ACKSYS
COMMUNICATIONS & SYSTEMS

APPLICATION NOTE

APNUS027 Rogue Device/AP Detection and Containment

June 2023

Content

1. Glossary

WIDS: Wireless Intrusion Detection Systems

WIPS: Wireless Intrusion Prevention Systems

RAP: Rogue Access Point, an Access Point that has been installed on a secure network without explicit authorization from a system administrator.

SNMP: Simple Network Management System

2. Introduction

Internet as service in transportation is offered in order to encourage passengers to use public transport and others use cases.
The goal for this service to improve user experiences and to increase security in data protection but unfortunately it is possible to meet an Access Point installed with no authorization.

One of the most common security threats to enterprise networks is Rogue Access Points installed without the authorization from the IT system administrator on the LAN infrastructure.
This allows unauthorized access to the secured network's wired infrastructure for any wireless user to bypass wireless security controls and monitor network traffic.

Rogue Access Point is an Access Point installed on a network without the network owner's permission in order to collect confidential information. This article explains with details about Rogue Access Point Detection in Wireless Intrusion Detection Settings (WIDS) implemented in WaveOs.

Rogue Access Points are threats for the security of your company and business.

The objective of the Rogue Ap Detector is to protect a WiFi infrastructure and its clients from known attacks at level 2 of the OSI layer. It is part of the Wireless Intrusion Detection System (WIDS), as the first step of the network access control.

3. Concepts

Rogue AP Attack

The Rogue Access Point is installed on a secure network without explicit authorization from a local network administrator, whether added by a well-meaning employee or by a malicious attacker.

Rogue Access Points are often named "Evil Twin". In the IEEE 802.11 standard for Wi-Fi, there are only two identifiers that allow users to recognize an AP: the Service Set Identifier (SSID) and the Basic Service Set Identifier (BSSID). However, these identifiers can be easily spoofed. Cloning a legitimate AP generates an Evil Twin AP.

The "Evil Twins" or RAP can exist in two forms:

- coexistence
- replacement.

In both cases the RAPs use the same SSID as the allowed APs.

In the first case (coexistence), the legitimate AP and the Evil Twin coexist in the same place.
The attacker increases the signal strength of the RAP to force users to connect to it, as the IEEE 802.11 standard states that WLAN clients must connect to the AP with the strongest signal.

In the "Replacement" type, the Evil Twin replaces the legitimate access point by shutting it down, thanks to an active attack on it. To remain undetectable by its victims, the RAP must have a valid Internet connection (or connectivity to the same network as the access point) while in the former case, it could relay packets through the legitimate AP, as long as it can connect to the latter.

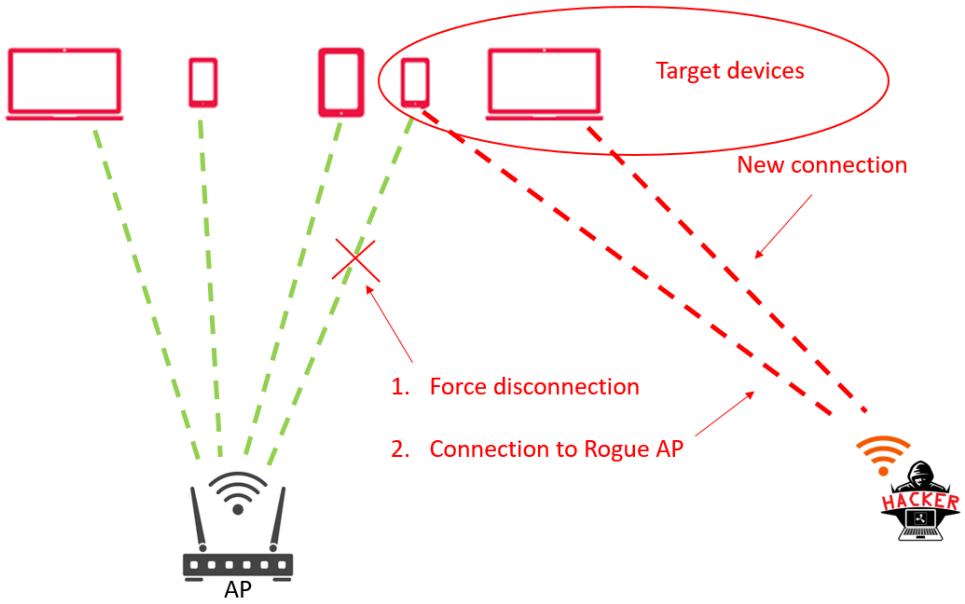


Figure 1: Rogue Access Point Coexistence concept

Another case is a misconfigured AP, thus considered as a weakness. This type of RAP, as the name suggests, is an AP that has been improperly configured regarding RAP detector parameters. In this case it's not an attack but a vulnerability. Anyway the RAP detector will trigger an alert.

This can happen when, for example, an administrator does not use strong authentication and encryption settings, leading to a network that can be easily compromised.

How do Rogue APs impact the WLAN?

Rogue access points undermine the security of an enterprise network by potentially allowing unchallenged access to the network by any user or client in the nearby area or redirect end users to untrusted networks.

Rogue access points can impact your wireless network in many ways:

- They can create security holes in your network:
    - By allowing a hacker to conduct a "man-in-the-middle" attack, where the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is tempered by the attacker.
    - Send fake SSIDs advertising attractive features such as free Internet connectivity. Once a user connects, the fake SSID is added to the client's wireless configuration and the client begins to broadcast the fake SSID, thereby infecting other clients.
    - Provide a conduit for the theft of company information.
    - Install malware on passengers' smartphones and laptops
- They can negatively impact your company reputation and workflow:
    - When users try to connect to them thinking they are not valid access points and they cannot get to the proper resources due to VLAN differences, which can also generate a lot of help desk calls to your IT department.

Rogue AP Detector concept

The RAP detection module uses the classic whitelist approach, where we use information from the configuration profile regarding SSIDs and their expected BSSIDs.
The parameters scanned by the RAP Detector are:

- SSID,
- BSSIDs,
- Channel,
- Encryption,
- Signal strength.

Since SSID or BSSID are likely to be bypassed (BSSID spoofing: RAP emitting the same SSID and MAC address as legitimate ap), we also compare the type of encryption used by the access point. (OPEN = Open, WEP = Wired Equivalent Privacy, WPA = Wi-Fi Protected Access version 1, 2 and 3).

Another heuristic implemented by the detection module is the variation in signal strength. The algorithm uses a user-expected authorized RSSI (auth_rssi) for the authorized AP, and the RSSI value read must fall within the allowable range of [auth_rssi - delta; auth_rssi + delta]. (The value of the delta is 15db.) An alert is triggered when the RSSI read leaves this interval.

Rogue AP detector

Rogue access point detection is an important component in securing your wireless network. Rogue access point detection does two things, detection and alert. Whatever you decide to install on your network, it has to have the ability (from the beginning of your RF design) to be able to detect rogue access points and alert the network administrators.

