Erkennung nicht autorisierter APs auf den Access Points WAP351 und WAP371

Ziel

Ein nicht autorisierter Access Point (AP) ist ein Access Point, der ohne ausdrückliche Autorisierung eines Systemadministrators in einem Netzwerk installiert wurde. Nicht autorisierte Access Points stellen eine Sicherheitsbedrohung dar, da jeder, der Zugriff auf den Bereich hat, einen Wireless Access Point installieren kann, der nicht autorisierten Parteien den Zugriff auf das Netzwerk ermöglicht. Auf der Seite *Erkennung nicht autorisierter APs* werden Informationen zu diesen Access Points angezeigt. Sie können der Liste der vertrauenswürdigen Access Points alle autorisierten Access Points hinzufügen.

Ziel des Dokuments ist es zu erklären, wie nicht autorisierte Access Points (APs) auf den WAP351- und WAP371-Access Points erkannt werden.

Anwendbare Geräte

WAP351
WAP371

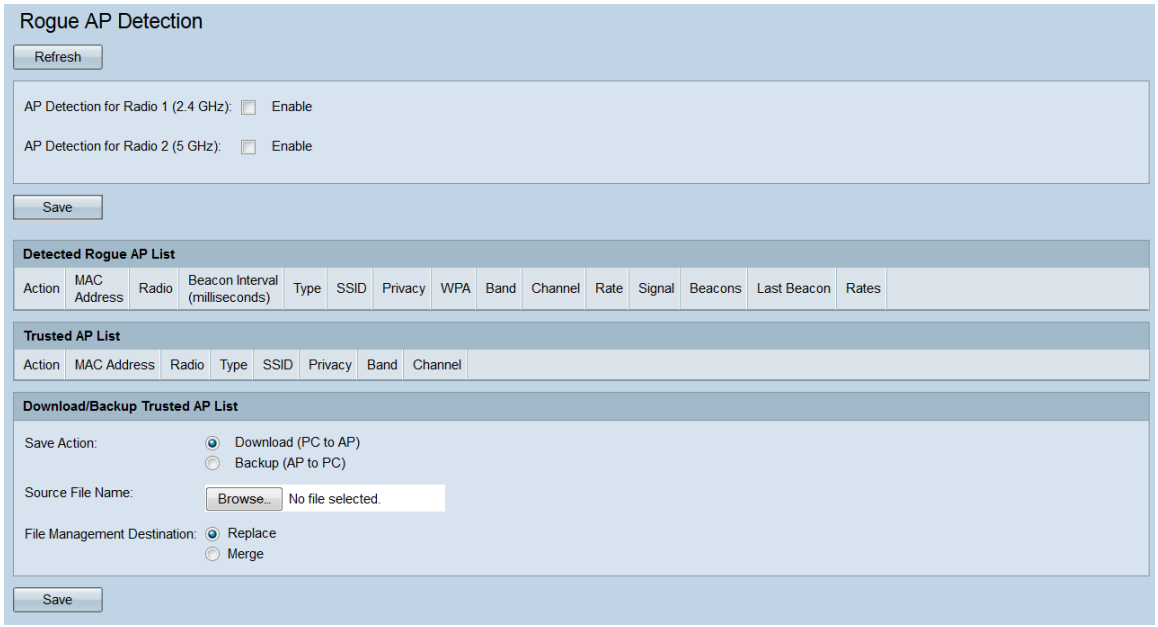
Softwareversion

·1.0.0.39 (WAP351)
· 1.2.0.2 (WAP371)

