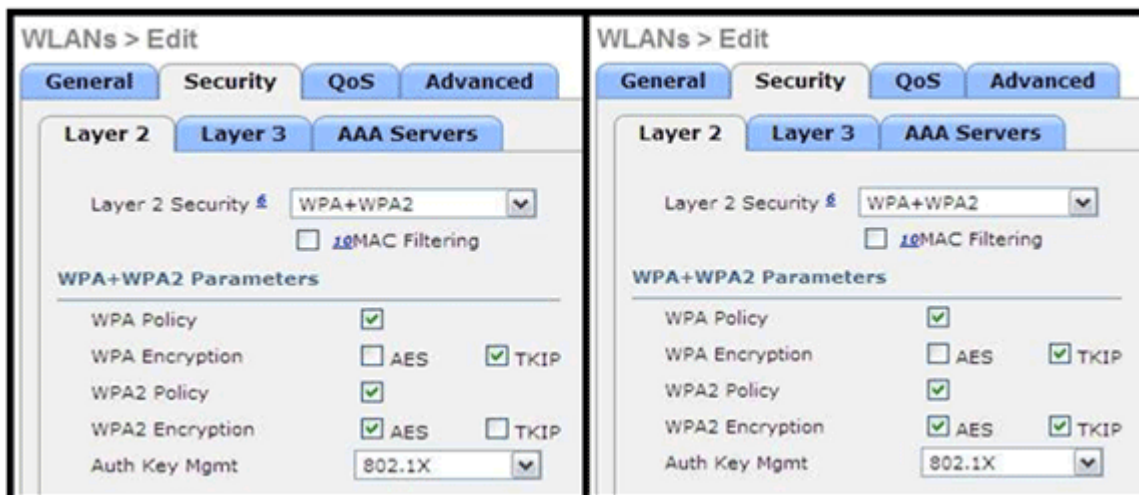


Nota: Sólo se debe seleccionar 802.1x o PSK.

La configuración de encriptación de seguridad debe ser idéntica para WPA y WPA2 para TKIP y AES, como se muestra en esta imagen:

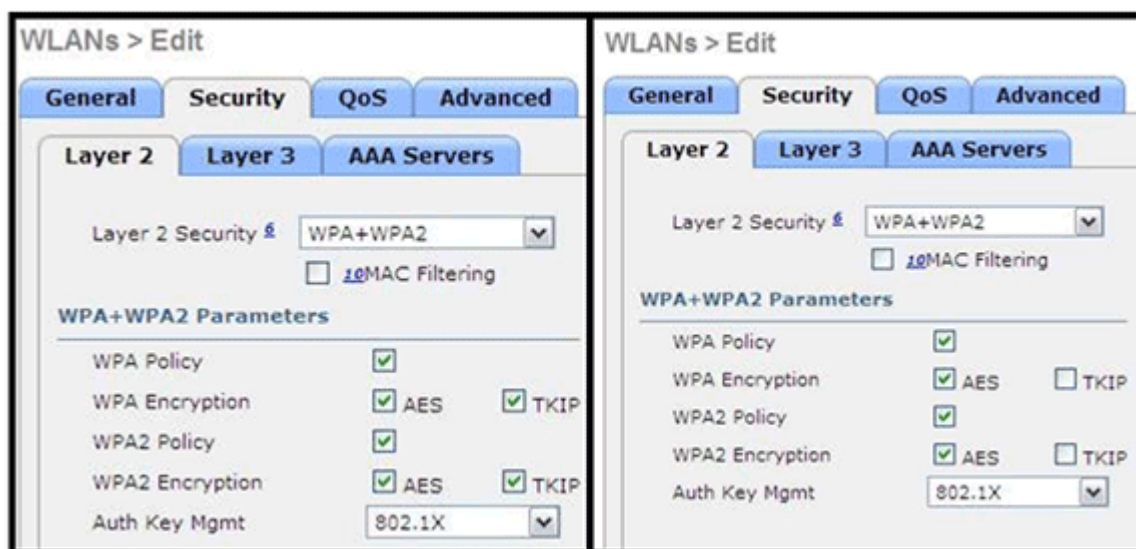


Estas imágenes proporcionan ejemplos de configuraciones incompatibles para TKIP y AES:



Nota: Tenga en cuenta que la configuración de seguridad permite funciones no admitidas.

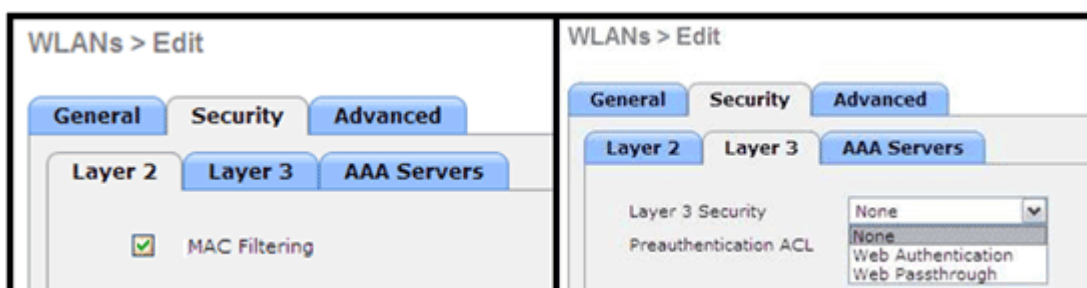
Estas imágenes proporcionan ejemplos de configuraciones compatibles:



Filtrado de MAC

La configuración de seguridad se puede dejar abierta, establecer para el filtrado de MAC o establecer para la autenticación Web. El valor predeterminado es utilizar el filtrado de MAC.

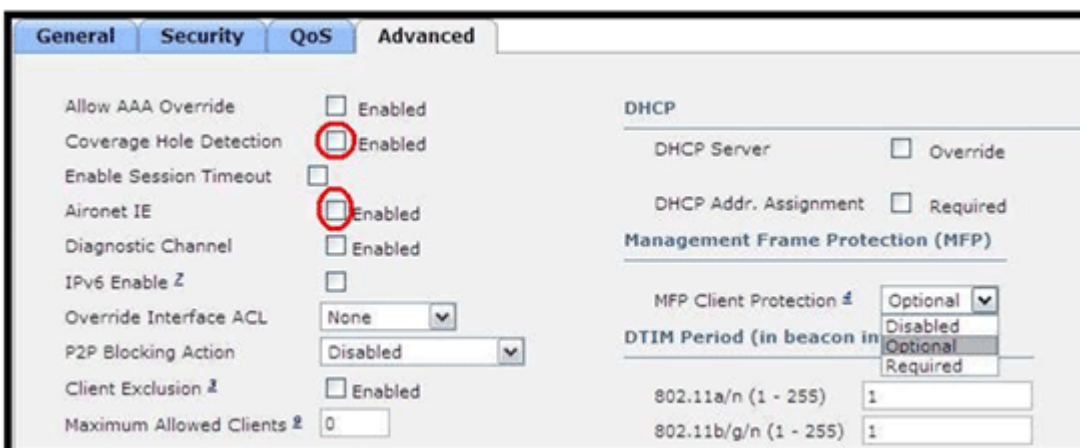
Esta imagen muestra el filtrado de MAC de capa 2 y capa 3:



La configuración de QoS se gestiona:

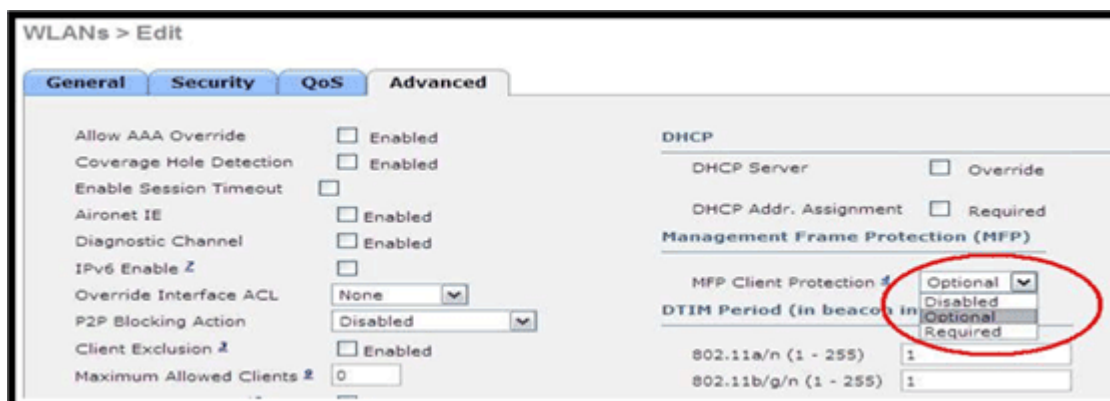


La configuración avanzada también se debe administrar:



Notas:

- La detección de taladros de cobertura no debe estar activada.
- Aironet IE (elementos de información) no debe estar habilitado, ya que no se utilizan.
- Tampoco se admite la protección de tramas de administración (MFP), por lo que debe desactivarse o configurarse como opcional, tal y como se muestra en esta imagen:



- No se admiten el equilibrio de carga de cliente ni la selección de banda de cliente, por lo que no deben habilitarse:



Recuento de usuarios admitidos

Solo quince usuarios pueden conectarse a la vez a las WLANs del Controlador WLAN provistas en la serie 600. Un decimosexto usuario no puede autenticarse hasta que uno de los primeros clientes no realice la autenticación o se agote el tiempo de espera en el controlador.

Nota: Este número es acumulativo a través de las WLANs del controlador en la serie 600.

Por ejemplo, si se configuran dos WLAN de controlador y hay quince usuarios en una de las WLAN, ningún usuario podrá unirse a la otra WLAN en la serie 600 en ese momento. Este límite no se aplica a las WLAN privadas locales que el usuario final configura en la serie 600 diseñada para uso personal y los clientes conectados en estas WLAN privadas o en los puertos cableados no afectan estos límites.

