

# Détection du point d'accès non autorisé (AP) sur WAP561 et WAP551

## Objectif

Un point d'accès non autorisé (AP) est un Point d'accès qui est installé sur un réseau sécurisé sans consentement de l'administrateur réseau. Les aps escrocs peuvent constituer une menace de Sécurité parce que n'importe qui qui installent un routeur Sans fil dans la marge de votre réseau peut potentiellement accéder à votre réseau. La page de *détection de l'escroc AP* fournit des informations au sujet des réseaux Sans fil qui sont dans la marge à vous. Cet article explique comment détecter des aps escrocs et créer une liste de confiance AP.

**Remarque:** La page de *détection de l'escroc AP* n'a aucune fonctionnalité de sécurité. La liste de confiance par AP est pour votre propre utiliser-et n'est pas plus sécurisé qu'AP non approuvé.

## Périphériques applicables

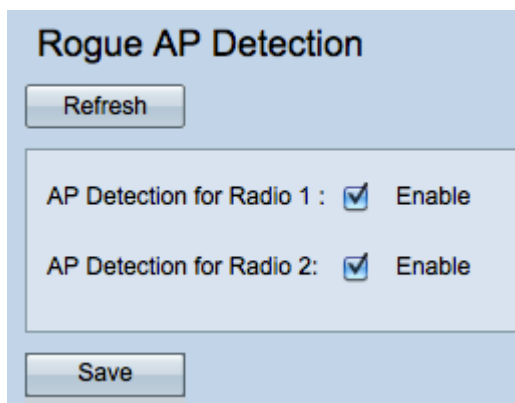
- WAP551
- WAP561

## Version de logiciel

- 1.0.4.2

## Configuration escroc de détection AP

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **détection de radio > d'escroc AP**. La page de *détection de l'escroc AP* s'ouvre :



Rogue AP Detection

Refresh

AP Detection for Radio 1 :  Enable

AP Detection for Radio 2:  Enable

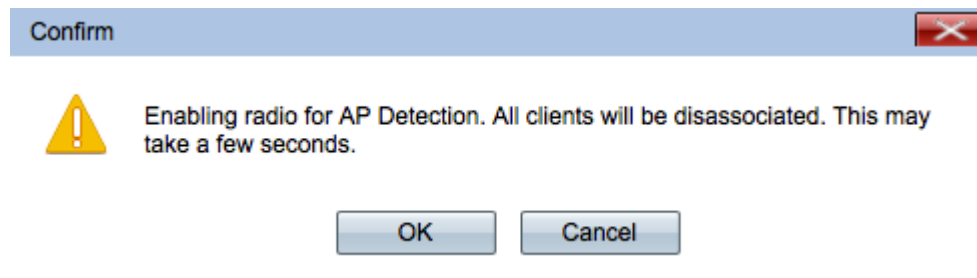
Save

## Statistiques escrocs de la vue AP

Étape 1. Vérifiez l'**enable** pour permettre à la détection AP pour que la radio désirée affiche les statistiques de l'escroc AP.

**Remarque:** Le WAP561 a deux radios que vous pouvez activer tandis que le WAP551 a seulement une radio à activer.

Étape 2. **Sauvegarde de clic** après que vous permettiez à la détection AP d'afficher la liste de points d'accès non autorisé détectés. Une fenêtre de confirmation apparaîtra.



Étape 3. Cliquez sur OK pour poursuivre.

**Remarque:** Les clients sans fil sur votre réseau perdront leur connexion momentanément.

Les informations suivantes pour les Points d'accès détectés sont affichées :

- Adresse MAC — L'adresse MAC de l'escroc AP.
- Radio — La radio physique sur l'escroc AP que vous pouvez joindre.
- Intervalle de balise — L'intervalle de balise qui est utilisé par l'escroc AP. Chaque AP envoie des trames balise à intervalles réguliers pour annoncer l'existence de leur réseau Sans fil.
- Type — Le type du périphérique détecté. Peut être AP ou ad hoc.
- SSID — L'Identifiant SSID (Service Set Identifier) de l'escroc AP, également connu sous le nom de nom de réseau.
- Intimité — Indique si la Sécurité est activée sur l'escroc AP. Outre de indiquer que l'escroc AP n'a aucune sécurité activée tandis qu'indique en fonction que l'escroc AP fait activer des mesures de sécurité.
- WPA — Indique si la sécurité WPA est activée pour l'escroc AP.