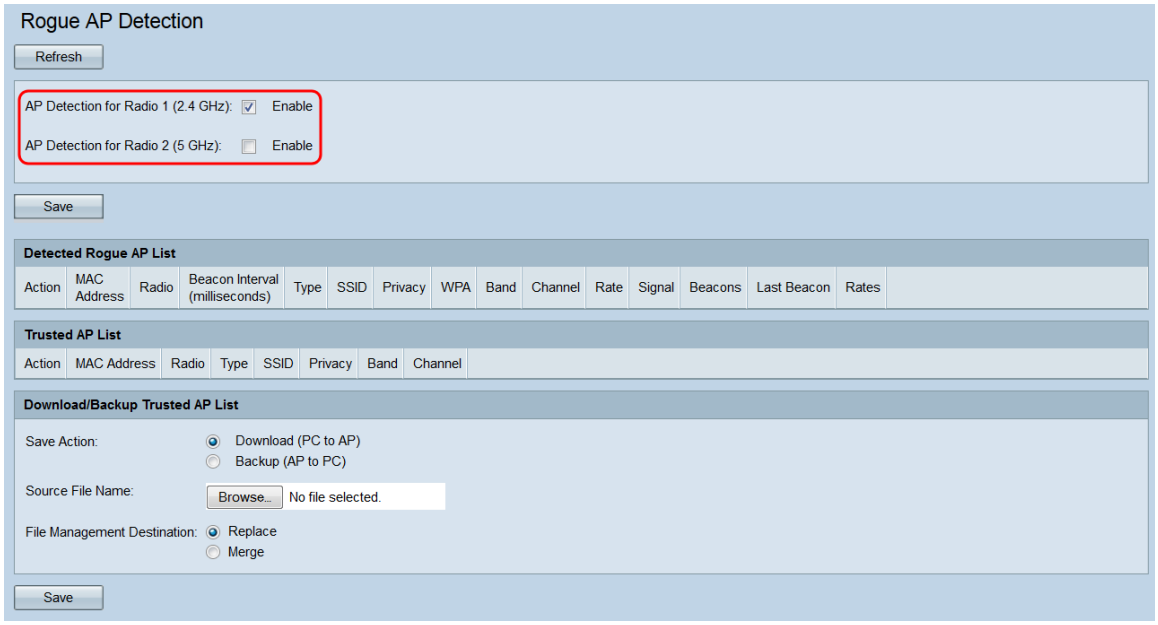
Konfiguration zur Erkennung nicht autorisierter APs

Hinweis: Um die Erkennung nicht autorisierter APs für eine Funkverbindung zu konfigurieren, muss diese Funkverbindung zuerst im Abschnitt **Wireless > Radio** aktiviert werden. Weitere Informationen finden Sie in den Artikeln *Konfigurieren grundlegender Funkeinstellungen für WAP131 und WAP351* und *Grundeinstellungen für Funkmodule auf dem WAP371*.

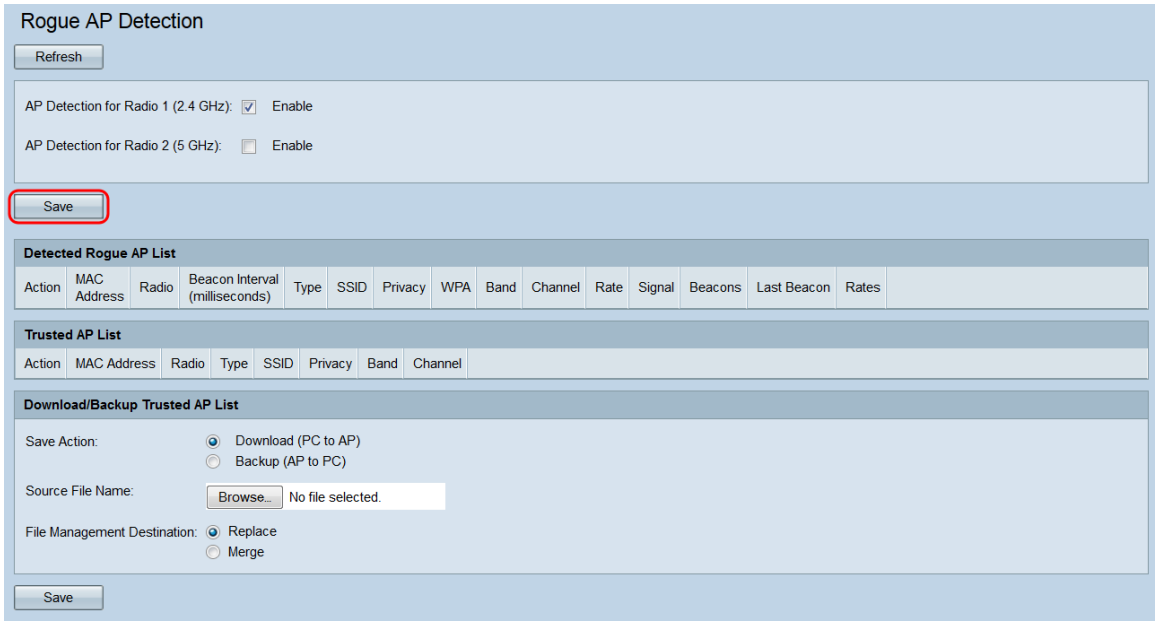
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Wireless > Rogue AP Detection aus**. Das Fenster *Erkennung nicht autorisierter APs* wird angezeigt:



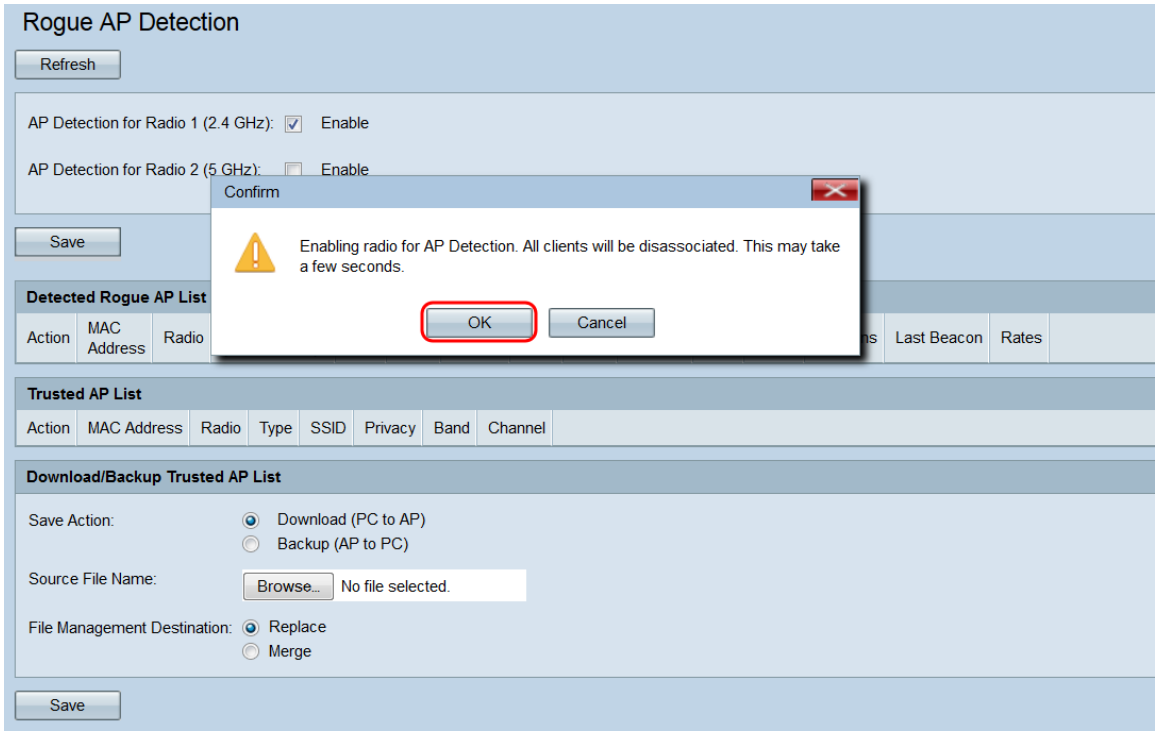
Schritt 2: Aktivieren Sie die Kontrollkästchen *AP Detection for Radio 1* or *AP Detection for Radio 2 (AP-Erkennung für Funkmodul 2)*, um die Funkschnittstelle(en) auszuwählen, für die Sie die Erkennung nicht autorisierter APs aktivieren möchten. Auf dem WAP351 kann Radio 1 APs nur im 2,4-GHz-Bereich erkennen, und Radio 2 kann nur APs im 5-GHz-Bereich erkennen. Auf dem WAP371 kann Radio 1 APs nur im 5-GHz-Bereich erkennen, und Radio 2 kann APs nur im 2,4-GHz-Bereich erkennen.



