Technical Guide

Wireless Management for the TQR Series using the Device GUI

Feature Overview and Configuration Guide

Introduction

The TQR Series Wireless AP Routers deliver high-speed Wi-Fi 6/6E connectivity for wireless devices and secure Internet access via a built-in VPN router. Their single-unit design offers a streamlined yet comprehensive network solution—ideal for small businesses or enterprises with multiple locations, such as retail stores, cafés, and more.

Secure WAN routing ensures reliable connectivity to the Internet, head office, and other branch locations. A zone-based firewall protects critical data, while secure IPsec VPNs enable remote access to cloud-based or head-office business applications.

Products and software version that apply to this guide

This guide applies to the following Allied Telesis TQR Series Wireless AP Routers:

- TQ6702 GEN2-R running AlliedWare Plus™ software version 5.5.3-1.1 or later
- TQ7403-R running AlliedWare Plus™ software version 5.5.4-1.5 or later

The TQ7403-R uses the same wireless configuration and features as the TQ6702 GEN2-R but differs in the following ways:

  - Supports Wi-Fi 6E
  - Includes a third radio (Radio 3 - 6GHz)
  - Supports two external antennas

Feature support may change in later software versions. For the latest information, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

From software version 5.5.4-0.1 onwards, AlliedWare Plus supports the following wireless enhancements for the TQ6702 GEN2-R wireless AP router:

- Device GUI version 2.18.0
- Passpoint, see "Passpoint" on page 29
- More Radio Mode options, see "Basic Radio1 settings" on page 38
- Multicast to Unicast conversion, see "Multicast to Unicast conversion" on page 49
- Airtime Fairness for each VAP, see "Airtime Fairness for each VAP" on page 50

From software version 5.5.4-2.3 onwards, AlliedWare Plus supports the following wireless enhancements for the TQ6702 GEN2-R wireless AP router:

- Device GUI version 2.19.0
- New cipher parameter CCMP for WPA3, see "Edit VAP 0 - Advanced Settings Security" on page 47
- Removal of requirement to specify a basic rate for Radio 1, see "Advanced Radio settings" on page 40
- Dynamic VLAN with MAC Authentication supported, see "MAC Authentication with Dynamic VLAN" on page 20

From software version 5.5.5-0.2 onwards, AlliedWare Plus supports the following wireless enhancements for the TQR Series (i.e. TQ6702 GEN2-R and TQ7403-R).

- Device GUI version 2.20.0
- TQR Series RFScan Improvements, see "Radio scanning" on page 43
- Proxy ARP option to allow ARP packets from unknown addresses, see "Proxy ARP handling" on page 52
- Two-step authentication with MAC and Captive Portal, see "Two-step authentication with MAC authentication and Captive Portal" on page 53

Related documents

You also may find the following AlliedWare Plus Feature Guides useful:

- Getting Started with the TQ6702 GEN2-R Wireless Router using the Device GUI
- Link Aggregation and Ethernet Bonding Feature Overview and Configuration Guide

Acronyms

The following acronyms are used in this document:

Table 1: Acronyms used in Wireless Management

ACRONYM	DESCRIPTION
BSSID	Basic Service Set Identifier - or the APs physical MAC address.
SSID	Service Set Identifier - a unique name for the wireless network.
VAP	Virtual Access Point is a concept of assigning multiple wireless networks to a wireless radio configuration.
WAP or AP	Wireless Access Point or Access Point is a networking hardware device that allows a Wi-Fi device to connect to a wired network.
WDS	Wireless Distribution System. It enables wireless interconnection of access points in an IEEE 802.11 network.
WEP	Wired Equivalent Privacy.
WPA	Wi-Fi Protected Access.

Content

Connecting to the wireless AP router

This section describes how to connect to your router using the Device GUI. Your router will have a GUI already loaded.

Supported web browsers for connecting to the Device GUI are:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge™
- Apple Safari™

Connecting to the GUI

To connect to the GUI, use the following steps:

Note: You will need to manually assign your device an IP address in the 192.168.1.0/24 network.

1. Connect to LAN1 (referred to as eth1 in the firmware).
2. Open a web browser and browse to the default IP address for eth1.
    - The default IP address is 192.168.1.1
3. Log in with the default username of ***manager*** and the default password of ***friend***.

Applying and saving your configuration

Use the following procedure to save your configuration to the device.

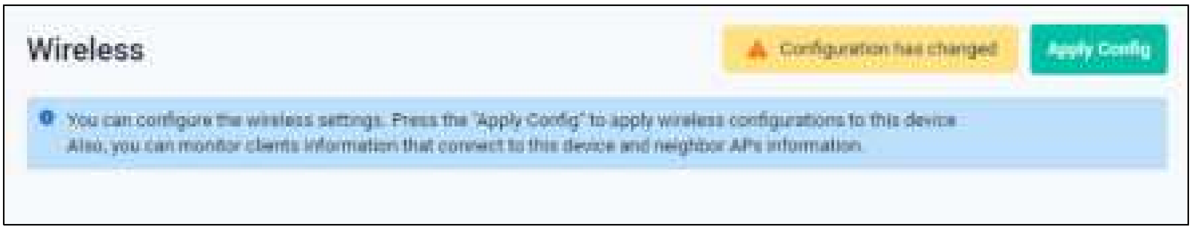
When you configure the wireless router through its GUI, the configuration becomes part of its running-configuration. Once you are sure your configuration changes work, you need to make them part of the boot configuration, so they can be backed up and will survive a reboot of the wireless router.

Caution: Back up the default configuration before you save and apply your configuration.

Once you are happy with the functionality of your configuration, you can then save it.

1. Click the **Apply Config** button to apply the settings to your device.

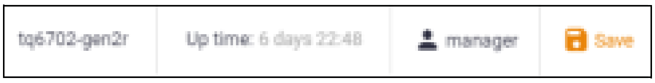
   This step saves the wireless configuration to your device. Notice that the button is orange colored when the configuration requires saving:



You can configure the wireless settings. Press the "Apply Config" to apply wireless configurations to this device
Also, you can monitor clients information that connect to this device and neighbor APs information.

2. Click the **Save** button at the top right of the GUI screen (you may need to scroll up to see it).

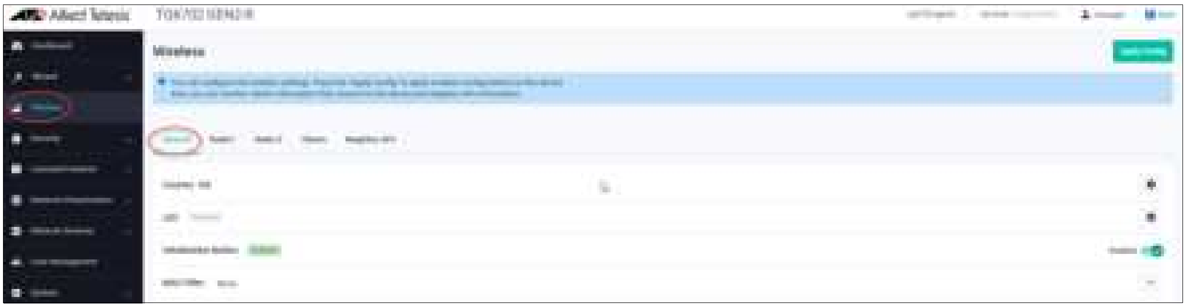
The **Save** button will be orange if there is unsaved configuration and blue when it is saved:



Setting up security for your wireless network

This section shows you how to set up your wireless network, which includes setting up your security.

To set up security on your wireless network, click on **Wireless** from the menu bar. The Wireless page is displayed, opening at the **General** tab:



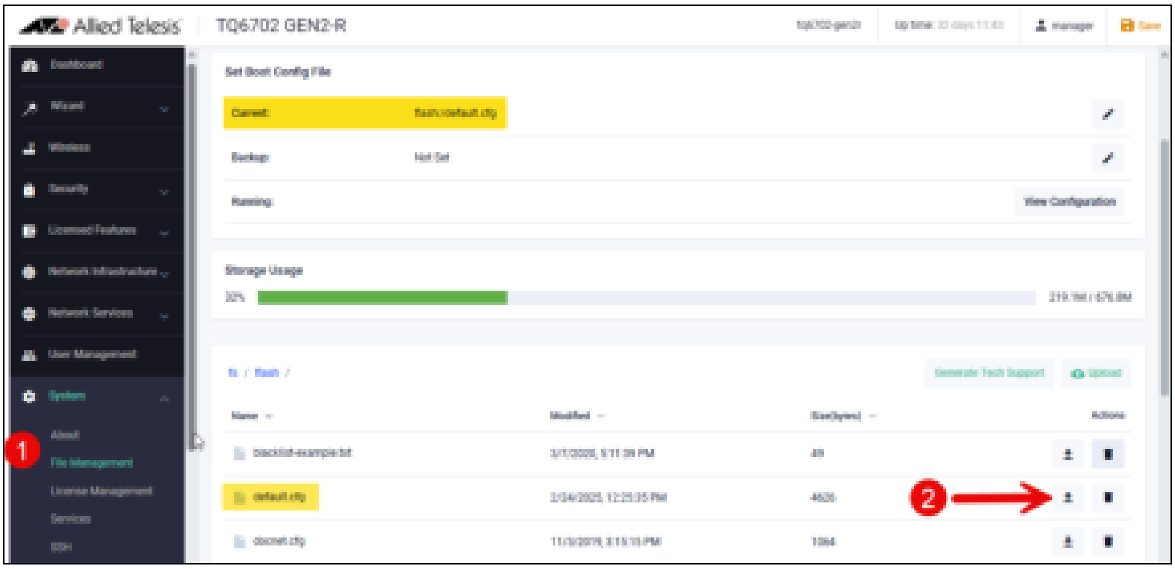
This section shows you how to set up the security for your wireless router using the following features:

1. "WPA Personal" on page 8
2. "WPA Enterprise with a RADIUS server" on page 9
3. "WPA Enterprise with Dynamic VLANs" on page 13
4. "MAC Authentication" on page 18

Make a backup configuration file

Before you start configuring the wireless router, back up its current configuration file.

1. Go to **System** > **File Management**
2. Select the current configuration file and download it.
3. Save it to a location where you can access it if needed.



Set Boot Config File

Current: flash:/default.cfg

Backup: Not Set

Running: View Configuration

Storage Usage

32% 219.1M / 676.8M

fs / flash /

Generate Tech Support

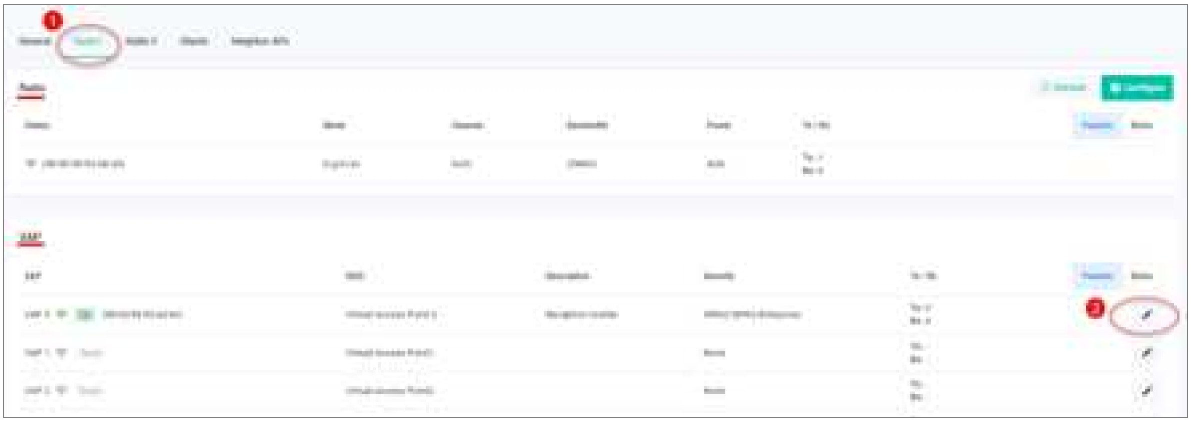
Upload

Name	Modified	Size(bytes)	Actions
blacklist-example.txt	3/1/2020, 5:11:39 PM	49	
default.cfg	2/24/2025, 12:25:35 PM	4626	
docnet.cfg	11/3/2019, 3:15:13 PM	1064	

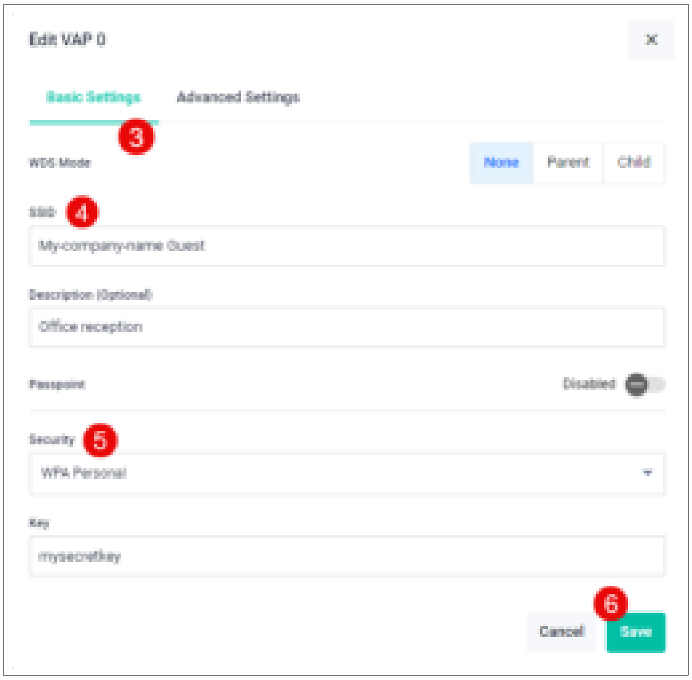
WPA Personal

The following steps show you how to configure WPA Personal to secure your wireless network for a home or remote access environment.

1. Click on a **Radio** tab to display the **Radio** and **VAP** settings.
2. Click on the VAP 0 **Edit** button.



3. Select the **Basic Settings** tab.
4. Enter the **SSID** and optional Description.
5. In the **Security** field, select **WPA Personal** and enter a **Key**.
6. Click **Save**.



