

Detección de puntos de acceso (AP) desconocidos en los puntos de acceso WAP121 y WAP321

Objetivo

Un punto de acceso (AP) no autorizado es un punto de acceso que se ha instalado en una red sin autorización explícita del administrador del sistema. Los puntos de acceso no autorizados suponen una amenaza para la seguridad, ya que cualquier persona con acceso a la zona puede instalar, consciente o inconscientemente, un punto de acceso inalámbrico que permita el acceso a la red a usuarios no autorizados. La página Rogue AP Detection muestra información sobre estos puntos de acceso. Puede agregar cualquier punto de acceso autorizado a la lista de puntos de acceso de confianza. En este artículo se explica cómo detectar un punto de acceso (AP) no autorizado en los puntos de acceso WAP121 y WAP321

Dispositivos aplicables

- WAP121
- WAP321

Versión del software

- 1.0.3.4

Configuración de Detección de AP Rogue

Paso 1. Inicie sesión en la Utilidad de configuración del punto de acceso y elija Wireless > Rogue AP Detection. Se abre la página Rogue AP Detection:

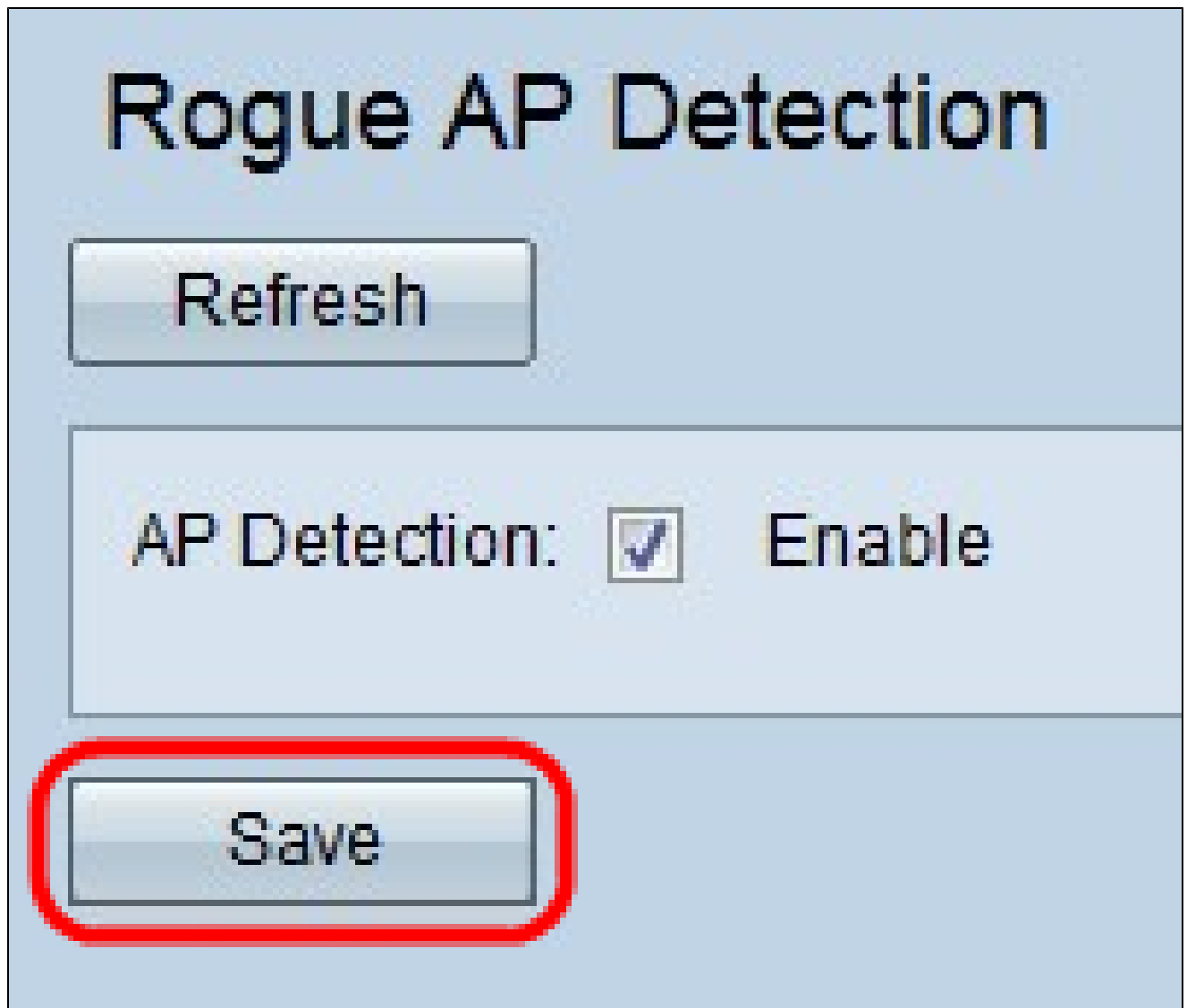
Rogue AP Detection

Refresh

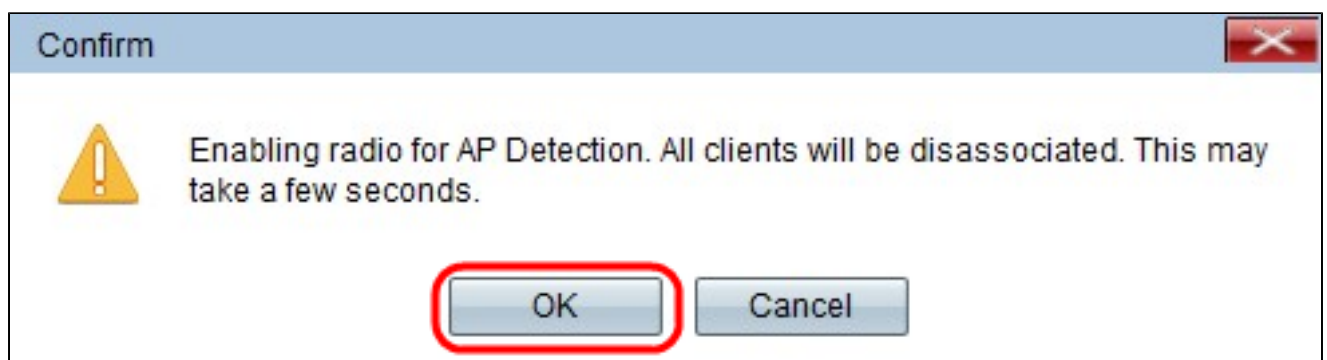
AP Detection: Enable

Save

Paso 2. Marque Enable para habilitar la detección de AP.



Paso 3. Haga clic en Guardar después de habilitar la detección AP para mostrar la lista de puntos de acceso rogue detectados. Aparecerá una pantalla de advertencia.



