

Rilevamento di punti di accesso non autorizzati sui punti di accesso WAP351 e WAP371

Obiettivo

Un punto di accesso non autorizzato è un punto di accesso che è stato installato in una rete senza esplicita autorizzazione da parte di un amministratore di sistema. I punti di accesso non autorizzati rappresentano una minaccia per la sicurezza in quanto chiunque abbia accesso all'area può installare un punto di accesso wireless che potrebbe consentire l'accesso alla rete a utenti non autorizzati. La pagina *Rilevamento access point non autorizzati* visualizza le informazioni su questi access point. All'elenco punti di accesso attendibili è possibile aggiungere qualsiasi punto di accesso autorizzato.

L'obiettivo del documento è spiegare come rilevare i punti di accesso non autorizzati sui punti di accesso WAP351 e WAP371.

Dispositivi interessati

- WAP351
- WAP371

Versione del software

- 1.0.0.39 (WAP351)
- 1.2.0.2 (WAP371)

Configurazione rilevamento punti di accesso non autorizzati

Nota: Per configurare il rilevamento di un punto di accesso non autorizzato per una radio, è necessario che la radio sia prima abilitata nella sezione **Wireless > Radio**. Per ulteriori informazioni, consultare gli articoli [Configurazione delle impostazioni radio base su WAP131 e WAP351](#) e [Impostazioni radio base su WAP371](#).

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Wireless > Rilevamento punti di accesso non autorizzati**. Viene visualizzata la finestra *Rogue AP Detection*:

Rogue AP Detection

Refresh

AP Detection for Radio 1 (2.4 GHz): Enable

AP Detection for Radio 2 (5 GHz): Enable

Save

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates

Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel

Download/Backup Trusted AP List

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

Source File Name: No file selected.

File Management Destination: Replace Merge

Save

Passaggio 2. Selezionare le caselle di controllo *Rilevamento access point per radio 1* o *Rilevamento access point per radio 2* per selezionare le interfacce radio su cui si desidera abilitare il rilevamento access point non autorizzato. Su WAP351, Radio 1 è in grado di rilevare solo i punti di accesso nella gamma di 2,4 GHz, mentre Radio 2 è in grado di rilevare solo i punti di accesso nella gamma di 5 GHz. Su WAP371, Radio 1 può rilevare solo access point nella gamma 5 GHz e Radio 2 può rilevare solo access point nella gamma 2.4 GHz.

Rogue AP Detection

Refresh

AP Detection for Radio 1 (2.4 GHz): Enable

AP Detection for Radio 2 (5 GHz): Enable

Save

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates

Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel

Download/Backup Trusted AP List

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

Source File Name: No file selected.

File Management Destination: Replace Merge

Save

Passaggio 3. Fare clic sul pulsante **Save** per abilitare il rilevamento dei punti di accesso non autorizzati per le interfacce radio selezionate.

Rogue AP Detection

Refresh

AP Detection for Radio 1 (2.4 GHz): Enable

AP Detection for Radio 2 (5 GHz): Enable

Save

Detected Rogue AP List

Action	MAC Address	Radio	Beacon Interval (milliseconds)	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
--------	-------------	-------	--------------------------------	------	------	---------	-----	------	---------	------	--------	---------	-------------	-------

Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
--------	-------------	-------	------	------	---------	------	---------

Download/Backup Trusted AP List

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

Source File Name: No file selected.

File Management Destination: Replace Merge

Save

Passaggio 4. Se si abilita il rilevamento di punti di accesso non autorizzati, verrà visualizzata una finestra popup che indica che tutti i client attualmente connessi verranno disconnessi. Fare clic su **OK** per continuare.

Rogue AP Detection

Refresh

AP Detection for Radio 1 (2.4 GHz): Enable

AP Detection for Radio 2 (5 GHz): Enable

Save

Detected Rogue AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
--------	-------------	-------	------	------	---------	------	---------	------	--------	---------	-------------	-------

Trusted AP List

Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
--------	-------------	-------	------	------	---------	------	---------

Download/Backup Trusted AP List

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

Source File Name: No file selected.

File Management Destination: Replace Merge

Save

Confirm

⚠ Enabling radio for AP Detection. All clients will be disassociated. This may take a few seconds.

OK Cancel

Una volta abilitato il rilevamento di punti di accesso non autorizzati, tutti i punti di accesso rilevati verranno visualizzati nell'*elenco dei punti di accesso non autorizzati rilevati*.

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

Vengono visualizzate le seguenti informazioni per i punti di accesso rilevati:

·Azione: facendo clic sul pulsante **Trust** in questo campo, il punto di accesso

corrispondente viene aggiunto all'*elenco di punti di accesso attendibili* e rimosso dall'elenco di punti di accesso non autorizzati *rilevati*.

