Rogue Access Point (AP) Detection on WAP561 and WAP551

Objective

A rogue access point (AP) is an access point that is installed on a secure network without the consent of the network administrator. Rogue APs can pose a security threat because anyone who installs a wireless router within range of your network can potentially gain access to your network. The *Rogue AP Detection* page provides information about the wireless networks that are within range of yours. This article explains how to detect rogue APs and create a Trusted AP List.

Note: The *Rogue AP Detection* page has no security features. The AP Trusted List is for your own use and is no more secure than an untrusted AP.

Applicable Devices

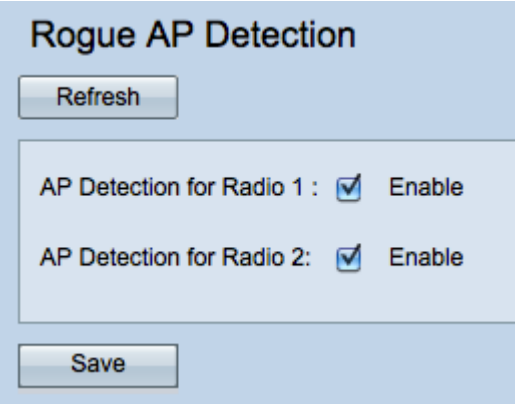
- WAP551
- WAP561

Software Version

- 1.0.4.2

Rogue AP Detection Configuration

Step 1. Log in to the web configuration utility and choose **Wireless > Rogue AP Detection**. The *Rogue AP Detection* page opens:



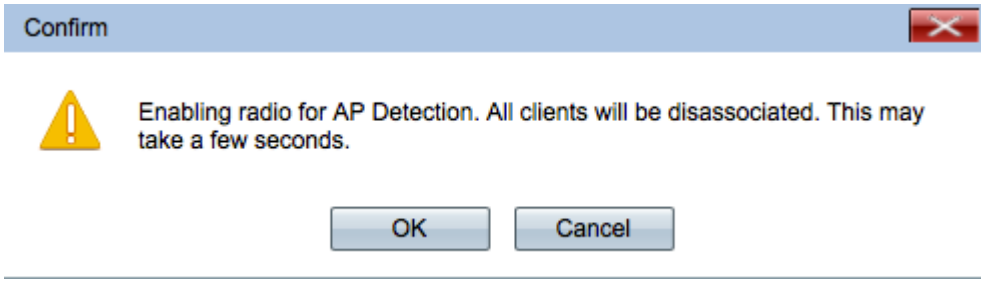
View Rogue AP Statistics

Step 1. Check **Enable** to enable AP Detection for the desired radio to display the rogue AP statistics.

Note: The WAP561 has two radios that you can enable while the WAP551 only has one radio to enable.

Step 2. Click **Save** after you enable AP detection to show the list of detected rogue access

points. A confirmation window will appear.



Step 3. Click **OK** to proceed.

Note: Wireless clients on your network will lose their connection momentarily.

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
Trust	[illegible]	wlan0	102	AP	[illegible]	On	On
Trust	[illegible]	wlan0	102	AP	[illegible]	Off	Off
Trust	[illegible]	wlan0	100	AP	[illegible]	On	Off
Trust	[illegible]	wlan0	102	AP	[illegible]	On	On

The following information for the detected access points is displayed:

- MAC Address — The MAC address of the rogue AP.
- Radio — The physical radio on the rogue AP that you can join.
- Beacon Interval — The beacon interval that is used by the rogue AP. Every AP sends beacon frames at regular intervals to advertise the existence of their wireless network.
- Type — The type of the detected device. Can be either AP or Ad hoc.
- SSID — The Service Set Identifier (SSID) of the rogue AP, also known as the network name.
- Privacy — Indicates whether or not security is enabled on the rogue AP. Off indicates that the rogue AP has no security enabled while On indicates that the rogue AP does have security measures enabled.
- WPA — Indicates whether WPA security is enabled for the rogue 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

- Band — The IEEE 802.11 mode that is used on the rogue AP.

– 2.4 — IEEE 802.11b, 802.11g, or 802.11n mode (or a combination) is in use.

– 5 — IEEE 802.11a or 802.11n mode (or both) is in use.

• Channel — The channel (part of the radio spectrum) that the rogue AP broadcasts on.

• Rate — The rate in megabytes per second at which the rogue AP currently transmits.

