Grandstream Networks, Inc.

GWN76XX

Wi-Fi Access Points

Rogue AP Detection Guide

Table of Content

Table of Figures

SUPPORTED DEVICES

Following table shows Grandstream Wi-Fi Access Points supporting the Rogue AP Detection feature:

Model	Supported	Firmware
GWN7615	Yes	1.0.19.9 or higher
GWN7600 / GWN7600LR	Yes	1.0.19.9 or higher
GWN7605 / GWN7605LR	Yes	1.0.19.9 or higher
GWN7630 / GWN7630LR	Yes	1.0.19.9 or higher

Note: This feature is not supported in GWN7610 and GWN7602.

INTRODUCTION

The GWN Access Points offer the ability to prevent malicious intrusion to the network and increases the wireless security access of clients when introducing Rogue AP Detection feature.

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from network administrators. Rogue access points can negatively impact the performance of wireless networks and pose a security threat because anyone with access to the premises can ignorantly or maliciously plug a wireless AP to the local network which can undermine the security of an enterprise network by potentially allowing unchallenged and unauthorized access.

In this guide, we will go through the configuration steps to enable the AP Rogue Detection feature on a GWN76xx access point.

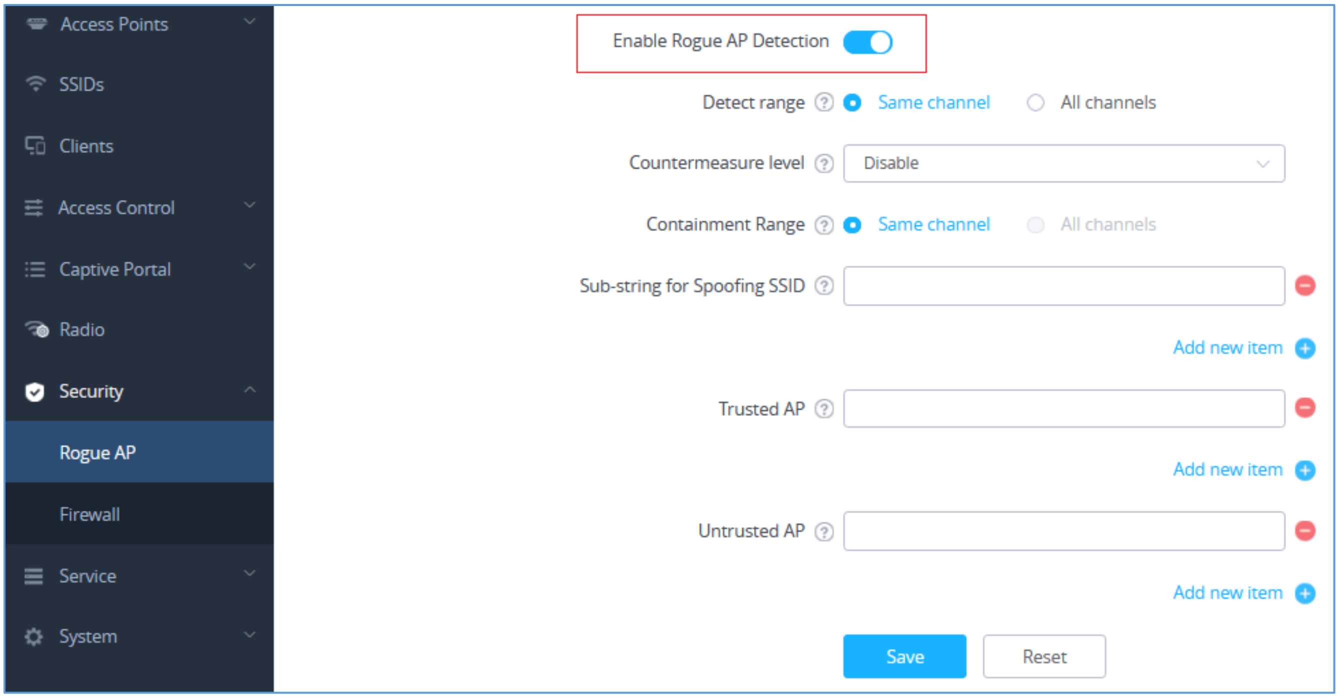
ROGUE AP DETECTION CONFIGURATION

Configuration Steps

In the next sections, we provide the needed configuration steps to enable Rogue AP Detection feature on GWN access points:

Enabling Rogue AP Detection Feature

To enable the Rogue AP Detection feature, Access the GWN76xx web GUI, and navigate to “**Security”** → “**Rogue AP”** → **“Configuration”** as shown in below screenshot.