Gestión y configuración de canales

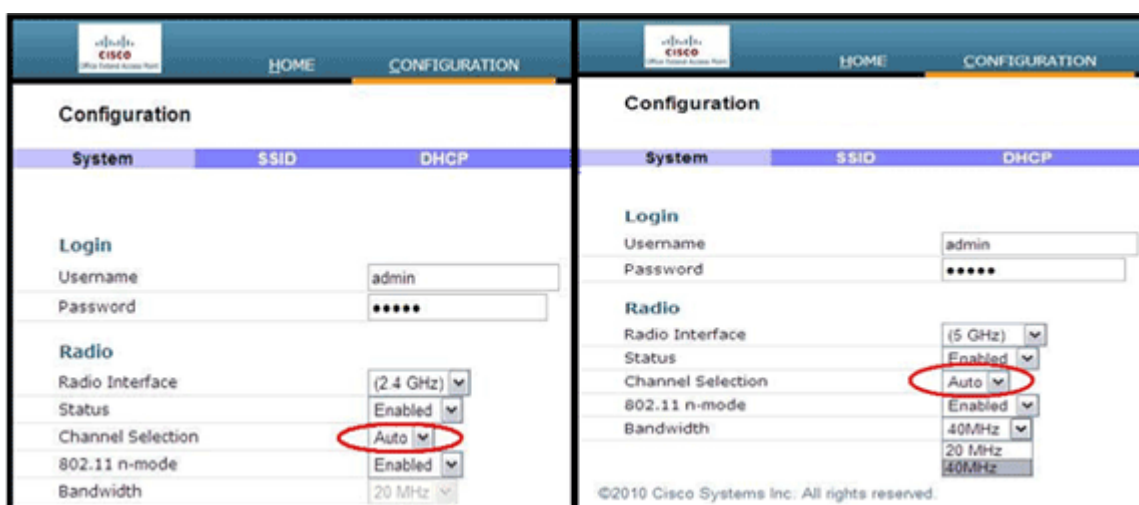
Las radios para la serie 600 se controlan a través de la GUI local en la serie 600 y no a través del controlador de LAN inalámbrica.

Intentar controlar el canal del espectro, la alimentación o desactivar las radios a través del controlador no tendrá ningún efecto en la serie 600.

La serie 600 escaneará y elegirá canales para 2,4 GHz y 5,0 GHz durante el inicio, siempre y cuando los ajustes predeterminados de la GUI local se dejen como predeterminados en ambos espectros.

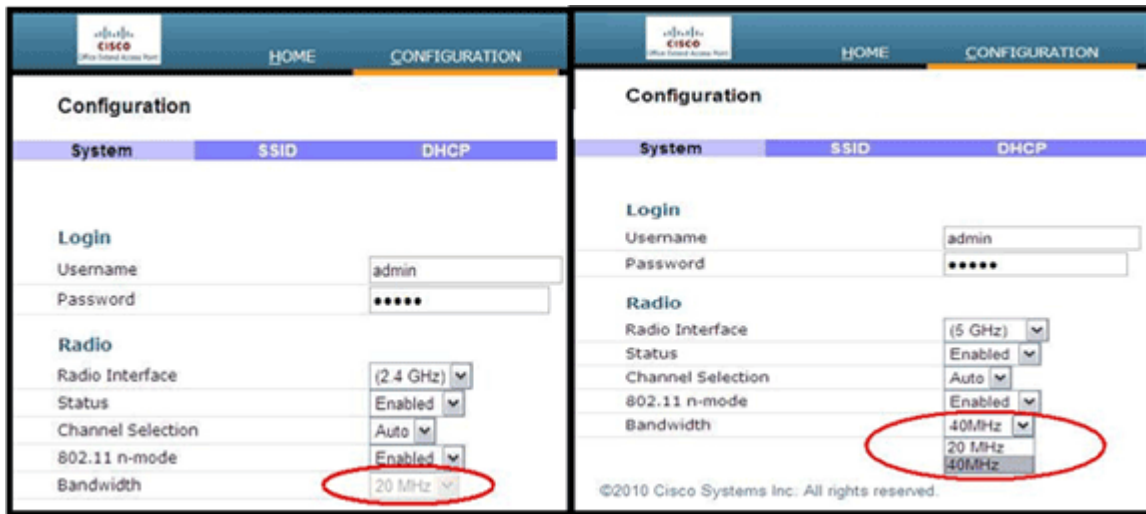
Nota: Si el usuario inhabilita una o ambas radios localmente (esa radio también está inhabilitada para el acceso corporativo), también como se indicó anteriormente, RRM y las funciones avanzadas como monitor, H-REAP, sniffer están más allá de las capacidades del OEAP Cisco Aironet serie 600 que se posiciona para el uso en el hogar y el teletrabajador.

La selección de canal y el ancho de banda para 5,0 GHz se configuran aquí en la GUI local del OEAP Cisco Aironet serie 600.



Notas:

- Los parámetros de ancho de 20 y 40 MHz están disponibles para 5 GHz.
- No se admite la banda de 2,4 GHz de 40 MHz de ancho y está fijada en 20 MHz.
- El ancho de 40 MHz (enlace de canal) no es compatible con 2,4 GHz.



Advertencias adicionales

El OEAP Cisco Aironet serie 600 está diseñado para implementaciones de un solo punto de acceso. Por lo tanto, no se admite el roaming del cliente entre las series 600.

Nota: Es posible que la desactivación de 802.11a/n o 802.11b/g/n en el controlador no desactive estos espectros en el OEAP Cisco Aironet serie 600 porque es posible que el SSID local siga funcionando.

El usuario final tiene el control habilitado/inhabilitado sobre las radios dentro del OEAP Cisco Aironet serie 600.



Compatibilidad con 802.1x en el puerto con cables

En esta versión inicial, 802.1x sólo se admite en la interfaz de línea de comandos (CLI).

Nota: aún no se ha agregado la compatibilidad con la GUI.

Este es el puerto cableado (el puerto #4 en amarillo) en la parte posterior del Cisco Aironet 600 Series OEAP y está vinculado a la LAN remota (consulte la sección anterior sobre configuración de LAN remota).

En cualquier momento, puede utilizar el comando **show** para mostrar la configuración de LAN remota actual:

<#root>

```
show remote-lan <remote-lan-id>
```

Para cambiar la configuración LAN remota, primero debe inhabilitarla:

```
<#root>
```

```
remote-lan disable <remote-lan-id>
```

Active la autenticación 802.1X para la LAN remota:

```
<#root>
```

```
config remote-lan security 802.1X enable <remote-lan-id>
```

Puede deshacer esta acción mediante este comando:

```
<#root>
```

```
config remote-lan security 802.1X disable <remote-lan-id>
```

Para la LAN remota, "Encryption" (Encriptación) siempre es "None" (Ninguno) (como se muestra en **show remote-lan**) y no se puede configurar.

Si desea utilizar el EAP local (en el controlador) como servidor de autenticación:

```
<#root>
```

```
config remote-lan local-auth enable <profile-name> <remote-lan-id>
```

Donde el perfil se define a través del controlador GUI (Seguridad > EAP local) o CLI (**config local-auth**). Consulte la guía del controlador para obtener detalles sobre este comando.

Puede deshacerlo con este comando:

```
<#root>
```

```
config remote-lan local-auth disable <remote-lan-id>
```

O bien, si utiliza un servidor de autenticación AAA externo:

- **config remote-lan radius_server auth add/delete** <remote-lan-id> <server-id>
- **config remote-lan radius_server auth enable/disable** <remote-lan-id>

Donde server se configura a través del controlador GUI (Seguridad > RADIUS > Autenticación) o CLI (**config radius auth**). Consulte la guía del controlador para obtener más información sobre este comando.

Una vez finalizada la configuración, habilite la LAN remota:

```
<#root>
```

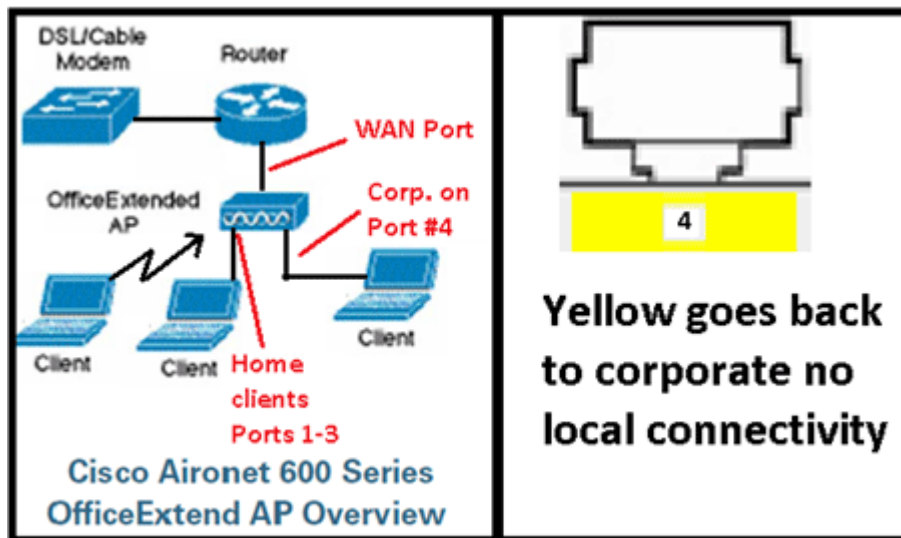
```
config remote-lan enable <remote-lan-id>
```

Utilice el comando **show remote-lan <remote-lan-id>** para verificar su configuración.

Para el cliente LAN remoto, debe habilitar la autenticación 802.1X y configurar en consecuencia. Consulte la guía del usuario del dispositivo.

Configuración del punto de acceso OEAP-600

Esta imagen muestra el diagrama de cableado para el OEAP Cisco Aironet serie 600:

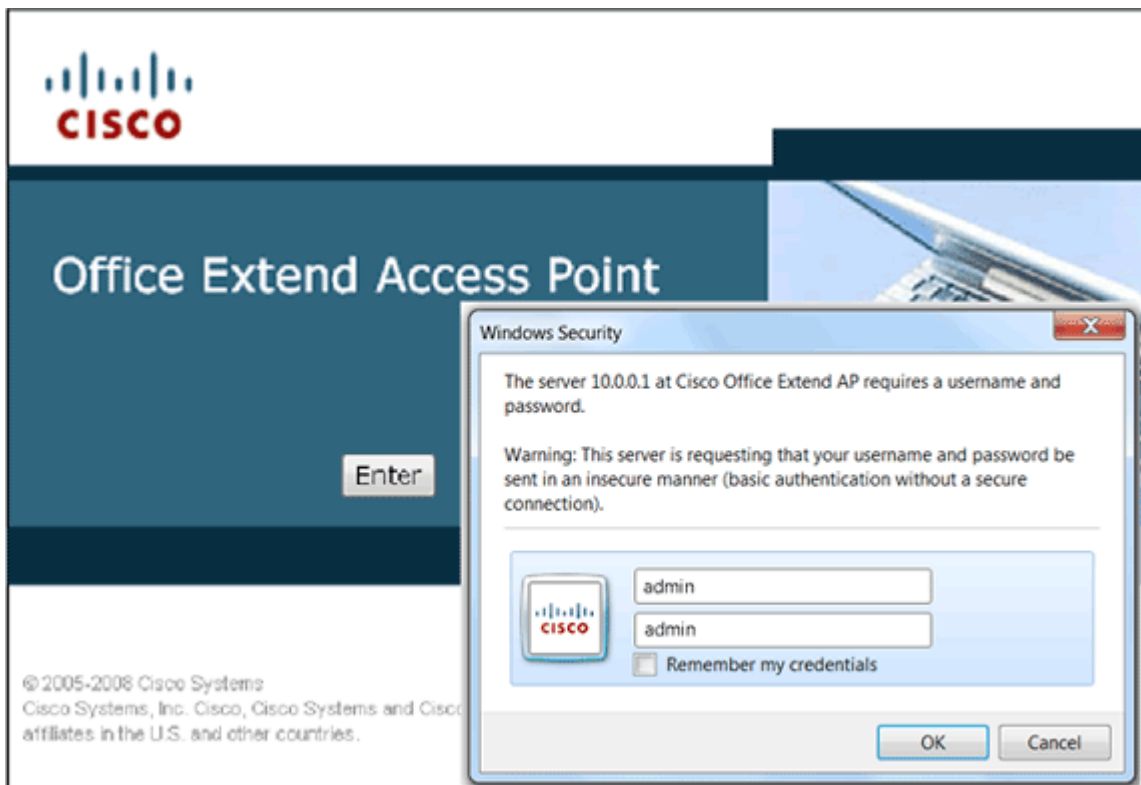


El alcance DHCP predeterminado de Cisco Aironet 600 Series OEAP es 10.0.0.x, por lo que puede navegar al AP en los puertos 1-3 usando la dirección 10.0.0.1. El nombre de usuario y la contraseña predeterminados son admin.

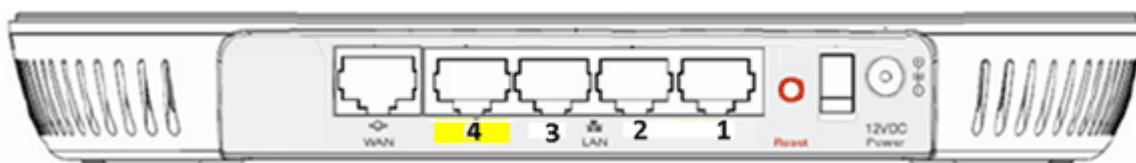
Nota: Esto es diferente de los AP1040, 1130, 1140 y 3502i que utilizaban Cisco como nombre de usuario y contraseña.

Si las radios están activas y ya se ha configurado un SSID personal, puede acceder a la pantalla de configuración de forma inalámbrica. De lo contrario, deberá utilizar los puertos Ethernet locales 1-3.

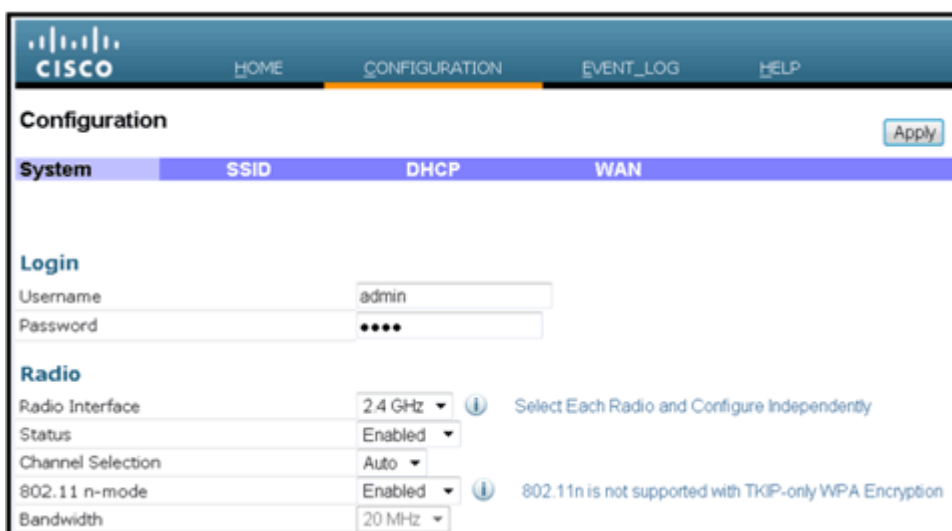
Para iniciar sesión, el nombre de usuario y la contraseña predeterminados son admin.



Nota: El puerto amarillo #4 no está activo para uso local. Si se configura una LAN remota en el controlador, este puerto se tuneliza nuevamente después de que el AP se une exitosamente al controlador. Para buscar el dispositivo, utilice localmente los puertos 1-3:



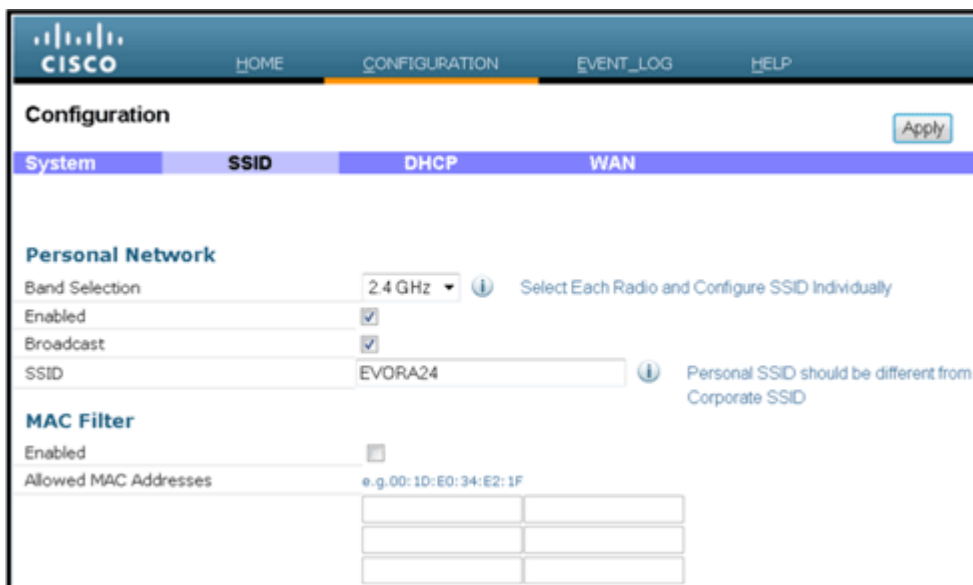
Una vez que navegue hasta el dispositivo correctamente, verá la pantalla de estado de inicio. Esta pantalla proporciona estadísticas de radio y MAC. Si no se han configurado los radios, la pantalla de configuración permite al usuario activar los radios, establecer canales y modos, configurar SSID locales y activar los parámetros de WLAN.



En la pantalla SSID, el usuario puede configurar la red WLAN personal. Los parámetros de seguridad y

SSID de radio corporativos se configuran y se introducen desde el controlador (después de configurar la WAN con la IP del controlador) y se ha producido una unión correcta.

Esta imagen muestra una configuración de filtrado MAC local SSID:



Una vez que el usuario haya configurado el SSID personal, la pantalla siguiente le permite configurar la seguridad en el SSID doméstico privado, activar radios y configurar el filtrado de MAC si lo desea. Si la red personal utiliza velocidades 802.11n, se recomienda que el usuario elija un tipo de autenticación, un tipo de encriptación y una frase de paso que permitan WPA2-PSK y AES.

Nota: Estos parámetros SSID son diferentes de los parámetros corporativos si el usuario decide desactivar una o ambas radios (ambas también están desactivadas para uso corporativo).

Los usuarios que tienen acceso de forma local a la configuración del control de administración tienen control sobre las funciones principales, como la activación y desactivación de radio, a menos que el administrador proteja y configure el dispositivo mediante contraseña. Por lo tanto, se debe tener cuidado de no deshabilitar ambas radios ya que esto puede resultar en una pérdida de conectividad incluso si el dispositivo se une con éxito al controlador.

Esta imagen muestra la configuración de seguridad del sistema:



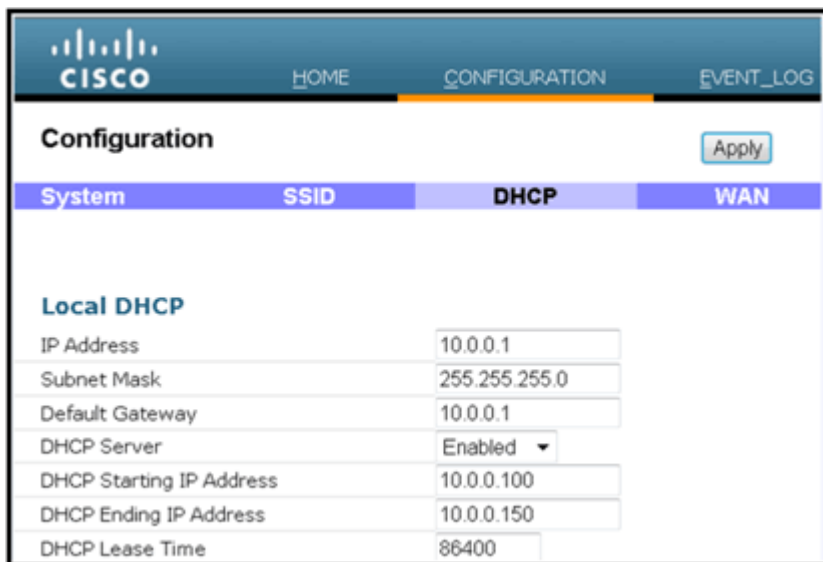
Se espera que el teletrabajador doméstico instale el Cisco Aironet 600 Series OEAP detrás de un router doméstico, ya que este producto no está diseñado para reemplazar la funcionalidad de un router doméstico. Esto se debe a que la versión actual de este producto no es compatible con firewall, PPPoE ni con el reenvío de puertos. Estas son características que los clientes esperan encontrar en un router doméstico.

Aunque este producto puede funcionar sin un router doméstico, se recomienda no colocarlo de esa manera por las razones indicadas. Además, puede haber problemas de compatibilidad al conectarse directamente a algunos módems.

Dado que la mayoría de los routers domésticos tienen un alcance DHCP en el rango 192.168.x.x, este dispositivo tiene un alcance DHCP predeterminado de 10.0.0.x y es configurable.

Si el router doméstico utiliza 10.0.0.x, debe configurar el Cisco Aironet 600 Series OEAP para utilizar una dirección IP 192.168.1.x o compatible para evitar conflictos de red.