Edit VAP 0

Basic Settings | Advanced Settings

WDS Mode: [✓ None] Parent Child

SSID: My-company-name Guest

Description (Optional): Office reception

Passpoint: Disabled

Security: WPA Personal

Key: mysecretkey

Cancel | Save

7. Apply and then save the configuration. See "Applying and saving your configuration" on page 6 for instructions.

Table 2: Options for VAP0 Basic settings

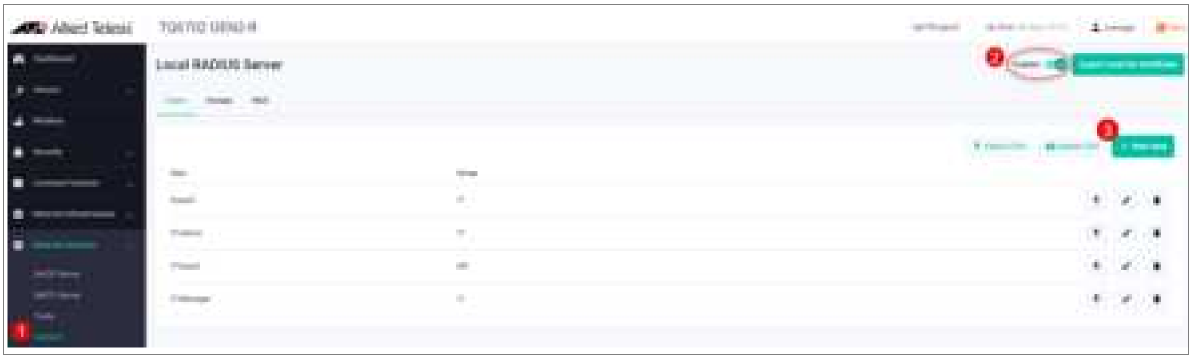
FIELD	DESCRIPTION
WDS Mode	The Wireless Distribution System (WDS) enables wireless interconnection of access points in an IEEE 802.11 network. WDS Mode defaults to **None**. Use the default option unless you need to configure WDS. **WDS allows you to** expand a wireless network using multiple access points without needing a wired backbone between them. WDS connections are based on MAC addresses. A key advantage of WDS over other solutions is that it preserves the MAC addresses of client frames across the wireless links between access points. WDS is typically used for wireless bridging between APs. WDS mode options: ■ **None** – The AP operates independently (not controlled by or controlling another AP). ■ **Parent** – The AP controls one or more child APs. ■ **Child** – The AP is controlled by a parent AP.
SSID	Service Set Identifier - a unique name for the wireless network. Give this field a meaningful name because it is how clients devices identify your network. For example, **My-company-name Guest**.
Description	Optional. Enter a meaningful description, for example **Office Reception**.
Security	Select **WPA Personal** from the drop down options. The options are WPA Personal or WPA Enterprise. The default is **None**.
Key	Enter a secure key, for example **mysecurekey**.

WPA Enterprise with a RADIUS server

This section explains how to set up WPA Enterprise with a RADIUS server to secure your wireless network in a business environment. Follow the steps below to configure it:

Enable the RADIUS server

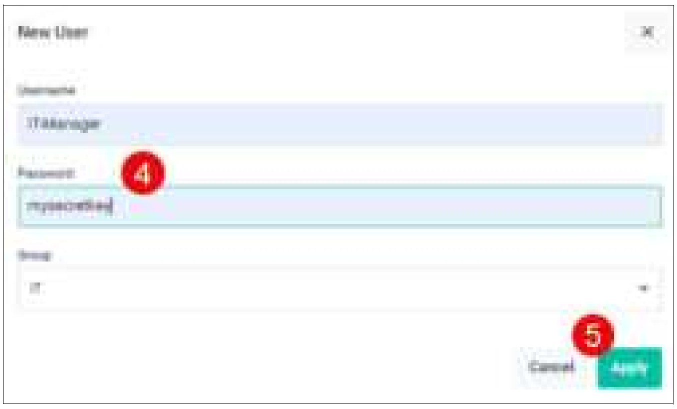
1. From the **Network Services** menu select **RADIUS**.
2. Click on the local RADIUS server **toggle switch** to turn it on (it defaults to off).
3. Click **+New User**.



Add user

4. From the **New User** dialog enter a username, password and optionally a group. If you want to add a user to a group, create the group from the **Groups** tab first and then select it from the **Group** drop down list.

5. Click **Apply**.



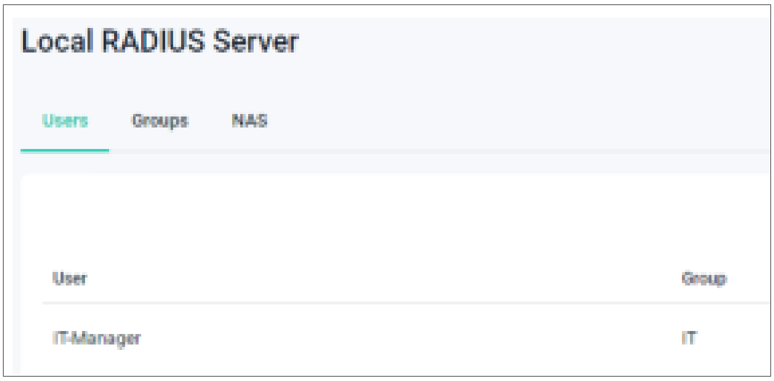
New User

Username: ITManager

Password: mysecretkey

Group: IT

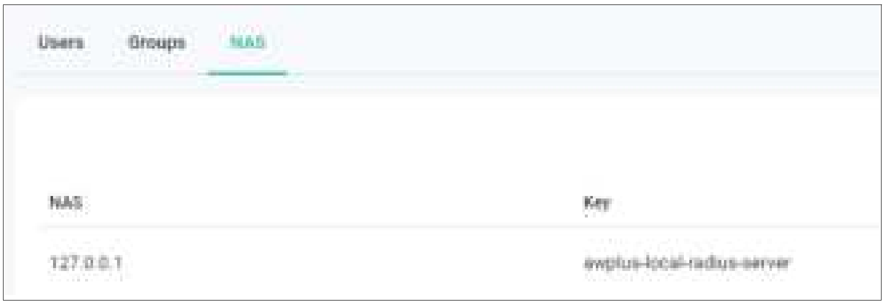
You can see and edit the Users from this window:



Local RADIUS Server

User	Group
IT-Manager	IT

From the **NAS** (Network Access Server) tab, notice that the **NAS** and **Key** fields automatically populate for the user you added:

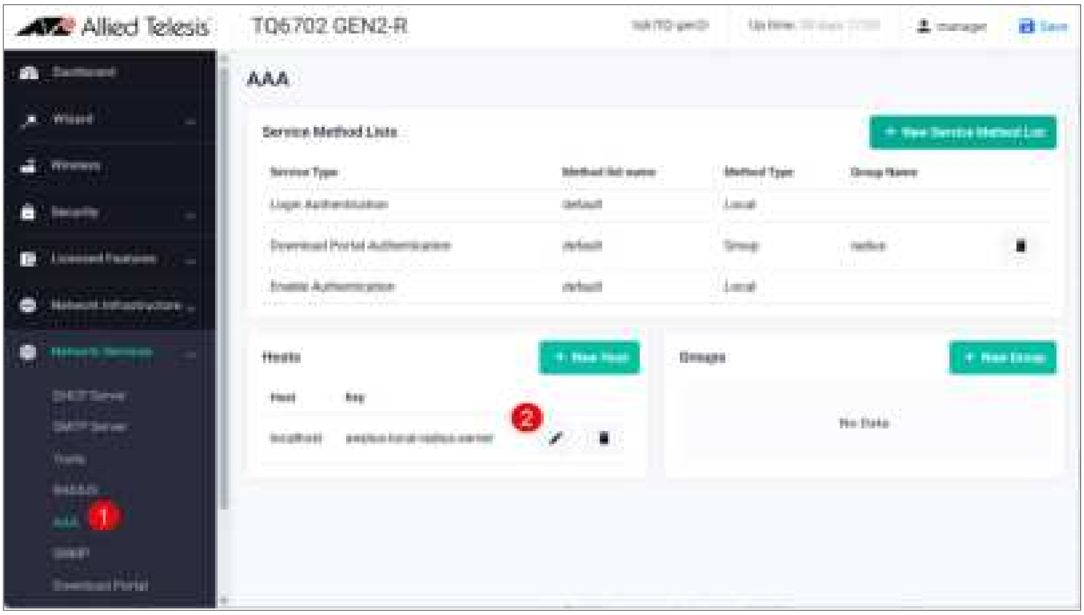


NAS	Key
127.0.0.1	awplus-local-radius-server

Set up AAA

1. From **Network Services**, select **AAA**.

2. Notice the fields populate automatically. If you need to edit the host information, click on the **Edit** button.



Service Method Lists

Service Type	Method list name	Method Type	Group Name
Login Authentication	default	Local	
Download Portal Authentication	default	Group	radius
Enable Authentication	default	Local	

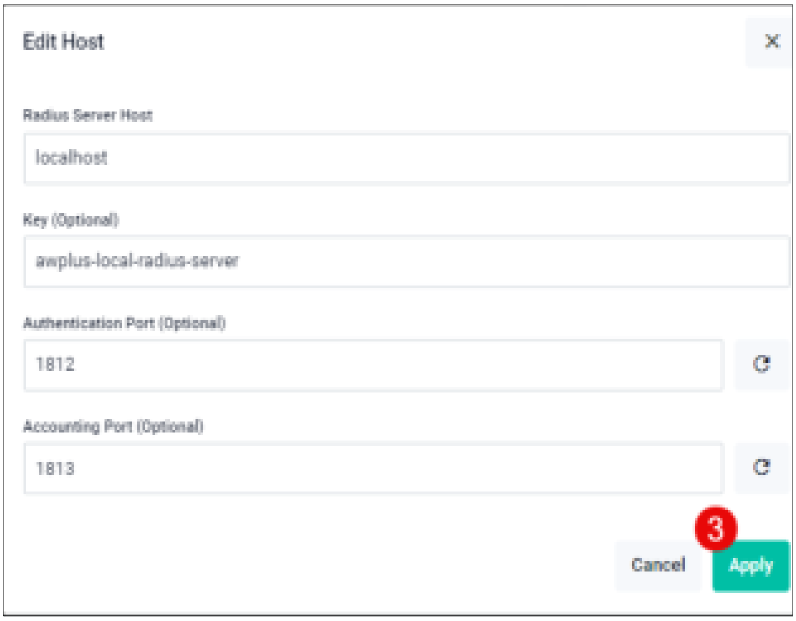
Hosts

Host	Key
localhost	awplus-local-radius-server

Groups

No Data

3. Edit the host if necessary and click **Apply**:



Edit Host

Radius Server Host
localhost

Key (Optional)
awplus-local-radius-server

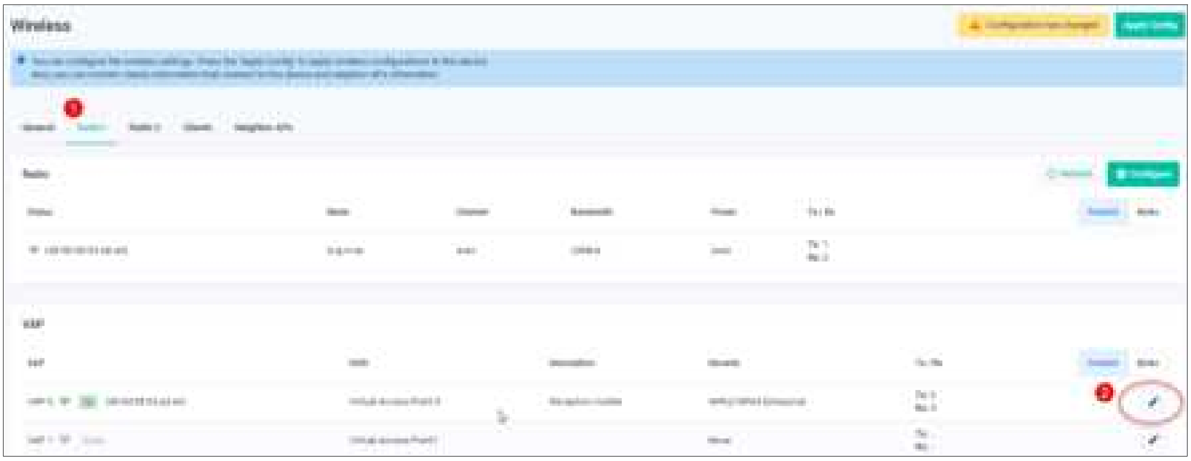
Authentication Port (Optional)
1812

Accounting Port (Optional)
1813

Set up WPA Enterprise

1. From the **Wireless** page, click on a **Radio** tab to display the **Radio** and **VAP** settings.

2. Click the **Edit** button for VAP 0.

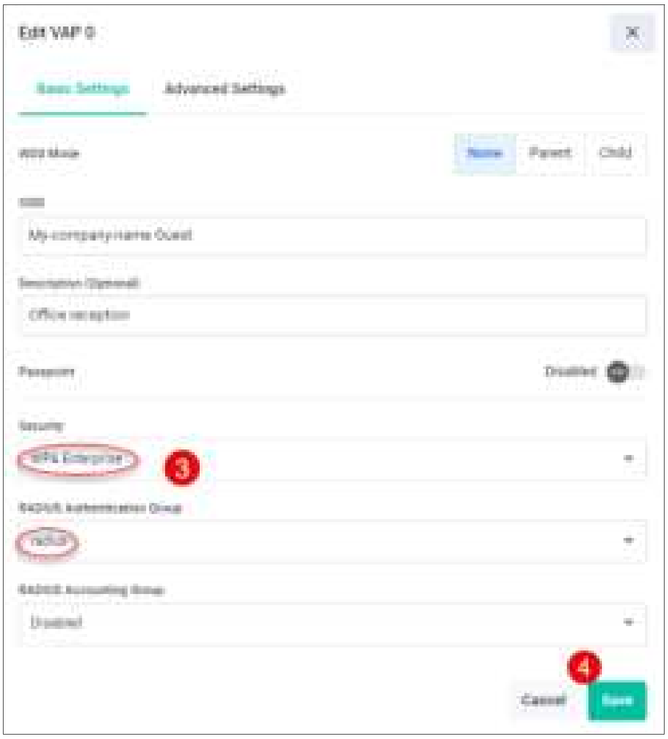


3. Configure **WPA Enterprise**.

   In the **Edit VAP 0** dialog from the **Basic Settings** tab, select:

   - **WPA Enterprise** from the **Security** drop down list.
   - **radius** from the **RADIUS Authentication Group** drop down list.