Enable Rogue AP Detection: enabled

Detect range: ● Same channel ○ All channels

Countermeasure level: Disable

Containment Range: ● Same channel ○ All channels

Sub-string for Spoofing SSID:

Trusted AP:

Untrusted AP:

Figure 1: Enable Rogue AP Detection Feature

In below table you can find the description for the related parameters and options.

Table 1: Rogue AP Parameters Description

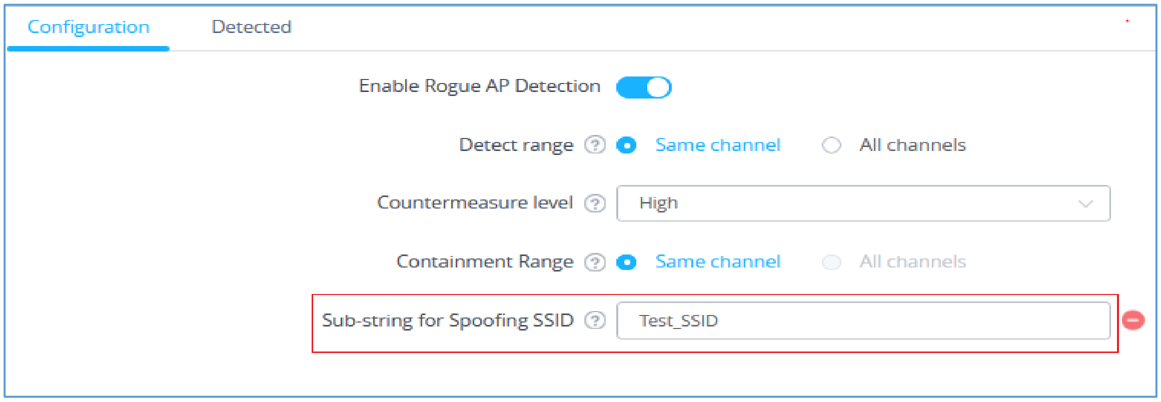
Field	Description
Enable Rogue AP Detection	Select to either to enable or disable Rogue AP scan.
Detect range	Specify the Rogue AP detect range. • **Same channel:** AP will execute simple detection on the APs around, this mode almost has no effects on the wireless network communication.

	- **All channels:** AP will execute a deep detection every 5 minutes. And the clients connecting to the AP will have few seconds of communication interrupt. Default is **Same channel**.
Countermeasure level	Countermeasures level specifies the type of attacks which will be suspected by the AP. Select different levels: - **High:** Untrusted BSSID, Illegal access without authentication, Illegal access, Spoofing SSID. - **Medium:** Untrusted BSSID, Illegal access without authentication, Illegal access. - **Low:** Untrusted BSSID, Illegal access without authentication. Default is **Disabled**. **Notes**: - **Illegal access**: Rogue AP does not use open authentication and encryption in local network. For example, if you need a password to connect to the SSID of the rogue AP, then it belongs to "Illegal access". - **Illegal access without authentication**: Rogue AP use open authentication and encryption in local network. For example, if you do not need a password to connect to the SSID of rogue AP, then it belongs to "Illegal access without authentication".
Containment Range	Specify the containment range: - **Same channel:** detect AP will countermeasure the APs in the same channel. - **All channels:** detect AP will countermeasure the APs in all channels at the cost of consuming of much AP performance. Default is **Same channel**.
Sub-string for Spoofing SSID	The AP broadcasting SSID with the specified string will be classified as a Spoofing SSID.

Trusted AP	You can specify MAC address of the trusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as trusted AP, no countermeasures will be executed on it.
Untrusted AP	You can specify MAC address of the untrusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as untrusted AP, countermeasures will be executed on it when countermeasure is enabled.

Adding the Spoofing SSID String

Users can specify an SSID string to be checked for potential rogue access points transmitting the same SSID, this is to prevent SSID spoofing rogue access points from masquerading the legitimate SSID broadcasted by GWN76xx. In the example from below screenshot we have added **Test_SSID** as the spoofing SSID string.