- Indirizzo MAC — visualizza l'indirizzo MAC del punto di accesso rilevato.
- Radio: indica la radio del WAP su cui è stato rilevato il punto di accesso.
- Intervallo beacon: visualizza l'intervallo del beacon in millisecondi utilizzato dall'access point rilevato. I frame dei beacon vengono trasmessi da un punto di accesso a intervalli regolari per annunciare l'esistenza della rete wireless. Il tempo predefinito per l'invio di un frame di beacon è una volta ogni 100 millisecondi.
- Type - Visualizza il tipo della periferica rilevata. Può essere un punto di accesso o ad hoc. Un dispositivo ad hoc utilizza una connessione wireless locale che non implica un punto di accesso wireless.
- SSID — visualizza il SSID del punto di accesso rilevato.
- Privacy: indica se l'access point adiacente è protetto.
- WPA - Indica se la protezione WPA è attivata o disattivata per l'access point rilevato.
- Banda: indica la modalità IEEE 802.11 utilizzata sull'access point rilevato. Può essere 2,4 o 5.
- Canale: visualizza il canale su cui sta trasmettendo l'access point rilevato.
- Velocità: visualizza la velocità di trasmissione in Mbps dell'access point rilevato.
- Segnale: visualizza la potenza del segnale radio proveniente dall'access point.
- Beacon: visualizza il numero totale di beacon ricevuti dal punto di accesso dal momento del primo rilevamento. I frame dei beacon vengono trasmessi da un punto di accesso a intervalli regolari per annunciare l'esistenza della rete wireless. Il tempo predefinito per l'invio di un frame di beacon è una volta ogni 100 millisecondi.
- Ultimo beacon: visualizza la data e l'ora dell'ultimo beacon ricevuto dall'access point.
- Velocità: elenca le velocità supportate e di base dell'access point rilevato (in megabit al secondo).

Passaggio 5. Se si considera attendibile o si riconosce un access point rilevato, fare clic sul pulsante **Trust** accanto alla relativa voce nell'elenco. Il punto di accesso corrispondente viene aggiunto all'*elenco di punti di accesso attendibili* e rimosso dall'*elenco di punti di accesso non autorizzati rilevato*. L'attendibilità di un punto di accesso ne comporta solo l'aggiunta all'elenco e non influisce sul funzionamento del punto di accesso. Gli elenchi sono uno strumento organizzativo che può essere utilizzato per eseguire ulteriori azioni.

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 18:12:55 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

Passaggio 6. Per gestire i punti di accesso attendibili, scorrere verso il basso fino a *Elenco*

punti di accesso attendibili. In questa posizione vengono rilevati i punti di accesso non autorizzati quando si fa clic sui rispettivi pulsanti di **trust**.

Trusted AP List							
Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
<input type="button" value="Untrust"/>	██████████	Radio 1:VAP0	AP	██████████	On	2.4	1
<input type="button" value="Untrust"/>	██████████	Radio 1:VAP0	AP	██████████	Off	2.4	1

Passaggio 7. Se un access point attendibile non è più considerato attendibile, fare clic sul pulsante **Untrust** corrispondente. In questo modo, la password verrà reinserita nell'*elenco dei punti di accesso non autorizzati rilevati*.

Trusted AP List							
Action	MAC Address	Radio	Type	SSID	Privacy	Band	Channel
<input type="button" value="Untrust"/>	██████████	Radio 1:VAP0	AP	██████████	On	2.4	1
<input type="button" value="Untrust"/>	██████████	Radio 1:VAP0	AP	██████████	Off	2.4	1

Backup/download dell'elenco di punti di accesso attendibili

Passaggio 1. Se si desidera scaricare o eseguire il backup dell'elenco dei punti di accesso attendibili, scorrere verso il basso la sezione *Scarica/ esegui backup elenco punti di accesso attendibili*.

Download/Backup Trusted AP List	
Save Action:	<input checked="" type="radio"/> Download (PC to AP) <input type="radio"/> Backup (AP to PC)
Source File Name:	<input type="button" value="Browse..."/> No file selected.
File Management Destination:	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="button" value="Save"/>	

Passaggio 2. Nel campo *Salva azione*, scegliere uno dei pulsanti di opzione:

- Scarica (da PC ad AP): selezionare questa opzione se si desidera scaricare un elenco di punti di accesso attendibili esistente dal PC al WAP.
- Backup (da punto di accesso a PC): selezionare questa opzione se si desidera eseguire il backup dell'elenco di punti di accesso attendibili sul PC. Se si seleziona questa opzione, andare al [passaggio 5](#).

Download/Backup Trusted AP List

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

Source File Name: No file selected.

File Management Destination: Replace
 Merge

Passaggio 3. Se nel passaggio precedente è stato selezionato **Scarica (da PC a punto di accesso)**, fare clic sul pulsante **Sfogli...** nel campo *Nome file di origine* per selezionare il file dell'elenco dei punti di accesso attendibili nel PC.