4. Click **Save**.


Edit VAP 0

Basic Settings | Advanced Settings

WDS Mode: None | Parent | Child

SSID: My-company-name Guest

Description (Optional): Office reception

Passpoint: Disabled

Security: WPA Enterprise

RADIUS Authentication Group: radius

RADIUS Accounting Group: Disabled

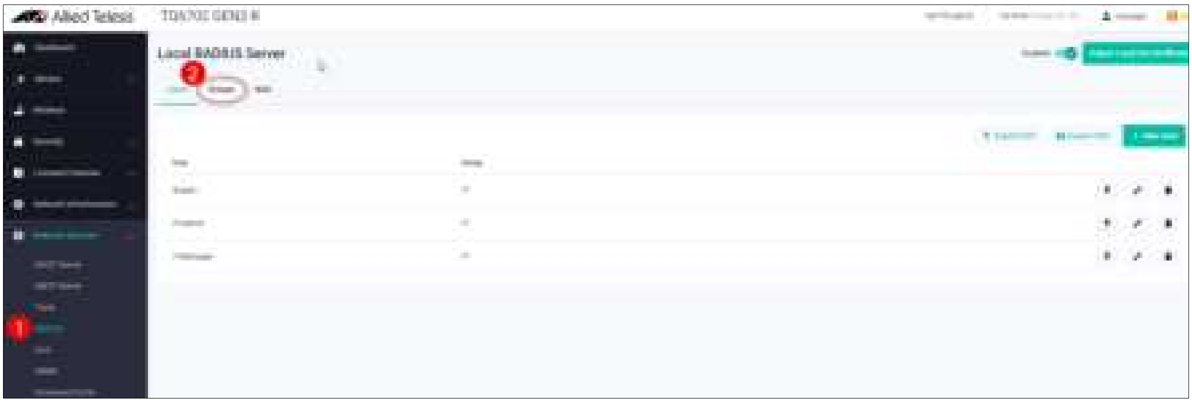
5. Apply and then save the configuration. See "Applying and saving your configuration" on page 6 for instructions.

WPA Enterprise with Dynamic VLANs

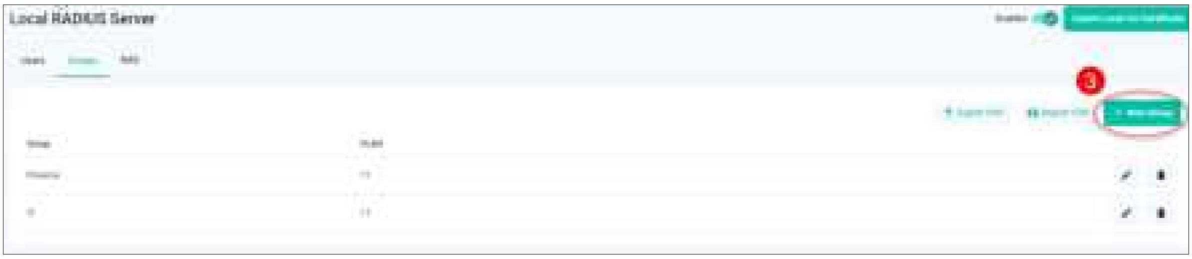
This section shows you how to set up WPA enterprise with Dynamic VLANs to secure your wireless network in a business environment.

Set up a new group for your VLAN

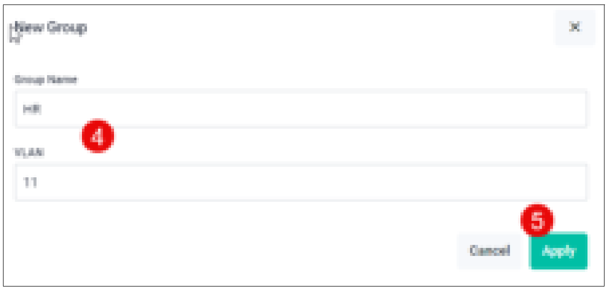
1. From **Network Services**, click on **RADIUS** to display the **Local RADIUS Server** page.
2. Click on the **Groups** tab.



3. From the **Groups** tab, click **+New Group**.



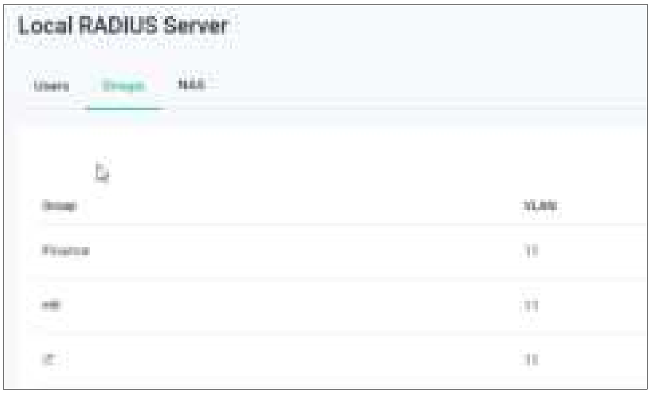
4. Enter your Group Name and VLAN, for example **HR** and VLAN **11**.
5. Click **Apply**.


New Group

Group Name: HR

VLAN: 11

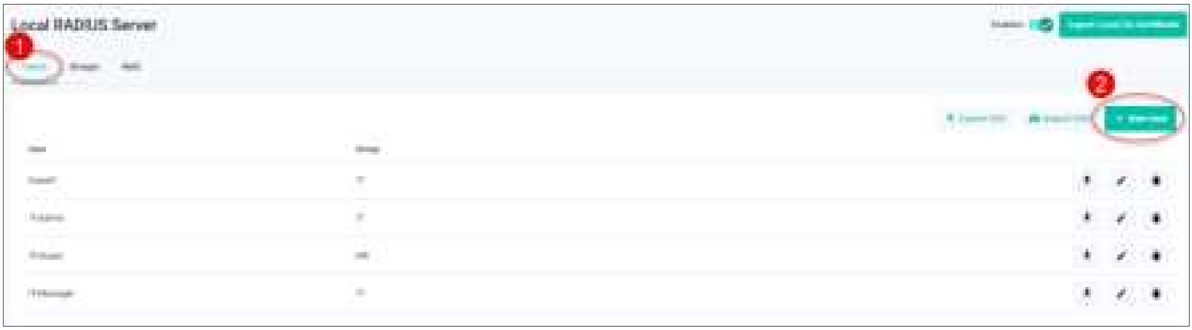
You can see the group that you have added. You can edit the group later if required.



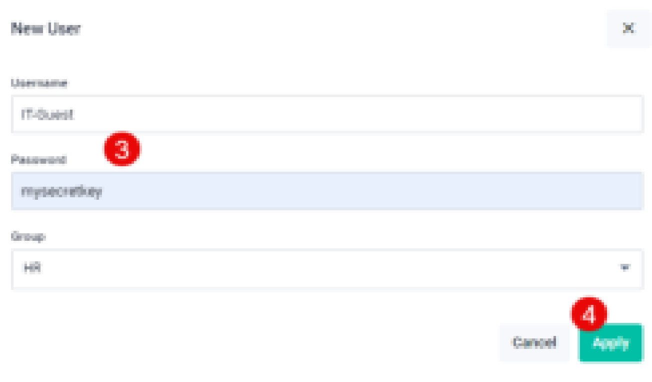
Group	VLAN
Finance	11
HR	11
IT	11

Set up new users for your VLAN

1. From the **Local RADIUS Server** page, click on the **Users** tab.
2. From the **Users** tab, click **+New User**.



3. Enter the Username and Password. Choose the VLAN group that you created earlier in the Group field. In the example, the user **IT-Guest** with the password **mysecretkey** has been added to the **HR** group.
4. Click **Apply**.



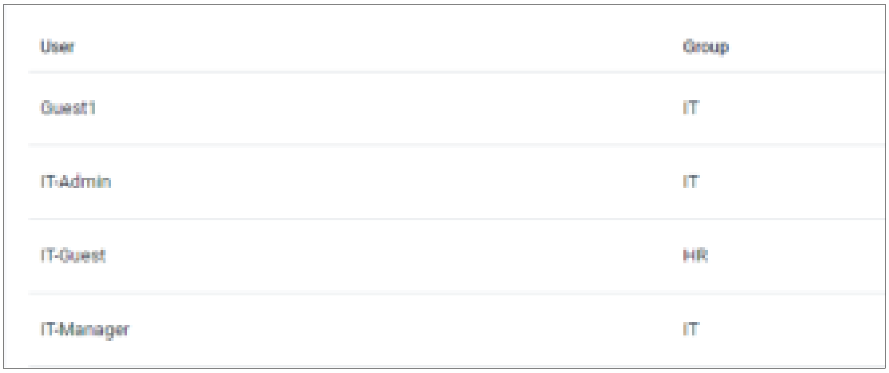
New User

Username: IT-Guest

Password: mysecretkey

Group: HR

You can see the users that you have added. You can edit users later if required.

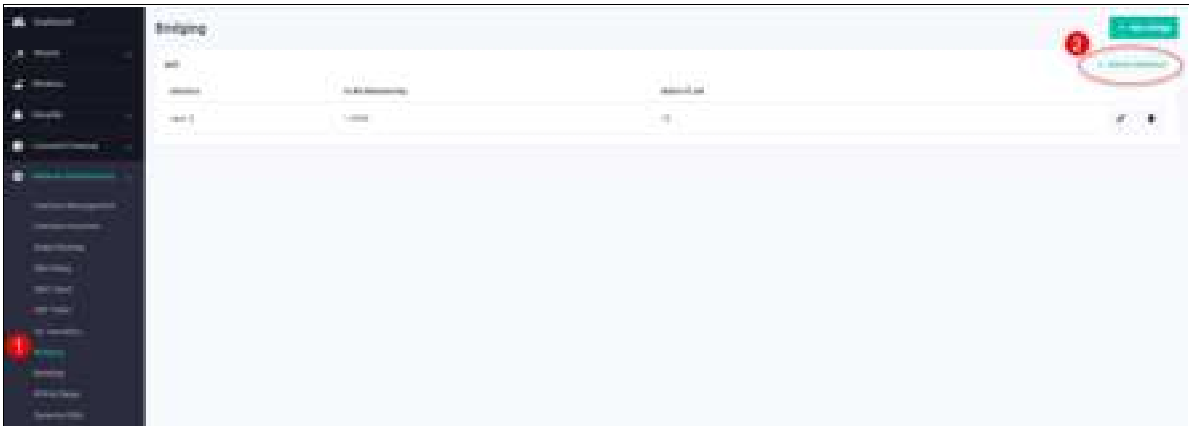


User	Group
Guest1	IT
IT-Admin	IT
IT-Guest	HR
IT-Manager	IT

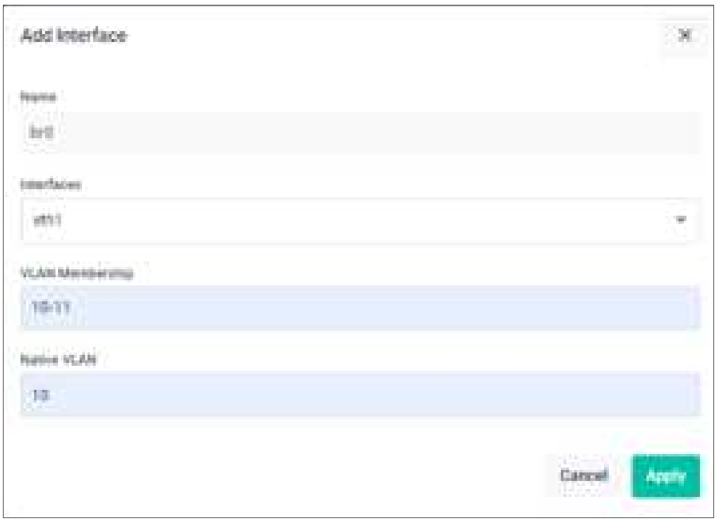
Add a bridge

Set up the VLAN-aware bridge and add the VAP interface to it to enable the use of multiple VLANs on a single VAP. Follow the steps below to add a bridge:

1. From **Network Infrastructure** select **Bridging** to display the **Bridging** page.
2. From the **Bridging** page click **+Attach Interface** to display the **Add Interface** dialog.



3. Enter the Name, Interface, VLAN Membership and Native VLAN. In this example:
   - the bridge is br0.
   - VLANs 10 and 11 are bridged to the native VLAN, VLAN10.
   - vap1.0 is added to the bridge.