Enable Rogue AP Detection: on

Detect range: ● Same channel ○ All channels

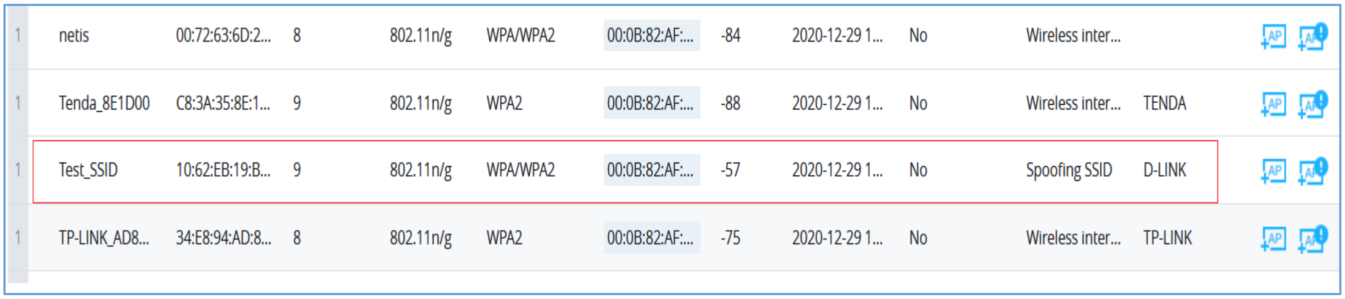
Countermeasure level: High

Containment Range: ● Same channel ○ All channels

Sub-string for Spoofing SSID: Test_SSID

Figure 2: Spoofing SSID String

Once the GWN76xx detects an AP broadcasting the exact SSID string like in our example "Test_SSID", it will be reported in the "**Detected"** page as "**Spoofing SSID**", and if enabled a countermeasure to contain that AP could be taken from the GWN76xx AP to prevent wireless clients from associating with that SSID.

