Rogue AP Detection on the WAP351 and WAP371 Access Points

Objective

A rogue access point (AP) is an access point that has been installed on a network without explicit authorization from a system administrator. Rogue access points pose a security threat because anyone with access to the area can install a wireless access point that may allow unauthorized parties access to the network. The *Rogue AP Detection* page displays information about these access points. You can add any authorized access points to the Trusted AP List.

The objective of the document is to explain how to detect rogue access points (AP) on the WAP351 and WAP371 Access Points.

Applicable Devices

- WAP351
- WAP371

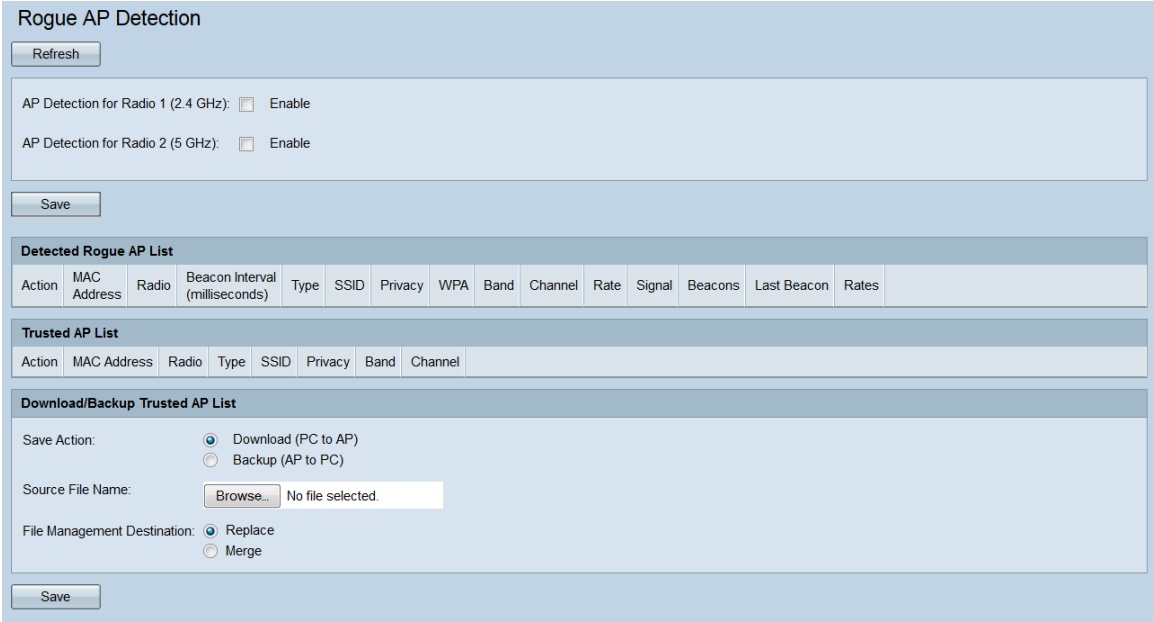
Software Version

- 1.0.0.39 (WAP351)
- 1.2.0.2 (WAP371)

