

Detección de punto de acceso no deseado (AP) en WAP561 y WAP551

Objetivo

Un punto de acceso no autorizado (AP) es un punto de acceso que se instala en una red segura sin el consentimiento del administrador de la red. Los puntos de acceso no autorizados pueden suponer una amenaza para la seguridad, ya que cualquiera que instale un router inalámbrico dentro del alcance de su red puede potencialmente obtener acceso a su red. La página *Rogue AP Detection* proporciona información sobre las redes inalámbricas que están dentro del alcance del suyo. En este artículo se explica cómo detectar AP rogue y crear una lista AP de confianza.

Nota: La página *Rogue AP Detection* no tiene funciones de seguridad. La lista de confianza de AP es para su propio uso y no es más segura que un AP no confiable.

Dispositivos aplicables

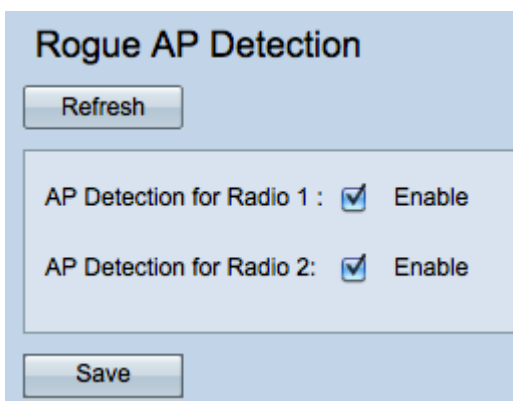
- WAP551
- WAP561

Versión del software

- 1.0.4.2

Configuración de detección de puntos de acceso no autorizados

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Wireless > Rogue AP Detection**. Se abre la página *Detección de puntos de acceso no autorizados*:



Rogue AP Detection

Refresh

AP Detection for Radio 1 : Enable

AP Detection for Radio 2: Enable

Save

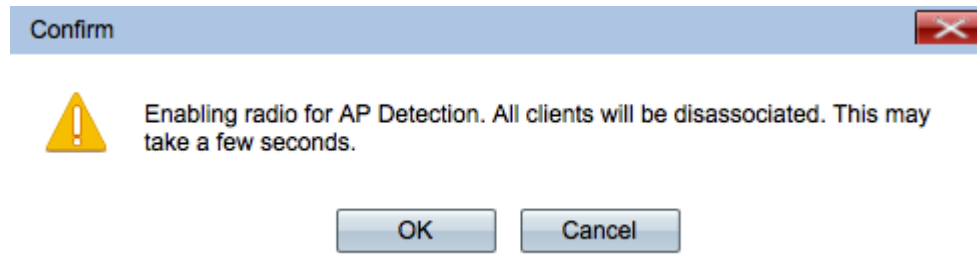
Ver estadísticas de puntos de acceso no autorizados

Paso 1. Marque **Enable** para habilitar la Detección de AP para la radio deseada para mostrar las estadísticas de AP rogue.

Nota: El WAP561 tiene dos radios que puede habilitar mientras que el WAP551 sólo tiene

una radio para habilitar.

Paso 2. Haga clic en **Guardar** después de habilitar la detección de AP para mostrar la lista de puntos de acceso sospechosos detectados. Aparecerá una ventana de confirmación.



Paso 3. Haga clic en **Aceptar** para continuar.

Nota: Los clientes inalámbricos de la red perderán su conexión momentáneamente.

Detected Rogue AP List							
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
<input type="button" value="Trust"/>	08:00:20:08:00:20	wlan0	102	AP	WiFi-Rogue-1	On	On
<input type="button" value="Trust"/>	08:00:20:08:00:20	wlan0	102	AP	WiFi-Rogue-2	Off	Off
<input type="button" value="Trust"/>	08:00:20:08:00:20	wlan0	100	AP	WiFi-Rogue-3	On	Off
<input type="button" value="Trust"/>	08:00:20:08:00:20	wlan0	102	AP	WiFi-Rogue-4	On	On

Se muestra la siguiente información para los puntos de acceso detectados:

Dirección MAC : la dirección MAC del AP no autorizado.

Radio : la radio física en el AP rogue al que puede unirse.

·Beacon Interval: Intervalo de baliza que utiliza el AP rogue. Cada AP envía tramas de baliza a intervalos regulares para anunciar la existencia de su red inalámbrica.

Tipo de : el tipo del dispositivo detectado. Puede ser AP o ad hoc.

·SSID: el identificador del conjunto de servicios (SSID) del punto de acceso no autorizado, también conocido como nombre de red.

Privacidad : indica si la seguridad está o no habilitada en el AP rogue. Off indica que el AP rogue no tiene la seguridad habilitada mientras On indica que el AP rogue tiene las medidas de seguridad habilitadas.