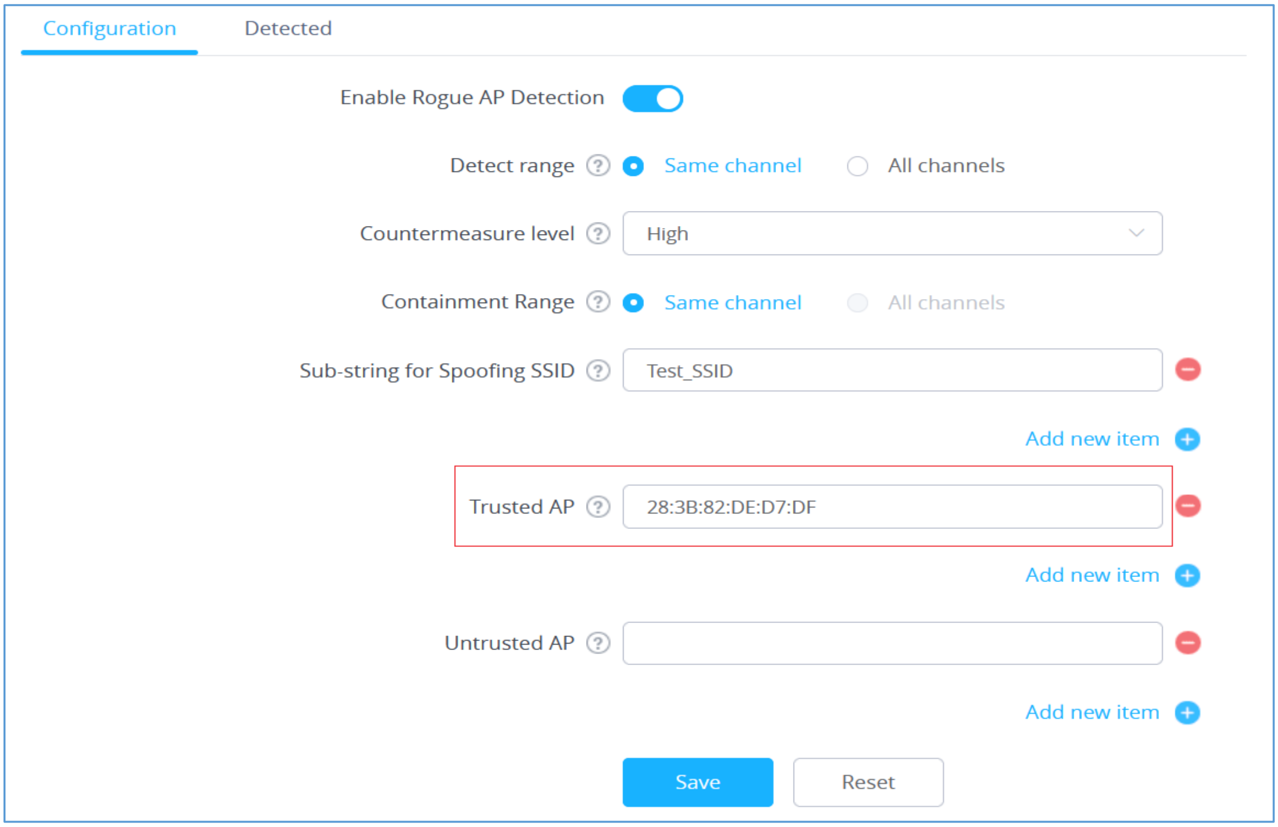


1	netis	00:72:63:6D:2...	8	802.11n/g	WPA/WPA2	00:0B:82:AF:...	-84	2020-12-29 1...	No	Wireless inter...	
1	Tenda_8E1D00	C8:3A:35:8E:1...	9	802.11n/g	WPA2	00:0B:82:AF:...	-88	2020-12-29 1...	No	Wireless inter...	TENDA
1	Test_SSID	10:62:EB:19:B...	9	802.11n/g	WPA/WPA2	00:0B:82:AF:...	-57	2020-12-29 1...	No	Spoofing SSID	D-LINK
1	TP-LINK_AD8...	34:E8:94:AD:8...	8	802.11n/g	WPA2	00:0B:82:AF:...	-75	2020-12-29 1...	No	Wireless inter...	TP-LINK

Figure 3: Detected Spoofing SSID

Adding Trusted AP

Users can add trusted access points by specifying their MAC addresses under “**Security**” → “**Rogue AP**” → “**Configuration**”



Enable Rogue AP Detection ●

Detect range ? ● Same channel ○ All channels

Countermeasure level ? High

Containment Range ? ● Same channel ○ All channels

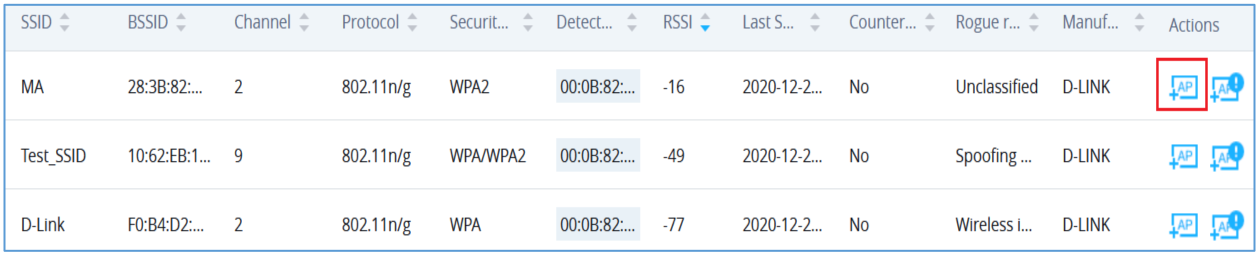
Sub-string for Spoofing SSID ? Test_SSID

Trusted AP ? 28:3B:82:DE:D7:DF

Untrusted AP ?

Figure 4: Add Trusted AP – Configuration Page

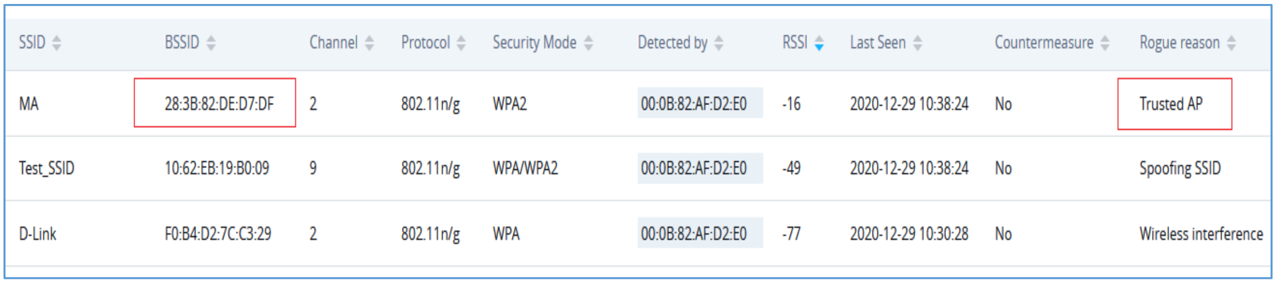
You can also define an AP as trusted from the **“Actions”** tab located under “**Security**” → “**Rogue AP**” → “**Detected**” by clicking the icon AP as shown in below screenshot.