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

- Bande — Le mode d'IEEE 802.11 qui est utilisé sur l'escroc AP.
  - 2.4 — L'IEEE 802.11b, le mode 802.11g, ou 802.11n (ou une combinaison) est en service.
  - 5 — Le mode 802.11a ou 802.11n d'IEEE (ou chacun des deux) est en service.
- La Manche — Le canal (une partie du spectre radio) que l'escroc AP annonce en fonction.
- Débit — Le débit dans les mégaoctets par seconde à l'où l'escroc AP transmet actuellement.
- Signal — Le point fort du signal radio émis de l'escroc AP. Pour voir le point fort du signal dans les décibels, passer au-dessus votre souris au-dessus des barres.
- Balises — Nombre total de balises reçues de l'escroc AP puisqu'il a été détecté la première fois.
- Dernière balise — La date et l'heure que la dernière balise a été reçue de l'escroc AP.
- Débits — Pris en charge et le débit de base place pour AP détecté (dans les mégabits par seconde).

## Créez a fait confiance à la liste AP

**Remarque:** La détection escroc AP doit être activée créer une liste de confiance AP. Remplissez la section intitulée des *statistiques de l'escroc AP de vue* si vous n'avez pas déjà fait ainsi.

Étape 1. **Confiance de clic** à côté d'une entrée AP pour l'ajouter à la liste de confiance AP.

Trusted AP List								
Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel	
<input type="button" value="Untrust"/>		wlan0	AP		On	2.4	1	
Download/Backup Trusted AP List								
Save Action:								
<input type="radio"/> Download (PC to AP) <input checked="" type="radio"/> Backup (AP to PC)								
<input type="button" value="Save"/>								

Étape 2. (facultative) pour retirer une entrée AP de la liste de confiance AP, clic **Untrust**.

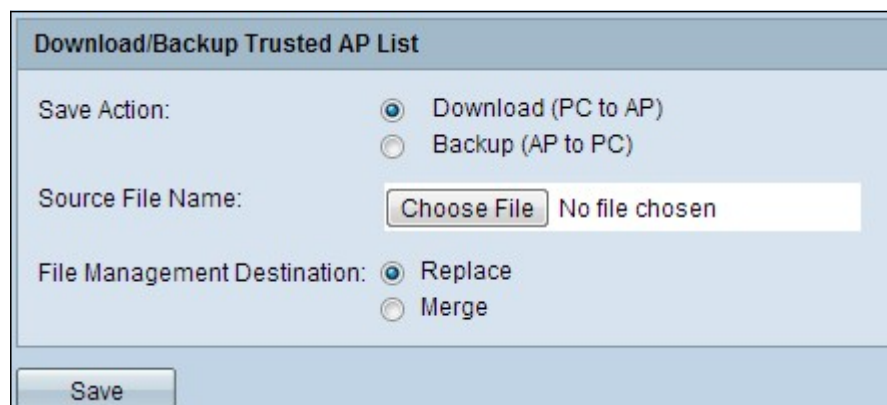
Étape 3. Cliquez sur **(AP au PC)** la case d'option de **sauvegarde** dans le champ action de sauvegarde pour sauvegarder la liste de confiance AP à un fichier.

Étape 4. **Sauvegarde de** clic pour sauvegarder la liste de confiance AP. Le WAP crée un fichier .cfg qui contient une liste de toutes les adresses MAC dans la liste de confiance AP.

## Importez une liste de confiance AP

**Remarque:** La détection escroc AP doit être activée créer une liste de confiance AP. Remplissez la section intitulée des *statistiques de l'escroc AP de vue* si vous n'avez pas déjà fait ainsi.

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **détection de radio > d'escroc AP**. La page de *détection de l'escroc AP* s'ouvre :



The screenshot shows a web-based configuration window titled "Download/Backup Trusted AP List". It contains the following elements:

- Save Action:** Two radio buttons. The first, "Download (PC to AP)", is selected. The second, "Backup (AP to PC)", is unselected.
- Source File Name:** A text input field with a "Choose File" button to its left. The text inside the field is "No file chosen".
- File Management Destination:** Two radio buttons. The first, "Replace", is selected. The second, "Merge", is unselected.
- Save:** A button located at the bottom left of the window.

Étape 2. Faites descendre l'écran au téléchargement/à sauvegarde a fait confiance à la région de liste AP et clique sur la case d'option du **téléchargement (PC à AP)** pour importer une liste d'aps connus d'une liste enregistrée.

Étape 3. Cliquez sur **parcourent** dans le domaine de nom du fichier de source et choisissent votre fichier. Le fichier que vous importez doit avoir une extension de .txt ou .cfg. Le fichier devrait être une liste d'adresses MAC dans le format hexadécimal.

Étape 4. Dans le champ de destination de gestion de fichiers, le clic **remplacent** pour remplacer la liste AP ou la **fusion** de confiance de clic pour ajouter à la liste de confiance AP.

Étape 5. **Sauvegarde de** clic pour importer le fichier.

**Remarque:** Les aps qui sont définis dans le fichier vous les téléchargent sont déplacés de la liste détectée AP à la liste de confiance AP.