• Signal — The strength of the emitted radio signal from the rogue AP. To see the strength of the signal in decibels, hover your mouse over the bars.

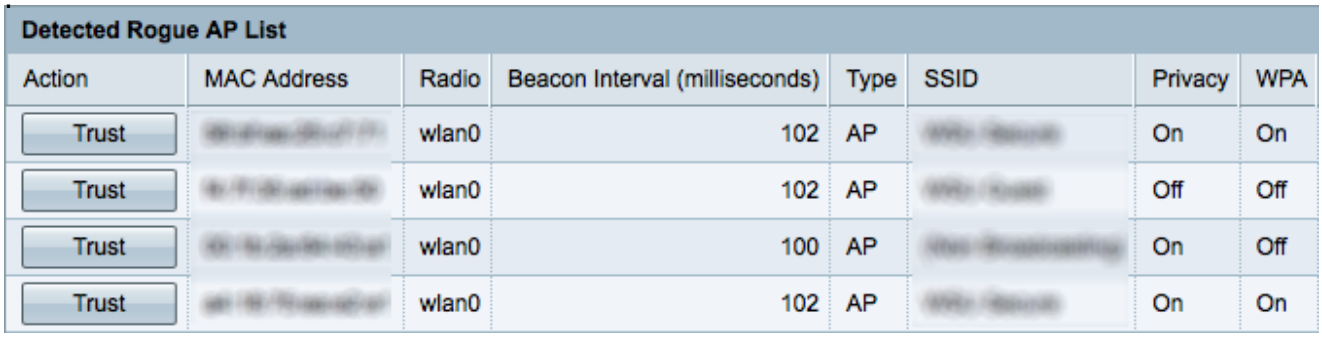
• Beacons — Total number of beacons received from the rogue AP since it was first detected.

• Last Beacon — The date and time that the last beacon was received from the rogue AP.

• Rates — The supported and basic rate sets for the detected AP (in megabits per second).

Create Trusted AP List

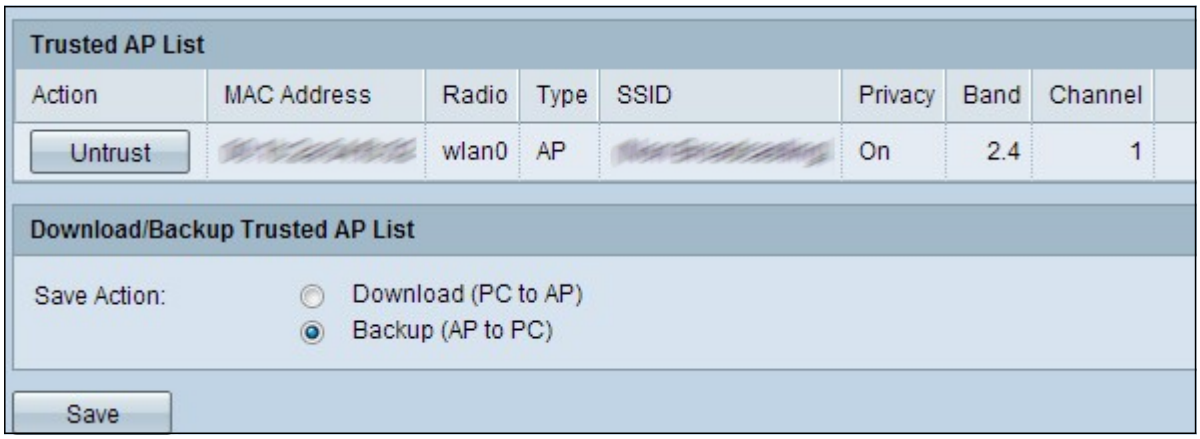
Note: Rogue AP Detection needs to be enabled to create a trusted AP list. Complete the section titled *View Rogue AP Statistics* if you have not already done so.



Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
Trust	[illegible]	wlan0	102	AP	[illegible]	On	On
Trust	[illegible]	wlan0	102	AP	[illegible]	Off	Off
Trust	[illegible]	wlan0	100	AP	[illegible]	On	Off
Trust	[illegible]	wlan0	102	AP	[illegible]	On	On

Step 1. Click **Trust** next to an AP entry to add it to the Trusted AP List.



Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
Untrust	[illegible]	wlan0	AP	[illegible]	On	2.4	1

Download/Backup Trusted AP List

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

Save

Step 2. (Optional) To remove an AP entry from the Trusted AP List, click **Untrust**.