SSID	BSSID	Channel	Protocol	Securit...	Detect...	RSSI	Last S...	Counter...	Rogue r...	Manuf...	Actions
MA	28:3B:82:...	2	802.11n/g	WPA2	00:0B:82:...	-16	2020-12-2...	No	Unclassified	D-LINK	AP AP
Test_SSID	10:62:EB:1...	9	802.11n/g	WPA/WPA2	00:0B:82:...	-49	2020-12-2...	No	Spoofing ...	D-LINK	AP AP
D-Link	F0:B4:D2:...	2	802.11n/g	WPA	00:0B:82:...	-77	2020-12-2...	No	Wireless i...	D-LINK	AP AP

Figure 5: Add Trusted AP - Detected Page

Once an AP is added as trusted, it will be displayed under “**Detected**” page as “**Trusted AP**”



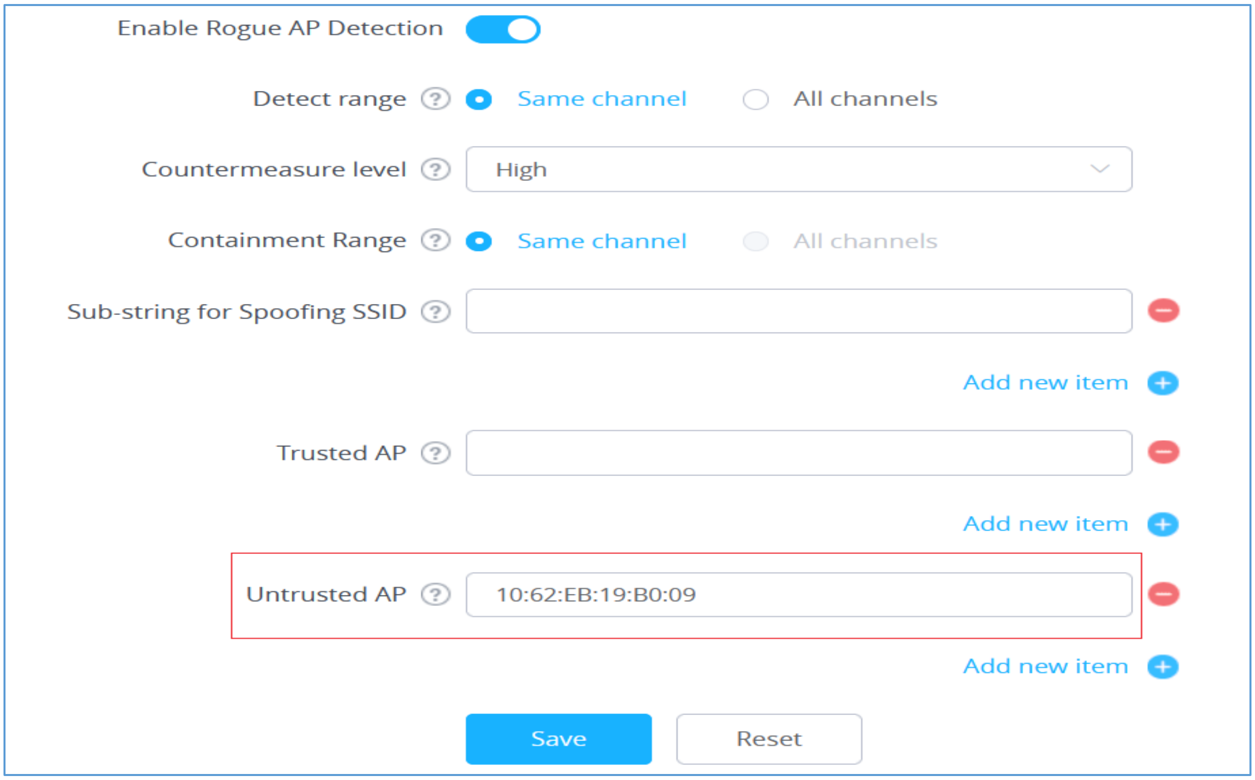
SSID	BSSID	Channel	Protocol	Security Mode	Detected by	RSSI	Last Seen	Countermeasure	Rogue reason
MA	28:3B:82:DE:D7:DF	2	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-16	2020-12-29 10:38:24	No	Trusted AP
Test_SSID	10:62:EB:19:B0:09	9	802.11n/g	WPA/WPA2	00:0B:82:AF:D2:E0	-49	2020-12-29 10:38:24	No	Spoofing SSID
D-Link	F0:B4:D2:7C:C3:29	2	802.11n/g	WPA	00:0B:82:AF:D2:E0	-77	2020-12-29 10:30:28	No	Wireless interference

Figure 6: Detected Trusted AP

Note: If an AP is defined as trusted AP, no countermeasures will be executed on it when countermeasure is enabled.