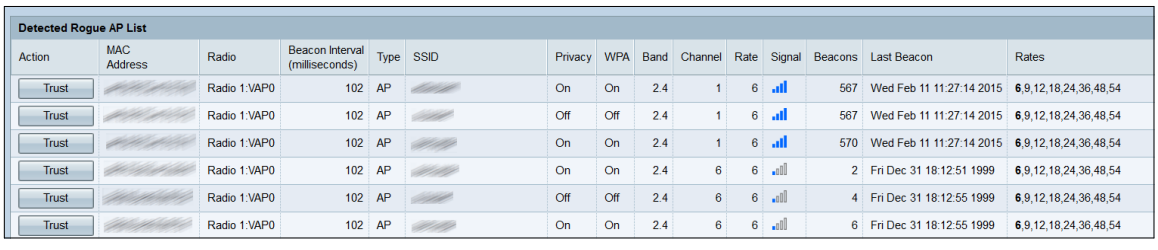
Schritt 3: Klicken Sie auf die Schaltfläche **Speichern**, um die Erkennung nicht autorisierter APs für die ausgewählten Funkschnittstellen zu aktivieren.



Schritt 4: Wenn Sie die Erkennung nicht autorisierter APs aktivieren, wird ein Popup-Fenster angezeigt, in dem bestätigt wird, dass alle aktuell verbundenen Clients getrennt werden. Klicken Sie auf **OK**, um fortzufahren.



Sobald die Erkennung nicht autorisierter APs aktiviert ist, wird jeder erkannte AP in der *Liste erkannter nicht autorisierter APs* angezeigt.



Die folgenden Informationen für die erkannten Access Points werden angezeigt:

·Aktion - Durch Klicken auf die Schaltfläche **Vertrauenswürdig** in diesem Feld wird der

entsprechende Access Point zur *Liste vertrauenswürdiger Access Points* hinzugefügt und aus der *Liste erkannter nicht autorisierter Access Points* entfernt.

·MAC Address (MAC-Adresse): Zeigt die MAC-Adresse des erkannten Access Points an.

·Radio (Funkübertragung): Zeigt das Funkmodul des WAP an, auf dem der Access Point erkannt wurde.

·Beacon Interval (Beacon-Intervall): Zeigt das Beacon-Intervall in Millisekunden an, das vom erkannten Access Point verwendet wird. Beacon-Frames werden von einem WAP in regelmäßigen Abständen übertragen, um das Vorhandensein des Wireless-Netzwerks anzukündigen. Die Standardzeit für das Senden eines Beacon-Frames beträgt einmal alle 100 Millisekunden.

·Type (Typ): Zeigt den Typ des erkannten Geräts an. Dabei kann es sich um einen AP oder einen Ad-hoc-Modus handeln. Ein Ad-hoc-Gerät verwendet eine lokale Wireless-Verbindung, an der kein Wireless Access Point angeschlossen ist.

·SSID (SSID): Zeigt die SSID des erkannten Access Points an.

·Datenschutz: Gibt an, ob der benachbarte Access Point sicher ist.

·WPA: Gibt an, ob die WPA-Sicherheit für den erkannten AP ausgeschaltet oder aktiviert ist.

·Band - gibt den IEEE 802.11-Modus an, der auf dem erkannten Access Point verwendet wird. Es kann entweder 2,4 oder 5 sein.

·Channel (Kanal): Zeigt den Kanal an, auf dem der erkannte Access Point derzeit sendet.

·Rate (Übertragungsrate): Zeigt die Übertragungsrate an, mit der der erkannte Access Point derzeit in Mbit/s sendet.

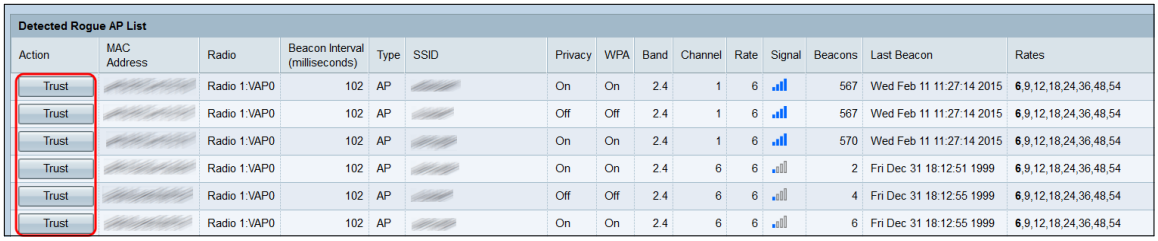
·Signal - Zeigt die Stärke des Funksignals des AP an.