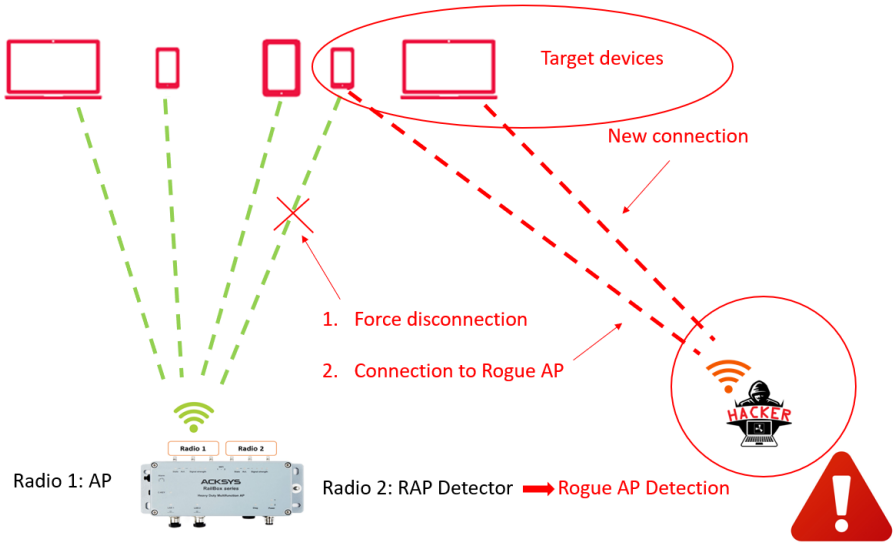


Figure 2: Rogue Access Point Detector concept: the second radio card is listening for Rogue APs

The Rogue AP Detector is monitoring the beacons emitted by the neighbour APs and check for the configured SSID if the MAC addresses of senders, the channel on which the beacons are emitted, the encryption type and the RSSI correspond to the configured parameters.
If not, it raises an alert to inform the operator. For example, you can send a trap in case of Rogue detection (in Events section, the 'Security alert' triggers the sending of a trap:

NAMES	EVENTS	EVENTS TRIGGER	ON DELAY	OFF DELAY	ACTIONS	PARAM.#1	PARAM.#2	EXTRA PARAMS
trap	Security alert		0	0	SNMP trap			192.168.1.20,public

A log is automatically generated so can be also sent to WaveManager if the syslog server IP address is defined in the Logs Settings (tab TOOLS).

4. Acksys Rogue AP Detector solution

To monitor the Customer Wireless Network, ACKSYS has developed Rogue AP detector to monitor unusual Activity and so ensure secure Network.
Rogue Ap Detector implemented in WaveOs performs these series of actions:

- Configure the expected status of the network,
- Act as a passive radar,
- Raise an alarm in case an anomaly is detected, compared to expected status.

The Rogue AP detection module uses the classic whitelist approach, where we use information from the configuration profile regarding SSIDs and their expected BSSIDs.

Wireless radios automatically scan the RF spectrum for other access points transmitting in the same spectrum. The RF scans discover third-party transmitters in addition to other ACKSYS radios in order to track any suspects potential rogues based on:

- SSID,
- BSSIDs,
- Channel,
- Encryption,
- Signal strength

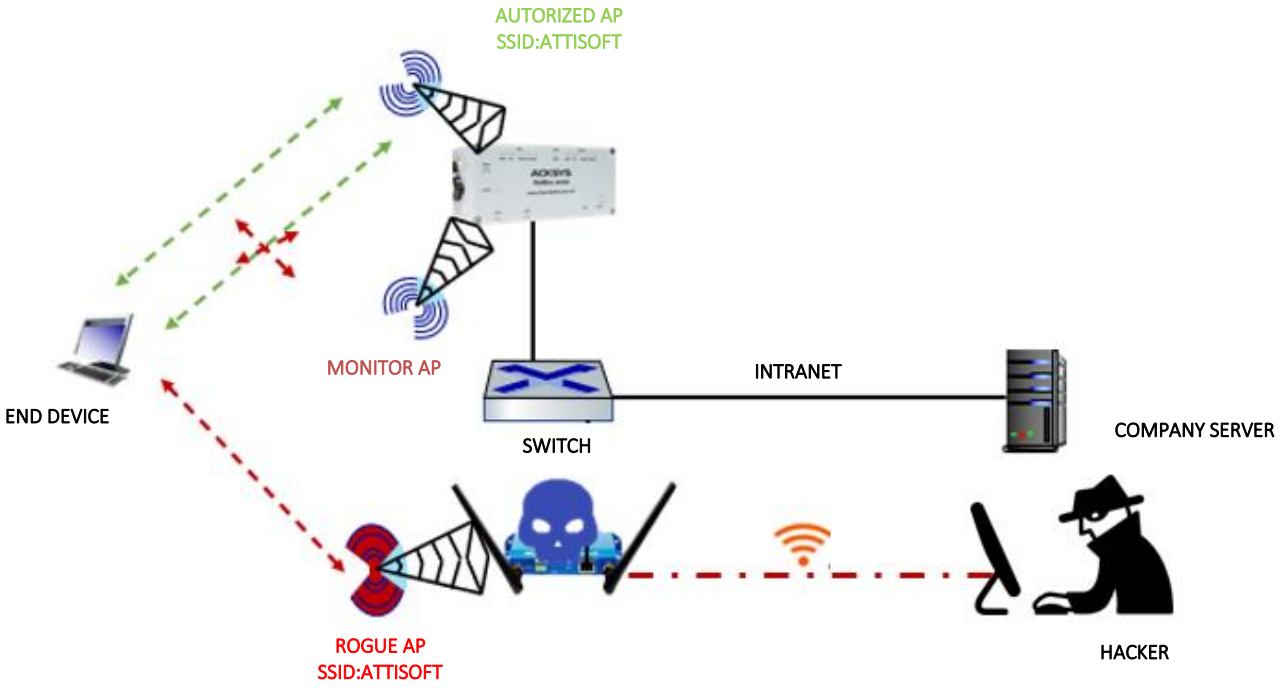
5. Installation Overview and Prerequesites

Before we begin, let's overview the configuration that we are attempting to achieve and the prerequisites that make it possible.