Adding Untrusted AP

Users can add Untrusted access points by specifying their MAC addresses under "**Security**" → "**Rogue AP**" → **"Configuration".**



Enable Rogue AP Detection: On

Detect range: ● Same channel ○ All channels

Countermeasure level: High

Containment Range: ● Same channel ○ All channels

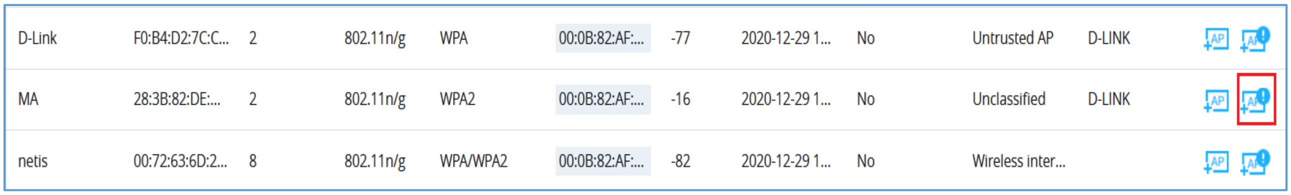
Sub-string for Spoofing SSID:

Trusted AP:

Untrusted AP: 10:62:EB:19:B0:09

Figure 7: Add Untrusted AP - Configuration Page

You can also define an AP as Untrusted from the **"Actions"** tab located under "**Security**" → "**Rogue AP**" → "**Detected"** by clicking the icon AP as shown in below screenshot.



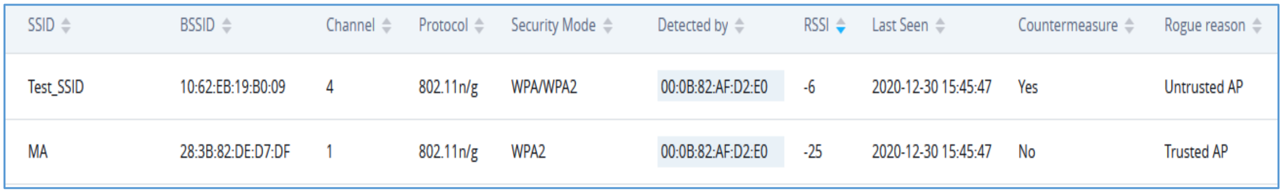
D-Link	F0:B4:D2:7C:C...	2	802.11n/g	WPA	00:0B:82:AF:...	-77	2020-12-29 1...	No	Untrusted AP	D-LINK	AP	AP
MA	28:3B:82:DE:...	2	802.11n/g	WPA2	00:0B:82:AF:...	-16	2020-12-29 1...	No	Unclassified	D-LINK	AP	AP
netis	00:72:63:6D:2...	8	802.11n/g	WPA/WPA2	00:0B:82:AF:...	-82	2020-12-29 1...	No	Wireless inter...		AP	AP

Figure 8: Add Untrusted AP - Detected Page

Note: If an AP is defined as Untrusted AP, countermeasures will be executed on it when countermeasure is enabled.