·Beacons (Beacons): Zeigt die Gesamtzahl der Beacons an, die seit der ersten Erkennung vom Access Point empfangen wurden. Beacon-Frames werden von einem WAP in regelmäßigen Abständen übertragen, um das Vorhandensein des Wireless-Netzwerks anzukündigen. Die Standardzeit für das Senden eines Beacon-Frames beträgt einmal alle 100 Millisekunden.

·Last Beacon (Letzter Beacon): Zeigt das Datum und die Uhrzeit des letzten Beacons an, das vom Access Point empfangen wurde.

·Rates (Übertragungsraten): Führt die unterstützten und grundlegenden Raten des erkannten Access Points (in Megabit pro Sekunde) auf.

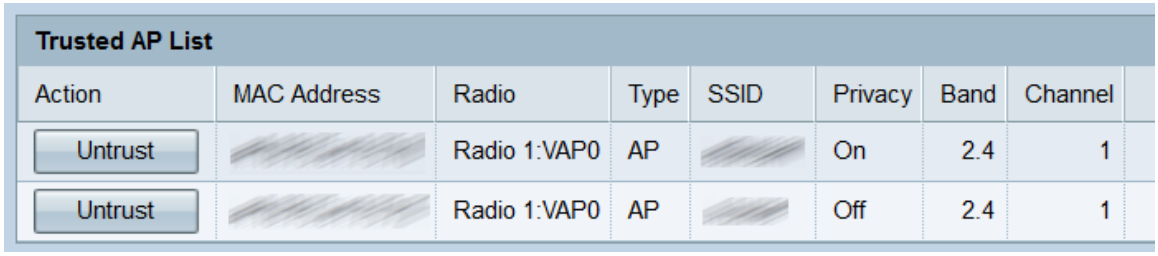
Schritt 5: Wenn Sie einem erkannten Access Point vertrauen oder ihn erkennen, klicken Sie auf die Schaltfläche **Vertrauenswürdig** neben dem Eintrag in der Liste. Dadurch wird der entsprechende Access Point der *Liste vertrauenswürdiger Access Points* hinzugefügt und aus der *Liste erkannter nicht autorisierter Access Points* entfernt. Durch das Vertrauen auf einen Access Point wird dieser nur der Liste hinzugefügt und hat keine Auswirkungen auf den Betrieb des WAP. Die Listen sind ein organisatorisches Tool, das für weitere Maßnahmen verwendet werden kann.



Detected Rogue AP List

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

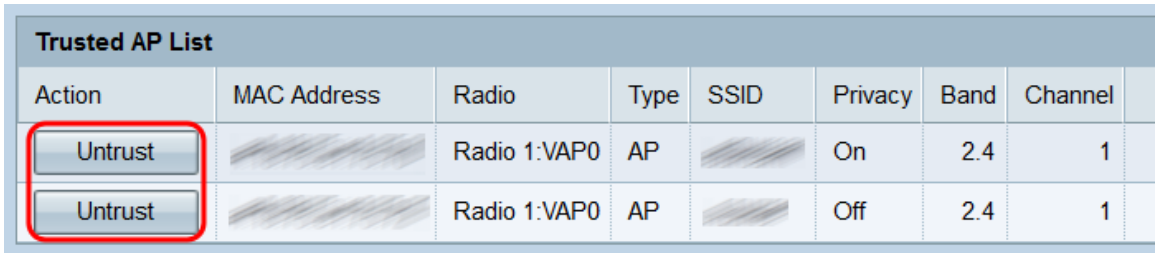
Schritt 6: Um vertrauenswürdige APs zu verwalten, scrollen Sie nach unten zur *Liste vertrauenswürdiger APs*. Hier befinden sich nicht autorisierte APs, wenn Sie auf die entsprechenden **Trust**-Schaltflächen klicken.