- Any Acksys Routers with two radio WIFI cards with a firmware 4.16.0.1 or more:
  - 1 radio WIFI in Access Point role
  - 1 radio configured in Rogue AP detector
- Any other WIFI device configure in the Access Point to play the malicious role
- A PC to configure the Router

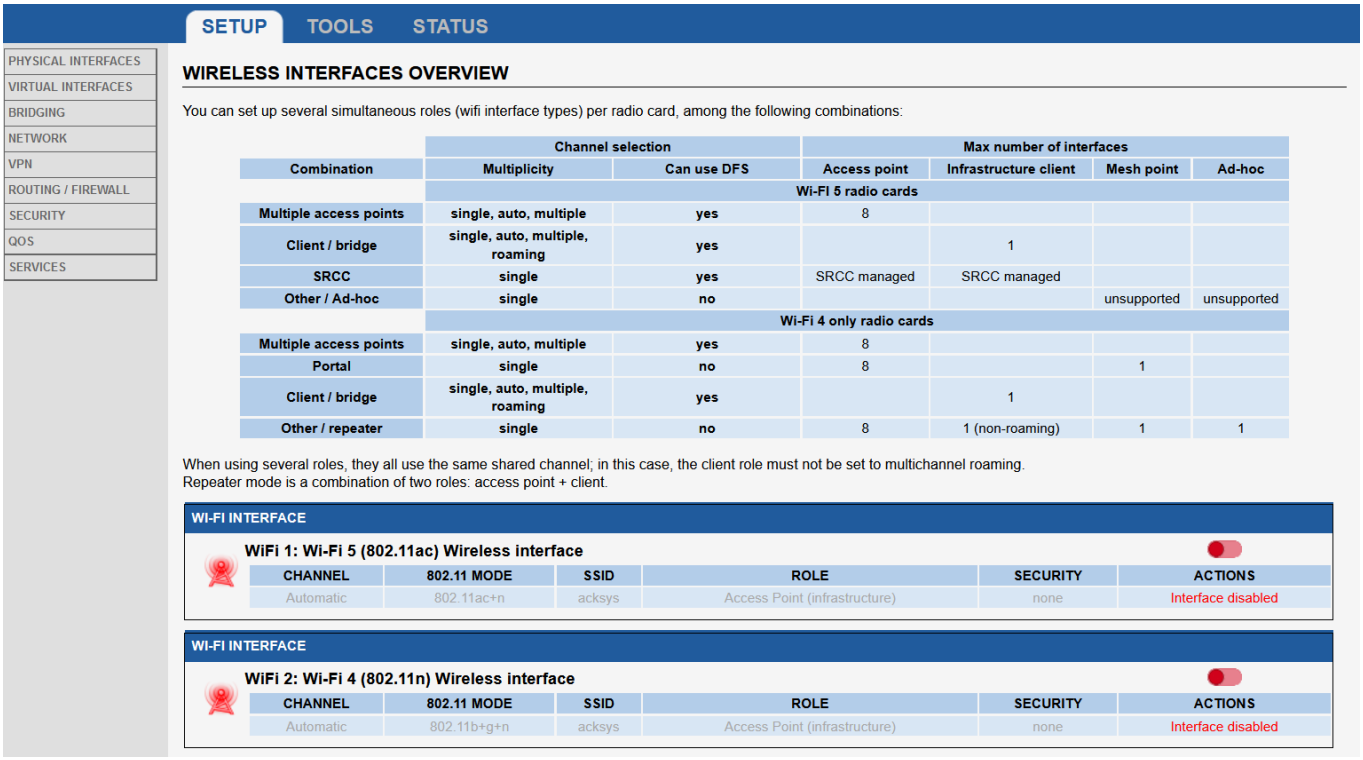
6. Configuration architecture

Let's overview the configuration that we are attempting to achieve and the prerequisites that make it possible to configure the Rogue AP detection and containment.



7. Routers configuration

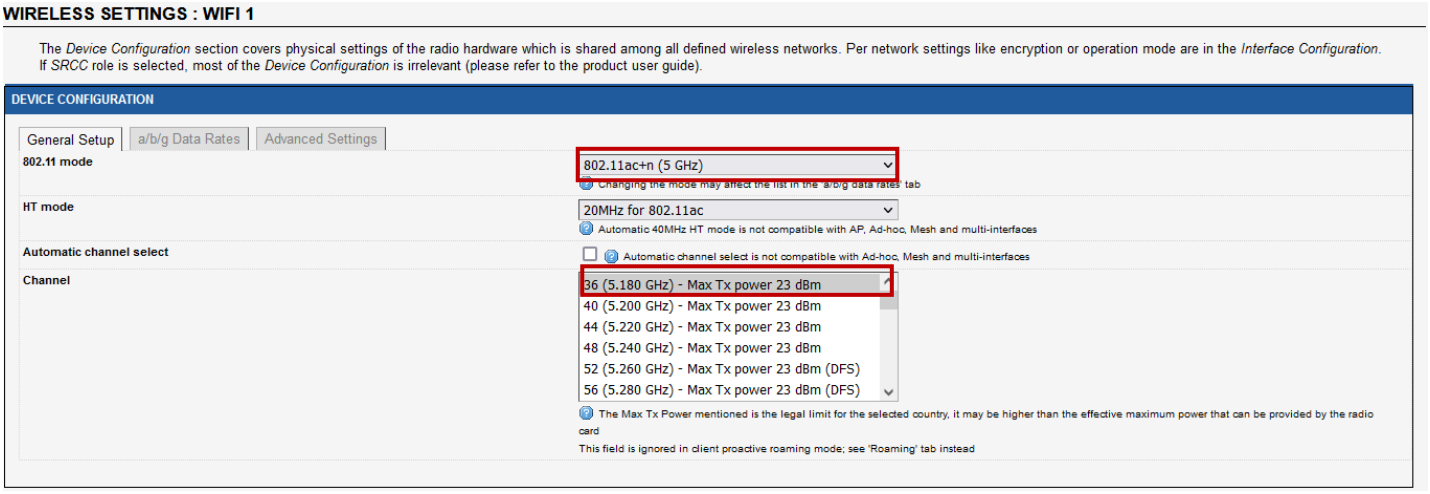
If you have familiarized yourself with the configuration scheme and have all of the devices in order, we can start configuring the routers using instructions provided in this section.



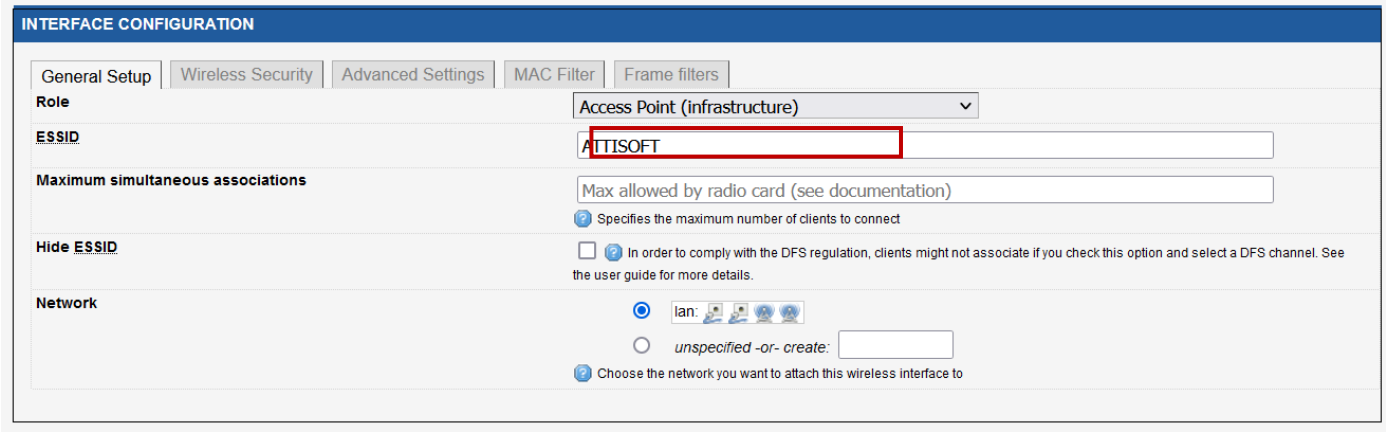
RAILBOX Radio 1:Configuring Authorized or Trusted AP

Login to the router's WebUI and let configure Radio 1 in AP role with the complete information provided in this test.

