

Détection des points d'accès indésirables sur WAP561 et WAP551

Objectif

Un point d'accès non autorisé est un point d'accès installé sur un réseau sécurisé sans le consentement de l'administrateur réseau. Les points d'accès non autorisés peuvent constituer une menace pour la sécurité car toute personne qui installe un routeur sans fil à portée de votre réseau peut potentiellement accéder à votre réseau. La page *Rogue AP Detection* fournit des informations sur les réseaux sans fil qui sont à portée de la vôtre. Cet article explique comment détecter les points d'accès indésirables et créer une liste de points d'accès approuvés.

Note: La page *Détection des points d'accès indésirables* ne comporte aucune fonctionnalité de sécurité. La liste de confiance AP est destinée à votre propre usage et n'est pas plus sécurisée qu'un AP non approuvé.

Périphériques pertinents

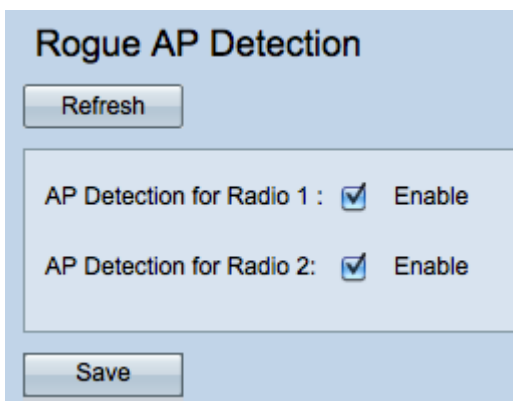
- WAP551
- WAP561

Version du logiciel

- 1.0.4.2

Configuration de la détection des points d'accès indésirables

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Wireless > Rogue AP Detection**. La page *Détection des points d'accès indésirables* s'ouvre :



Rogue AP Detection

Refresh

AP Detection for Radio 1 : Enable

AP Detection for Radio 2: Enable

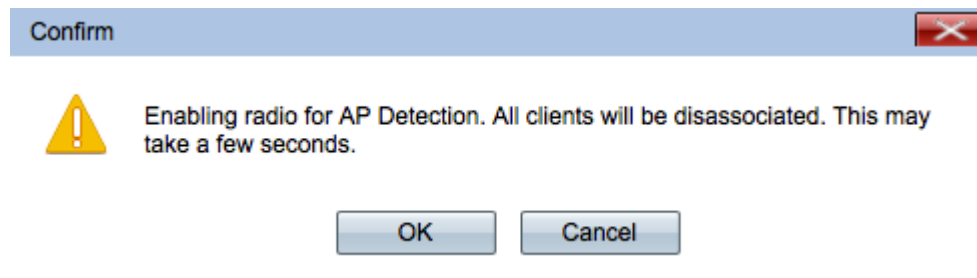
Save

Afficher les statistiques des points d'accès indésirables

Étape 1. Cochez **Enable** pour activer la détection AP pour que la radio désirée affiche les statistiques AP non fiables.

Remarque : le WAP561 dispose de deux radios que vous pouvez activer, tandis que le WAP551 n'a qu'une radio à activer.

Étape 2. Cliquez sur **Save** après avoir activé la détection AP pour afficher la liste des points d'accès non autorisés détectés. Une fenêtre de confirmation s'affiche.



Étape 3. Cliquez sur **OK** pour continuer.

Note: Les clients sans fil de votre réseau perdront momentanément leur connexion.

Detected Rogue AP List							
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
Trust	08:00:27:00:00:00	wlan0	102	AP	WiFi-Access	On	On
Trust	08:00:27:00:00:00	wlan0	102	AP	WiFi-Access	Off	Off
Trust	08:00:27:00:00:00	wlan0	100	AP	WiFi-Access	On	Off
Trust	08:00:27:00:00:00	wlan0	102	AP	WiFi-Access	On	On

Les informations suivantes relatives aux points d'accès détectés s'affichent :

- MAC Address : adresse MAC du point d'accès non autorisé.
- Radio : radio physique sur le point d'accès non autorisé auquel vous pouvez vous joindre.
- Beacon Interval : intervalle de balise utilisé par le point d'accès non autorisé. Chaque point d'accès envoie des trames de balise à intervalles réguliers pour annoncer l'existence de son réseau sans fil.
- Type : type du périphérique détecté. Peut être AP ou Ad hoc.
- SSID : SSID (Service Set Identifier) du point d'accès non autorisé, également appelé nom de réseau.
- Privacy : indique si la sécurité est activée sur le point d'accès non autorisé. Off indique que le point d'accès non autorisé n'a pas de sécurité activée tandis que On indique que les mesures de sécurité du point d'accès non autorisé sont activées.
- WPA : indique si la sécurité WPA est activée pour le point d'accès non autorisé.