·WPA: indica si la seguridad WPA está habilitada para el AP no autorizado.

Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
2.4	1	1		5	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11,12,18,24,36,48,54
2.4	1	1		4	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11,12,18,24,36,48,54
2.4	1	1		1	Wed Dec 31 16:00:23 1969	1,2,5,5,6,9,11,12,18,24,36,48,54
2.4	1	1		4	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11,12,18,24,36,48,54

Banda :: el modo IEEE 802.11 que se utiliza en el AP rogue.

- 2.4: el modo IEEE 802.11b, 802.11g o 802.11n (o una combinación) está en uso.
- 5: el modo IEEE 802.11a o 802.11n (o ambos) está en uso.

Canal :: el canal (parte del espectro de radio) en el que el AP no autorizado emite.

Velocidad de :: la velocidad en megabytes por segundo a la que el AP no autorizado transmite actualmente.

Señal :: la potencia de la señal de radio emitida desde el punto de acceso no autorizado. Para ver la fuerza de la señal en decibelios, pase el ratón sobre las barras.

·Beacons: número total de balizas recibidas del AP rogue desde que se detectó por primera vez.

·Last Beacon: la fecha y hora en que se recibió la última baliza del AP rogue.

Tasas de :: los conjuntos de velocidad soportados y básicos para el AP detectado (en megabits por segundo).

Crear lista de puntos de acceso de confianza

Nota: La Detección de AP no autorizado debe estar habilitada para crear una lista AP confiable. Complete la sección titulada *Ver estadísticas de AP rogue* si aún no lo ha hecho.

Detected Rogue AP List							
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
<input type="button" value="Trust"/>	08:00:27:00:00:00	wlan0	102	AP	WiFi-Trust	On	On
<input type="button" value="Trust"/>	08:00:27:00:00:00	wlan0	102	AP	WiFi-Trust	Off	Off
<input type="button" value="Trust"/>	08:00:27:00:00:00	wlan0	100	AP	WiFi-Trust	On	Off
<input type="button" value="Trust"/>	08:00:27:00:00:00	wlan0	102	AP	WiFi-Trust	On	On

Paso 1. Haga clic en **Trust** junto a una entrada AP para agregarla a la lista AP de confianza.

Trusted AP List								
Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel	
<input type="button" value="Untrust"/>	XXXXXXXXXX	wlan0	AP	XXXXXXXXXX	On	2.4	1	

Download/Backup Trusted AP List

Save Action: Download (PC to AP)
 Backup (AP to PC)

Paso 2. (Opcional) Para quitar una entrada AP de la lista AP de confianza, haga clic en **Untrust**.

Paso 3. Haga clic en el botón de opción **Copia de seguridad (AP a PC)** en el campo Guardar acción para guardar la lista AP de confianza en un archivo.

Paso 4. Haga clic en **Guardar** para guardar la lista AP de confianza. WAP crea un archivo .cfg que contiene una lista de todas las direcciones MAC en la lista AP de confianza.

Importar una lista de puntos de acceso de confianza

Nota: La Detección de AP no autorizado debe estar habilitada para crear una lista AP confiable. Complete la sección titulada *Ver estadísticas de AP rogue* si aún no lo ha hecho.

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Wireless > Rogue AP Detection**. Se abre la página *Detección de puntos de acceso no autorizados*:

Detected Rogue AP List							
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
<input type="button" value="Trust"/>	XXXXXXXXXX	wlan0	102	AP	XXXXXXXXXX	On	On
<input type="button" value="Trust"/>	XXXXXXXXXX	wlan0	102	AP	XXXXXXXXXX	Off	Off
<input type="button" value="Trust"/>	XXXXXXXXXX	wlan0	100	AP	XXXXXXXXXX	On	Off
<input type="button" value="Trust"/>	XXXXXXXXXX	wlan0	102	AP	XXXXXXXXXX	On	On

Download/Backup Trusted AP List

Save Action: Download (PC to AP)
 Backup (AP to PC)

Source File Name: No file chosen

File Management Destination: Replace
 Merge

Paso 2. Desplácese hacia abajo hasta el área Download/Backup Trusted AP List y haga clic en el botón de opción **Download (PC to AP)** para importar una lista de AP conocidos de una lista guardada.

Paso 3. Haga clic en **Examinar** en el campo Nombre de archivo de origen y elija su archivo. El archivo que importa debe tener una extensión .txt o .cfg. El archivo debe ser una lista de direcciones MAC en formato hexadecimal.

Paso 4. En el campo File Management Destination , haga clic en **Replace** para sobrescribir la lista AP de confianza o haga clic en **Merge** para agregar a la lista AP de confianza.

Paso 5. Haga clic en **Guardar** para importar el archivo.

Nota: Los AP definidos en el archivo que carga se mueven de la Lista de AP detectados a la Lista de AP de confianza.