

# Create or Import a Trusted Access Point List on a Wireless Access Point (WAP)

## 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 the range of your network can potentially gain access to your network. The Rogue AP Detection page in the web-based utility of the AP provides information about the wireless networks that are within range.

Having a trusted AP list can help keep track of the APs that an administrator trusts with the help of the details on the Detected Rogue AP List.

This article aims to show you how to create, import, and download an AP list on an access point.

## Applicable Devices

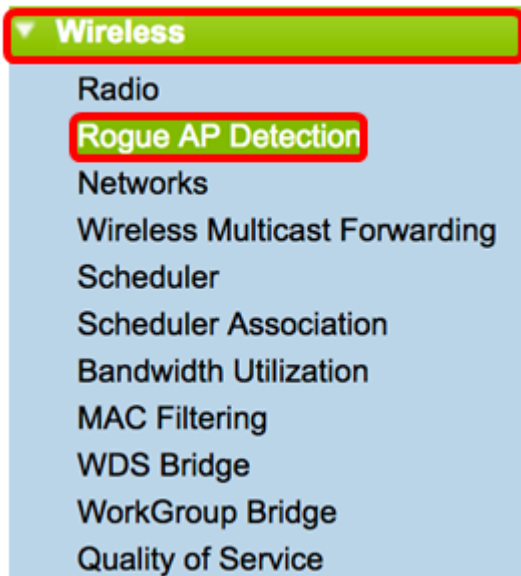
- 100 Series — WAP121, WAP150
- 300 Series
- 500 Series

## Software Version

- 1.0.1.7 — WAP150, WAP361
- 1.0.0.17 — WAP571, WAP571E
- 1.0.2.2 — WAP131, WAP351
- 1.0.6.5 — WAP121, WAP321
- 1.2.1.3 — WAP551, WAP561
- 1.3.0.3 — WAP371

## Create Trusted AP List

Step 1. Log in to the web-based utility of the access point and choose **Wireless > Rogue AP Detection**.



Step 2. If you trust or recognize an AP that was detected, click the **Trust** button next to its entry in the list. This adds the corresponding AP to the *Trusted AP List*, and removes it from the *Detected Rogue AP List*.

**Note:** Trusting an AP only adds it to the list, and has no impact on the operation of the AP. The lists are organizational tools that can be used to take further action.

The following information about the detected access points are 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 Wi-Fi Protected Access (WPA) security is enabled for the rogue AP.
- Band — The IEEE 802.11 mode that is used on the rogue AP. It can be either 2.4 GHz or 5 GHz.
- Channel — Displays the channel that the detected AP is currently broadcasting on.
- Rate — Shows the rate at which the detected AP current broadcasts in Mbps.
- Signal — Shows the strength of the radio signal from the AP.
- Beacons — Displays the total number of beacons received from the AP since it was first detected. Beacon frames are transmitted by an AP at a regular interval to announce the existence of the wireless network.
- Last Beacon — Displays the date and time of the last beacon received from the AP.
- Rates — Lists the supported and basic rates of the detected AP in megabits per second.

Detected Rogue AP List													
Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon
Trust		Radio 1:VAP0	102	AP		On	On	2.4	1	24		6896	Thu Dec 1
Trust		Radio 1:VAP0	100	AP		On	On	2.4	6	1		11279	Thu Dec 1
Trust		Radio 1:VAP0	100	AP		On	On	2.4	6	1		13306	Thu Dec 1
Trust		Radio 1:VAP0	100	AP		On	On	2.4	6	1		9113	Thu Dec 1
Trust		Radio 1:VAP0	100	AP		On	On	2.4	6	1		18189	Thu Dec 1

Step 3. (Optional) The Trusted AP List table is populated once an AP has been trusted. To remove an AP from the list, click **Untrust**.

Trusted AP List								
Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel	
Untrust		Radio 1:VAP0	AP	WAP571	On	2.4	6	
Untrust		Radio 1:VAP0	AP	ciscosb	On	2.4	6	
Untrust		Radio 1:VAP0	AP	CiscoSB-Setup	On	2.4	2	

Step 4. (Optional) In the Download/Backup Trusted AP List area, click a radio button to either download a configuration file to the AP from the PC or Backup to download the list from the AP to the PC. If you chose Download, proceed to the next step. If you chose **Backup**, skip to [Step 7](#).