Name: br0

Interfaces: eth1

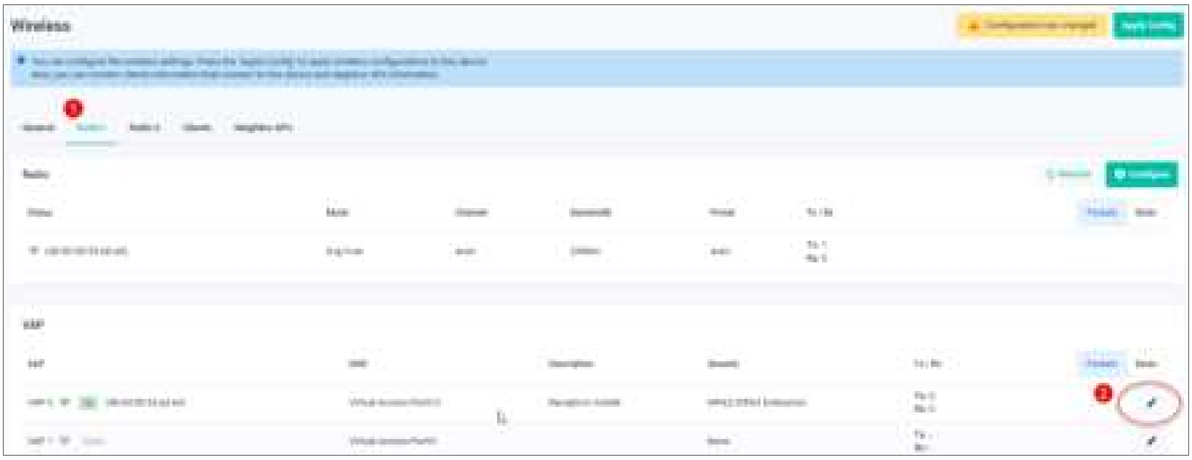
VLAN Membership: 10-11

Native VLAN: 10

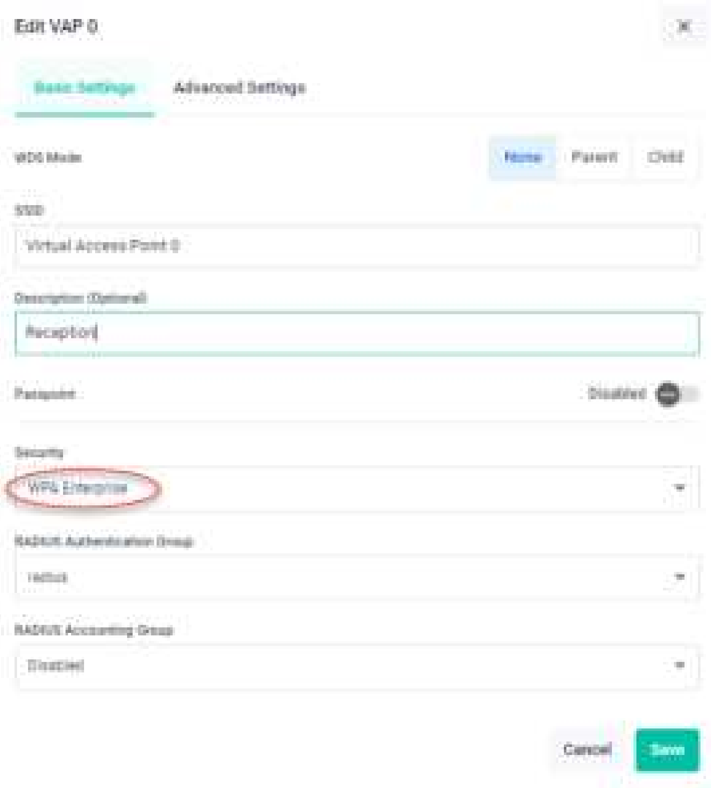
Set up WPA security

1. From the **Wireless** page, click on the **Radio1** tab to display the **Radio** and **VAP** settings.

2. Click on the **Edit** button for VAP 0.



3. Select **WPA Enterprise** from **Security**.



Edit VAP 0

WDS Mode: None | Parent | Child

SSID: Virtual Access Point 0

Description (Optional): Reception

Passpoint: Disabled

Security: WPA Enterprise

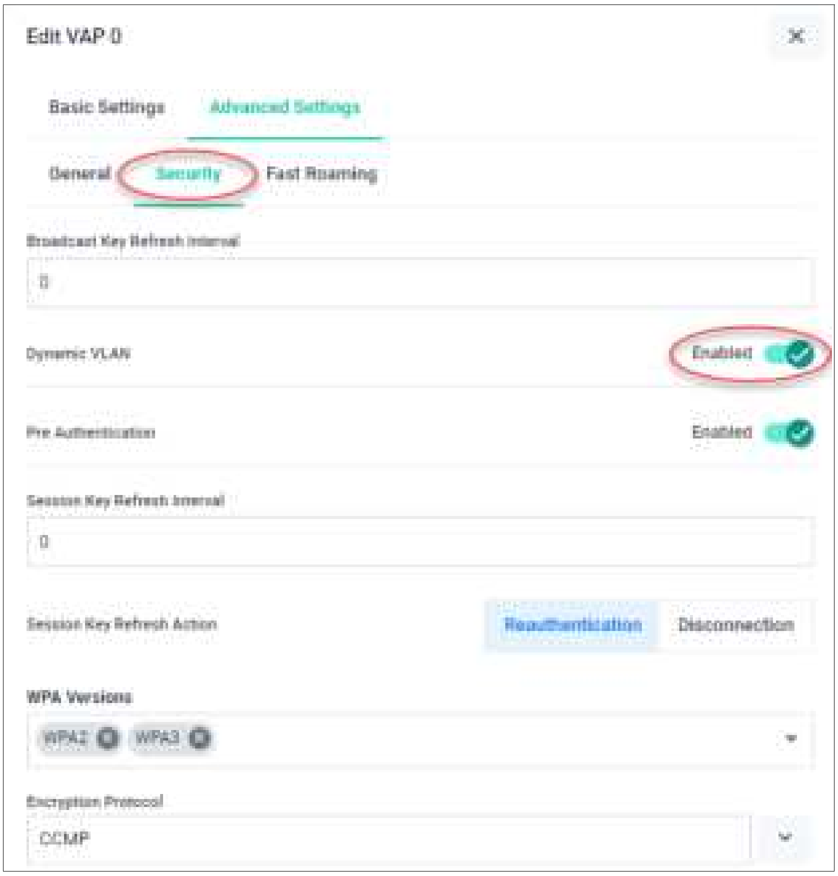
RADIUS Authentication Group: radtest

RADIUS Accounting Group: Disabled

4. Click on the **Advanced Settings** tab and then click on the **Security** tab.

5. **Enable** Dynamic VLAN.

6. Click **Save**.



Edit VAP 0

Broadcast Key Refresh Interval: 0

Dynamic VLAN: Enabled

Pre Authentication: Enabled

Session Key Refresh Interval: 0

Session Key Refresh Action: [✓ Reauthentication] Disconnection

WPA Versions: WPA2, WPA3

Encryption Protocol: CCMP

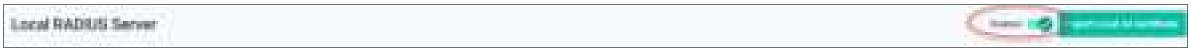
7. Click **Save**.

8. Apply and then save the configuration. See "Applying and saving your configuration" on page 6 for instructions.

MAC Authentication

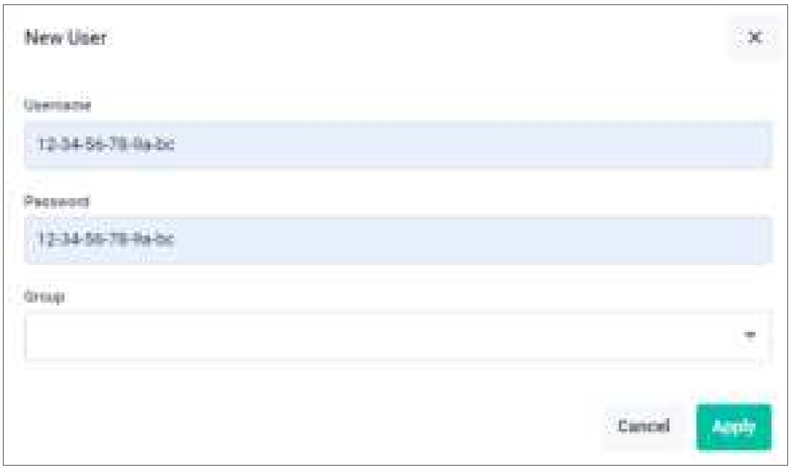
This section shows you how to set up MAC Authentication to secure your wireless network. You can use this in conjunction with WPA personal and WPA Enterprise.

1. From **Network Services** click on **RADIUS** to display the **Local RADIUS Server** page.
2. Enable the server with the **toggle** button to turn it on:



Add user

3. From the **Users** tab, click **+New User**.
4. Enter your device’s MAC address as the username and password. For example, if you add a printer with MAC address 12-34-56-78-9a-bc, then the password is also the same MAC address.
5. Click **Apply**.



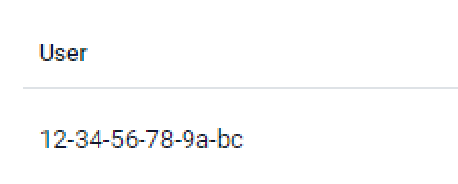
New User

Username: 12-34-56-78-9a-bc

Password: 12-34-56-78-9a-bc

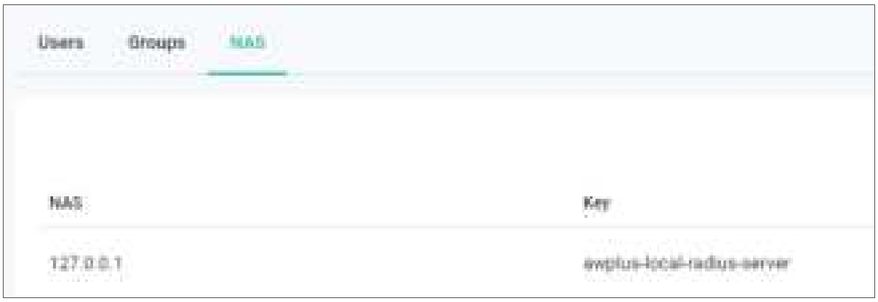
Group:

You can see the user that you added. You can edit it later if required:



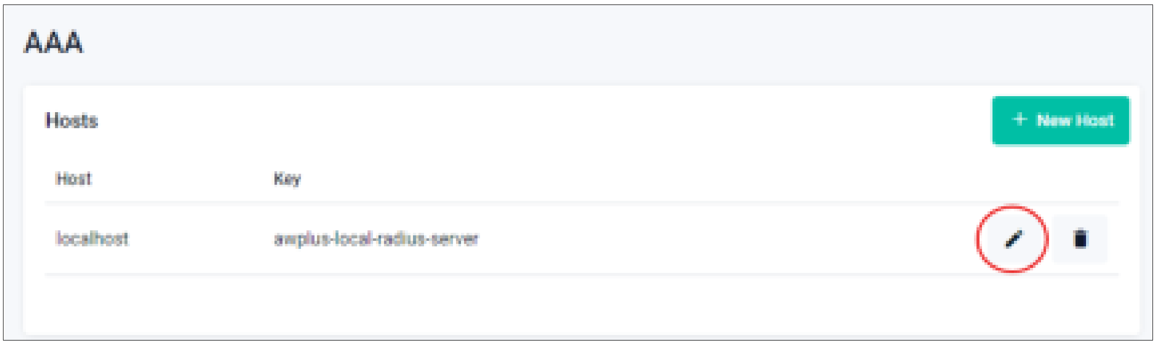
User
12-34-56-78-9a-bc

From the **NAS** tab notice that the **NAS** and **Key** fields automatically populate for the user you added:



NAS	Key
127.0.0.1	awplus-local-radius-server

6. From **Network Services > AAA**, check the Host is pointing to the RADIUS server. If required click the **Edit** button to make changes.



AAA

Hosts

Host	Key
localhost	awplus-local-radius-server

7. Apply and then save the configuration. See "Applying and saving your configuration" on page 6 for instructions.

MAC Authentication with Dynamic VLAN

From AlliedWare Plus version 5.5.4-2.3 and Device GUI version 2.19.0 onwards, Dynamic VLAN is supported for MAC Authentication.

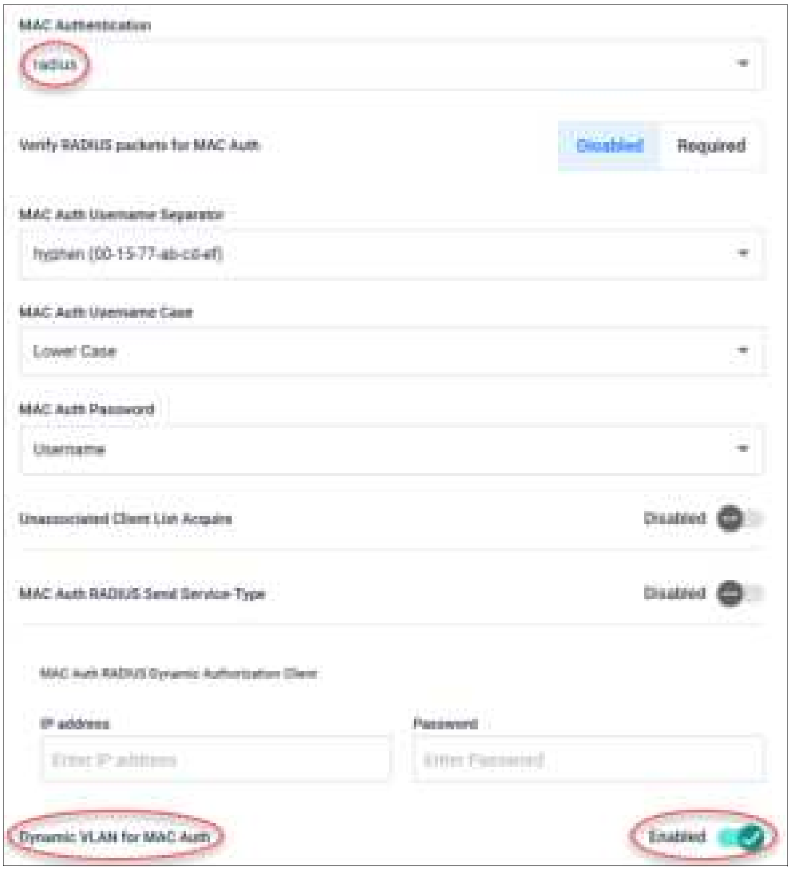
This enables dynamic VLAN assignment based on authentication, achieved through coordination between the TQR (authenticator) and the RADIUS server. When the RADIUS server sends a RADIUS Access-Accept message to the authenticator, it can include attributes specifying the VLAN to which the authenticated device should be assigned.

Previously, with MAC authentication, VLAN assignment was based on the VAP the client connected to. In contrast, Dynamic VLAN allows each client to be assigned a specific VLAN individually.

To enable MAC Authentication with Dynamic VLAN, select the required VAP as follows:

1. From **Wireless** > **Radio** > **Edit VAP**.
2. Click **Advanced Settings** > **Security**.
3. Select **radius** from the drop-down list for MAC Authentication.
4. Enable the **Dynamic VLAN for MAC Auth**.