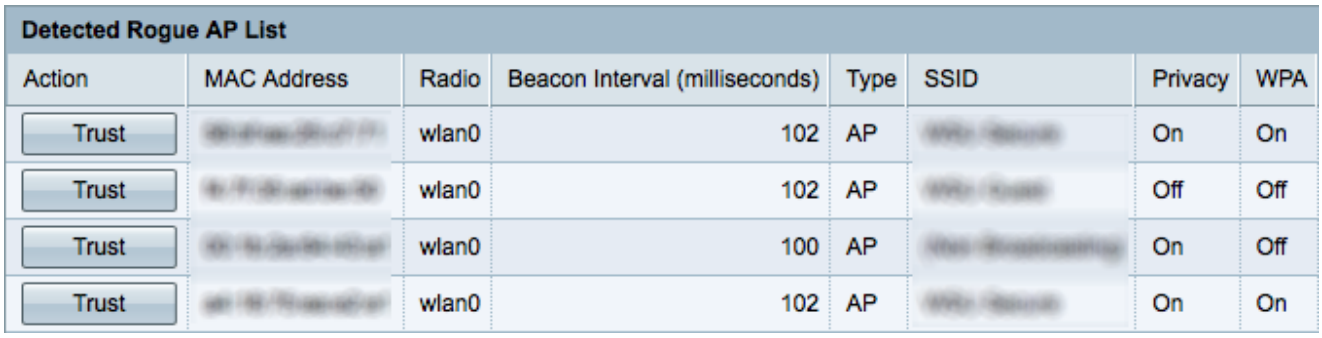
Step 3. Click the **Backup (AP to PC)** radio button in the Save Action field to save the Trusted AP List to a file.

Step 4. Click **Save** to save the Trusted AP List. The WAP creates a .cfg file that contains a list of all the MAC addresses in the Trusted AP List.

Import a Trusted AP List

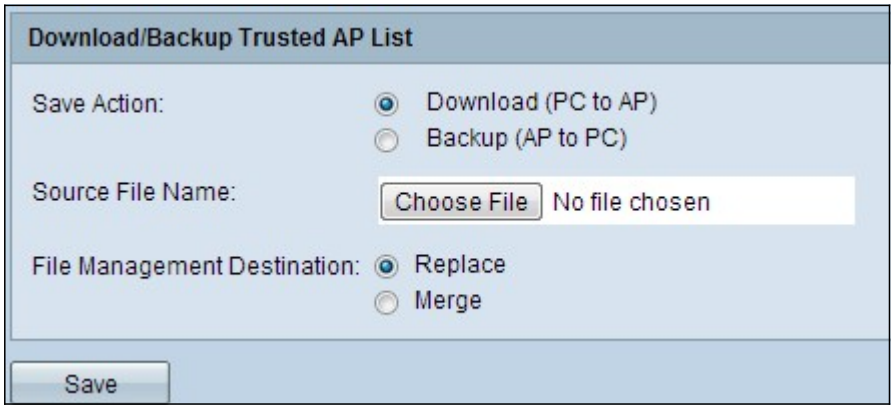
Note: Rogue AP Detection needs to be enabled to create a trusted AP list. Complete the section titled *View Rogue AP Statistics* if you have not already done so.

Step 1. Log in to the web configuration utility and choose **Wireless > Rogue AP Detection**. The *Rogue AP Detection* page opens:



Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA
Trust	[illegible]	wlan0	102	AP	[illegible]	On	On
Trust	[illegible]	wlan0	102	AP	[illegible]	Off	Off
Trust	[illegible]	wlan0	100	AP	[illegible]	On	Off
Trust	[illegible]	wlan0	102	AP	[illegible]	On	On



Step 2. Scroll down to the Download/Backup Trusted AP List area and click the **Download (PC to AP)** radio button to import a list of known APs from a saved list.

Step 3. Click **Browse** in the Source File Name field and choose your file. The file that you import must have a .txt or .cfg extension. The file should be a list of MAC addresses in hexadecimal format.

Step 4. In the File Management Destination field, click **Replace** to overwrite the Trusted AP List or click **Merge** to add to the Trusted AP List.

Step 5. Click **Save** to import the file.

Note: The APs that are defined in the file you upload are moved from the Detected AP List to the Trusted AP List.