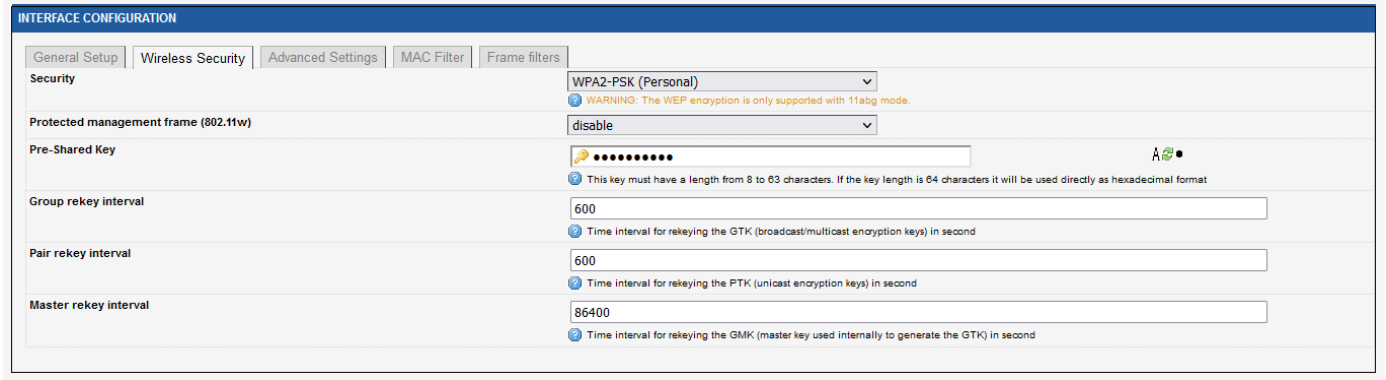
Go to **Tool → Physical Interfaces → Wireless Configuration> Access Point>Apply & save**. Enter a name for the new instance and click the "Add" button



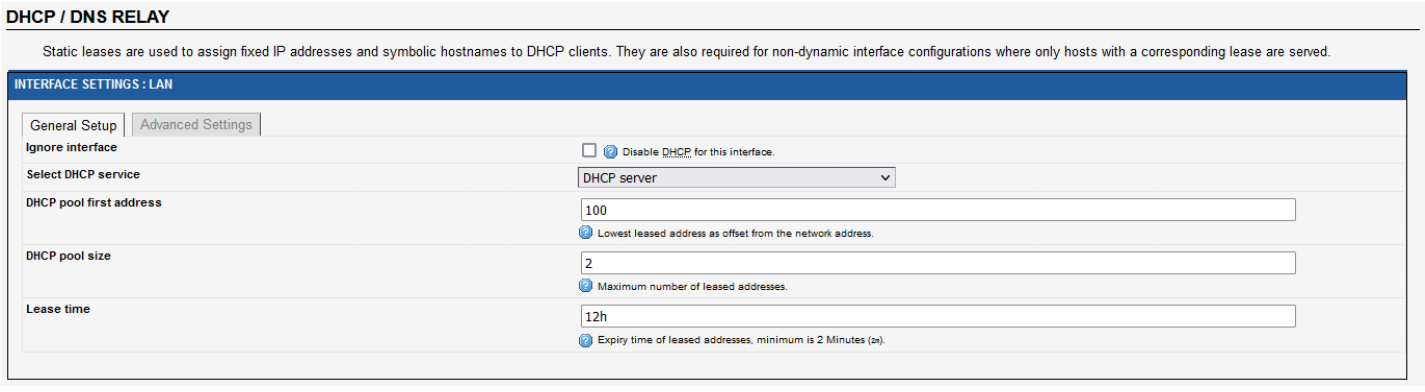
- INTERFACE CONFIGURATION
  - General Setup



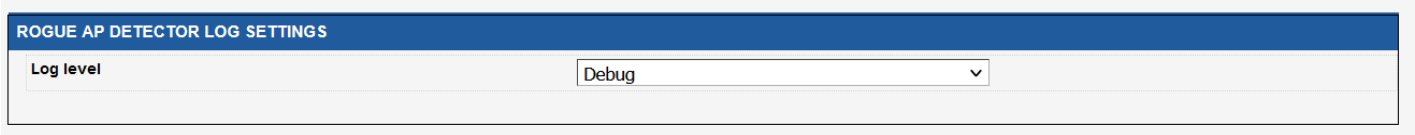
- Click the "Wireless Security" button and chose :
  - Security: WPA2-PSK (Personal in my test)
  - Pre-Shared Key: type your own password
  - Group rekey interval: 600 by default
  - Pair rekey interval:600 by default
  - Master rekey interval:86400 default



Go to **Tool → Services → DHCP/DNS Relay**. Enter the provide information below



Go to **Tool → Logs Setting →Log Level →Rogue AP detector Log Settings →Log level: Debug**

