

Erstellen oder Importieren einer Liste vertrauenswürdiger Access Points auf einem Wireless Access Point (WAP)

Ziel

Ein Rogue Access Point (AP) ist ein Access Point, der ohne Zustimmung des Netzwerkadministrators in einem sicheren Netzwerk installiert wird. Nicht autorisierte APs können eine Sicherheitsbedrohung darstellen, da jeder, der einen Wireless-Router im Netzwerkbereich installiert, möglicherweise Zugriff auf Ihr Netzwerk erhält. Die Seite zur Erkennung nicht autorisierter APs im webbasierten Dienstprogramm des AP enthält Informationen über die Wireless-Netzwerke, die sich in Reichweite befinden.

Mithilfe einer Liste vertrauenswürdiger APs können Administratoren anhand der Details in der Liste erkannter nicht autorisierter APs die APs verfolgen, denen ein Administrator vertraut.

In diesem Artikel erfahren Sie, wie Sie eine AP-Liste auf einem Access Point erstellen, importieren und herunterladen.

Anwendbare Geräte

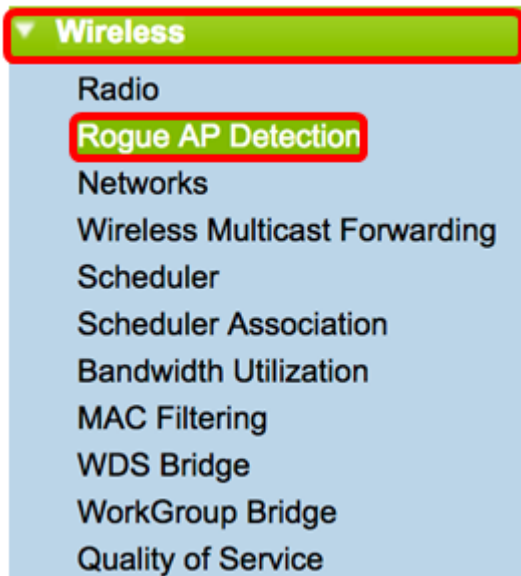
- Serie 100 - WAP121, WAP150
- Serie 300
- Serie 500

Softwareversion

- 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

Erstellen einer vertrauenswürdigen AP-Liste

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, und wählen Sie **Wireless > Rogue AP Detection** aus.



Schritt 2: 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.

Hinweis: Durch das Vertrauen auf einen Access Point wird dieser nur der Liste hinzugefügt und hat keine Auswirkungen auf den Betrieb des Access Points. Die Listen sind organisatorische Instrumente, die für weitere Maßnahmen genutzt werden können.

Folgende Informationen zu den erkannten Access Points werden angezeigt.

- MAC-Adresse - Die MAC-Adresse des nicht autorisierten Access Points.
- Radio - Das physische Radio auf dem nicht autorisierten Access Point, dem Sie beitreten können.
- Beacon-Intervall - Das Beacon-Intervall, das vom nicht autorisierten Access Point verwendet wird. Jeder Access Point sendet in regelmäßigen Abständen Beacon-Frames, um die Existenz seines Wireless-Netzwerks anzukündigen.
- Type (Typ): Der Typ des erkannten Geräts. Kann entweder AP oder Ad-hoc sein.
- SSID - Der Service Set Identifier (SSID) des nicht autorisierten Access Points, auch als Netzwerkname bezeichnet.
- Privacy (Datenschutz): Gibt an, ob Sicherheit auf dem nicht autorisierten Access Point aktiviert ist. Aus zeigt an, dass der nicht autorisierte Access Point keine Sicherheitseinstellungen aktiviert hat, während On anzeigt, dass die Sicherheitsmaßnahmen für den nicht autorisierten Access Point aktiviert sind.
- WPA: Gibt an, ob die WPA-Sicherheit (Wi-Fi Protected Access) für den nicht autorisierten Access Point aktiviert ist.
- Band - Der IEEE 802.11-Modus, der auf dem nicht autorisierten Access Point verwendet wird. Es kann entweder 2,4 GHz oder 5 GHz sein.
- Channel (Kanal): Zeigt den Kanal an, auf dem der erkannte Access Point derzeit sendet.
- Rate (Rate) - Zeigt die Geschwindigkeit an, mit der der erkannte AP aktuelle Broadcasts in Mbit/s aussendet.
- 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 in regelmäßigen Abständen von einem AP übertragen, um das Vorhandensein des Wireless-Netzwerks anzukündigen.

- 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.

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

Schritt 3: (Optional) Die Tabelle der Liste vertrauenswürdiger APs wird ausgefüllt, sobald ein WAP vertrauenswürdig ist. Um einen Access Point aus der Liste zu entfernen, klicken Sie auf **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

Schritt 4: (Optional) Klicken Sie im Bereich "Download/Backup Trusted AP List" (Vertrauenswürdige AP-Liste herunterladen/sichern) auf ein Optionsfeld, um entweder eine Konfigurationsdatei vom PC zum Access Point herunterzuladen oder die Liste vom Access Point auf den PC herunterzuladen. Wenn Sie Download ausgewählt haben, fahren Sie mit dem nächsten Schritt fort. Wenn Sie **Backup** ausgewählt haben, fahren Sie mit [Schritt 7 fort](#).

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

Schritt 5: Klicken Sie im Bereich Source File Name (Quelldateiname) auf **Choose File (Datei auswählen)**, um eine Datei auf Ihrem PC zum Herunterladen an den AP auszuwählen.

Hinweis: In diesem Beispiel wird Rogue1.cfg ausgewählt.

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

Schritt 6: Klicken Sie im Bereich File Management Destination (Dateiverwaltungs-Ziel) auf ein Optionsfeld, um die Datei entweder zu ersetzen oder mit der vorhandenen Liste zusammenzuführen. Folgende Optionen stehen zur Verfügung:

- Replace (Ersetzen): Importiert die Listen und ersetzt den Inhalt der Liste der vertrauenswürdigen Access Points.
- Zusammenführen: Importiert die Liste und fügt die APs in der importierten Datei den APs hinzu, die derzeit in der Liste der vertrauenswürdigen Access Points angezeigt werden.

Hinweis: In diesem Beispiel wird Replace ausgewählt.

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

[Schritt 7:](#) Klicken Sie auf **Speichern**.

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

Sie haben jetzt erfolgreich eine Liste vertrauenswürdiger Access Points auf einem WAP erstellt, gesichert und importiert.