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

·Band : mode IEEE 802.11 utilisé sur le point d'accès non autorisé.

- 2.4 - Le mode IEEE 802.11b, 802.11g ou 802.11n (ou une combinaison) est utilisé.

- 5 - Le mode IEEE 802.11a ou 802.11n (ou les deux) est utilisé.

·Channel : canal (faisant partie du spectre radio) sur lequel le point d'accès non autorisé diffuse.

·Rate : débit en mégaoctets par seconde auquel le point d'accès non autorisé transmet actuellement.

·Signal : force du signal radio émis par le point d'accès non autorisé. Pour voir la force du signal en décibels, passez votre souris sur les barres.

·Beacons : nombre total de balises reçues du point d'accès non autorisé depuis sa première détection.

·Dernière balise : date et heure auxquelles la dernière balise a été reçue du point d'accès non autorisé.

Débits : : ensembles de débits pris en charge et de base pour le point d'accès détecté (en mégabits par seconde).

Créer une liste de points d'accès approuvés

Note: La détection des points d'accès indésirables doit être activée pour créer une liste de points d'accès approuvés. Complétez la section intitulée *Afficher les statistiques des points d'accès indésirables* si vous ne l'avez pas déjà fait.

Detected Rogue AP List							
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
<input type="button" value="Trust"/>	00:11:22:33:44:55	wlan0	102	AP	WiFi-Access	On	On
<input type="button" value="Trust"/>	66:77:88:99:AA:BB	wlan0	102	AP	WiFi-Access	Off	Off
<input type="button" value="Trust"/>	CC:DD:EE:FF:00:11	wlan0	100	AP	WiFi-Access	On	Off
<input type="button" value="Trust"/>	22:33:44:55:66:77	wlan0	102	AP	WiFi-Access	On	On

Étape 1. Cliquez sur **Trust** en regard d'une entrée de point d'accès pour l'ajouter à la liste de points d'accès approuvés.

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:	<input type="radio"/> Download (PC to AP) <input checked="" type="radio"/> Backup (AP to PC)
<input type="button" value="Save"/>	

Étape 2. (Facultatif) Pour supprimer une entrée de point d'accès de la liste des points d'accès approuvés, cliquez sur **Annuler la confiance**.

Étape 3. Cliquez sur la case d'option **Sauvegarder (AP vers PC)** dans le champ Action de sauvegarde pour enregistrer la liste des AP approuvés dans un fichier.

Étape 4. Cliquez sur **Save** pour enregistrer la liste des points d'accès approuvés. Le WAP crée un fichier .cfg qui contient une liste de toutes les adresses MAC de la liste des points d'accès approuvés.

Importer une liste de points d'accès approuvés

Note: La détection des points d'accès indésirables doit être activée pour créer une liste de points d'accès approuvés. Complétez la section intitulée *Afficher les statistiques des points d'accès indésirables* si vous ne l'avez pas déjà fait.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Wireless > Rogue AP Detection**. La page *Détection des points d'accès indésirables* s'ouvre :

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:	<input checked="" type="radio"/> Download (PC to AP) <input type="radio"/> Backup (AP to PC)
Source File Name:	<input type="button" value="Choose File"/> No file chosen
File Management Destination:	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="button" value="Save"/>	

Étape 2. Faites défiler jusqu'à la zone Download/Backup Trusted AP List et cliquez sur la

case d'option **Download (PC to AP)** pour importer une liste des AP connus à partir d'une liste enregistrée.

Étape 3. Cliquez sur **Parcourir** dans le champ Nom du fichier source et choisissez votre fichier. Le fichier que vous importez doit avoir une extension .txt ou .cfg. Le fichier doit être une liste d'adresses MAC au format hexadécimal.

Étape 4. Dans le champ File Management Destination, cliquez sur **Replace** pour remplacer la liste des points d'accès approuvés ou cliquez sur **Merge** pour l'ajouter à la liste des points d'accès approuvés.

Étape 5. Cliquez sur **Enregistrer** pour importer le fichier.

Remarque : Les AP définis dans le fichier que vous téléchargez sont déplacés de la liste des AP détectés vers la liste des AP approuvés.