**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

Step 5. In the Source File Name area, click on **Choose File** to choose a file on your PC to download to the AP.

**Note:** For this example, Rogue1.cfg is chosen.

**Download/Backup Trusted AP List**

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

Source File Name:  **Rogue1.cfg**

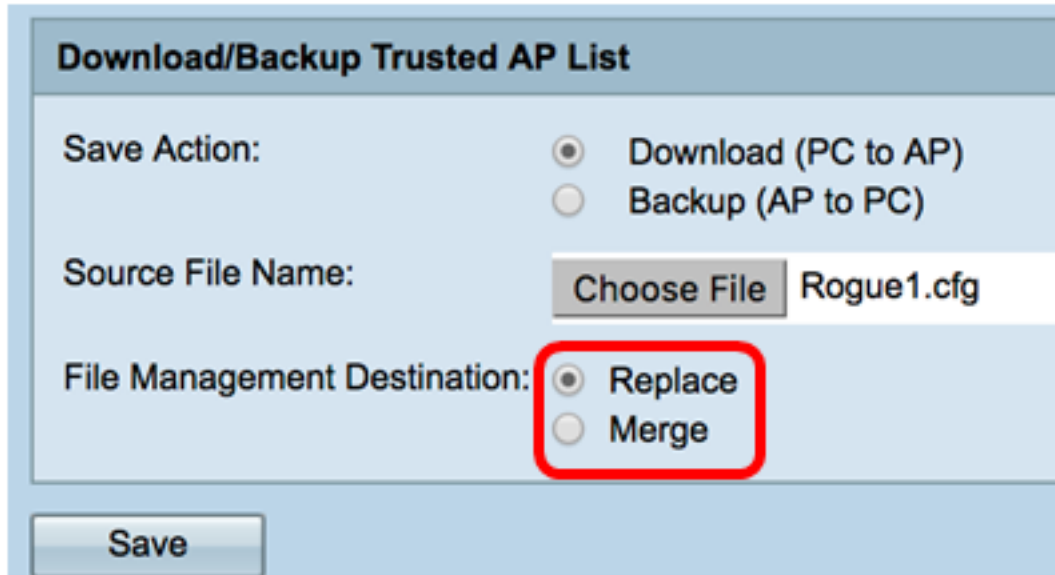
File Management Destination:  Replace  
 Merge

Step 6. In the File Management Destination area, click a radio button to either replace or

merge the file with the existing list. The options are:

- Replace — Imports the lists and replaces the contents of the Trusted AP List.
- Merge — Imports the list and adds the APs in the imported file to the APs currently shown in the Trusted AP List.

**Note:** For this example, Replace is chosen.



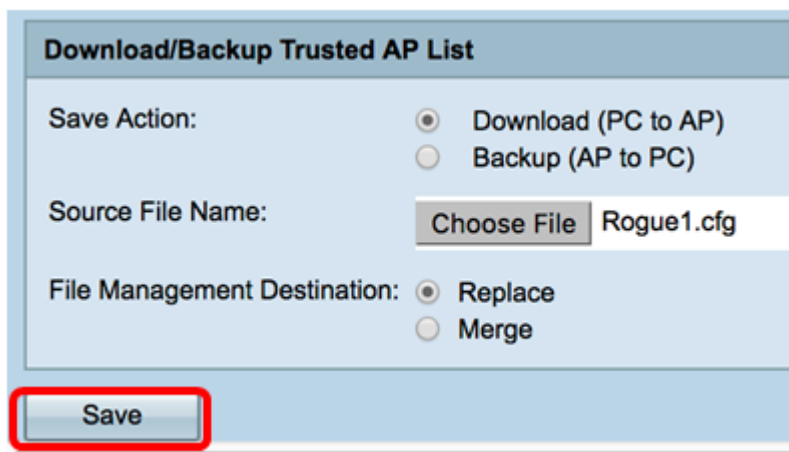
**Download/Backup Trusted AP List**

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

Source File Name:  Rogue1.cfg

File Management Destination:  Replace  
 Merge

[Step 7.](#) Click **Save**.



**Download/Backup Trusted AP List**

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

Source File Name:  Rogue1.cfg

File Management Destination:  Replace  
 Merge

You have now successfully created, backed up, and imported a Trusted AP List on a WAP.