Esta imagen muestra una configuración de alcance DHCP:



The screenshot shows the Cisco configuration web interface. At the top, there are navigation tabs: HOME, CONFIGURATION (selected), and EVENT_LOG. Below the tabs is a 'Configuration' section with an 'Apply' button. A table with four columns: System, SSID, DHCP, and WAN is visible. Under the 'Local DHCP' section, the following settings are displayed:

System	SSID	DHCP	WAN
Local DHCP			
IP Address		10.0.0.1	
Subnet Mask		255.255.255.0	
Default Gateway		10.0.0.1	
DHCP Server		Enabled	
DHCP Starting IP Address		10.0.0.100	
DHCP Ending IP Address		10.0.0.150	
DHCP Lease Time		86400	

Precaución: Si el administrador de TI no instala o configura el OEAP Cisco Aironet serie 600, el usuario debe ingresar la dirección IP del controlador corporativo (ver a continuación) para que el AP pueda unirse satisfactoriamente al controlador. Después de una unión exitosa, el AP debe descargar la imagen más reciente del controlador y los parámetros de configuración tales como las configuraciones WLAN corporativas. Además, si se configura, los ajustes de LAN remota conectan el puerto con cable #4 en la parte posterior del OEAP Cisco Aironet serie 600.

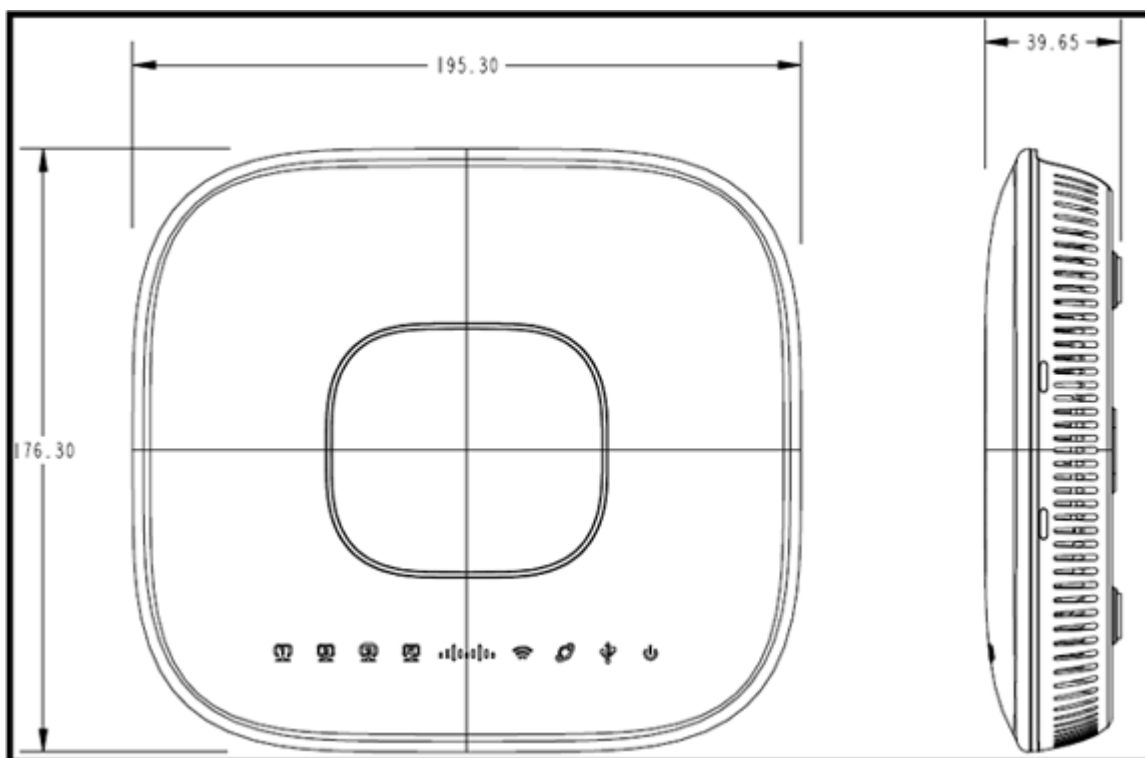
Si no se une, verifique que la dirección IP del controlador sea accesible a través de Internet. Si el filtrado de MAC está activado, compruebe que la dirección MAC se ha introducido correctamente en el controlador.

Esta imagen muestra la dirección IP del controlador Cisco Aironet 600 Series OEAP:



Instalación del hardware del punto de acceso OEAP-600

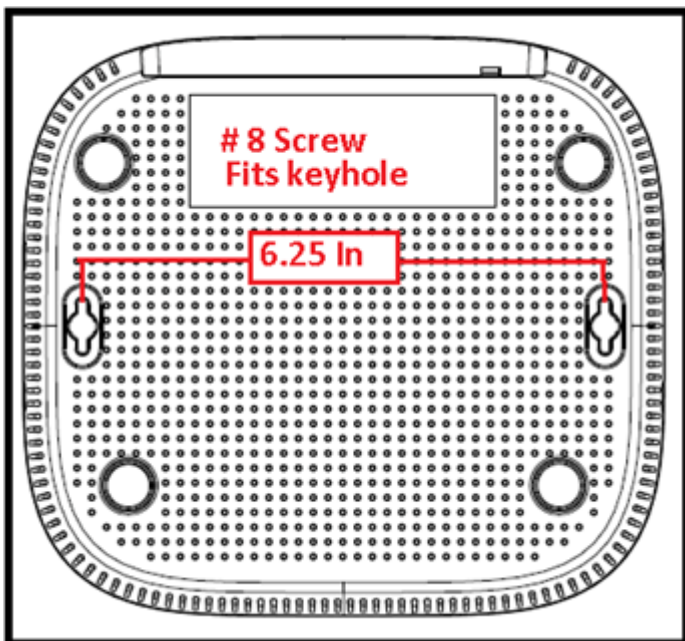
Esta imagen muestra los aspectos físicos del OEAP Cisco Aironet serie 600:



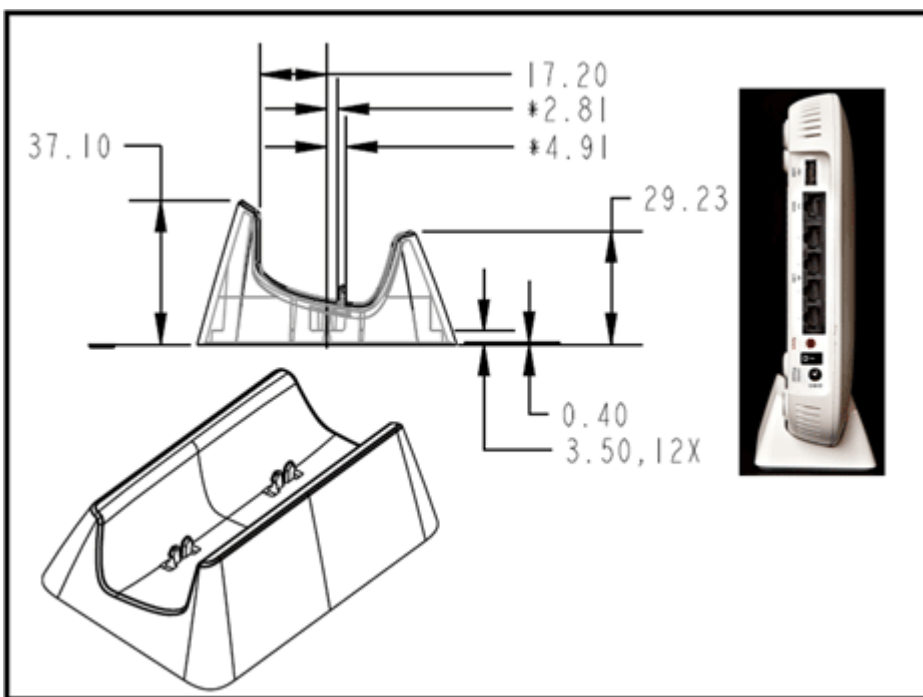
Este AP está diseñado para ser montado en una mesa y tiene pies de goma. También se puede montar en la pared o sentarse en posición vertical utilizando la base suministrada. Intente localizar el AP lo más cerca posible de los usuarios previstos. Evite las zonas con grandes superficies metálicas, como por ejemplo, el dispositivo sobre un escritorio metálico o cerca de un espejo grande. Cuantas más paredes y objetos haya entre el AP y el usuario, menor será la potencia de la señal y se reducirá el rendimiento.

Nota: Este punto de acceso utiliza una fuente de alimentación de +12 voltios y no utiliza alimentación a través de Ethernet (PoE). Además, el dispositivo no proporciona PoE. Asegúrese de que se utiliza el adaptador de corriente correcto con el AP. Además, asegúrese de no utilizar otros adaptadores de otros dispositivos como laptops y teléfonos IP ya que estos pueden dañar el AP.

La unidad se puede montar en la pared con anclajes de plástico o tornillos de madera.



La unidad se puede montar en posición vertical utilizando la base suministrada.



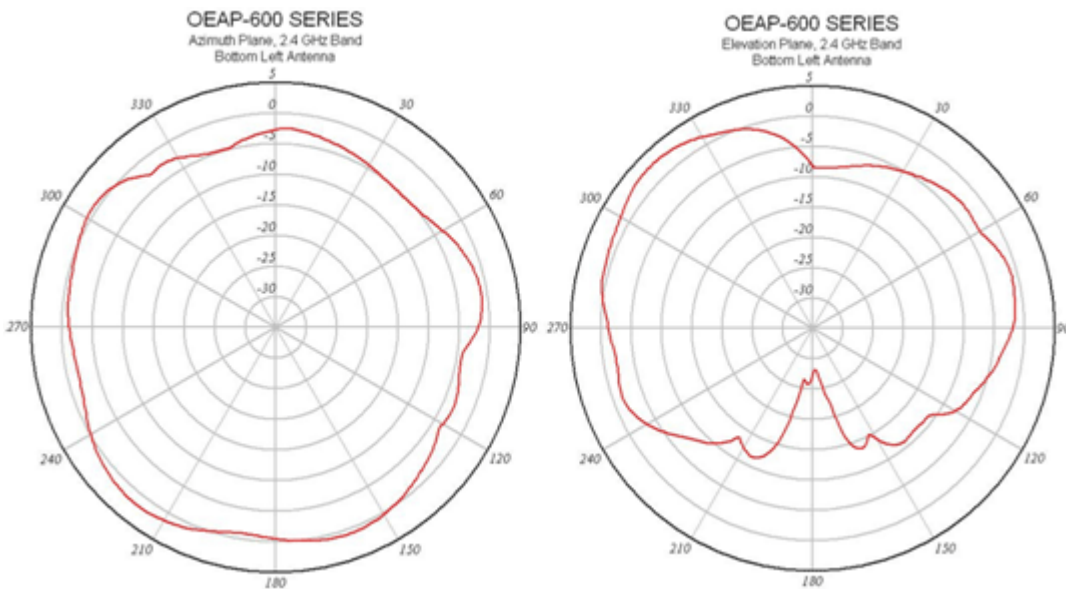
El OEAP Cisco Aironet serie 600 tiene antenas ubicadas en los bordes del AP. El usuario debe tener cuidado de no colocar el AP en áreas cercanas a objetos metálicos u obstrucciones que puedan causar que la señal se vuelva direccional o disminuya. La ganancia de la antena es de aproximadamente 2 dBi en ambas bandas y está diseñada para radiar en un patrón de 360 grados. Similar a una bombilla (sin pantalla), el objetivo es irradiar en todas las direcciones. Piense en el punto de acceso como si fuera una lámpara e intente colocarlo cerca de los usuarios.