Trusted AP List

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

Schritt 7: Wenn Sie einem vertrauenswürdigen AP nicht mehr vertrauen, klicken Sie auf die entsprechende Schaltfläche **Untrust**. Dadurch wird sie wieder in die *Liste* der *erkannten nicht autorisierten Access Points* verschoben.

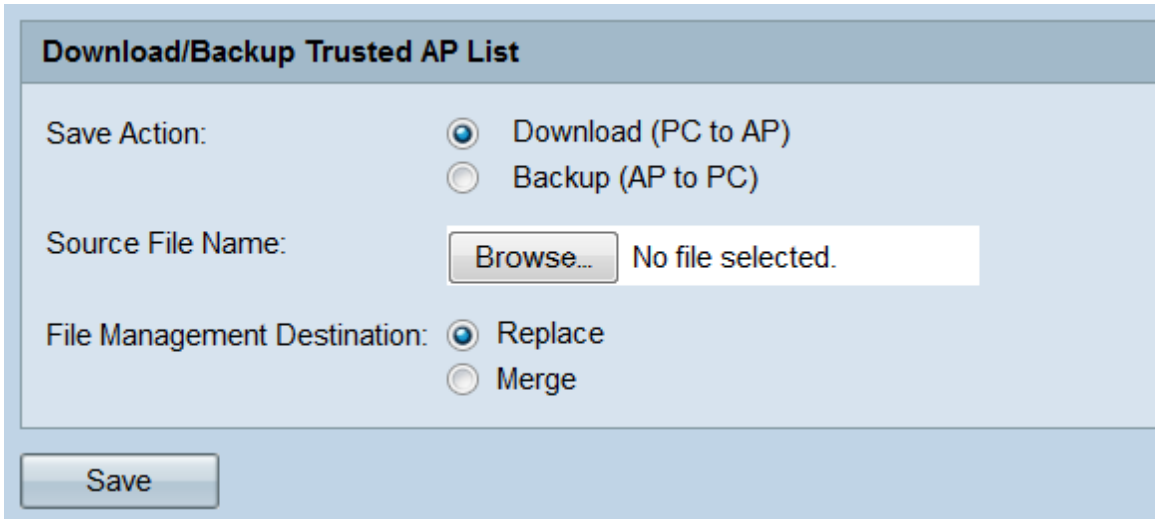


Trusted AP List

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

Sichern/Herunterladen der Liste der vertrauenswürdigen Access Points

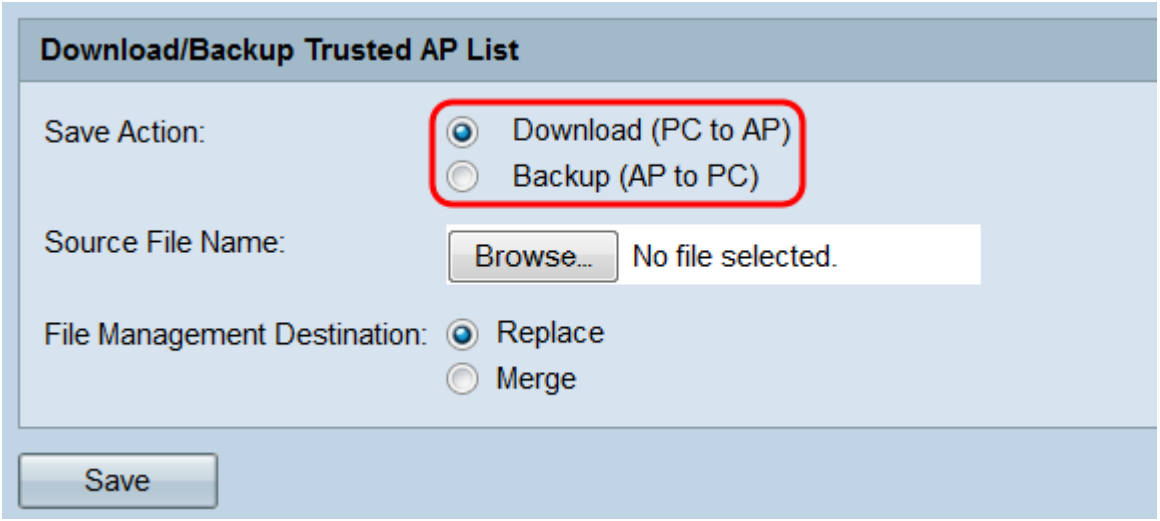
Schritt 1: Wenn Sie die Liste der vertrauenswürdigen Zugangspunkte herunterladen oder sichern möchten, führen Sie einen Bildlauf nach unten zum Abschnitt *"Liste vertrauenswürdiger* Zugangspunkte *herunterladen/sichern"*.