This example shows the MAC Authentication field with the radius server selected, and the Dynamic VLAN for MAC Auth enabled:



MAC Authentication: radius

Verify RADIUS packets for MAC Auth: Disabled | Required

MAC Auth Username Separator: hyphen (00-15-77-ab-cd-ef)

MAC Auth Username Case: Lower Case

MAC Auth Password: Username

Unassociated Client List Acquire: Disabled

MAC Auth RADIUS Send Service-Type: Disabled

MAC Auth RADIUS Dynamic Authorization Client

IP address: Enter IP address

Password: Enter Password

Dynamic VLAN for MAC Auth: Enabled

Captive Portal

A Captive Portal allows wireless users to log in or accept terms before they can access the Internet or the wireless network.

The most standard use for a Captive Portal is to provide a gateway to allow an outside guest access to a Wi-Fi network. This is typical for any office or business that wants to keep visiting guests on a separate network from their internal business network. This is a security feature that ensures the main business network is safe. It prevents guests who may knowingly or unknowingly download a malicious program or virus from spreading to the main business network, while also allowing a business to potentially restrict access.

This is how it works

Wireless AP's monitor traffic from wireless clients. When they detect the first HTTP/HTTPS packets from each client, they redirect HTTP/HTTPS traffic from that client to a page called Captive Portal.

There are three types of Captive Portal:

- **RADIUS Authentication** - this method authenticates wireless clients. Use this if you want guests to log into the guest network using a username and password that you provide them with.
- **Click-through** - this method only asks clients to agree to the terms of use (click-through agreement) before allowing them to connect to the wireless network.The click-through page does not require authentication with a username/password pair, but can be configured to show an arbitrary 'Terms of Use' that clients have to accept before use, or to redirect to an external page. Use this if you don't need guests to log in.
- **External Page Redirect** - this method redirects the authentication page to a user configured URL such as a third-party Captive Portal vendor page. Use this if you want guests to login via the third-party vendor.

The next section describes how to use the device GUI to configure Captive Portal.

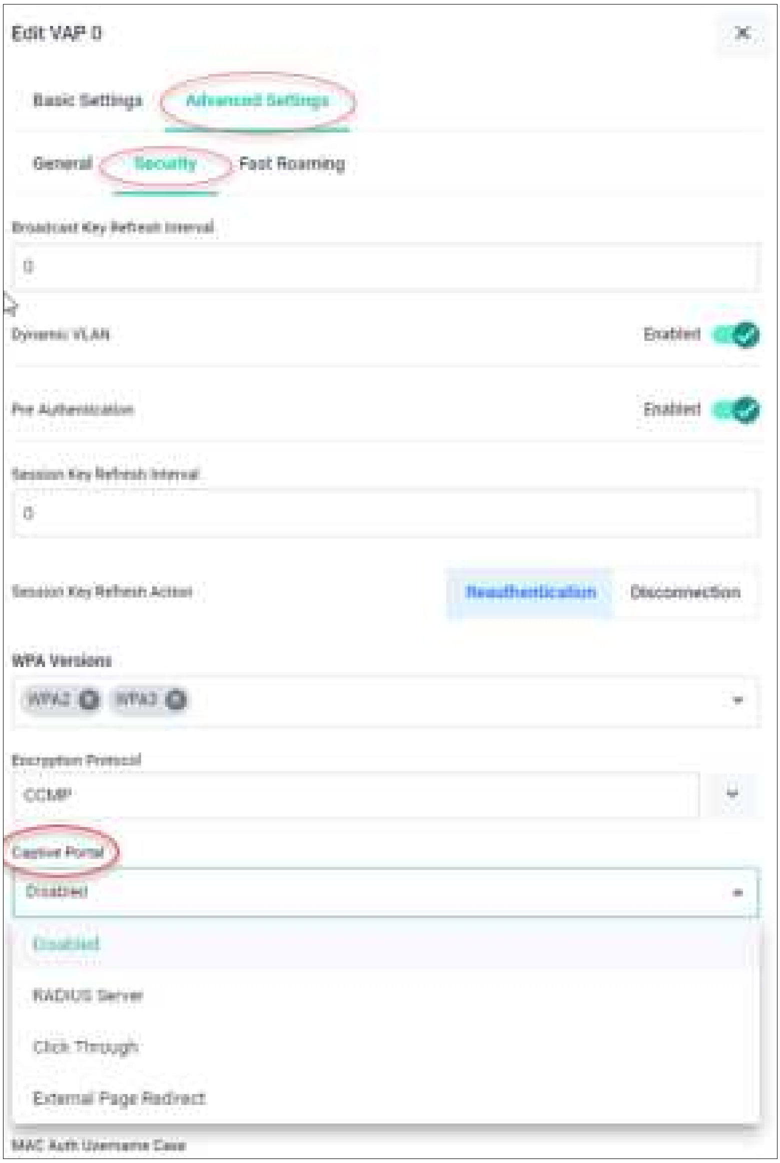
Configuring Captive Portal

This section describes how to configure Captive Portal.

Before you start, if you intend to use a RADIUS server with Captive Portal, you need to configure the RADIUS server first. See "WPA Enterprise with a RADIUS server" on page 9.

Selecting the type of Captive Portal installation

1. Click **Wireless** from the menu on the left, and then select the Radio you want to enable Captive Portal on. Click **Edit** VAP 0.
2. Click **Advanced Settings**.
3. Click the **Security** tab
4. Click on the **Captive Portal** options list to display the different types of installation. Notice that Captive Portal defaults to Disabled.



Edit VAP 0

Basic Settings | Advanced Settings

General | Security | Fast Roaming

Broadcast Key Refresh Interval: 0

Dynamic VLAN: Enabled

Pre Authentication: Enabled

Session Key Refresh Interval: 0

Session Key Refresh Action: Reauthentication | Disconnection

WPA Versions: WPA2, WPA3

Encryption Protocol: CCMP

Captive Portal: Disabled

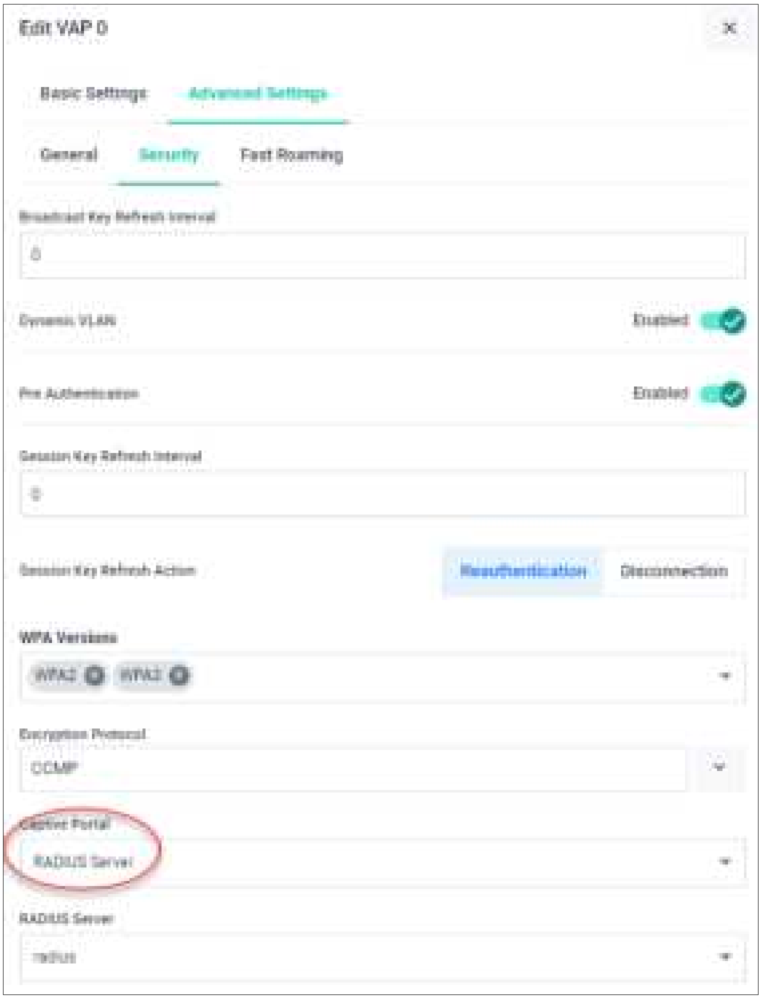
- Disabled
- RADIUS Server
- Click Through
- External Page Redirect

MAC Auth Username Case

Configuring RADIUS server

RADIUS uses the AP's local RADIUS server to authenticate clients.

1. Select RADIUS Server:



Edit VAP 0

Broadcast Key Refresh Interval: 0

Dynamic VLAN: Enabled

Pre Authentication: Enabled

Session Key Refresh Interval: 0

Session Key Refresh Action: Reauthentication | Disconnection

WPA Versions: WPA2, WPA3

Encryption Protocol: CCMP

Captive Portal: RADIUS Server

RADIUS Server: radius

2. (Optional) Select the RADIUS group. The default group is named 'radius'. If you want to use another RADIUS group that you have created, select that instead.

3. (Optional) Enable RADIUS Accounting if desired.

When accounting is enabled, the access point sends client information such as usage time to the RADIUS server.

4. (Optional) Configure Page Proxy if desired.

Page Proxy lets you display a customized authentication page. To use this, enable Page Proxy and then enter the URL that the proxy will use. When someone wants to login to the wireless network, the proxy will display the login page that is at URL/radius_login.html. You need to create the radius_login.html page, and failure and success pages; see "Configuring the Page Proxy" on page 27 for details.

5. (Optional) Configure Redirect Mode if desired.

Redirect Mode specifies what page the user will be shown after authentication.

- **Disabled** (the default): Do not redirect the browser after successful web authentication. The client will stay on the authentication page.
- **Fixed**: Always redirects to a fixed URL. Specify the URL in the Redirect URL field.
- **Session Keep**: Shows the page that was entered in the client's browser before web authentication. For example, if the client is trying to access the airport departures page from the airport Wi-Fi network, they will be redirected back to that departures page.

6. (Optional) Change the Session Timeout setting if desired.

You can change the timeout interval (how long before the client’s session ends) and specify whether to ask the client to re-authenticate or to end their session.

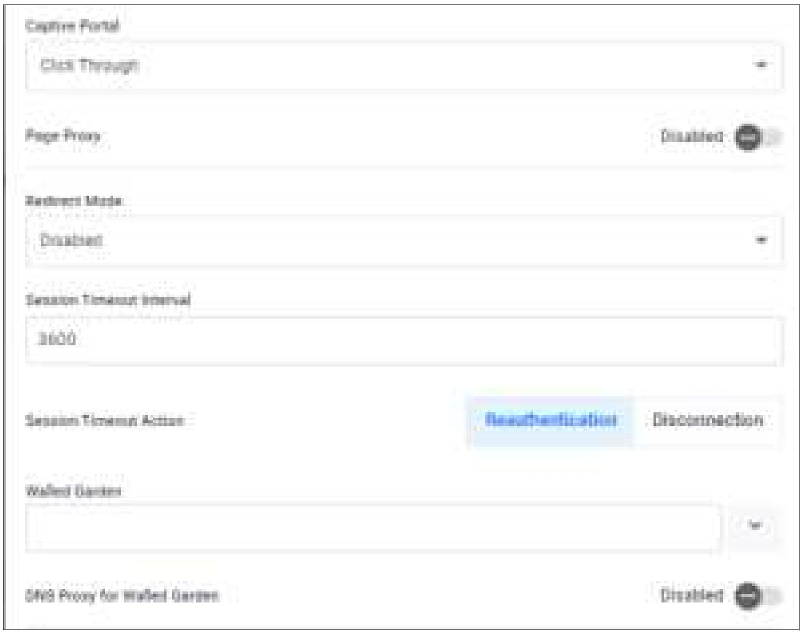
7. (Optional) Configure Walled Garden if desired.

A walled garden limits clients to accessing only a selection of web pages. Specify the IP, network, or FQDN address of the walled garden, and change other settings if required.

Configuring Click Through

Click Through requires clients to agree to terms of use, and then allows them to connect to the wireless network without authentication.

1. Select Click Through:



Captive Portal

Click Through

Page Proxy Disabled

Redirect Mode

Disabled

Session Timeout Interval

3600

Session Timeout Action Reauthentication Disconnection

Walled Garden

DNS Proxy for Walled Garden Disabled

2. (Optional) Configure Page Proxy if desired.

Page Proxy lets you display a customized authentication page. To use this, enable Page Proxy and then enter the URL that the proxy will use. When someone goes to login to the wireless network, the proxy will display the login page that is at URL/radius_login.html. You need to create the radius_login.html page, and failure and success pages; see "Configuring the Page Proxy" on page 27 for details.

3. (Optional) Configure Redirect Mode if desired.

Redirect Mode specifies what page the user will be shown after authentication.

- **Disabled (the default):** Do not redirect the browser after successful web authentication. The client will stay on the authentication page.
- **Fixed**: Always redirects to a fixed URL. Specify the URL in the Redirect URL field.
- **Session Keep**: Shows the page that was entered in the client's browser before web authentication. For example, if the client is trying to access the airport departures page from the airport Wi-Fi network, they will be redirected back to that departures page.

4. (Optional) Change the Session Timeout settings if desired.

You can change the timeout interval (how long before the client's session ends) and specify whether to ask the client to re-authenticate or to end their session.

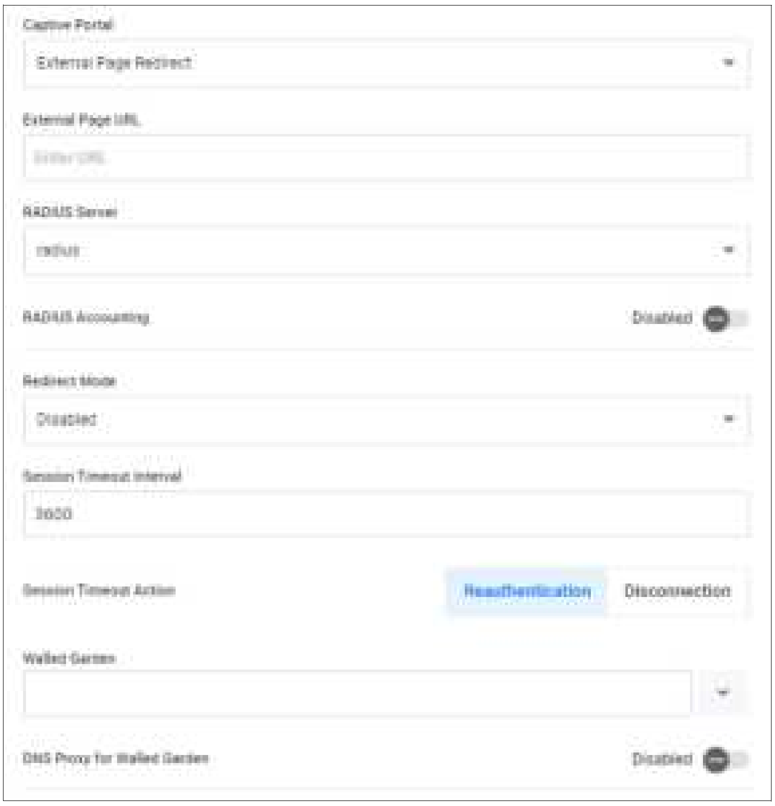
5. (Optional) Configure Walled Garden if desired.