Los objetos metálicos, como los espejos, obstruyen la señal de forma muy similar a la analogía de la pantalla. Si la señal debe penetrar en objetos sólidos o pasar a través de ellos, puede experimentar un rendimiento o alcance degradados. Si espera conectividad, por ejemplo en una casa de tres pisos, evite colocar el AP en el sótano e intente montar el AP en una ubicación central dentro de la casa.

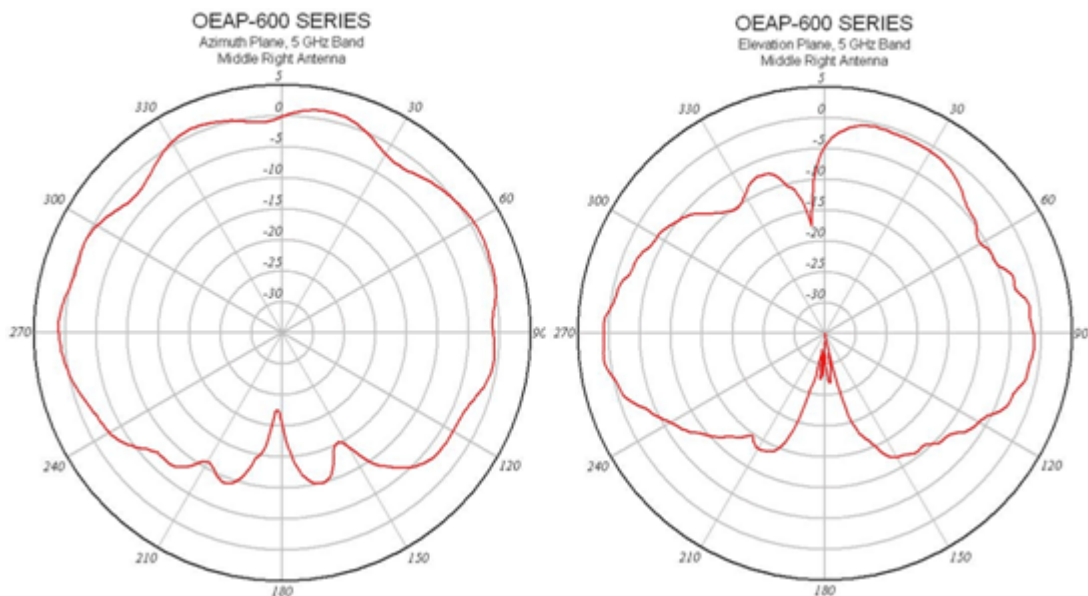
El punto de acceso tiene seis antenas (tres por banda).



Esta imagen muestra un patrón de radiación de antena de 2,4 GHz (tomado de la antena inferior izquierda).



Esta imagen muestra un patrón de radiación de antena de 5 GHz (tomado de la antena central derecha):



Resolución de problemas de OEAP-600

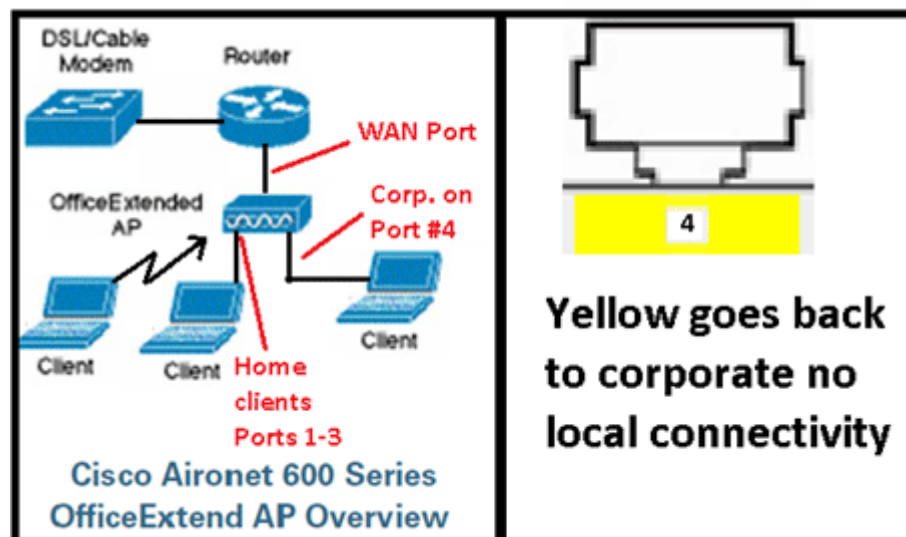
Compruebe que el cableado inicial es correcto. Esto confirma que el puerto WAN del OEAP Cisco Aironet serie 600 está conectado al router y puede recibir una dirección IP correctamente. Si el AP no parece unirse al controlador, conecte una PC al puerto 1-3 (puertos del cliente de inicio) y vea si puede navegar al AP usando la dirección IP predeterminada de 10.0.0.1. El nombre de usuario y la contraseña predeterminados son admin.

Verifique que la dirección IP para el controlador corporativo esté configurada. Si no es así, ingrese la dirección IP y reinicie el Cisco Aironet 600 Series OEAP para que pueda intentar establecer un link con el controlador.

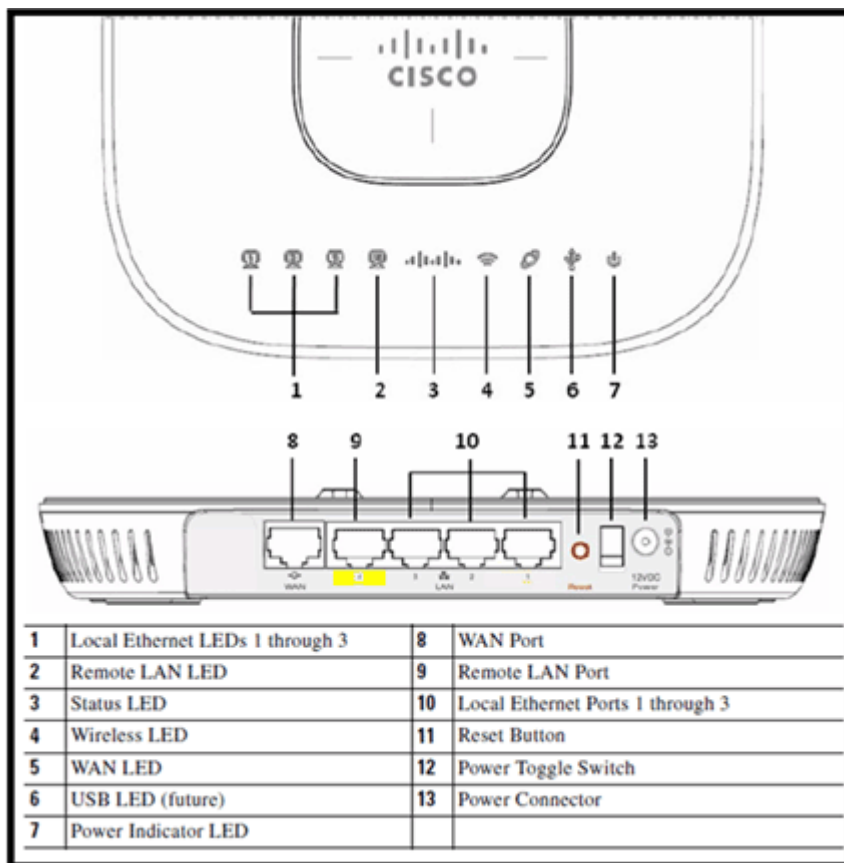
Nota: El puerto corporativo #4 (en amarillo) no se puede utilizar para navegar hasta el dispositivo con fines de configuración. Básicamente, se trata de un "puerto muerto" a menos que se configure una LAN remota. A continuación, volverá al túnel corporativo (utilizado para la conectividad empresarial por cable)

Compruebe el registro de eventos para ver cómo progresó la asociación (más adelante encontrará más información sobre este tema).

Esta imagen muestra el diagrama de cableado OEAP de Cisco Aironet serie 600:



Esta imagen muestra los puertos de conectividad OEAP de Cisco Aironet serie 600:



Si el OEAP Cisco Aironet serie 600 no puede unirse al controlador, se recomienda que verifique estos elementos:

1. Verifique que el router esté funcional y conectado al puerto WAN del Cisco Aironet 600 Series EAP.
2. Conecte un PC a uno de los puertos 1-3 del OEAP Cisco Aironet serie 600. Debería ver Internet.
3. Verifique que la dirección IP del controlador corporativo esté en el AP.
4. Confirme que el controlador está en DMZ y es accesible a través de Internet.
5. Verifique que se une y confirme que el LED del logotipo de Cisco es azul o morado fijo.
6. Deje tiempo suficiente en caso de que el AP necesite cargar una nueva imagen y reiniciar.
7. Si hay un firewall en uso, verifique que los puertos UDP 5246 y 5247 no estén bloqueados.