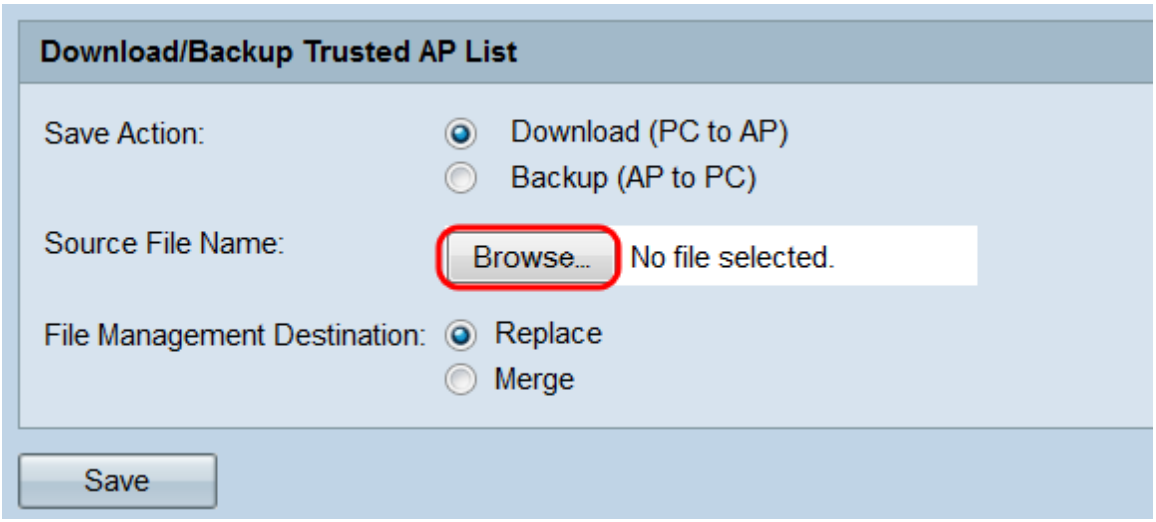
Schritt 2: Wählen Sie im Feld *Aktion speichern* eine der folgenden Optionsschaltflächen:

·Download (PC an AP): Wählen Sie diese Option aus, wenn Sie eine vorhandene Liste vertrauenswürdiger APs von Ihrem PC auf den WAP herunterladen möchten.

·Backup (AP to PC) - Wählen Sie diese Option aus, wenn Sie die Liste der vertrauenswürdigen Access Points auf Ihrem PC sichern möchten. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 5 fort.