DETECTED ROGUE ACCESS POINTS

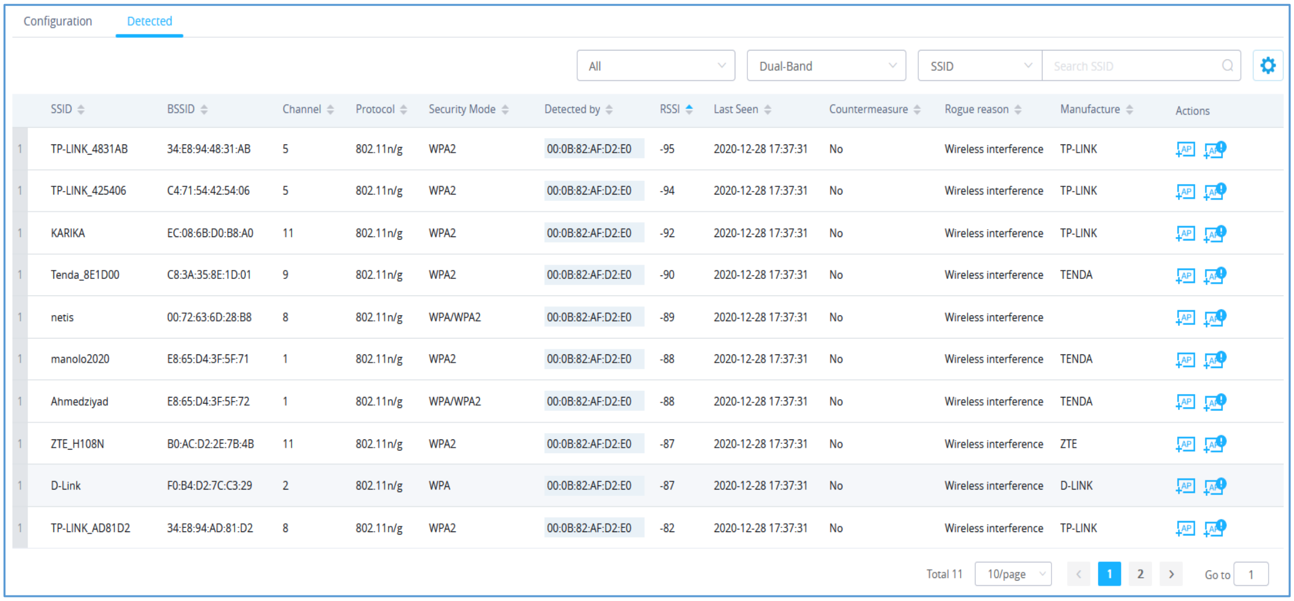
The "**Detected**" page shows all the SSIDs within the Wi-Fi coverage of the GWN76xx, including the APs that have been set as Trusted or Untrusted.



SSID	BSSID	Channel	Protocol	Security Mode	Detected by	RSSI	Last Seen	Countermeasure	Rogue reason
Test_SSID	10:62:EB:19:B0:09	4	802.11n/g	WPA/WPA2	00:0B:82:AF:D2:E0	-6	2020-12-30 15:45:47	Yes	Untrusted AP
MA	28:3B:82:DE:D7:DF	1	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-25	2020-12-30 15:45:47	No	Trusted AP

Figure 9: Detected Trusted and Untrusted APs

When the GWN76xx AP detects the signal of another neighboring wireless access point, it compares the characteristics of the AP to a list of configured Trusted or Untrusted APs. If the discovered access point does not match any trusted or untrusted AP, the GWN76xx reports the device as a "**Wireless interference**" under the web GUI "**Detected**" page as shown in below screenshot.



	SSID	BSSID	Channel	Protocol	Security Mode	Detected by	RSSI	Last Seen	Countermeasure	Rogue reason	Manufacture	Actions
1	TP-LINK_4831AB	34:E8:94:48:31:AB	5	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-95	2020-12-28 17:37:31	No	Wireless interference	TP-LINK	AP AP
1	TP-LINK_425406	C4:71:54:42:54:06	5	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-94	2020-12-28 17:37:31	No	Wireless interference	TP-LINK	AP AP
1	KARIKA	EC:08:6B:D0:B8:A0	11	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-92	2020-12-28 17:37:31	No	Wireless interference	TP-LINK	AP AP
1	Tenda_8E1D00	C8:3A:35:8E:1D:01	9	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-90	2020-12-28 17:37:31	No	Wireless interference	TENDA	AP AP
1	netis	00:72:63:6D:28:B8	8	802.11n/g	WPA/WPA2	00:0B:82:AF:D2:E0	-89	2020-12-28 17:37:31	No	Wireless interference		AP AP
1	manolo2020	E8:65:D4:3F:5F:71	1	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-88	2020-12-28 17:37:31	No	Wireless interference	TENDA	AP AP
1	Ahmedziyad	E8:65:D4:3F:5F:72	1	802.11n/g	WPA/WPA2	00:0B:82:AF:D2:E0	-88	2020-12-28 17:37:31	No	Wireless interference	TENDA	AP AP
1	ZTE_H108N	B0:AC:D2:2E:7B:4B	11	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-87	2020-12-28 17:37:31	No	Wireless interference	ZTE	AP AP
1	D-Link	F0:B4:D2:7C:C3:29	2	802.11n/g	WPA	00:0B:82:AF:D2:E0	-87	2020-12-28 17:37:31	No	Wireless interference	D-LINK	AP AP
1	TP-LINK_AD81D2	34:E8:94:AD:81:D2	8	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-82	2020-12-28 17:37:31	No	Wireless interference	TP-LINK	AP AP