Esta imagen muestra el estado del LED del logotipo EAP de Cisco Aironet serie 600:

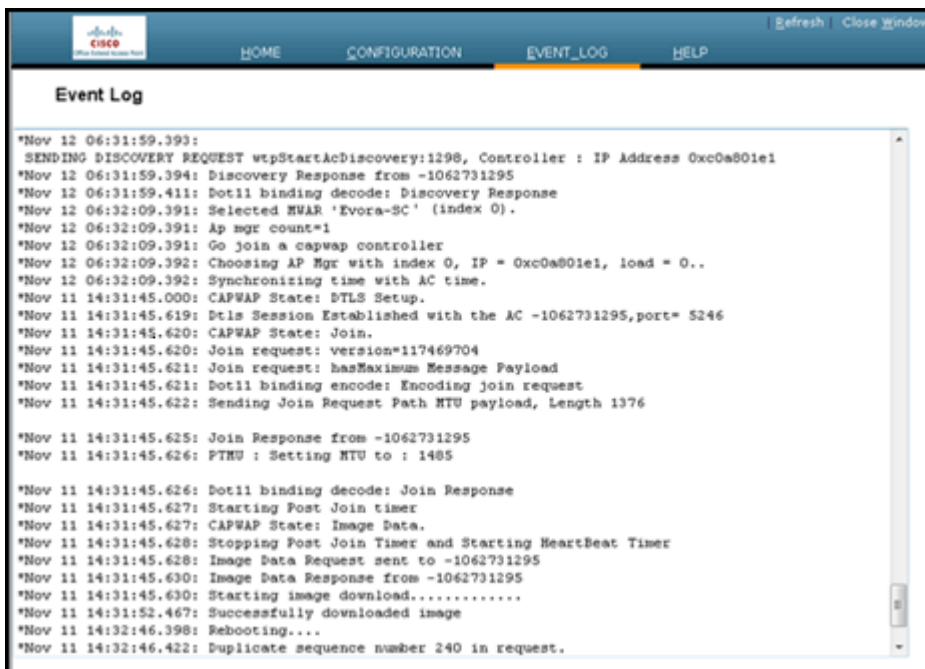


Understanding Cisco Aironet 600 Series OfficeExtend AP LEDs

Status LED	Meaning
Purple	Association status, when CAPWAP is connected: Normal operating condition, but no wireless client associated.
Blue	Association status, when CAPWAP is connected: Normal operating condition, at least one wireless client association.
Flashing blue	Operating Status: Software upgrade in progress.
Flashing orange	Operating Status: No IP address, waiting for DHCP IP.
Cycling through purple, orange and blue	Operating Status: Discovery/join process in progress, no client associated.
Cycling through purple, orange	Operating Status: Discovery/join process in progress, with client associated.
Orange	Cisco IOS errors: Software failure; try disconnecting and reconnecting unit power.

Si el proceso de unión falla, el LED cambia de color o parpadea en naranja. Si esto ocurre, consulte el registro de eventos para obtener más detalles. Para acceder al registro de eventos, navegue hasta el AP (usando SSID personal o puertos cableados 1-3) y capture estos datos para que el administrador de TI los revise.

Esta imagen muestra el registro de eventos OEAP de Cisco Aironet serie 600:



Si el proceso de unión falla y esta es la primera vez que el OEAP Cisco Aironet 600 Series ha intentado conectarse al controlador, verifique las estadísticas de unión de AP para el OEAP Cisco Aironet 600 Series. Para hacer esto, necesita la radio MAC básica del AP. Esto se puede encontrar en el registro de eventos. A continuación se muestra un ejemplo de un registro de eventos con comentarios que le ayudarán a interpretar lo siguiente:

Event log 1

```

WAN port has not obtained IP address,
otherwise it will be shown here.
AP Mac address
Base Radio MAC is 00:22:BD:DA:86:00

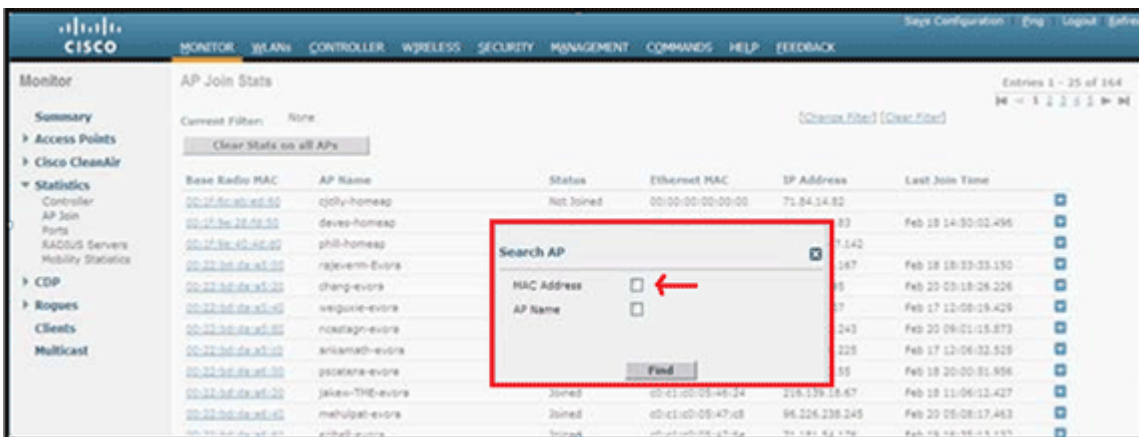
*Jan 01 08:00:05.420: eth0 Linkencap:Ethernet HWaddr C0:C1:C0:05:48:86
*Jan 01 08:00:05.420: UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.420: RX packets:1 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.420: TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.420: collisions:0 txqueuelen:100
*Jan 01 08:00:05.421: RX bytes:64 (64.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.421: Interrupt:4 Base address:0x2000
*Jan 01 08:00:05.421:
*Jan 01 08:00:05.444: eth1 Linkencap:Ethernet HWaddr 00:22:BD:DA:86:07
*Jan 01 08:00:05.444: UP BROADCAST RUNNING ALLMULTI MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.444: RX packets:0 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.444: TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.444: collisions:0 txqueuelen:100
*Jan 01 08:00:05.444: RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.445: Interrupt:3 Base address:0x1000
*Jan 01 08:00:05.445:
*Jan 01 08:00:05.467: Kernel IP routing table
*Jan 01 08:00:05.467: Destination Gateway Genmask Flags Metric Ref Use Iface
*Jan 01 08:00:05.467: 127.0.0.0 * 255.0.0.0 U 0 0 0 lo
*Jan 01 08:00:05.489: IP address HW type Flags HW address Mask Device
*Jan 01 08:00:05.540: ocap_mwar_ipaddr0= Y.Y.Y.Y
*Jan 01 08:00:07.074: Subject: C=US, ST=California, L=San Jose, O=CISCO, OU=WNBU, CN=OEAP602-C0C1C0054886/emailAd
Certificate
Controller IP address configured in local GUI

```

Una vez que se sepa esto, puede consultar las estadísticas del monitor del controlador para determinar si el OEAP Cisco Aironet serie 600 se ha unido al controlador o si alguna vez se ha unido al controlador. Además, esto debe proporcionar una indicación de por qué, o si, se ha producido un fallo.

Si se requiere autenticación de AP, verifique que la dirección MAC de Ethernet OEAP de Cisco Aironet 600 Series (no la dirección MAC de radio) se haya ingresado en el servidor Radius en minúsculas. También puede determinar la dirección MAC de Ethernet a partir del registro de eventos.

Búsqueda del controlador para el OEAP Cisco Aironet serie 600



Si ha determinado que se puede acceder a Internet desde un PC conectado al puerto Ethernet local, pero el AP todavía no puede unirse al controlador, y ha confirmado que la dirección IP del controlador está configurada en la GUI del AP local y es alcanzable, confirme si el AP se ha unido exitosamente alguna vez. Tal vez el AP no está en el servidor AAA. O bien, si falla el protocolo de enlace DTLS, el AP podría tener un certificado incorrecto o un error de fecha/hora en el controlador.

Si ninguna unidad OEAP Cisco Aironet serie 600 puede unirse al controlador, verifique que el controlador esté en la DMZ y que tenga abiertos los puertos UDP 5246 y 5247.

Cómo depurar problemas de asociación de cliente

El AP se une al controlador correctamente, pero el cliente inalámbrico no puede asociarse con el SSID corporativo. Verifique el registro de eventos para ver si un mensaje de asociación llega al AP.

La siguiente figura muestra los eventos normales para la asociación de clientes con SSID corporativo con WPA o WPA2. Para SSID con autenticación abierta o WEP estática, solo hay un evento ADD_MOBILE.

Registro de eventos - Asociación de clientes

```
*Feb 19 20:26:58.876: (Re)Assoc-Req from 00:24:d7:2a:72:c0 forwarded to WLC, wired: no
*Feb 19 20:26:58.941: received assoc-rsp for wireless client, status=0000
*Feb 19 20:26:58.942:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=1
*Feb 19 20:26:58.942: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
*Feb 19 20:27:00.648:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=4
*Feb 19 20:27:00.649: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
```

Si el evento (Re)Assoc-Req no está en el registro, verifique que el cliente tenga la configuración de seguridad correcta.

Si el evento (Re)Assoc-Req aparece en el registro pero el cliente no puede asociarse correctamente, habilite el comando **debug client <dirección MAC>** en el controlador para el cliente e investigue el problema de la misma manera que un cliente que trabaja con otros puntos de acceso Cisco no EAP.

Cómo interpretar el registro de eventos

Los siguientes registros de eventos con comentarios pueden ayudarle a solucionar otros problemas de conexión de Cisco Aironet 600 Series EAP.

Estos son algunos ejemplos recopilados de los archivos de registro de eventos OEAP de Cisco Aironet serie 600 con comentarios para ayudar con la interpretación del registro de eventos:

Event log 2

*Jan 01 08:00:07.093: Build version 7.0.112.66 (compiled Feb 19 2011 at 16:29:58).
 *Jan 01 08:00:08.975: CAPWAP State: Init.
 *Jan 01 08:00:09.009: CAPWAP State: Discovery.
 *Jan 01 08:00:09.042: Starting Discovery.
 *Jan 01 08:00:09.044: CAPWAP State: Discovery.
 *Jan 01 08:00:09.193: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
 *Jan 01 08:00:09.194: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
 *Jan 01 08:00:09.194:
 SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1338, Controller Cisco_7d:88:00: IP Address
 *Jan 01 08:00:09.195: Discovery Request sent to Y.Y.Y.Y with discovery type set to 0
 *Jan 01 08:00:09.256: Discovery Response from Y.Y.Y.Y
 *Jan 01 08:00:09.272: Dot11 binding decode: Discovery Response
 *Jan 01 08:00:09.272: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
 *Jan 01 08:00:09.272: Discovery Response from Y.Y.Y.Y
 *Jan 01 08:00:09.273: Dot11 binding decode: Discovery Response
 *Jan 01 08:00:09.273: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
 *Jan 01 08:00:09.273: Discovery Response from Y.Y.Y.Y
 *Jan 01 08:00:09.274: Dot11 binding decode: Discovery Response
 *Jan 01 08:00:09.274: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
 *Jan 01 08:00:12.133: Dropping dtls packet since session is not established. ab462383, 147e, c0a80121, 147e, 0
 *Jan 01 08:00:19.182: Selected MWAR 'Cisco_7d:88:00'(index 0).
 *Jan 01 08:00:19.183: Selected MWAR 'Cisco_7d:88:00' (index 0).
 *Jan 01 08:00:19.183: Ap mgr count=1
 *Jan 01 08:00:19.183: Go join a capwap controller
 *Jan 01 08:00:19.183: Choosing AP Mgr with index 0, IP = Y.Y.Y.Y , load=151.
 *Jan 01 08:00:19.183: Synchronizing time with AC time.
 *Feb 19 23:33:56.000: CAPWAP State: DTLS Setup.
 *Feb 19 23:34:16.813: Dtls Session Established with the AC Y.Y.Y.Y , port= 5246