Download/Backup Trusted AP List

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

Source File Name: No file selected.

File Management Destination: Replace
 Merge

Nota: Il file deve terminare con .cfg.

Passaggio 4. Nel campo *Destinazione gestione file*, selezionare i pulsanti di opzione **Sostituisci** o **Unisci**. **Sostituisci** fa sì che il file scaricato sovrascriva completamente l'elenco dei punti di accesso attendibili esistente sul WAP, mentre **Unisci** aggiunge solo i nuovi punti di accesso del file all'elenco dei punti di accesso attendibili.

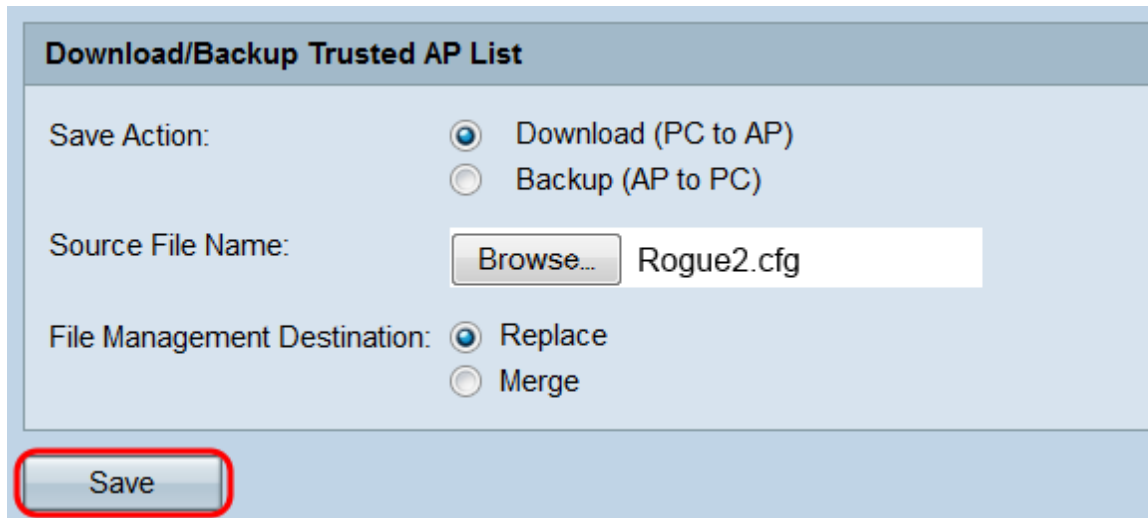
Download/Backup Trusted AP List

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

Source File Name: Rogue2.cfg

File Management Destination: Replace
 Merge

Passaggio 5. Fare clic su **Salva**. A seconda della selezione effettuata nel campo *Salva azione*, il punto di accesso Windows eseguirà il backup dell'elenco dei punti di accesso attendibili nel PC o scaricherà l'elenco dei punti di accesso attendibili specificato nel punto di accesso Windows.



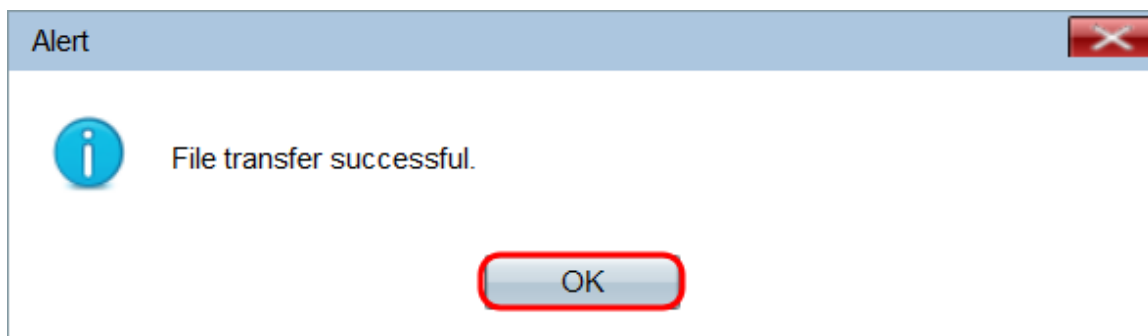
Download/Backup Trusted AP List

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


Source File Name: Rogue2.cfg

File Management Destination: Replace
 Merge

Passaggio 6. Se si sta eseguendo un backup, viene visualizzata una finestra di dialogo che richiede di salvare l'elenco dei punti di accesso attendibili nel computer. Se si sta scaricando il file, viene visualizzata una finestra popup che indica che il trasferimento è stato completato. Fare clic su **OK**.



Alert

 File transfer successful.