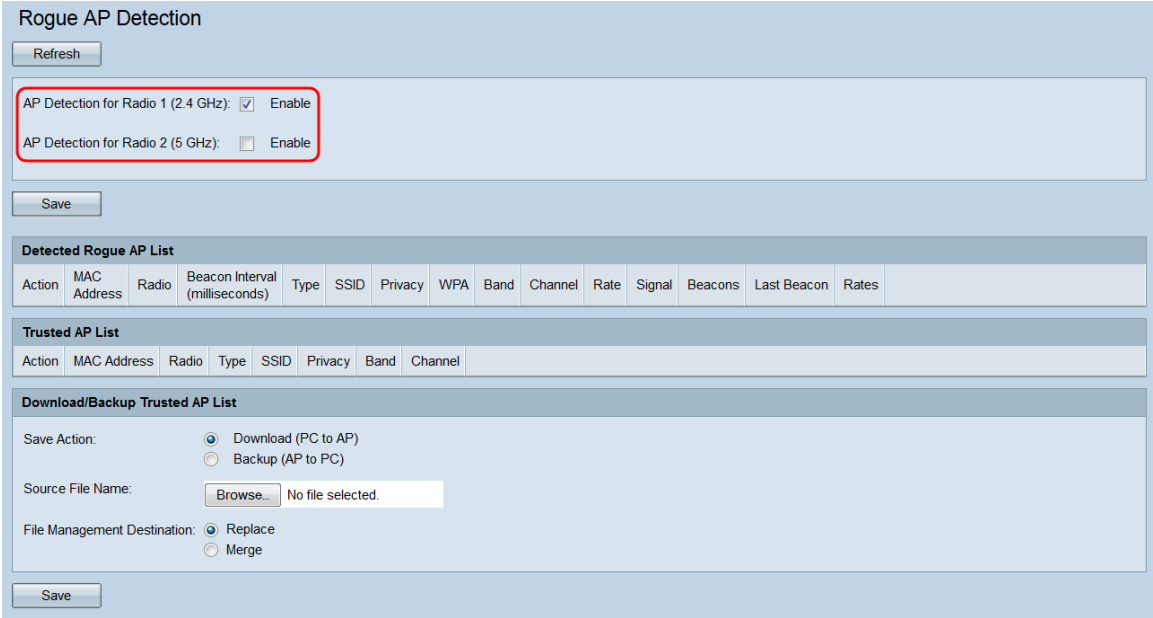
Rogue AP Detection Configuration

Note: In order to configure rogue AP detection for a radio, that radio must first be enabled in the **Wireless > Radio** section. For more information, refer to the articles *Configuring Basic Radio Settings on the WAP131 and WAP351* and *Basic Radio Settings on the WAP371*.

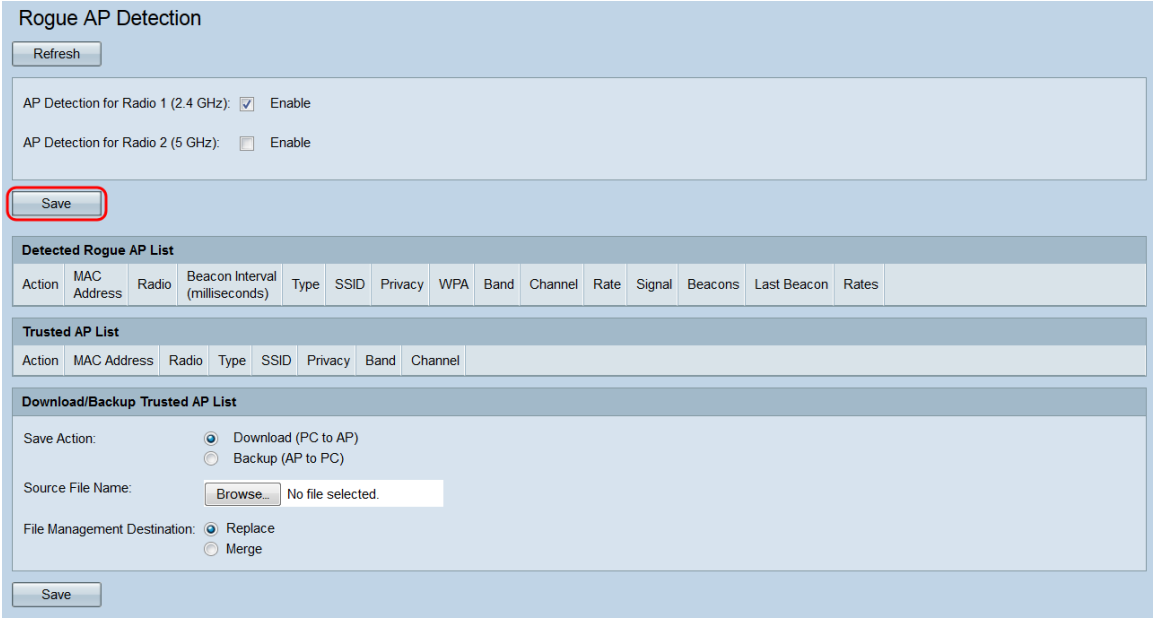
Step 1. Log into the web configuration utility and choose **Wireless > Rogue AP Detection**. The *Rogue AP Detection* window appears:



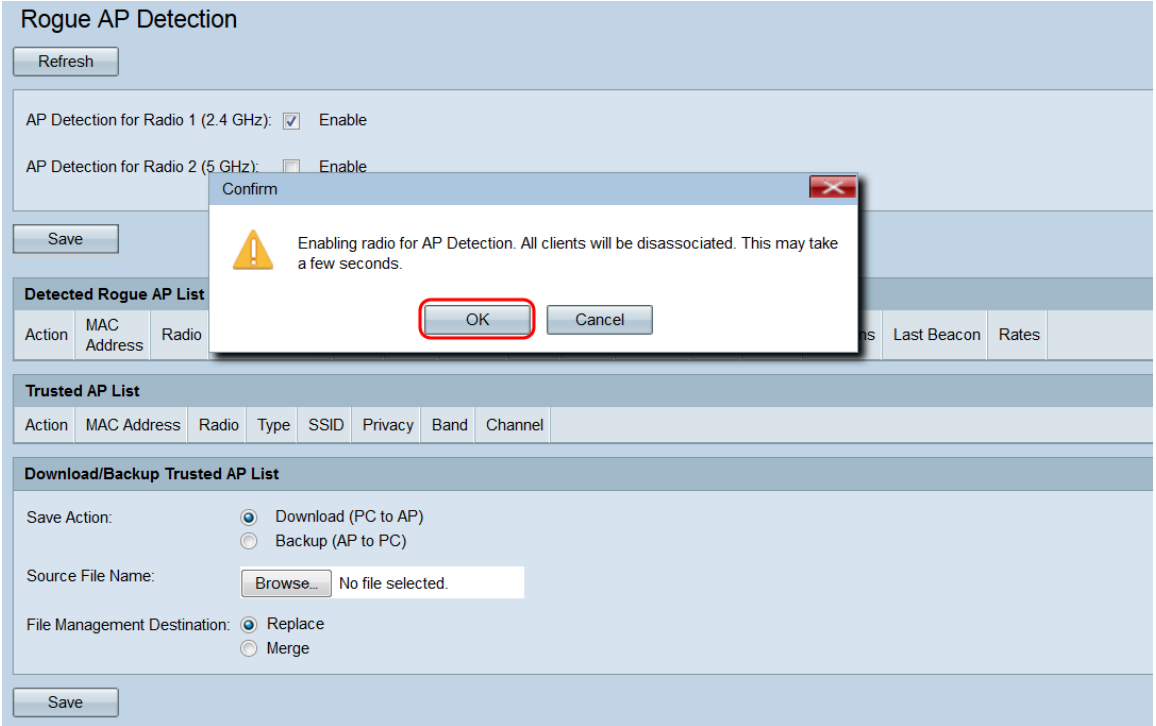
Step 2. Check the *AP Detection for Radio 1* or *AP Detection for Radio 2* checkboxes to select which radio interface(s) you want to enable rogue AP detection on. On the WAP351, Radio 1 can only detect APs in the 2.4 GHz range, and Radio 2 can only detect APs in the 5 GHz range. On the WAP371, Radio 1 can only detect APs in the 5 GHz range, and Radio 2 can only detect APs in the 2.4 GHz range.



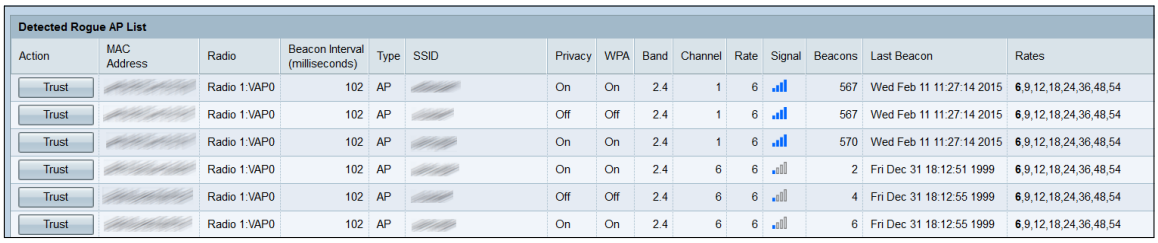
Step 3. Click the **Save** button to enable rogue AP detection for the selected radio interfaces.



Step 4. If enabling rogue AP detection, a pop-up window will appear saying that all currently connected clients will be disconnected. Click **OK** to continue.



Once rogue AP detection is enabled, every detected AP will be displayed in the *Detected Rogue AP List*.



Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Trust		Radio 1:VAP0	102	AP		On	On	2.4	1	6		567	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		Off	Off	2.4	1	6		567	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		On	On	2.4	1	6		570	Wed Feb 11 11:27:14 2015	6,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		On	On	2.4	6	6		2	Fri Dec 31 18:12:51 1999	6,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		Off	Off	2.4	6	6		4	Fri Dec 31 18:12:55 1999	6,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		On	On	2.4	6	6		6	Fri Dec 31 18:12:55 1999	6,9,12,18,24,36,48,54

The following information for the detected access points is displayed:

- Action — Clicking the **Trust** button in this field will add the corresponding AP to the *Trusted AP List*, and remove it from the *Detected Rogue AP List*.

• MAC Address — Displays the MAC address of the detected AP.

• Radio — This indicates the radio of the WAP on which the access point was detected.

• Beacon Interval — Displays the beacon interval in milliseconds that is used by the detected AP. Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default time to send a beacon frame is once every 100 milliseconds.

• Type — Displays the type of the detected device. It can be either an AP or Ad hoc. An Ad hoc device uses a local wireless connection that does not involve a wireless access point.

• SSID — Displays the SSID of the detected AP.

• Privacy — Indicates whether there is any security on the neighboring AP.

• WPA — Indicates whether WPA security is off or on for the detected AP.

• Band — Indicates the IEEE 802.11 mode that is used on the detected AP. It can be either 2.4 or 5.

• Channel — Displays the channel that the detected AP is currently broadcasting on.

• Rate — Shows the rate at which the detected AP currently broadcasts in Mbps.

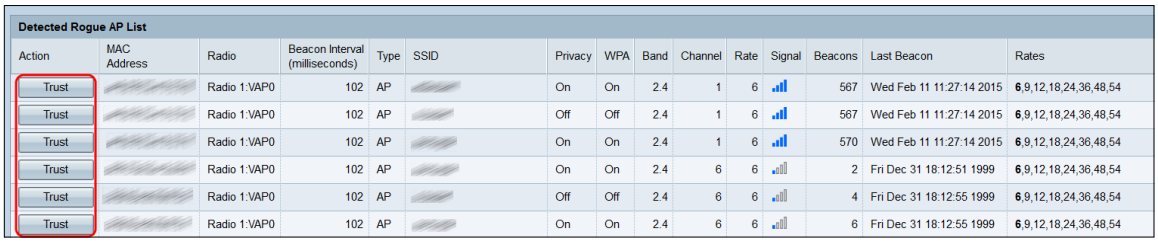
• Signal — Shows the strength of the radio signal from the AP.

• Beacons — Displays the total number of beacons received from the AP since it was first detected. Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default time to send a beacon frame is once every 100 milliseconds.

• 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).

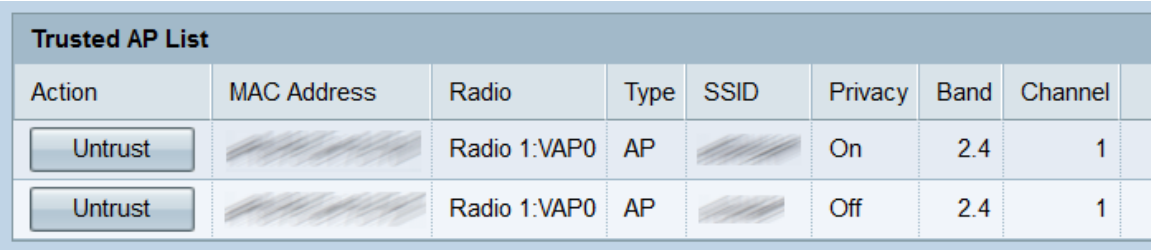
Step 5. If you trust or recognize an AP that was detected, click the **Trust** button next to its entry in the list. This adds the corresponding AP to the *Trusted AP List*, and removes it from the *Detected Rogue AP List*. Trusting an AP only adds it to the list, and has no impact on the operation of the WAP. The lists are organizational tool that can be used to take further action.



Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Trust		Radio 1:VAP0	102	AP		On	On	2.4	1	6		567	Wed Feb 11 11:27:14 2015	**6**,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		Off	Off	2.4	1	6		567	Wed Feb 11 11:27:14 2015	**6**,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		On	On	2.4	1	6		570	Wed Feb 11 11:27:14 2015	**6**,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		On	On	2.4	6	6		2	Fri Dec 31 18:12:51 1999	**6**,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		Off	Off	2.4	6	6		4	Fri Dec 31 18:12:55 1999	**6**,9,12,18,24,36,48,54
Trust		Radio 1:VAP0	102	AP		On	On	2.4	6	6		6	Fri Dec 31 18:12:55 1999	**6**,9,12,18,24,36,48,54

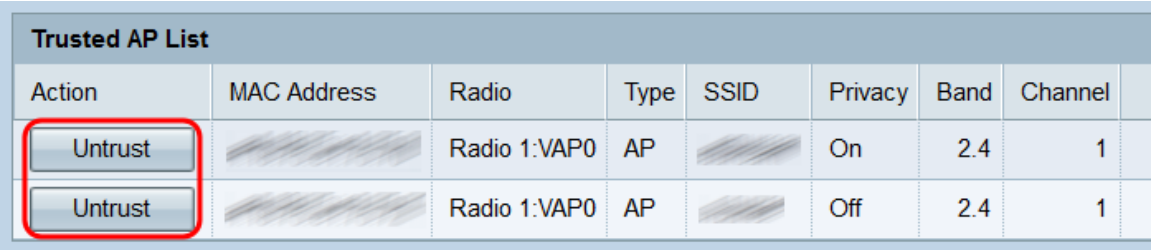
Step 6. To manage your trusted APs, scroll down to the *Trusted AP List*. This is where detected rogue APs are located when you click their respective **Trust** buttons.



Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
Untrust		Radio 1:VAP0	AP		On	2.4	1
Untrust		Radio 1:VAP0	AP		Off	2.4	1

Step 7. If you no longer trust a trusted AP, click on its corresponding **Untrust** button. This will move it back into the *Detected Rogue AP List*.

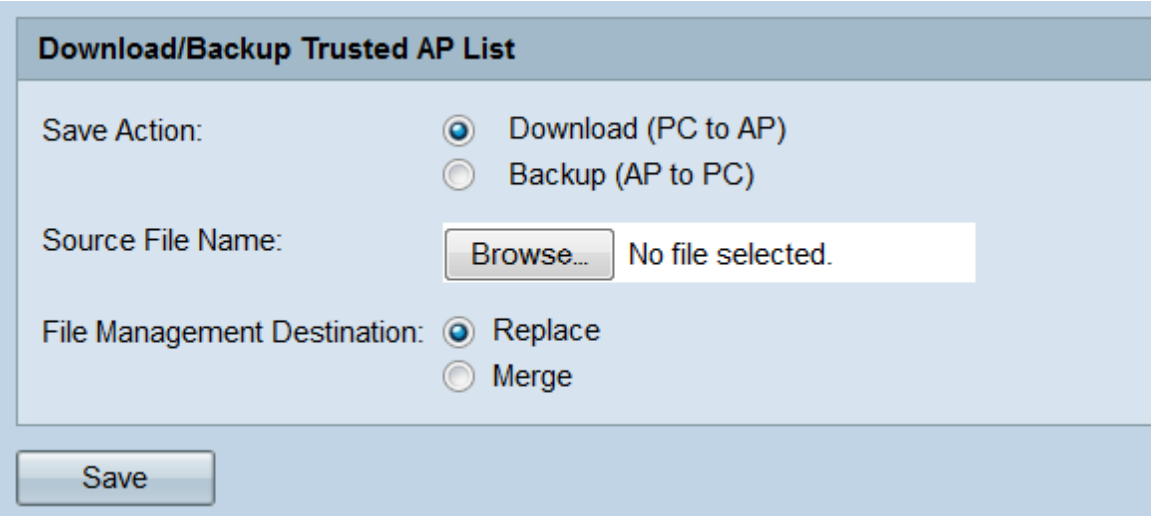


Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
Untrust		Radio 1:VAP0	AP		On	2.4	1
Untrust		Radio 1:VAP0	AP		Off	2.4	1