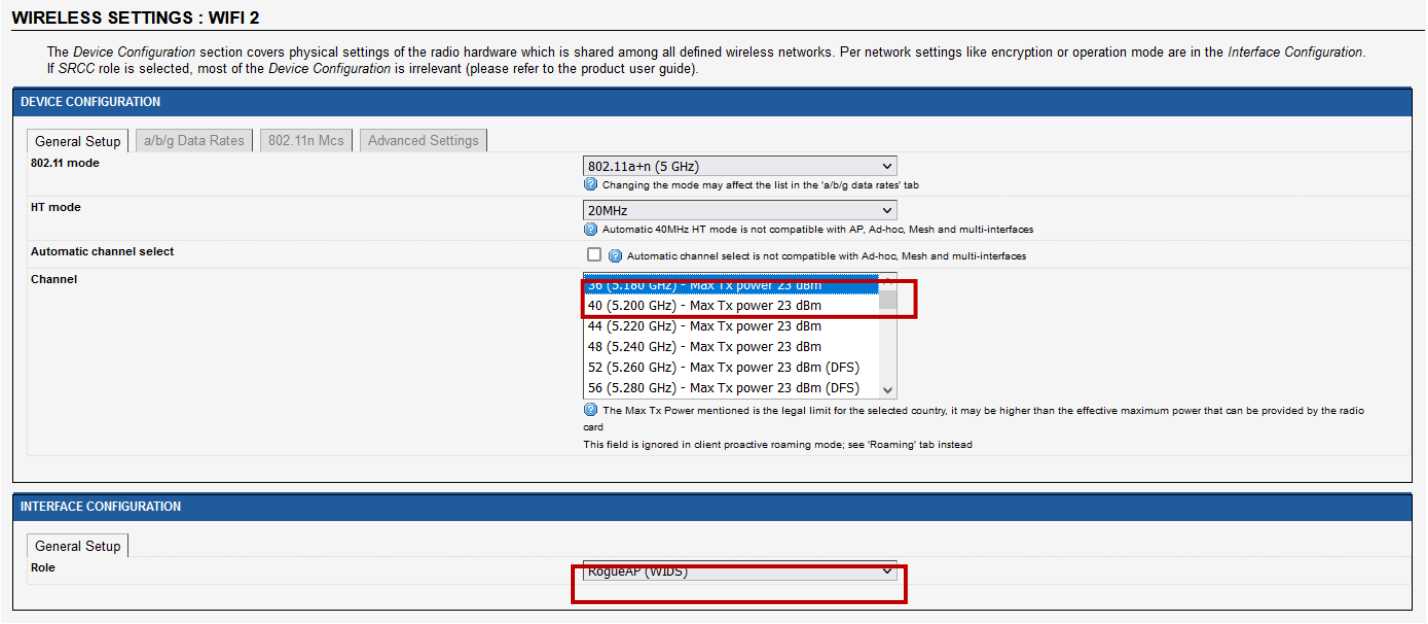


- Apply & save.

RAILBOX Radio2 : Configuring Rogue AP Detector

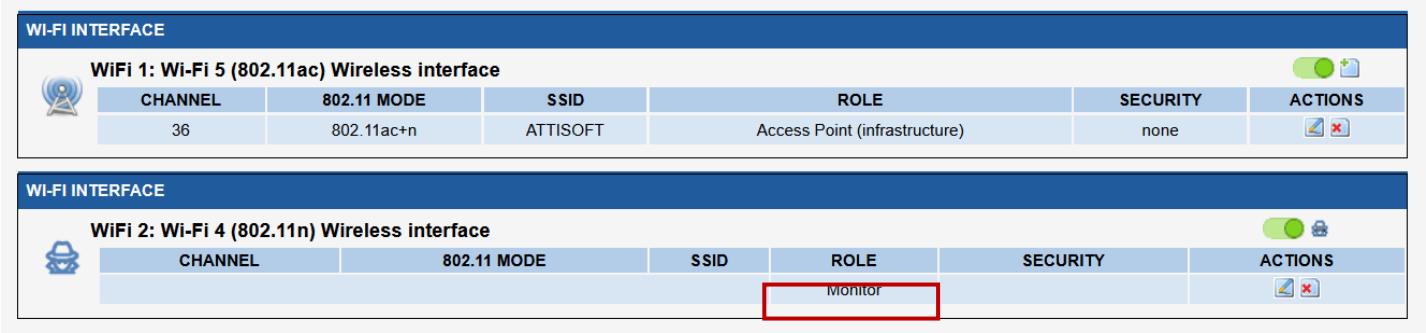
Login to the router's WebUI and let configure Radio 2 in Rogue AP role:

go to Tool → Physical Interfaces → Interface Configuration→ RogueAP (WIDS) →Apply & save

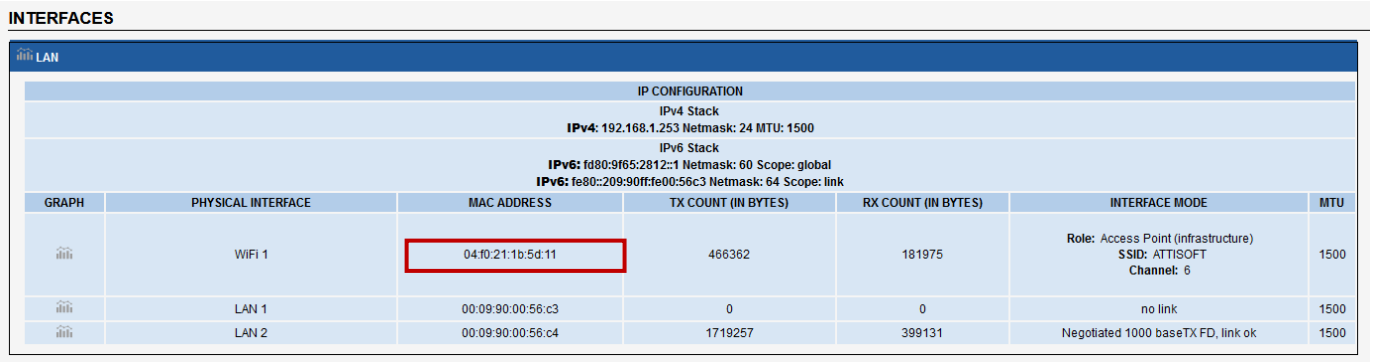


Let look at GUI Tools→Physical

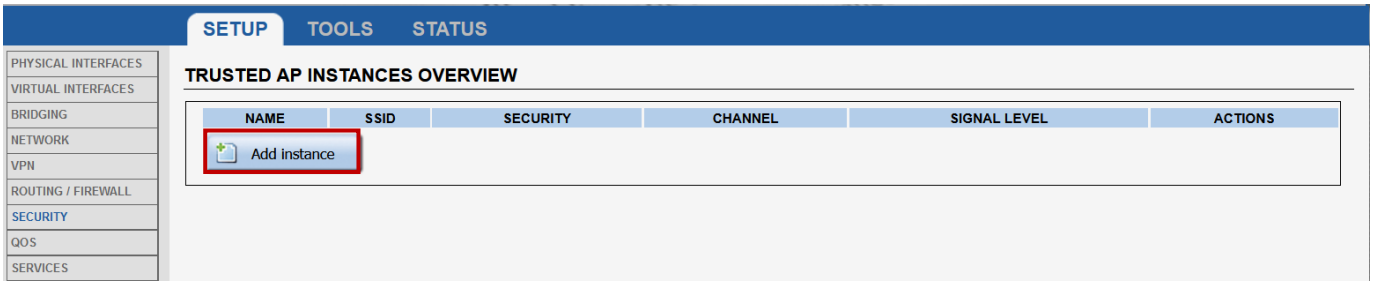
We have WIFI1 configured in AP and WIFI2 in Monitor



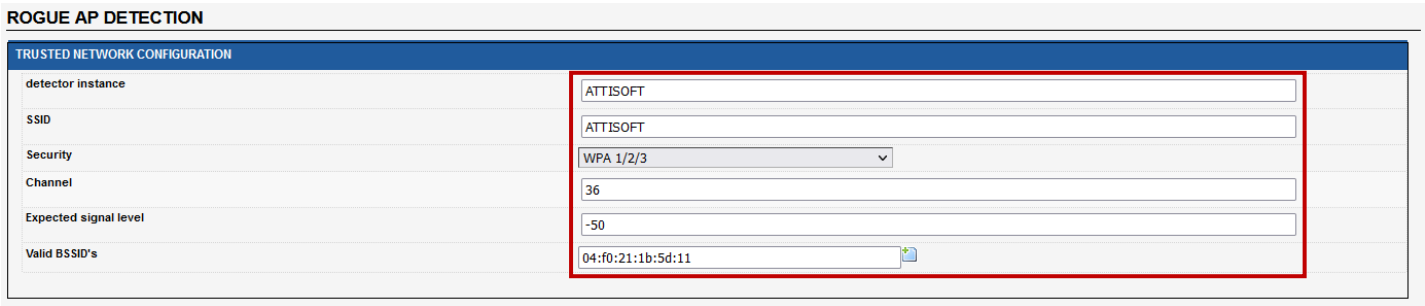
In the configuration of the Rogue AP detector , we need to provide the mac address of the Authorized AP therefore, let go in Gui, Status → Network



let go in Gui, Setup → Security → Click on Add instance to create RogueAP instance.