Discovery Request sent
 If AP can not get IP address,
 then Discovery Req. will not be sent

Discovery resp. received from
 controller. If no response from
 controller, then need to check
 whether controller
 is accessible

Selected controller to join, timestamp synced to the controller

DTLS handshaking with the controller
 completed. If certificate has problem, then
 the failure will happen here

Event log 3

*Feb 19 23:34:16.813: CAPWAP State: Join.
 *Feb 19 23:34:16.814: Join request: version=7.0.114.76
 *Feb 19 23:34:16.815: Join request: hasMaximum Message Payload
 *Feb 19 23:34:16.815: Dot11 binding encode: Encoding join request
 *Feb 19 23:34:16.815: Sending Join Request Path MTU payload, Length 1376
 *Feb 19 23:34:16.887: Join Response from Y.Y.Y.Y
 *Feb 19 23:34:16.888: PTMU: Setting MTU to: 1485
 *Feb 19 23:34:16.888: Dot11 binding decode: Join Response
 *Feb 19 23:34:16.889: Starting Post Join timer
 *Feb 19 23:34:16.890: CAPWAP State: Image Data.
 *Feb 19 23:34:16.890: Controller Version: 7.0.114.76
 *Feb 19 23:34:16.890: AP Version: 7.0.114.76
 *Feb 19 23:34:16.891: CAPWAP State: Configure.
 *Feb 19 23:34:16.891: Dot11 binding encode: Encoding configuration status request.
 *Feb 19 23:34:16.893: lwapp_encode_ap_reset_button_payload: reset button state off
 *Feb 19 23:34:16.895: Configuration Status sent to Y.Y.Y.Y
 *Feb 19 23:34:17.019: Configuration Status Response from Y.Y.Y.Y
 *Feb 19 23:34:17.022: CAPWAP State: Run.
 *Feb 19 23:34:17.022: Dot11 binding encode: Encoding change state event request.
 *Feb 19 23:34:17.023: CAPWAP State: Run.

Join Resp. from controller
 If AP is not added to AAA server,
 this step will fail.

Controller and AP have same version
 SW, no image download is need. When
 controller is upgraded to new version
 SW, image download will happen.

Capwap configuration completes

Event log 4

*Feb 19 23:34:17.023: CAPWAP moved to RUN state stopping post join timer
 *Feb 19 23:34:17.399: capwapWtpDIForwarding() returned 1
 *Feb 19 23:34:17.602: capwapWtpDIForwarding() returned 1
 *Feb 19 23:34:17.762: Change State Event Response from -1421466749
 *Feb 19 23:34:17.853: SSID alpha,WLAN ID 1, added to the slot[0], enabled
 *Feb 19 23:34:18.045: SSID alpha_phone,WLAN ID 2, added to the slot[0], enabled
 *Feb 19 23:34:18.118: Ethernet Backhaul WLAN ID = 3,qos=0
 *Feb 19 23:34:18.281: SSID alpha,WLAN ID 1, added to the slot[1], enabled
 *Feb 19 23:34:18.522: SSID alpha_phone,WLAN ID 2, added to the slot[1], enabled

WLANs are configured for
 2.4 GHz Radio

Remote-lan is configured

WLANs are configured for
 5 GHz Radio

Cuando la conexión a Internet no es fiable

El ejemplo de registro de eventos de esta sección puede producirse cuando la conexión a Internet falla o termina siendo muy lenta o intermitente. Esto puede deberse a la red del ISP, al módem del ISP o al router doméstico. A veces, la conectividad del ISP cae o se vuelve poco confiable. Cuando esto ocurre, el link CAPWAP (túnel de regreso a corporativo) puede fallar o tener dificultades.

Aquí hay un ejemplo de tal falla en el registro de eventos:

```
*Feb 16 07:13:24.918: Re-Tx Count=0, Max Re-Tx Value=5, NumofPendingMsgs=1
*Feb 16 07:13:36.919: Re-Tx Count=4, Max Re-Tx Value=5, NumofPendingMsgs=2
*Feb 16 07:13:39.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:39.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808), 2}
*Feb 16 07:13:39.919: Retransmission count exceeded max, ignoring as the ethernet is overloaded
*Feb 16 07:13:42.918: Re-Tx Count=6, Max Re-Tx Value=5, NumofPendingMsgs=2
Comment : This Retransmission continues on..... Multiple times..
*Feb 16 07:13:42.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:42.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808)}
*Feb 16 07:14:09.919: GOING BACK TO DISCOVER MODE
*Feb 16 07:14:09.920: CAPWAP State: DTLS Teardown.
*Feb 16 07:14:14.918: DTLS session cleanup completed. Restarting capwap state machine.
*Feb 16 07:14:14.919:
Lost connection to the controller, going to re-start evora...
```

Comandos debug adicionales

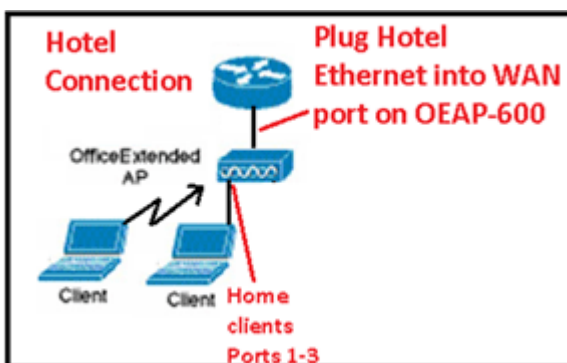
Cuando utilice el OEAP Cisco Aironet serie 600 en un hotel u otro lugar de pago por uso, antes de que el OEAP Cisco Aironet serie 600 pueda tunelizar de nuevo al controlador, debe atravesar el jardín amurallado. Para ello, conecte un ordenador portátil a uno de los puertos locales con cables (puerto 1-3) o utilice un SSID personal para iniciar sesión en el hotel y mostrar la pantalla de bienvenida.

Una vez que tenga conectividad a Internet desde el lado de inicio del AP, la unidad establece un túnel DTLS y sus SSID corporativos. A continuación, el puerto con cable #4 (suponiendo que se haya configurado una LAN remota) se activa.

Nota: Puede tardar unos minutos, observe el LED del logotipo de Cisco en azul o morado para indicar que la unión se ha realizado correctamente. En este momento, tanto la conectividad personal como la corporativa están activas.

Nota: El túnel se rompe cuando el hotel u otro ISP se desconecta (normalmente 24 horas). Entonces, usted tiene que comenzar el mismo proceso de nuevo. Esto es por diseño y es normal.

Esta imagen muestra Office Extend en la configuración de pago por uso:



Esta imagen muestra comandos debug adicionales (información de interfaz de radio):

Below are the new diagnostics commands for the OEAP 600

The WLC CLI of "show tech" is:

```
debug ap enable <apname>
```

then:

```
debug ap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
```

```
debug ap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
```

```
debug ap command "evoraTechSupport 3" <apname> → more info about radio slot 1 (5G)
```

The "show eventlog" is the same as other APs:

```
show ap eventlog <apname>
```

Problemas conocidos/Advertencias

Cuando carga el archivo de configuración desde un controlador a un servidor TFTP/FTP, las configuraciones de LAN remota se cargan como configuraciones WLAN. Consulte [Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.0.116.0](#) para obtener más información.

En el OEAP-600, si la conexión CAPWAP falla debido a una falla de autenticación en el controlador, el LED del logotipo de Cisco en el OEAP-600 puede apagarse por algún tiempo antes de que el OEAP-600 intente reiniciar el intento CAPWAP. Esto es normal, por lo que debe tener en cuenta que el AP no murió si el LED del logotipo se apaga momentáneamente.

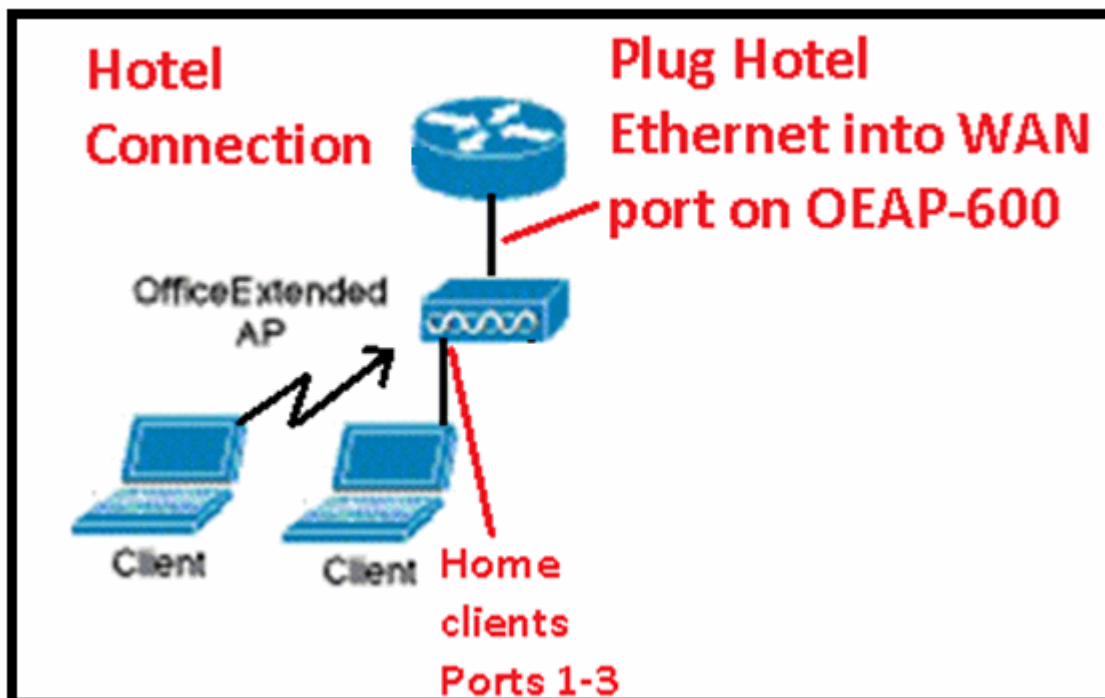
Este producto EAP-600 tiene un nombre de inicio de sesión diferente al de los puntos de acceso OEAP anteriores. Para ser coherente con productos domésticos como Linksys, el nombre de usuario predeterminado es *admin* con una contraseña de *admin*; los demás puntos de acceso OEAP de Cisco, como AP-1130 y AP-1140, tienen un nombre de usuario predeterminado de *Cisco* con una contraseña de *Cisco*.