A walled garden limits clients to accessing only a selection of web pages. Specify the IP, network, or FQDN address of the walled garden, and change other settings if required.

Configuring External Page Redirect

External Page Redirect gets clients to login via a third-party service.

1. Select External Page Redirect:



Captive Portal

External Page Redirect

External Page URL

Enter URL

RADIUS Server

radius

RADIUS Accounting: Disabled

Redirect Mode

Disabled

Session Timeout Interval

3600

Session Timeout Action: [✓ Reauthentication] Disconnection

Walled Garden

DNS Proxy for Walled Garden: Disabled

2. Enter the External Page URL of the third-party service.
3. Configure the RADIUS settings. The third party service will prove the settings to use.
4. (Optional) Configure Redirect Mode if desired.

Redirect Mode specifies what page the user will be shown after authentication.

- **Disabled (the default):** Do not redirect the browser after successful web authentication. The client will stay on the authentication page.
- **Fixed**: Always redirects to a fixed URL. Specify the URL in the Redirect URL field.
- **Session Keep**: Shows the page that was entered in the client's browser before web authentication. For example, if the client is trying to access the airport departures page from the airport Wi-Fi network, they will be redirected back to that departures page.

5. (Optional) Change the Session Timeout settings if desired.

   You can change the timeout interval (how long before the client's session ends) and specify whether to ask the client to re-authenticate or to end their session.

6. (Optional) Configure Walled Garden if desired.

A walled garden limits clients to accessing only a selection of web pages. Specify the IP, network, or FQDN address of the walled garden, and change other settings if required.

Configuring the Page Proxy

If you configure a Page Proxy so you can use a customized authentication page, you need to create login, failure, and success pages. This section describes the requirements for these pages.

Authentication login page

- Filename

The filename of the external authentication page must be ‘radius_login.html’.

For example, when you specify ‘http://www.example.com/captive_portal’ in the Page Proxy URL field, APs will present the content of the page at ‘http://www.example.com/captive_portal/radius_login.html’ to connecting clients.

- HTML File Content

The authentication page on the external Web server should contain the following HTML form elements:

```
<form method="POST">
<input type="text" name="userid">
<input type="password" name="password">
<input type="submit" value="Connect">
</form>
```

The value of the **submit** button does not have to be ‘Connect’. Also, the submit button can be a <button> element instead of <input type="submit">.

Authentication login failure page

- Filename

The external authentication failure page must be named ‘radius_login_fail.html’. For example, if the Page Proxy URL is ‘http://www.example.com/captive_portal’, APs will serve ‘http://www.example.com/captive_portal/radius_login_fail.html’ to clients.”

- HTML File Content

This is the same as the Authentication Login Page. The authentication page on the external Web server should contain the following HTML form elements:

```
<form method="POST">
<input type="text" name="userid">
<input type="password" name="password">
<input type="submit" value="Connect">
</form>
```

The value of the submit button does not have to be ‘Connect’. Also, the submit button can be a <button> element instead of <input type="submit">.

Authentication success page (welcome)

- Filename

The filename of the external successful authentication page must be ‘welcome.html’.

For example, if you specify ‘http://www.example.com/captive_portal’ in the ‘Page Proxy URL’, APs will present the content of the page at ‘http://www.example.com/captive_portal/welcome.html’ to connecting clients.

- HTML File Content

There is no special HTML form requirement for the authentication success page.

Passpoint

Introduction

You can enable Passpoint on your wireless networks from the Device GUI version 2.18.0 and AlliedWare Plus software version 5.5.4-1.1 or later.

Passpoint™, also known as Hotspot 2.0, is the open standard for public Wi-Fi, introduced by the Wi-Fi Alliance™. Passpoint brings seamless, secure Wi-Fi connectivity to any network employing Passpoint enabled Wi-Fi hotspots. It also provides user connections with WPA3™ security protection, enabling users to feel confident that their data is safe.

How does it work?

Passpoint lets users sign in to a WI-Fi hotspot once, then uses their credentials as their devices hop from one access point to the next. Users' authentication occurs every time they connect. Of course, the hotspot (i.e., router) must support Passpoint for this connectivity transfer to happen.

Once a user accesses the Wi-Fi network offered at a location, the Passpoint-enabled client device will automatically connect upon subsequent visits. This eliminates the need for users to search for and choose a network, request Wi-Fi access, and re-enter authentication credentials each time they visit.

Passpoint improves the mobile user experience by offering:

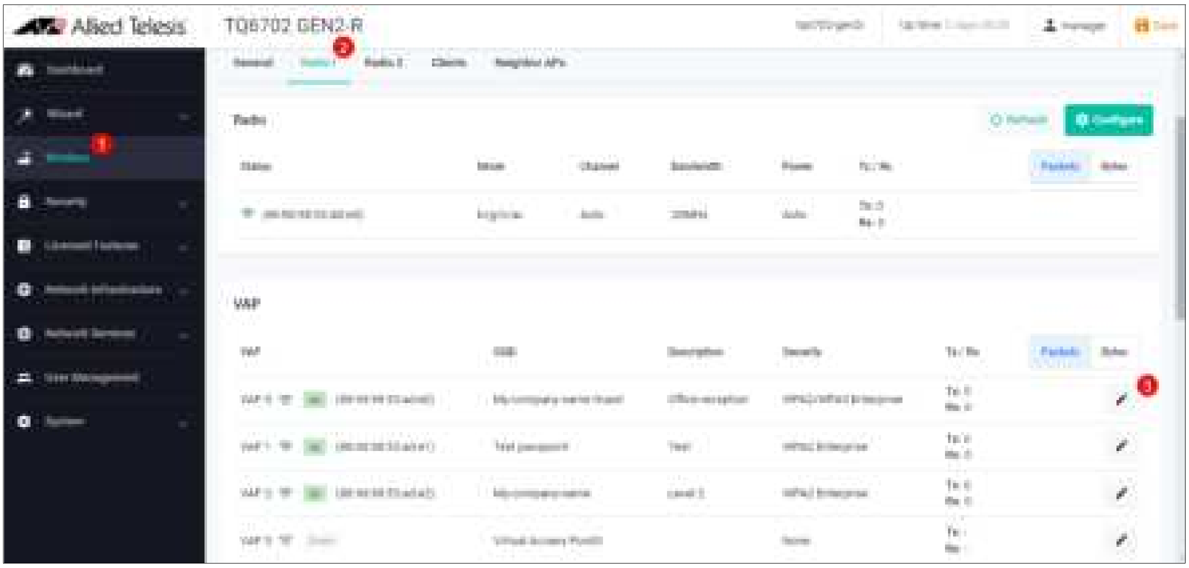
- Automatic network discovery and selection
- Simplified online sign-up and instant account provisioning
- Seamless network access and cellular-like roaming between hotspots
- Enhanced security.

Configuring Passpoint

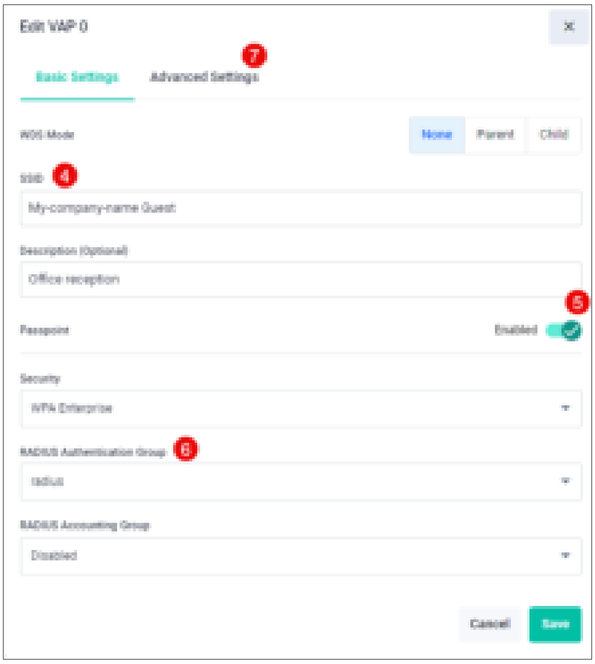
Step 1: **Enable Passpoint**

Follow these steps to enable Passpoint on a VAP. You can edit an existing VAP or create a new one.

1. Click on **Wireless** from the menu bar.
2. Select the Radio tab to configure one of the radios (The default is Radio1).
3. Click on the **Edit** button to select a VAP to configure (The default is VAP0).



4. Enter the **SSID** and optional **Description** if required.
5. Enable Passpoint (**WPA Enterprise** automatically populates the **Security** field).
6. Select **radius** from the RADIUS Authentication Group drop down list.
7. Click on the **Advanced Settings** tab to configure 802.11u and Passpoint.



WDS Mode: None

SSID: My-company-name Guest

Description (Optional): Office reception

Passpoint: Enabled

Security: WPA Enterprise

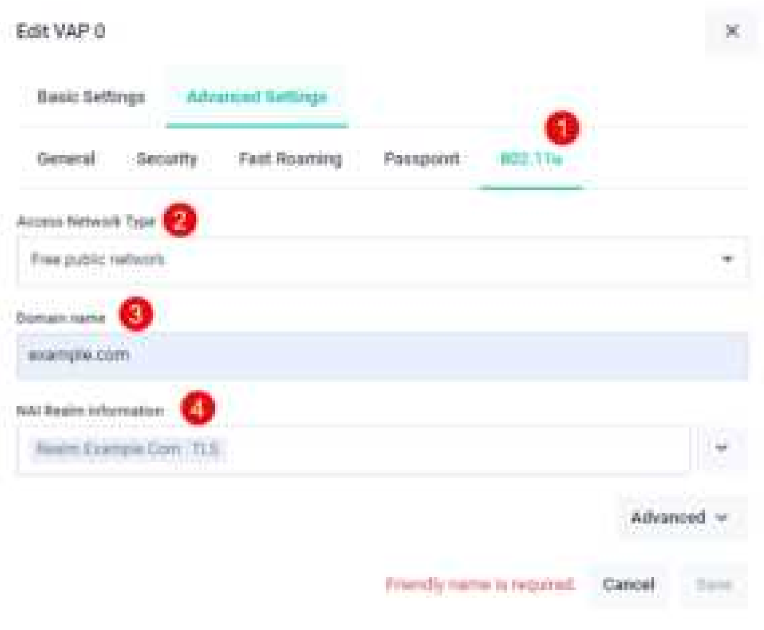
RADIUS Authentication Group: radius

RADIUS Accounting Group: Disabled

Step 2: Configure 802.11u

1. Click on the **802.11u** tab.
2. Select the **Access Network Type** from the drop down list.
3. Enter the **Domain Name**.
4. Enter the **NAI Realm information**.

See the table **Basic options for 802.11u settings** for field descriptions.



Edit VAP 0

Basic Settings | Advanced Settings

General | Security | Fast Roaming | Passpoint | 802.11u

Access Network Type: Free public network

Domain name: example.com

NAI Realm information: Realm Example Com : TLS

Friendly name is required.

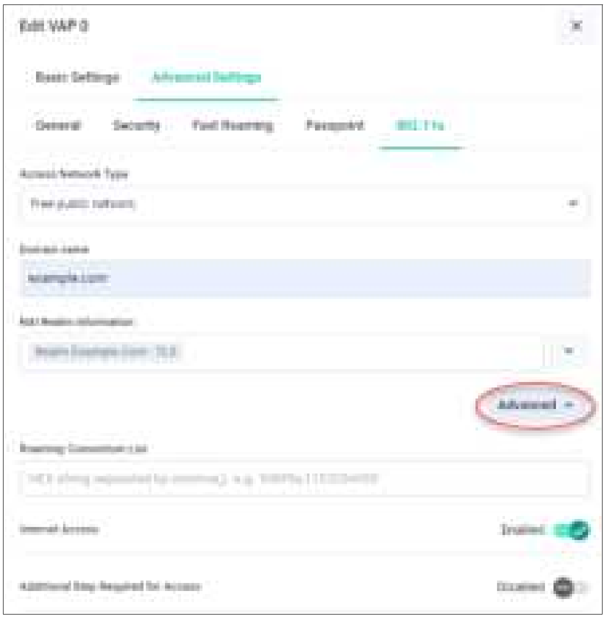
Table 3: Basic options for 802.11u settings

FIELD	DESCRIPTION
Access Network Type	Specify any of the following 802.11u network types. **Private network** — This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. **Private network with guest access**— This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. **Chargeable public network** — This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. **Free public network** —This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. **Personal device network** — This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. **Emergency service only network** —This network is limited to accessing emergency services only. **Test or experimental** — This network is used for test purposes only. **Wildcard** —This network indicates a wildcard network.
Domain Name	Domain name of the access network operator, which is the identifier of the operated Hotspot2.0 network. For example, 'example.com, example.net.'

Table 3: Basic options for 802.11u settings (continued)

FIELD	DESCRIPTION
NAI Realm information	The Network Access Identifier (NAI) Realm information. The realm in the NAI format is represented after the @ symbol, which is specified as domain.com. For example: user@realm.example.com. The EAP method is the method that this NAI realm uses for authentication: ■ TLS (the default) ■ TTLS ■ SIM ■ AKA

If you want to configure Advanced settings for 802.11u, click on the **Advanced** button to expand more settings. See the table **Advanced options for 802.11u settings** for field descriptions.