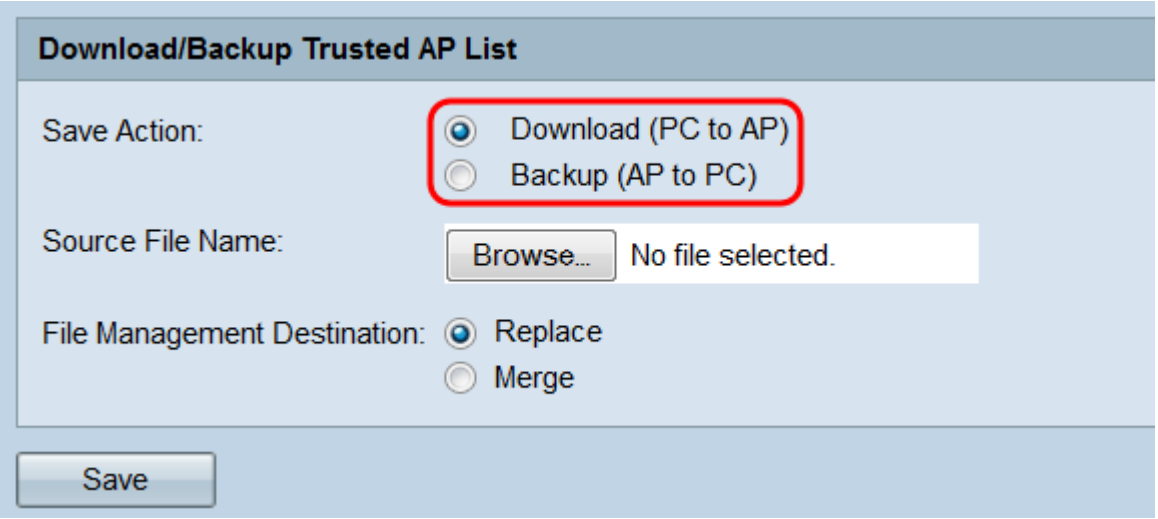
Backing Up / Downloading Trusted AP List

Step 1. If you want to download or backup the trusted AP list, scroll down to the *Download/Backup Trusted AP List* section.

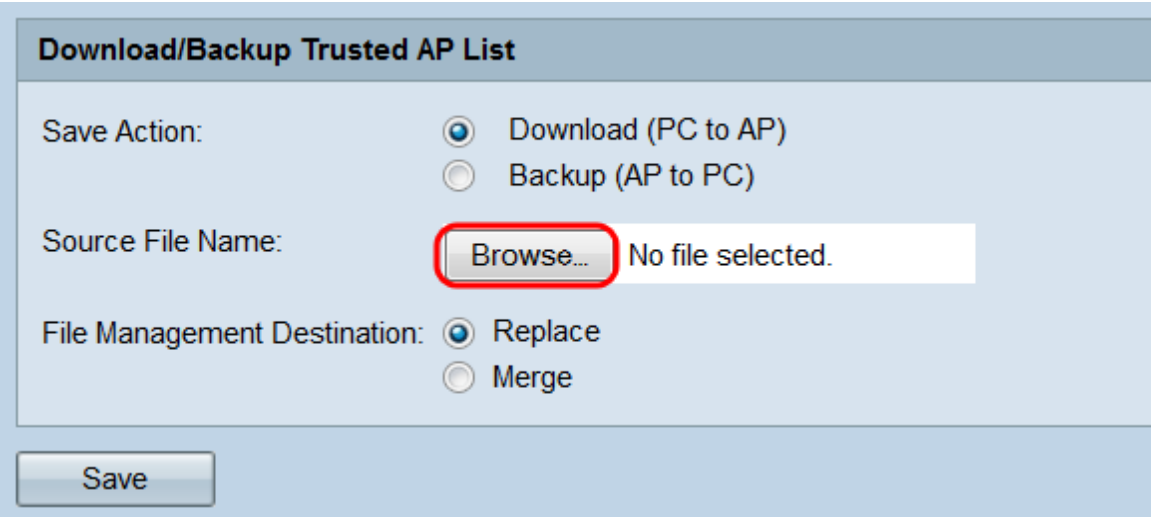


Step 2. In the *Save Action* field, choose one of the radio buttons:

- Download (PC to AP) — Select this if you want to download an existing trusted AP list from your PC to the WAP.
- Backup (AP to PC) — Select this if you want to backup the trusted AP list to your PC. If you select this, skip to Step 5.