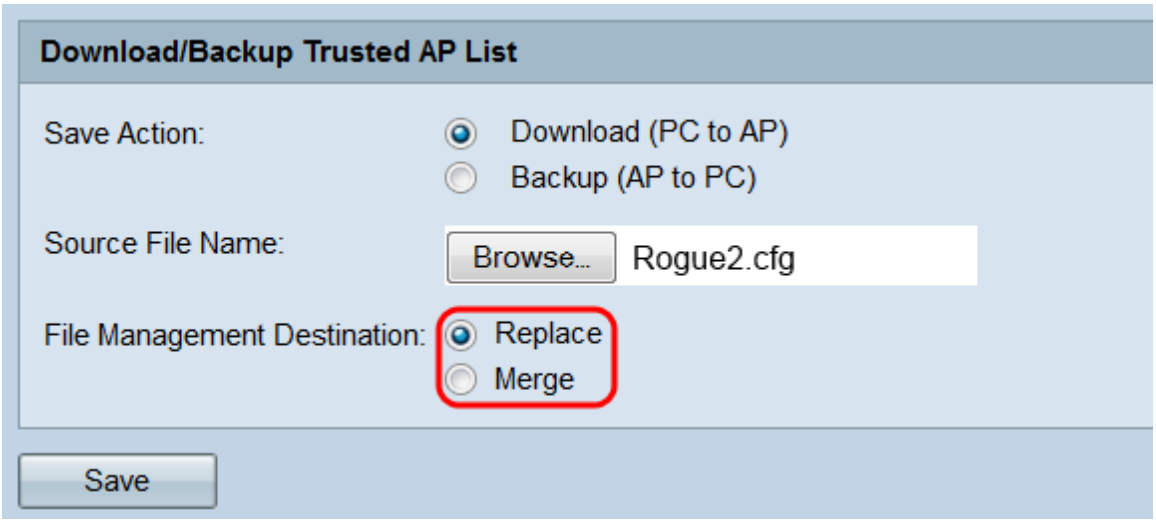


Schritt 3: Wenn Sie im vorherigen Schritt **Download (PC zu AP)** ausgewählt haben, klicken Sie auf die **Schaltfläche Durchsuchen..** im Feld *Quelldateiname*, um die vertrauenswürdige AP-Listendatei auf Ihrem PC auszuwählen.

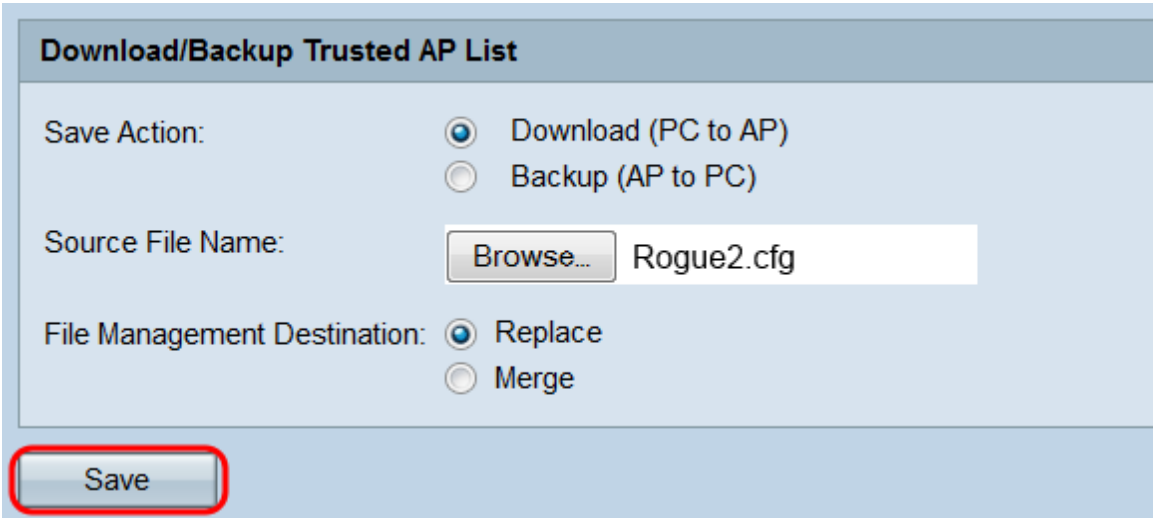


Hinweis: Die Datei muss in .cfg enden.

Schritt 4: Wählen Sie im Feld *Dateiverwaltungs-Ziel* entweder die Optionsschaltflächen **Ersetzen** oder **Zusammenführen aus**. **Replace** bewirkt, dass die heruntergeladene Datei die bestehende vertrauenswürdige AP-Liste auf dem WAP vollständig überschrieben, während **Merge** nur die neuen APs in der Datei zur Liste der vertrauenswürdigen APs hinzufügt.



Schritt 5: Klicken Sie auf **Speichern**. Je nach Auswahl im Feld *Save Action* (*Aktion speichern*) sichert der WAP entweder die Liste der vertrauenswürdigen Access Points auf Ihrem PC oder lädt die angegebene Liste der vertrauenswürdigen Access Points auf den WAP herunter.



Schritt 6: Wenn Sie eine Sicherung durchführen, wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, die Liste der vertrauenswürdigen Access Points auf Ihrem Computer zu speichern. Wenn Sie die Datei herunterladen, wird ein Popup-Fenster angezeigt, das angibt, dass die Übertragung erfolgreich war. Klicken Sie auf **OK**.