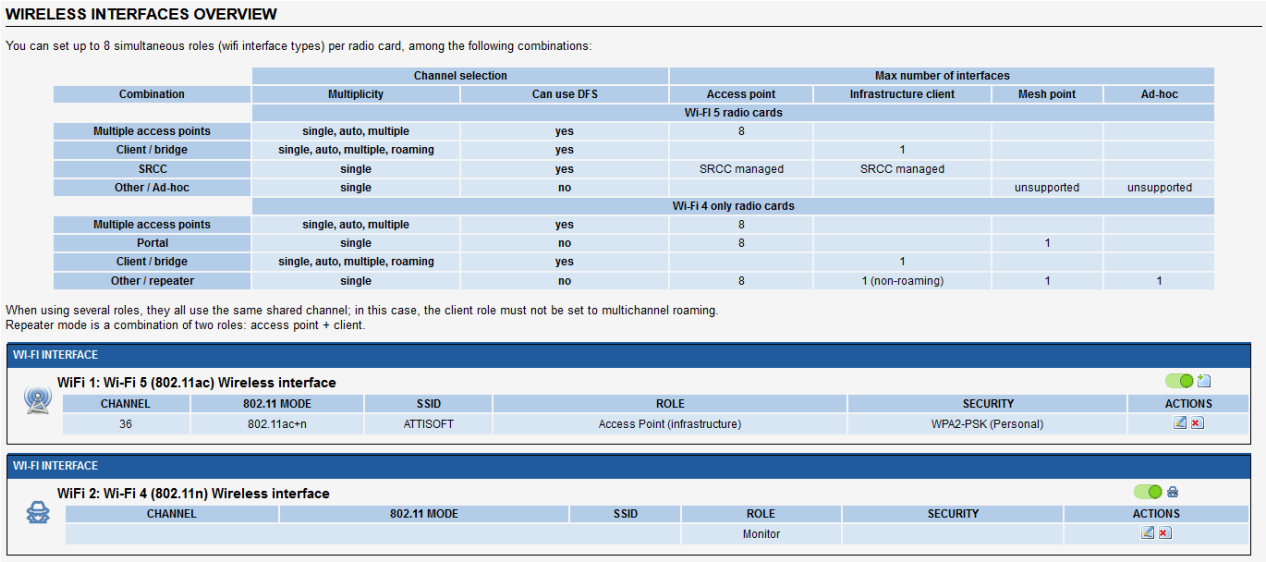
As soon as clicking on "Add instance button" You will be redirected to the settings **Security window** where you can start configuring the Rogue AP instance with the information provided below:



- Below are explanations of the parameters highlighted in the figure above.
  - **Detector instance**– ATTISOFT
  - **SSID** - ATTISOFT to monitor
  - **Security** – Open in this test but invite partner to use a strong encryption
  - **Channel** – 36
  - **Expected signal level** -50dBm ,the minimum signal level to monitor
  - **Valid BSSI** - **04:f0:21:1b:5d:11** (BSSIDs of the allowed AP or list of SSID)
  - **Click on Save and Apply**

WIRELESS INTERFACES OVERVIEW

The Wireless Overview on the RailBox shows the both radio configuration where WIFI1 is configure in AP role where the WIFI2 in configure in Monitor Role (Rogue AP).



WIRELESS INTERFACES OVERVIEW

You can set up to 8 simultaneous roles (wifi interface types) per radio card, among the following combinations:

Combination	Channel selection		Max number of interfaces			
	Multiplicity	Can use DFS	Access point	Infrastructure client	Mesh point	Ad-hoc
			Wi-Fi 5 radio cards			
Multiple access points	single, auto, multiple	yes	8			
Client / bridge	single, auto, multiple, roaming	yes		1		
SRCC	single	yes	SRCC managed	SRCC managed		
Other / Ad-hoc	single	no			unsupported	unsupported
			Wi-Fi 4 only radio cards			
Multiple access points	single, auto, multiple	yes	8			
Portal	single	no	8		1	
Client / bridge	single, auto, multiple, roaming	yes		1		
Other / repeater	single	no	8	1 (non-roaming)	1	1

When using several roles, they all use the same shared channel; in this case, the client role must not be set to multichannel roaming.
Repeater mode is a combination of two roles: access point + client.

WI-FI INTERFACE

WiFi 1: Wi-Fi 5 (802.11ac) Wireless interface

CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
36	802.11ac+n	ATTISOFT	Access Point (infrastructure)	WPA2-PSK (Personal)	