Access Network Type: Free public network

Domain name: example.com

NAI Realm information: Realm Example.com : TLS

Roaming Consortium List: HEX string separated by comma(,), e.g. 506f9a,1122334455

Internet Access: Enabled

Additional Step Required for Access: Disabled

Table 4: Advanced options for 802.11u settings

FIELD	DESCRIPTION
Roaming Consortium List	A group of subscription service providers (SSPs) having inter-SSP roaming agreements. The Roaming Consortium list tells a mobile device which roaming consortiums or service providers are available through an AP. The list must be in Hexadecimal format. For example, ‘506f9a, 001aeb, 1122334455’.
Internet Access	Internet access, enable or disable.
Additional Step Required for Access (ASRA)	Enable or disable. The ASRA field tells the higher layer protocols on the client device what steps to take (e.g. URL redirection, terms and conditions, etc.) after the connection is made.
Emergency services reachable	Enable or disable. 802.11u provides a means for the client devices to learn about emergency services prior to association and then to support them at the link-level.

Table 4: Advanced options for 802.11u settings (continued)

FIELD	DESCRIPTION
Unauthenticated emergency service accessible	Controls whether the VAP can supply access to unauthenticated individuals to emergency services. Here are the settings: Enabled: The VAP can provide access to unauthenticated individuals to emergency services. Disabled: The VAP cannot provide access to emergency services. This is the default
Venue Group	The general class of venue, such as: ■ Assembly ■ Business ■ Educational ■ Industrial ■ Residential ■ Vehicular ■ Outdoor Specifies the venue group code, which identifies the general category of the physical site of the access point. The default is 7, Residential.
Venue Type	The code of the specific type of venue within each group. For example, venue types in the ‘Assembly’ group include: ■ Arena ■ Stadium ■ Place of Worship ■ Library ■ Restaurant The default is 1, Hotel or motel.
Homogeneous ESS Identifier HEISS	Homogeneous Extended Service Set Identifier. The device MAC address in a hexadecimal format separated by colons. For example, 10:22:33:44:55:66.
Network Authentication Type	Network Authentication Type Information — if this is an unsecured network, specify the additional steps required for access (ASRA): ■ Terms and conditions ■ Online enrollment ■ Redirect http/https ■ Redirect DNS ■ Redirect URL - For each Network Authentication Type you can enter a re-direct URL. The maximum length is 128 characters with ASCII. The following symbols are not permitted: { } l \ ^ [ ]

Table 4: Advanced options for 802.11u settings (continued)

FIELD	DESCRIPTION
IP Address Type Availability	IPv4 and IPv6 address type availability information. Options include: ■ Exist ■ No exist ■ Public ■ Port restrict ■ Private Nat1 and Nat 2 ■ Port private Nat1 and Nat 2 ■ Unknown
Venue Name	Venue Name information — a pair of name and language code (as defined in ISO 639). This indicates the name of the venue for the network, which may be useful to a user for network selection.
3GPP Cellular Network Information	The cellular network identifier. This is a string concatenated Mobile Country Code (MCC) and comma(,) and Mobile Network Code (MNC). The MCC code is three digits, and the MNC is two or three digits. For example: '440,10' means 'NTT DoCoMo, Inc' which is a mobile network in Japan. Each 'MCC, MNC' pair is separated by a semi-colon(;). For example: '440,10;440,50' For more information on mobile network codes, see: Mobile Network Codes
Arbitrary ANQP-element configuration	ANQP (Access Network Query Protocol), consists of a pair of ID (1-99) and payload (Hex) elements. For more information, see IEEE specification 802.11-2016.pdf. You can find information on this in Table 9-271—ANQP-element definitions, page 1127. ANQP is a query and response protocol used by stations to discover information about the network. GAS frames are used to transport the Access Network Query Protocol.
GAS Address 3 behavior	The Generic Advertisement Service (GAS) is a framework that provides transport for advertisement services like ANQP. GAS is used as a container for ANQP elements sent between clients and APs. Select one of the following options: ■ P2P Specification ■ IEEE 802.11 Standard ■ Force Non-Compliant Behavior
GAS Comeback Delay	The GAS Comeback Delay is the delay, in milliseconds, between the initial GAS response and the first comeback request. (0-65535)

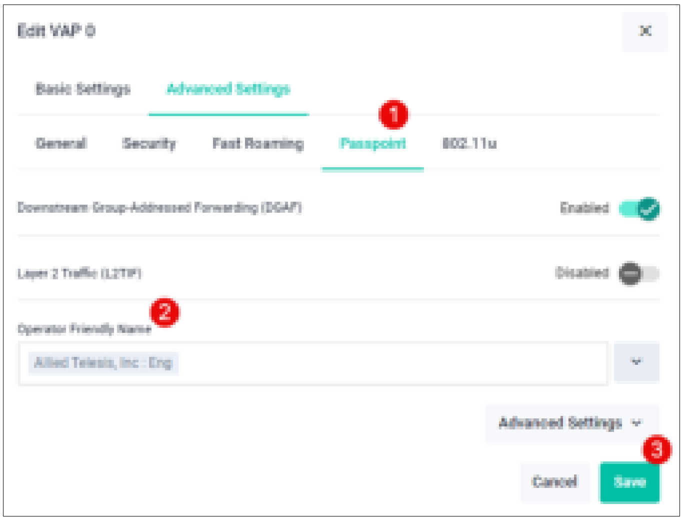
Table 4: Advanced options for 802.11u settings (continued)

FIELD	DESCRIPTION
QoS Map Set	The QoS Map Set Information element. This element contains a list of 802.11 user priorities (UP), to which a range of DSCP (i.e. IP QoS) values are mapped. When 802.11u-compatible client stations receive the QoS map, they use it to map the IP layer priority (i.e. DSCP field) to an 802.11 priority. As frames are passed from the IP layer of the device's networking stack to the MAC layer, they are mapped according to the 802.11u policy provided by the AP. Likewise, APs follow these maps on downlink QoS frames received from the wired network and sent to the client. This mapping enables the consistent end-to-end policies desired by service providers. Example data: 53,2,22,6,8,15,0,7,255,255,16,31,32,39,255,255,40,47,255,255 Format: [<DSCP Exceptions[DSCP,UP]>,[<UP 0 range[low,high]>,...<UP 7 range[low,high]> DSCP Exception 1: 53,2 (The DSCP Value 53 would use User Priority 2 exceptionally) DSCP Exception 2: 22,6 (The DSCP Value 22 would use User Priority 6 exceptionally) User Priority 0 : 8,15 (The DSCP Range is 8 to 15) User Priority 1 : 0,7 (The DSCP Range is 0 to 7) User Priority 2 : 255,255 (Unuse) User Priority 3 : 16,31 (The DSCP Range is 16 to 31) User Priority 4 : 32,39 (The DSCP Range is 32 to 39) User Priority 5 : 255,255 (Unuse) User Priority 6 : 40,47 (The DSCP Range is 40 to 47) User Priority 7 : 255,255 (Unuse)

Step 3: **Configure Passpoint**

1. Click on the **Passpoint** tab.
2. Enter the **Operator Friendly Name**.
3. Click **Save**.

See the table **Basic Options for Passpoint settings** for field descriptions.


Edit VAP 0

Downstream Group-Addressed Forwarding (DGAF): Enabled

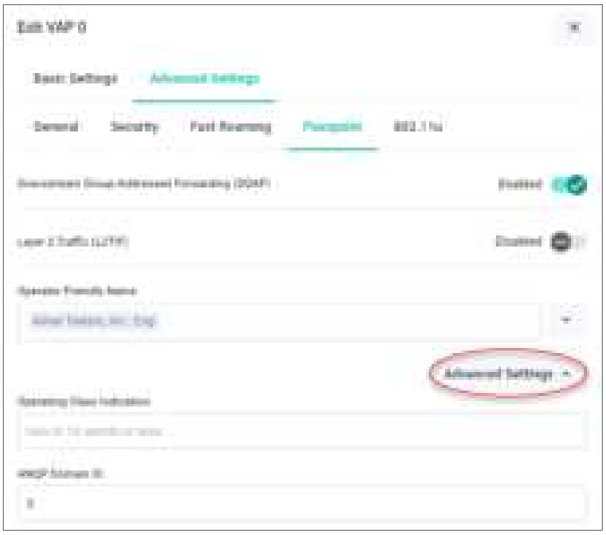
Layer 2 Traffic (L2TIF): Disabled

Operator Friendly Name: Allied Telesis, Inc : Eng

Table 5: Basic Options for Passpoint settings

Field	Description
Downstream Group-Address Forwarding (DGAF)	Select Enabled to disable Downstream Group-Addressed Forwarding.
L2 Traffic Inspection and Filtering	If you want to discard L2 traffic between VAPs, enable L2 Traffic Injection and Filtering. The packets that TQ restricts are: ARP, ICMP, and TDLS.
Operator Friendly Name	Friendly Name: the name of the operator you are providing. Language Code: the language code For example: <friendly name><language code> Allied Telesis Inc.eng

If you want to configure Advanced settings for Passpoint, click on the **Advanced** button to expand more settings. See the table **Advanced Options for Passpoint settings** for field descriptions.


Edit VAP 0

Downstream Group-Addressed Forwarding (DGAF): Enabled

Layer 2 Traffic (L2TIF): Disabled

Operator Friendly Name: Allied Telesis, Inc : Eng

Operating Class Indication

Table 6: Advanced Options for Passpoint settings

Field	Description
Operating Class Indication	The HEX number of the radio information. For example, ‘517376’ means using 1-13ch and 36-64ch(20MHz). The default is blank.
ANQP Domain ID	Configures the Hotspot 2.0 ANQP (Access Network Query Protocol) domain identifier. Optional - If you don’t configure this, the default ‘0’ is set.
Deauthentication Request Timeout	Optional - If you don’t configure this, the default ‘60’ is set.
Connection Capabilities	Optional, and includes the following fields: ■ IP Protocol Number ■ Port Number ■ Port Status
WAN Metrics	Optional, and includes the following fields: ■ At Capacity ■ Symmetric Link ■ Link Status ■ Uplink Load ■ Downlink Load ■ Uplink Speed ■ Downlink Speed ■ Load Measure Duration

Optional advanced features

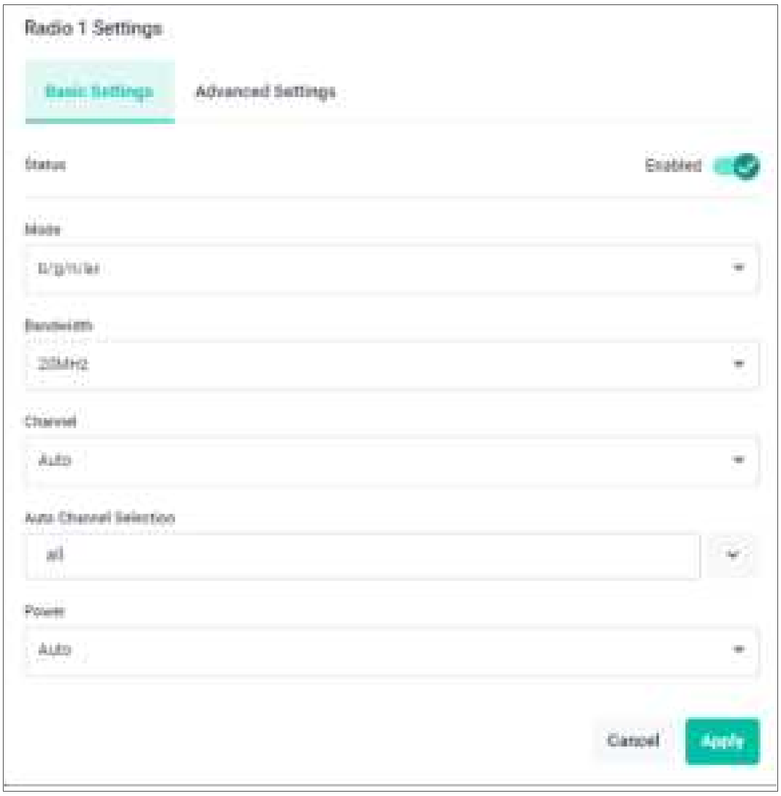
Radio settings

The following basic and advanced radio settings are available from the **Wireless > Radio 1** and **Radio 2** tabs for the TQ6702 GEN2-R. For the TQ7403-R, Radio 3 options are available from the **Wireless > Radio 3** tab.

Radio 1 settings

1. Click the **Configure** button from **Radio** settings.

From the **Radio 1 Settings** dialog **Basic Settings** tab, the following options are available:



Radio 1 Settings

Status: Enabled

Mode: b/g/n/ax

Bandwidth: 20MHz

Channel: Auto

Auto Channel Selection: all

Power: Auto

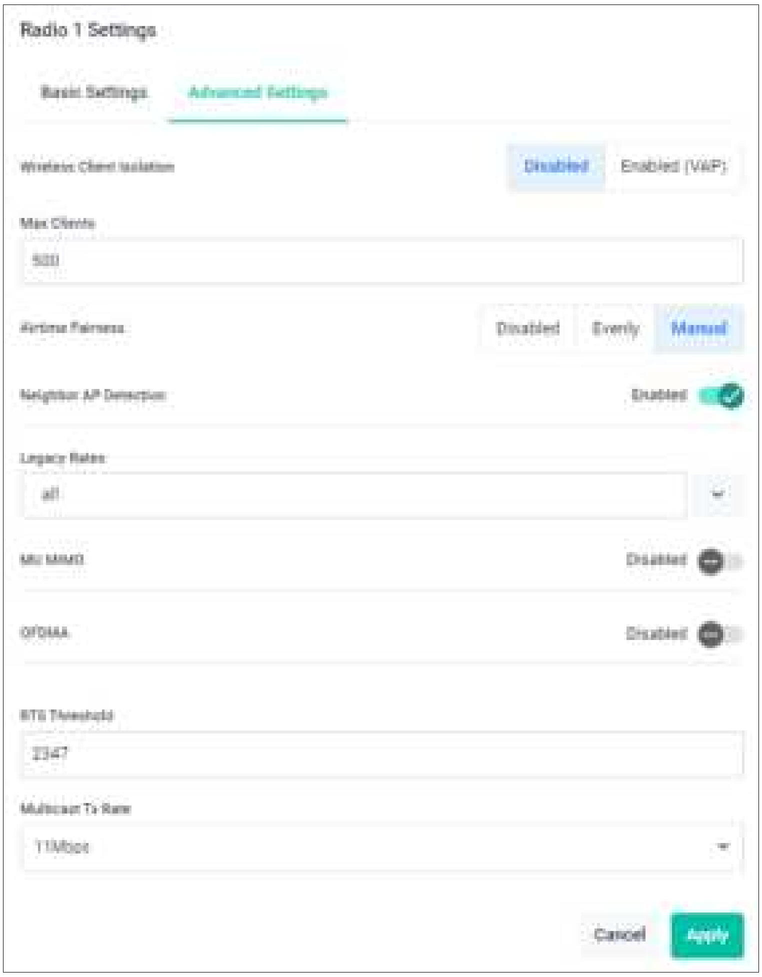
Table 7: Basic Radio1 settings

FIELD	DESCRIPTION
Status	The default is Enabled and displays the Up or Down status and MAC address for each VAP. The Status can be enabled or disabled.
Mode	The mode can be set to b/g, b/g/n or b/g/n/ax. The default is b/g/n/ax. When you select the mode, the bandwidth displays what is available for each mode.
Bandwidth	The bandwidth can be set to 20MHz or 40MHz. The default is 20MHz.
Channel	The default is auto. You can select different channels if required.
Auto Channel Selection	The default is all. You can select specific channels if required.
Power	The default is auto.You can select from Max, High, Middle, Low or Min if required.