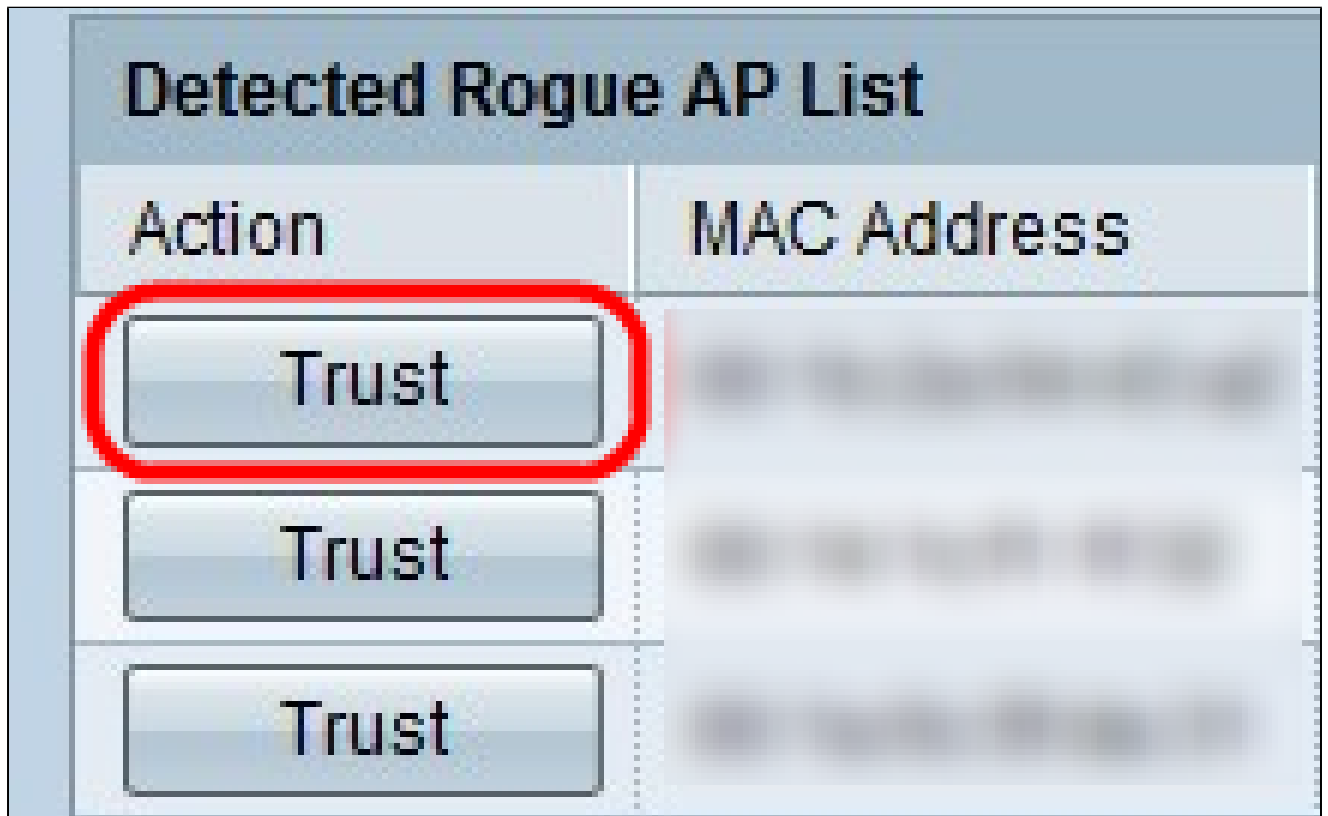
Paso 4. Haga clic en Aceptar para continuar. La lista Detected Rogue AP se muestra como se muestra a continuación.

Detected Rogue AP List													
Action	MAC Address	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Trust	08:00:27:00:00:00	102	AP	WiFi-Island	Off	Off	2.4	1	1		5	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Island	Off	Off	2.4	1	1		3	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	100	AP	(Non Broadcasting)	On	Off	2.4	1	1		5	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	100	AP	(Non Broadcasting)	On	Off	2.4	1	1		3	Fri Dec 31 12:00:02 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Island	On	On	2.4	1	1		6	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Island	Off	Off	2.4	1	1		5	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11
Trust	08:00:27:00:00:00	102	AP	WiFi-Island	Off	Off	2.4	1	1		4	Fri Dec 31 12:00:04 1999	1,2,5,5,6,9,11

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

- Dirección MAC: la dirección MAC del AP detectado.
- Intervalo de baliza (milisegundos): el intervalo de baliza que utiliza el AP detectado. Las tramas de baliza son transmitidas por un AP a intervalos regulares para anunciar la existencia de la red inalámbrica. El tiempo predeterminado para enviar una trama de baliza es una vez cada 100 milisegundos.
- Tipo: el tipo de dispositivo detectado. Puede ser AP o Ad hoc.
- SSID: SSID del AP detectado.
- Privacidad: indica si hay alguna seguridad en el AP vecino.
- WPA: indica si la seguridad WPA está desactivada o activada para el punto de acceso detectado.
- Banda: indica el modo IEEE 802.11 que se utiliza en el AP detectado. Puede ser 2.4 o 5.
- Canal: el canal en el que el AP detectado transmite actualmente.
- Velocidad: la velocidad a la que el AP detectado transmite actualmente.
- Signal: Potencia de la señal de radio que emite el AP detectado.
- Balizas: el número total de balizas recibidas desde el AP desde que se detectaron por primera vez.
- Última Baliza: La fecha y hora de la última baliza recibida desde el AP detectado.

· Tasas: los conjuntos de velocidades básica y admitida para el AP detectado (en megabits por segundo).



Paso 5. Haga clic en Confianza junto a una entrada para agregarla a la tabla Lista de AP de confianza. Puede obtener la lista de confianza descargándola y puede guardar la lista actual en su PC. Para descargar/realizar una copia de seguridad, vaya a [Descargar/ realizar una copia de seguridad de la lista de puntos de acceso de confianza](#).