WI-FI INTERFACE

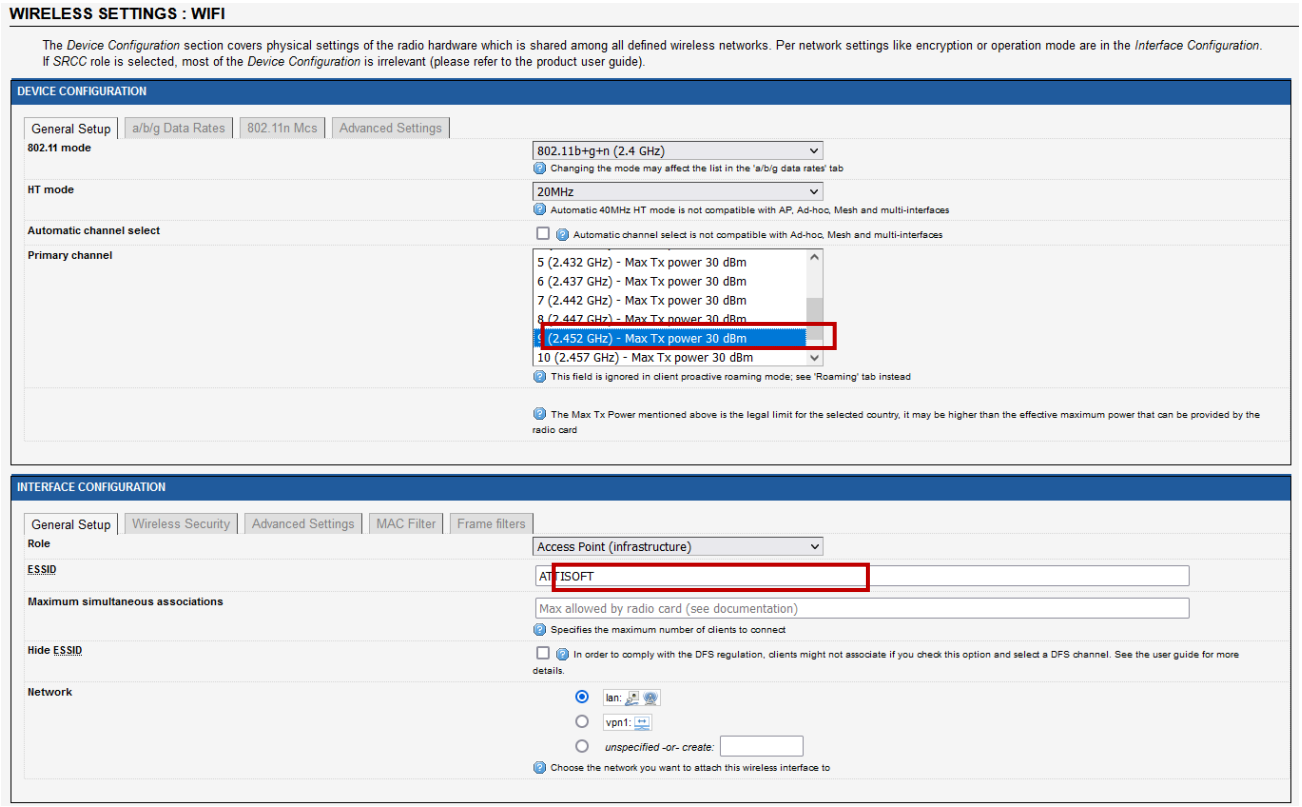
WiFi 2: Wi-Fi 4 (802.11n) Wireless interface

CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
			Monitor		

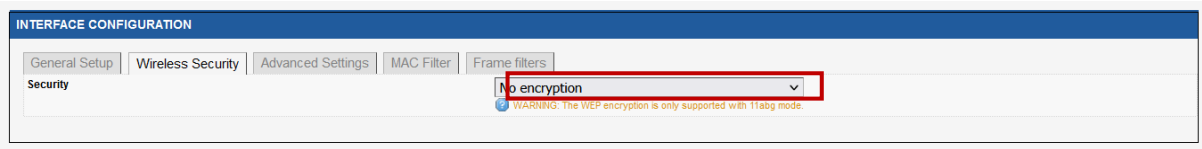
AIRLINK: Configuring Rogue AP

In this test the Acksys Airlink router plays the role of Rogue AP.We will use only the same ESSID ATTISOFT as the authorized AP ESSID.

Go to **Tool → Physical Interfaces → Wireless Configuration> Access Point>Apply & save**. Enter a name for the new instance and click the "Add" button



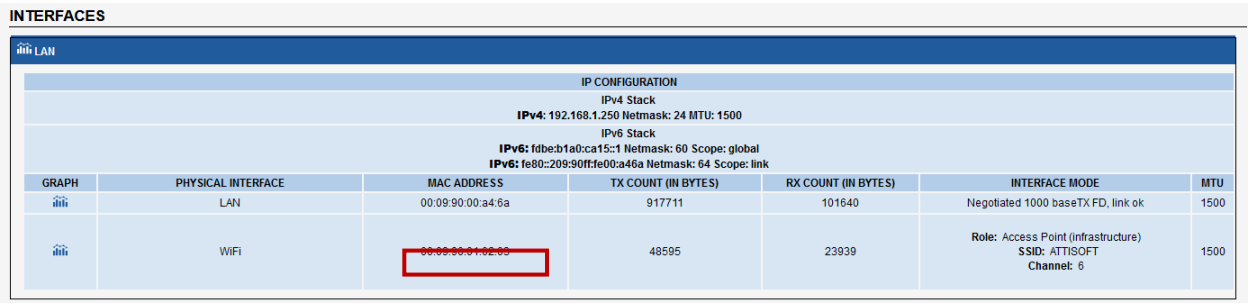
- Click the "Security" button and chose No encryption and apply & save in this example.



- Click the "Advanced" button and chose No encryption and apply & save in this example.
  - Apply & save

NETWORK INTERFACES OVERVIEW

For troubleshoot purpose, we need to know the MAC address used by the Rogue AP therefore in case of Rogue AP detector, we could identify this address. In this case the Rogue AP MAC Address is 00:09:90:01:02:03 as shown on the screenshot below:



INTERFACES

LAN

IP CONFIGURATION						
IPv4 Stack **IPv4:** 192.168.1.250 Netmask: 24 MTU: 1500						
IPv6 Stack **IPv6:** fdbe:b1a0:ca15::1 Netmask: 60 Scope: global **IPv6:** fe80::209:90ff:fe00:a46a Netmask: 64 Scope: link						
GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	LAN	00:09:90:00:a4:6a	917711	101640	Negotiated 1000 baseTX FD, link ok	1500
	WiFi	[redacted]	48595	23939	**Role:** Access Point (infrastructure) **SSID:** ATTISOFT **Channel:** 6	1500

8. Rogue AP Alerts and Logs

To verify the Rogue AP detector features, let have an overview of security logs Status→ Security.

The Rogue AP Detection feature in WaveOs is used to detect unexpected or unauthorized access point installed in a secure network environment.

When the Rogue AP Detector suspects an evil AP, it raises a unique alert. If it detects consequently several times the same potential RAP, it raises an alert on the first detection. If the RAP disappears then is detected again, a new alert is raised.

To check in Rogue AP logs if there are any Rogue AP detected by the router, let go to GUI in **Status → Security**.

We detect in log that the mac address of the Authorized Access Point (**04:F0:21:1B:5D:11**) with a possible Rogue AP with all its information provided to inform the IT Manager to identify the malicious AP is connected 00:09:90:01:02:03.The mac address is identified as the AirLink Router playing the role of the Rogue AP.

Detected Rogue AP

- MAC Address – The MAC Address of the Rogue AP
- SSID – The SSID of the Rogue AP
- Channel – The Channel of the Rogue AP
- Security – The Security method of the Rogue AP
- Signal – The signal level of the Rogue AP

ROGUEAP

EVENTS DETECTED

DATE	EVENT	CHANNEL	MAC
2018-08-16 08:30:46.000000	RogueAP detector service started on Wi-Fi interface wlan1.		
2018-08-16 08:30:49.000000	RogueAP detector service started on Wi-Fi interface wlan1.		
2018-08-16 08:31:03.953863	[6 | ATTISOFT | 00:09:90:01:02:03]Possible Rogue Access Point![Type] Multichannel AP.	6	00:09:90:01:02:03
2018-08-16 08:31:10.198444	[36 | ATTISOFT | 04:F0:21:1B:5D:11]Signal level -32 dBm out of [-65,-35] bounds.	36	04:F0:21:1B:5D:11
2018-08-16 08:31:45.000000	RogueAP detector service started on Wi-Fi interface wlan1.		
2018-08-16 08:31:59.440493	[6 | ATTISOFT | 00:09:90:01:02:03]Possible Rogue Access Point![Type] Multichannel AP.	6	00:09:90:01:02:03
2018-08-16 08:32:05.729270	[36 | ATTISOFT | 04:F0:21:1B:5D:11]Signal level -33 dBm out of [-65,-35] bounds.	36	04:F0:21:1B:5D:11

NOTE:

The Access Point in Monitor mode can perform an RF scan on all channels on each radio to detect all access points in the network. If Rogue APs are detected, they are shown on the Rogue detection logs with this template format: [Channel | ESSID | BSSID]Possible Rogue Access Point![Type] Multichannel AP.