Esta primera versión del OEAP-600 es compatible con 802.1x, pero solo lo es con la CLI. Los usuarios que intentan realizar cambios en la GUI pueden perder sus configuraciones.

Cuando utiliza el OEAP-600 en un hotel u otro lugar de pago por uso, antes de que el OEAP-600 pueda tunelizar de nuevo al controlador, debe atravesar el jardín amurallado. Basta con conectar un ordenador portátil en uno de los puertos locales con cables (puerto 1-3) o utilizar un registro SSID personal en el hotel y mostrar la pantalla de bienvenida. Una vez que tiene conectividad a Internet desde el lado de inicio del AP, la unidad establece un túnel DTLS y sus SSID corporativos y el puerto cableado #4, que se supone que se configura Remote-LAN, luego se activa. Tenga en cuenta que esta operación puede tardar unos minutos. Observe el LED del logotipo de Cisco en azul fijo o morado para indicar que la unión se ha realizado correctamente. En este momento, tanto la conectividad personal como la corporativa están activas.

Nota: El túnel puede romperse cuando el hotel u otro ISP se desconecta (generalmente 24 horas) y usted tendría que reiniciar el mismo proceso. Esto es por diseño y es normal.

Office Extend en un lugar de pago por uso

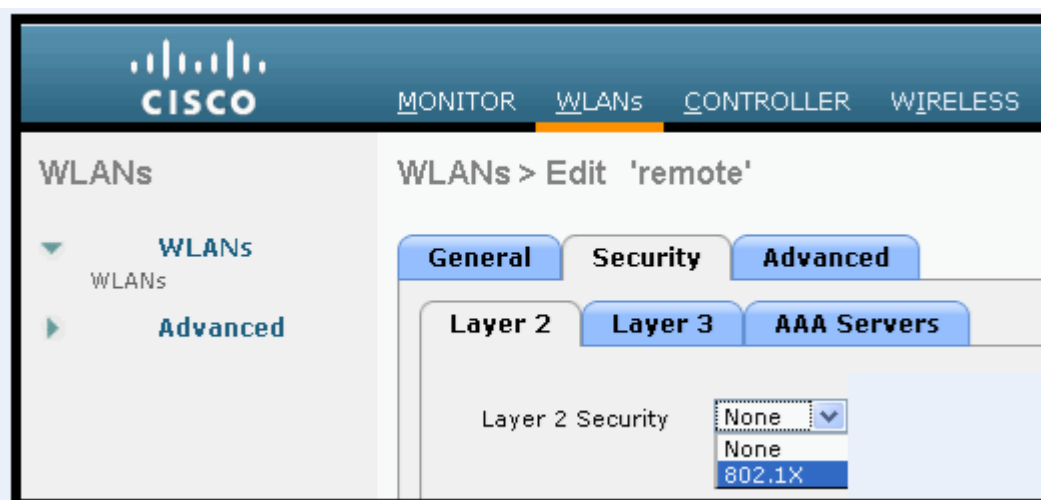


Estas son algunas mejoras adicionales introducidas en la versión 7.2 de Cisco:

- Incorporación de la seguridad 802.1x en la GUI
- Capacidad para inhabilitar el acceso WLAN local en el AP del controlador - inhabilitación de SSID personal que permite solamente la configuración corporativa
- Opciones seleccionables de asignación de canal
- Se ha cambiado la compatibilidad de 2 SSID corporativos a 3 SSID
- Compatibilidad con la función de puerto Dual RLAN

Incorporación de la seguridad 802.1x en la GUI

802.1x ahora añadido a la GUI



Notas sobre la autenticación para el puerto LAN remoto.

802.1x authentication for remote-LAN port

WCS shall be provided to enable 802.1x Layer 2 Security and configure AAA server for remote-LAN. WEP encryption shall be always disabled.

Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall be set to BSSID for remote-LAN. There is no data encryption for the Ethernet packets transferred on remote-LAN port. So there is no key exchange on EAPOL. The data security is provided by DTLS on CAPWAP data channel.

Following EAP methods are supported:

- EAP-TLS
- PEAP
- EAP-TTLS.

Capacidad para inhabilitar el acceso WLAN local en el AP del controlador - inhabilitación de SSID personal que permite solamente la configuración corporativa

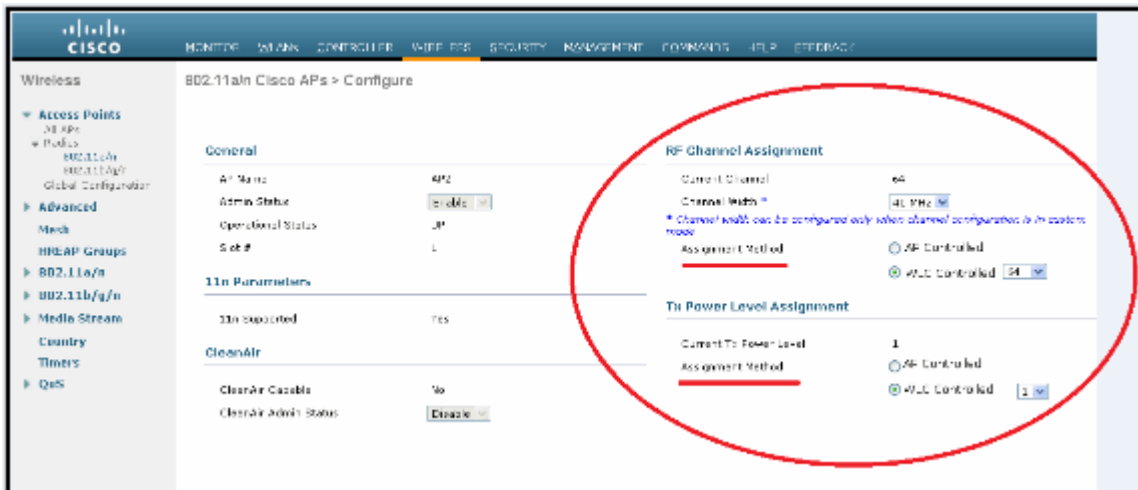
Desactivar el acceso WLAN local

The screenshot shows the Cisco WCS configuration page for Global Configuration. The left sidebar contains a navigation tree with options like 'Advanced', 'Media', 'RF Profiles', 'FlexConnect Groups', '802.11e/n', '802.11b/g/n', 'Media Stream', 'Country', and 'Timers'. The main content area is divided into several sections: 'RDP' (with 'RDP State' checked), 'Ethernet Interface' (with 'EAP State' checked for interfaces 1-3), 'Radio State' (with 'EAP State' checked for radios 1-3), 'Login Credentials', '802.1x Supplicant Credentials', 'AP Fallback Priority', 'High Availability' (with various timer and state settings), 'TCP MSS', 'AP Retransmit Config Parameters', and 'GEAP Config Parameters'. The 'GEAP Config Parameters' section is circled in red and contains a checkbox for 'Disable local access' which is currently unchecked.

Las opciones de asignación de canal seleccionables son:

- AP controlado localmente
- WLC controlado

Asignaciones de potencia y canal de RF ahora locales o controladas por WLC



Manually configure channel and power level

In JMR1 release, there is no configuration option for 802.11a/n and 802.11b/g/n radios for the OEAP-600 AP. In 7.2 release, the configuration window is added back with only “General”, “RF Channel Assignment” and “Tx Power Level Assignment” portions. The “Admin Status” in “General” shall be display only. The options for “Assign Method” are changed to “Custom Configured” and “AP Controlled”. By default “AP Controlled” is selected. Channel and Tx power level can be configured only when they are in “Custom Configured” mode.

OEAP-600 does not support DFS channels so that WLC shall not allow these channels to be configured. [This new assignment method is passed to AP with CAPWAP payload.

In AP, when the channel is “AP Controlled”, then the channel is controlled by the setting from local AP GUI. Otherwise the channel set by WCS is used.

The channel assign method and the assigned channel are saved in NVRAM and displayed in local GUI.

In AP, when the power is “AP controlled”, then the maximum power level is always used. Otherwise the power level set by WCS is used.

The assign method for TX power level and assigned TX power level shall be saved in flash so that they can take effect after AP reboots.

When “Reset to Default” operation is performed, the assign method is set to “AP controlled”.

Compatibilidad con la función de puerto Dual RLAN (sólo CLI)

Esta nota se aplica a los AP de la serie OEAP-600 que utilizan la función Dual RLAN Ports, que permite que el puerto Ethernet OEAP-600 3 funcione como una LAN remota. La configuración solo se permite a través de la CLI, y aquí hay un ejemplo:

```
Config network oep-600 dual-rlan-ports enable|disable
```

En el caso de que esta función no esté configurada, el único puerto 4 remote-lan continúa funcionando. Cada puerto utiliza una única LAN remota para cada puerto. La asignación de LAN remota es diferente, lo que depende de si se utiliza el grupo predeterminado o los grupos de AP.

Default-group

Si se utiliza el grupo predeterminado, se asigna una sola LAN remota con un ID de LAN remota uniforme al puerto 4. Por ejemplo, la lan remota con ID de LAN remota 2 se asigna al puerto 4 (en el OEAP-600). La LAN remota con un ID de LAN remota numerado impar se asigna al puerto 3 (en el OEAP-600).

Como ejemplo, tome estos dos LAN remotos:

```
(Cisco Controller) >show remote-lan summary
```

```
Number of Remote LANS..... 2
```

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

rlan2 tiene un ID de lan remota con numeración par, 2, y como tal se asigna al puerto 4. rlan3 tiene un ID de lan remota impar 3, y por lo tanto se asigna al puerto 3.

Grupos de AP

Si utiliza un grupo de AP, la asignación a los puertos EAP-600 se determina según el orden de los grupos de AP. Para utilizar un grupo AP, primero debe eliminar todos los LAN y WLAN remotos del grupo AP y dejarlo vacío. A continuación, agregue los dos planes remotos al grupo AP. Primero agregue el puerto 3 AP remote-LAN primero, luego agregue el puerto 4 remote group y finalmente agregue cualquier WLAN.

Una lan remota en la primera posición de la lista se asigna al puerto 3, y la segunda en la lista se asigna al puerto 4, como en este ejemplo:

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

Información Relacionada

- [Guía de configuración de controlador de LAN inalámbrica de Cisco, versión 7.0](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).