Trusted AP List							
Action	MAC Address	Type	SSID	Privacy	Band	Channel	
<input type="button" value="Untrust"/>	00:00:00:00:00:00	AP	00:00:00:00:00:00	Off	2.4	4	

Paso 6. (Opcional) Si desea eliminar la lista de puntos de acceso de confianza, haga clic en Desconfiar.

Descargar/ Copia de seguridad de la lista de puntos de acceso fiables

Download/Backup Trusted AP List

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

Source File Name: No file selected.

File Management Destination: Replace
 Merge

Paso 1. Elija si desea descargar la lista actual de puntos de acceso de confianza desde PC o guardar la lista actual en PC desde la acción Guardar.

- Descargar (PC a AP): si desea importar la lista de un archivo y reemplazar el contenido de la lista de AP conocida, vaya a [Descargar \(PC a AP\)](#).
- Copia de seguridad (AP a PC): Si desea guardar la lista actual en el PC, vaya a [Copia de seguridad \(AP a PC\)](#).

Descarga (PC a AP)

Download/Backup Trusted AP List

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

Source File Name: Example_test.txt

File Management Destination: Replace
 Merge

Paso 1. Haga clic en el botón de opción Download (PC to AP) para descargar la lista desde el PC.

Paso 2. Haga clic en Browse para localizar el archivo en el PC. El archivo de importación debe ser un archivo de texto sin formato con la extensión .txt o .cfg. Las entradas del archivo de importación son direcciones MAC en formato hexadecimal con cada octeto separado por dos puntos. Las entradas deben separarse con un solo espacio. El archivo debe contener solamente direcciones MAC y luego AP acepta el archivo.

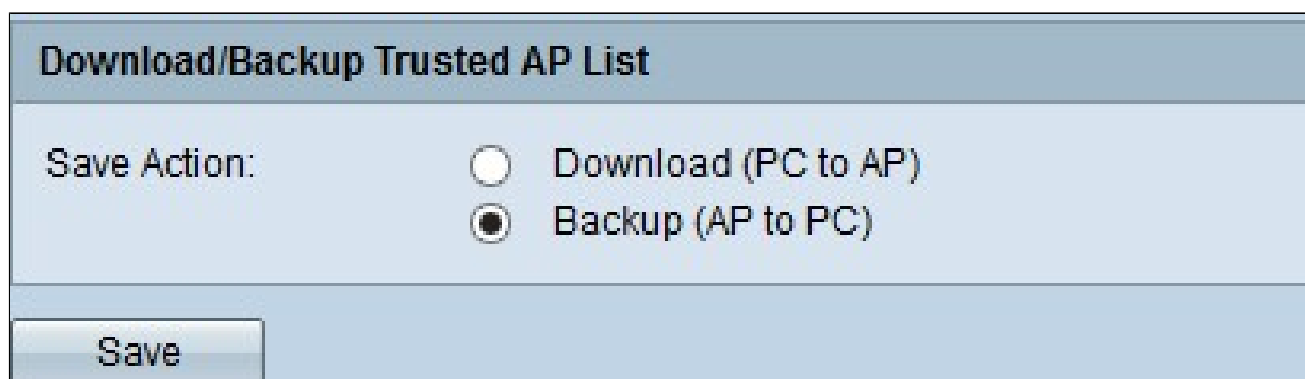
Paso 3. Seleccione File Management Destination para sustituir o agregar el contenido a la lista de puntos de acceso de confianza.

- Reemplazar: para importar la lista y reemplazar el contenido de la lista de puntos de acceso de confianza
- Fusionar: para importar y agregar los AP del archivo importado a la lista de AP de confianza.

Nota: Una vez completada la importación, la pantalla se actualiza y las direcciones MAC de los AP en el archivo importado aparecen en la Lista de AP conocidos.

Paso 4. Haga clic en Guardar para guardar todos los cambios realizados.

Copia de seguridad (AP a PC)



Download/Backup Trusted AP List

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

Save

Paso 1. Haga clic en el botón de opción Backup (AP to PC) para guardar la lista en su PC.

Paso 2. Haga clic en Guardar para guardar los cambios realizados y, a continuación, aparecerá una ventana de notificación como se muestra a continuación que proporciona información del archivo.

Opening Rogue2.cfg



You have chosen to open:



Rogue2.cfg

which is: Text Document

from: <http://192.168.1.245>

What should Firefox do with this file?

Open with Notepad (default) ▼

Save File

Do this automatically for files like this from now on.

OK

Cancel

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).