For advanced skills, Rogue AP Detector logs can be seen in CLI with the command below :

```
root@AUTORIZED-AP:~# tail -f /var/log/rogueap.log
[2018-08-16 08:31:44,511] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:44,562] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:44,612] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:44,704] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:44,753] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:44,865] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:44,915] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:44,943] rogueAPDetector[11560] INFO - Changing interface wlan1 to channel 11
[2018-08-16 08:31:59,400] rogueAPDetector[12337] ERROR - [6 | ATTISOFT | 00:09:90:01:02:03]Possible Rogue Access Point![Type] Multichannel AP.
[2018-08-16 08:32:05,689] rogueAPDetector[12337] ERROR - [36 | ATTISOFT | 04:F0:21:1B:5D:11]Signal level -33 dBm out of [-65,-35] bounds.
```

Alerts Managements

The Rogue AP features generated permanent logs from the Rogue AP daemon available on the router in GUI STATUS RogueAP LOG

```
[2018-08-16 08:31:04,210] rogueAPDetector[11560] INFO - SSID : MDY.
[2018-08-16 08:31:04,212] rogueAPDetector[11560] DEBUG - channel 6
[2018-08-16 08:31:04,216] rogueAPDetector[11560] DEBUG - Manufacturer NOT found.
[2018-08-16 08:31:04,217] rogueAPDetector[11560] DEBUG - Ignore unmanaged SSID MDY
[2018-08-16 08:31:04,218] rogueAPDetector[11560] INFO - MDY (Protected) 9c:c9:eb:b0:a9:c1 chan: 6 vendor:Not Found -86 dBm
[2018-08-16 08:31:04,805] rogueAPDetector[11560] INFO - Changing interface wlan1 to channel 7.
[2018-08-16 08:31:05,186] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:05,799] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:05,861] rogueAPDetector[11560] INFO - Changing interface wlan1 to channel 8.
[2018-08-16 08:31:05,870] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:06,890] rogueAPDetector[11560] INFO - Changing interface wlan1 to channel 9.
[2018-08-16 08:31:07,910] rogueAPDetector[11560] INFO - Changing interface wlan1 to channel 10.
[2018-08-16 08:31:08,153] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:08,558] rogueAPDetector[11560] DEBUG - Discard pkt due to channel/freq mismatch.
[2018-08-16 08:31:08,930] rogueAPDetector[11560] INFO - Changing interface wlan1 to channel 11.
[2018-08-16 08:31:09,119] rogueAPDetector[11560] DEBUG - ###[ RadioTap dummy ]###
  version   = 0
  pad       = 0
  len       = 48
  present   = TSFT+Flags+Rate+Channel+dBm_AntSignal+RXFlags+RadiotapNS+Ext
  \Ext       \
   |###[ RadioTap Extended presence mask ]###
   |  present   = b5+b11+b29+Ext
   |###[ RadioTap Extended presence mask ]###
   |  present   = b37+b43+b61+Ext
   |###[ RadioTap Extended presence mask ]###
   |  present   = b69+b75
  mac_timestamp= 11578647989341650944
  Flags     = FCS
  Rate      = 2
  Channel   = 2462
  ChannelFlags= CCK+2GHz
  dBm_AntSignal= -69dBm
  notdecoded= '\x00\x00\x00\xb5\x00\xa4\x01\xba\x02'
```

The template of the differents alerts are formatted like:

- Date: date and time where the RAP was detected,
- Event: type of possible Rogue Access Point,
- Channel: channel on which the SSID is emitted,
- MAC: MAC address of the Access Point emitting the SSID.

There are differents events which can be logged with Rogue AP instance as soon it was enabled:

- **RogueAP detector** service started on Wi-Fi interface wlan xx (This is an information only).
- **Evil Twin, different encryption.**
  The wireless security level is different from the expected value.
- **Multichannel AP.**
  The SSID is detected on a different channel from the configured channel for this instance.
- **Evil Twin, unauthorized BSSID.**
  The BSSID emitting the SSID is not defined in the allowed BSSID list.
- **Strange RSSI.**
  The RSSI value is out of the RSSI range expected for this SSID.

9. SNMP alerts

For SNMP alerts, you can optionally configure Management Information Base (MIB) variables for Rogue AP that appear in SNMP traps.

These variables can return some helpful for the Management of Rogue AP Detector.

	OBJECTS	OID	TYPE	VALUE
CONFIG	fileTransferType	.1.3.6.1.4.1.28097.1.2.8.2.0	INTEGER	wids-config(4)
	configPhyWifiWids	.1.3.6.1.4.1.28097.8.2.1.1.19	INTEGER	0:radio is not reserved for WIDS (default). 1:radio is reserved for rogue AP monitoring
STATUS	statusPhyWifiWids	.1.3.6.1.4.1.28097.7.3.1.9	INTEGER	0:not started. 1:currently monitoring for rogue APs.
	configInterfaceType	.1.3.6.1.4.1.28097.8.3.2.1.3	INTEGER	wifi-monitor(13) if the radio is on listening mode
NOTIFICATION	statusIfWlanMode	.1.3.6.1.4.1.28097.7.2.1.3	INTEGER	monitor(5) if the radio is on listening mode
	nbDescription	.1.3.6.1.4.1.28097.11.255.24.0	DISPLAYSTRING	Any available details about the event triggering the trap
	nbTimestamp	.1.3.6.1.4.1.28097.11.255.25.0	UNSIGNED32	Time of the event triggering the trap. Time is in seconds since the Epoch (1/1/1970 00:00 UTC)
	nbMacAddr	.1.3.6.1.4.1.28097.11.255.26.0	PhysAddress (OCTET STRING) (SIZE (6))	The BSSID for which the trap was triggered Format is binary Physical Address
	nbSource	.1.3.6.1.4.1.28097.11.255.27.0	DISPLAYSTRING	A tag which identifies the origin of the event
TRAP	SecurityAlarm	.1.3.6.1.4.1.28097.11.12		Security-related alarm

10. WARNING

The Rogue AP detection implementation in WaveOS is a WIDS, can send trap (SNMP request) but cannot block Rogue devices, preventing wireless or wired network access (so not a WIPS). The network administrator need to take decision to prevent wireless Dos attacks with WIPS.

Support : https://support.acksys.fr