Figure 10: Detected Rogue Page

Note: An Access point is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat since it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

ROGUE AP CONTAINMENT

When the countermeasure option is enabled and a client tries to associate with an untrusted or spoofing SSID access point, The GWN76xx AP automatically begins sending broadcast de-authentication messages spoofing the rogue's BSSID (MAC) to prevent wireless clients from connecting to that malicious rogue AP.

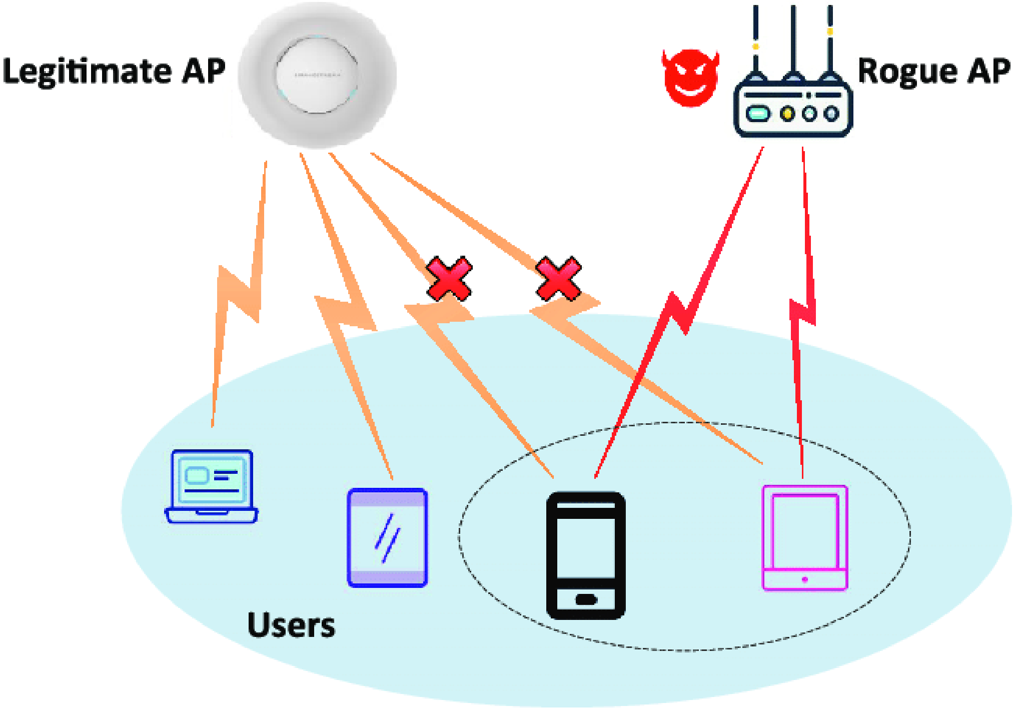
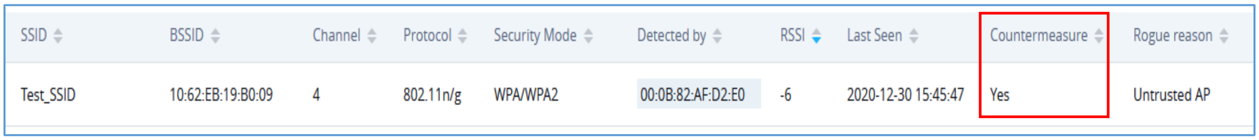


Figure 11: Rogue AP Containment

When a countermeasure is taken against a rogue Untrusted AP, It will be displayed in "**Detected**" page under **Security"** → "**Rogue AP"** as shown in below screenshot.



SSID	BSSID	Channel	Protocol	Security Mode	Detected by	RSSI	Last Seen	Countermeasure	Rogue reason
Test_SSID	10:62:EB:19:B0:09	4	802.11n/g	WPA/WPA2	00:0B:82:AF:D2:E0	-6	2020-12-30 15:45:47	Yes	Untrusted AP

Figure 12: Contained AP - Detected Page

⚠ **Note:**

Please make sure that the rogue device is within your network and poses a security risk before you launch the containment. As Containment can have legal implications when launched against legitimate neighbor networks.