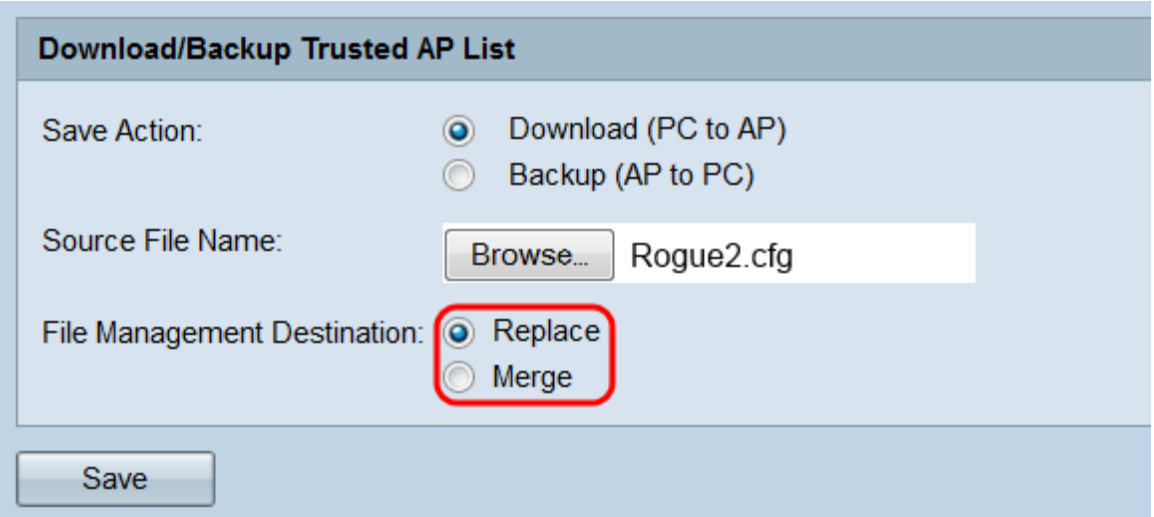


Step 3. If you selected **Download (PC to AP)** in the previous step, click the **Browse…** button in the *Source File Name* field to select the trusted AP list file on your PC.

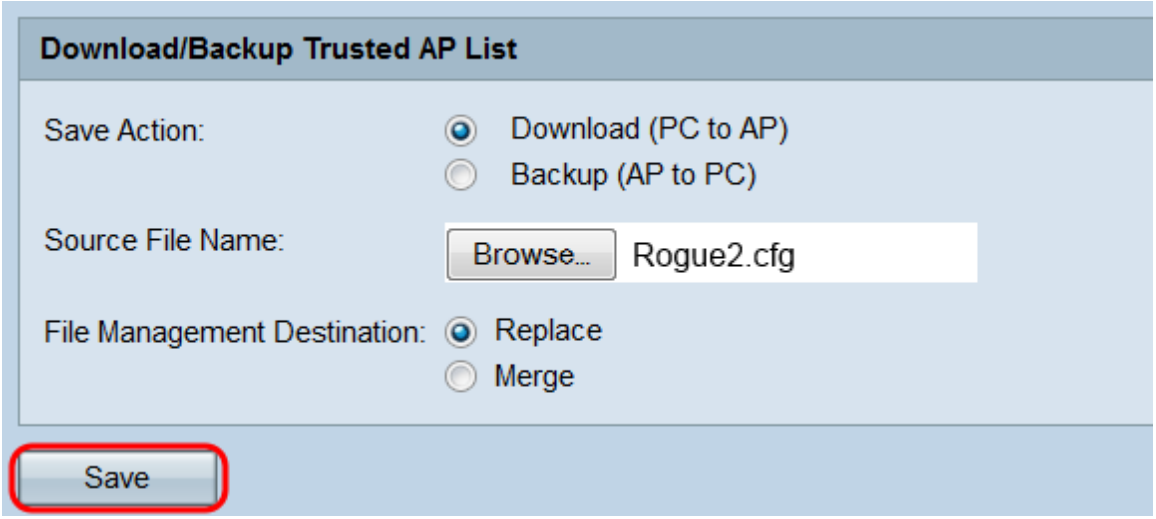


Note: The file must end in .cfg.

Step 4. In the *File Management Destination* field, select either the **Replace** or **Merge** radio buttons. **Replace** causes the downloaded file to completely overwrite the existing trusted AP list on the WAP, while **Merge** only adds the new APs in the file to the trusted AP list.



Step 5. Click **Save**. Depending on your selection in the *Save Action* field, the WAP will either backup the trusted AP list to your PC or download the specified trusted AP list to the WAP.



Step 6. If you are performing a backup, a dialog window will appear asking to save the trusted AP list to your computer. If you are downloading the file, a pop-up window will appear stating that the transfer was successful. Click **OK**.