2. Click the **Apply** button to apply any changes you have made.

3. Click on the **Advanced Settings** tab.

From the **Radio 1 Settings** dialog **Advanced Settings** tab, the following options are available:



Radio 1 Settings

Basic Settings | Advanced Settings

Wireless Client Isolation: [✓ Disabled] Enabled (VAP)

Max Clients: 500

Airtime Fairness: Disabled Evenly [✓ Manual]

Neighbor AP Detection: Enabled

Legacy Rates: all

MU MIMO: Disabled

OFDMA: Disabled

RTS Threshold: 2347

Multicast Tx Rate: 11Mbps

Table 8: Advanced Radio settings

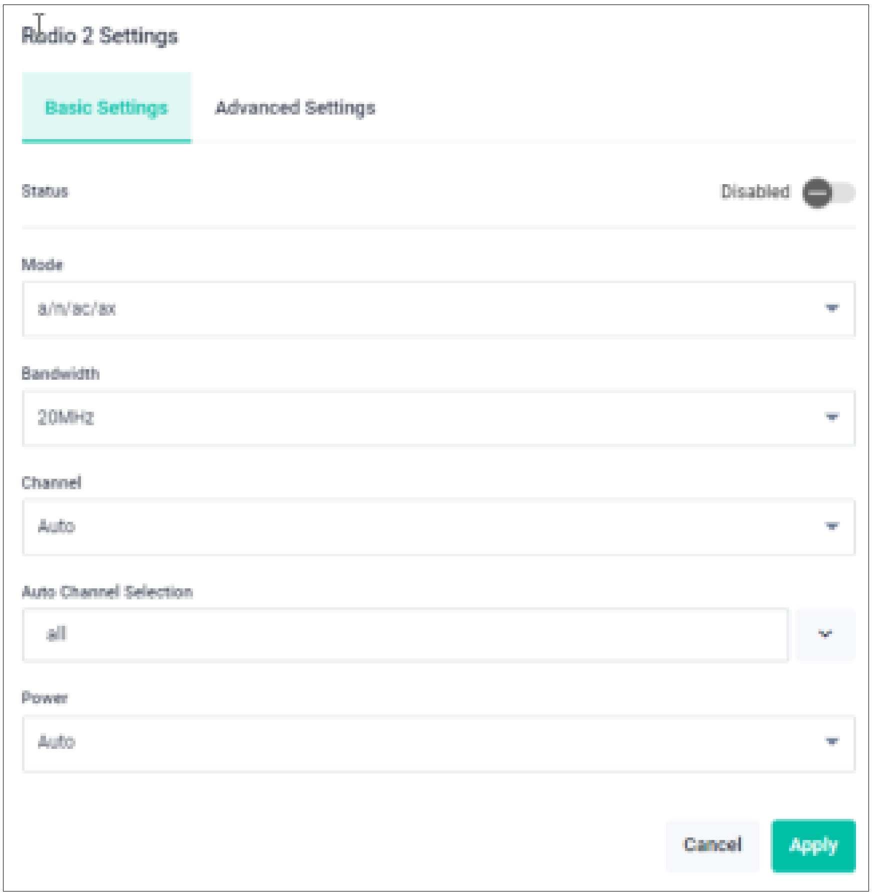
FIELD	DESCRIPTION
Wireless Client isolation	The default is disabled.
Max Clients	The maximum number of clients defaults to 500.
Airtime Fairness	Airtime fairness defaults to disabled.
Neighbor AP Detection	Neighbor AP detection defaults to disabled.
Legacy Rates	From release 5.5.4-2.3 onwards, you are no longer required to specify a basic rate for Radio 1. The legacy rates defaults to all. You can select one or more legacy rates from the drop down list if required. The selection is one or more of 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 or 1.
MU MIMO	MU MIMO defaults to disabled.
OFDMA	OFDMA defaults to disabled.
RTS Threshold	The RTS Threshold defaults to 2347.
Multicast Tx Rate	The Multicast Transmission Rate defaults to 11Mbps. You can select 54 Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 11Mbps, 9Mbps, 6Mbps, 5.5Mbps, 2Mbps, or 1Mbps if required.

4. Click the **Apply** button to apply any changes you have made.

Radio 2 settings

Basic and advanced radio settings are also available from **Wireless > Radio 2**.

From the **Radio 2 Settings** dialog **Basic Settings** tab, the options are the same as for Radio1 except the options listed in the table below:



Status: Disabled

Mode: a/n/ac/ax

Bandwidth: 20MHz

Channel: Auto

Auto Channel Selection: all

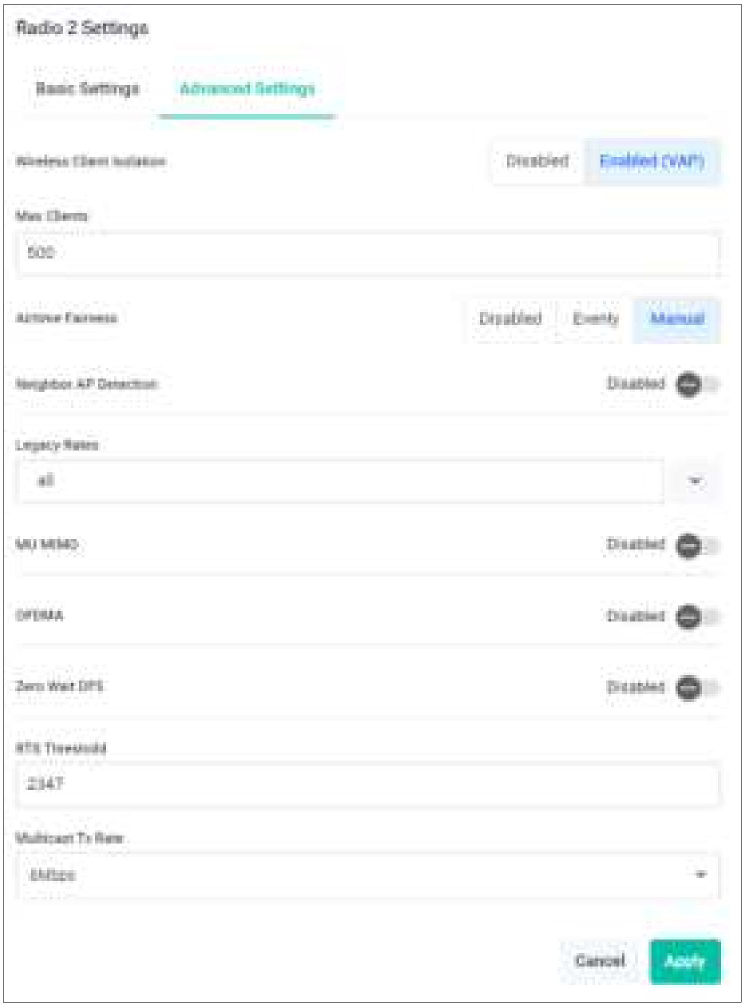
Power: Auto

Table 9: Basic Radio settings

FIELD	DESCRIPTION
Mode	The mode can be set to a, a/n, a/n/ac or a/n/ac/ax. The default is a/n/ac/ax. When you select the mode, the bandwidth displays what is available for each mode.
Bandwidth	The bandwidth can be set to 20MHz, 40MHz, 80MHz or 80+80MHz. The default is 20MHz.

Radio 2 Advanced settings has an additional setting for **Zero Wait DFS** which is not available for Radio1 and the **Multicast Tx Rate** has different options.

From the **Advanced Settings** tab the following options are available:



Radio 2 Settings

Wireless Client Isolation: Disabled | Enabled (VAP)

Max Clients: 500

Airtime Fairness: Disabled | Evenly | Manual

Neighbor AP Detection: Disabled

Legacy Rates: all

MU MIMO: Disabled

OFDMA: Disabled

Zero Wait DFS: Disabled

RTS Threshold: 2347

Multicast Tx Rate: 6Mbps

Table 10: Advanced Radio settings

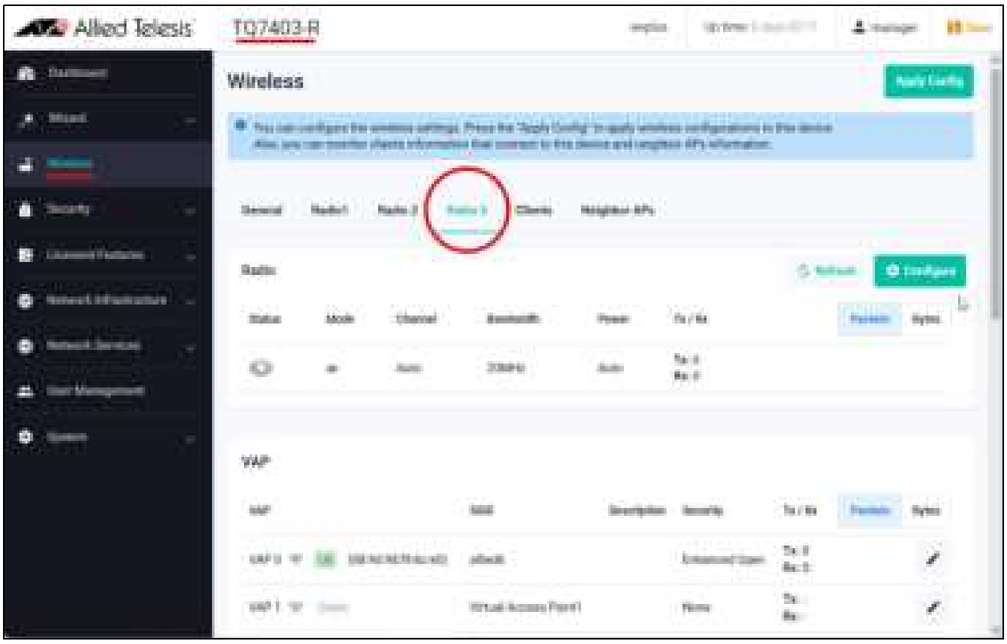
FIELD	DESCRIPTION
Zero Wait DFS	Zero Wait DFS defaults to Disabled.
Multicast Tx Rate	The Multicast Transmission Rate defaults to 6 Mbps. You can select 6 Mbps, 12 Mbps or 24 Mbps if required.

Click the **Apply** button to apply any changes you have made.

Radio 3 settings

Basic and advanced radio settings are also available for **Radio 3** on the **TQ7403-R** wireless router.

The TQ7403-R supports 2.4GHz, 5GHz, and 6GHz radios. The 6Hz band uses an internal antenna for increased efficiency and throughput, while the 2.4GHz and 5GHz bands use an external antenna.



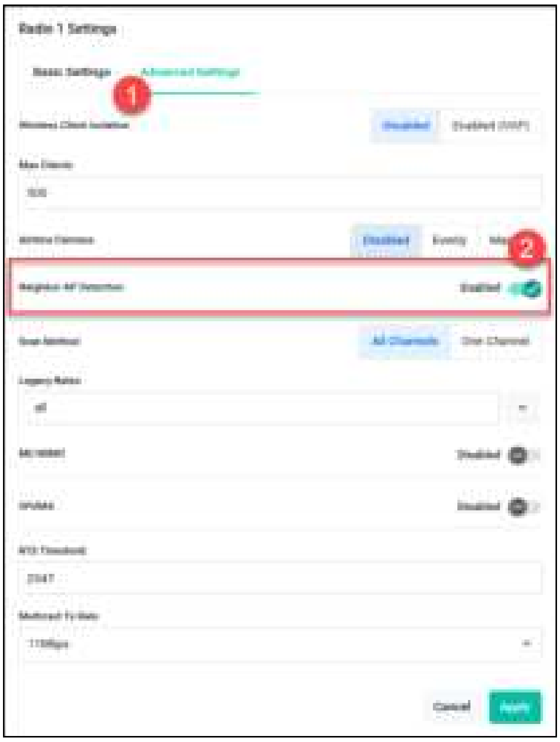
Radio scanning

The RFScan feature is used to detect neighbor APs. The scans in each Radio are performed in parallel. For each Radio, you can select between scanning one channel at a time and scanning all channels at once.

- **All-Channel Scan**: Scans all channels at once.
- **Single-Channel Scan**: Scans one channel at a time, allowing configuration of scan interval, duration, and data retention.

To configure these settings:

1. Go to: **Wireless** > **Radio X** > **Configure** > **Advanced Settings** tab
2. Enable **Neighbor AP Detection**
3. Select Scan Method, **All Channels** or **One Channel**



Radio 1 Settings

Basic Settings | Advanced Settings

Wireless Client Isolation: Disabled | Enabled (SAP)

Max Clients: 500

Airtime Fairness: Disabled | Evenly | Ma

Neighbor AP Detection: Enabled

Scan Method: All Channels | One Channel

Legacy Rates: all

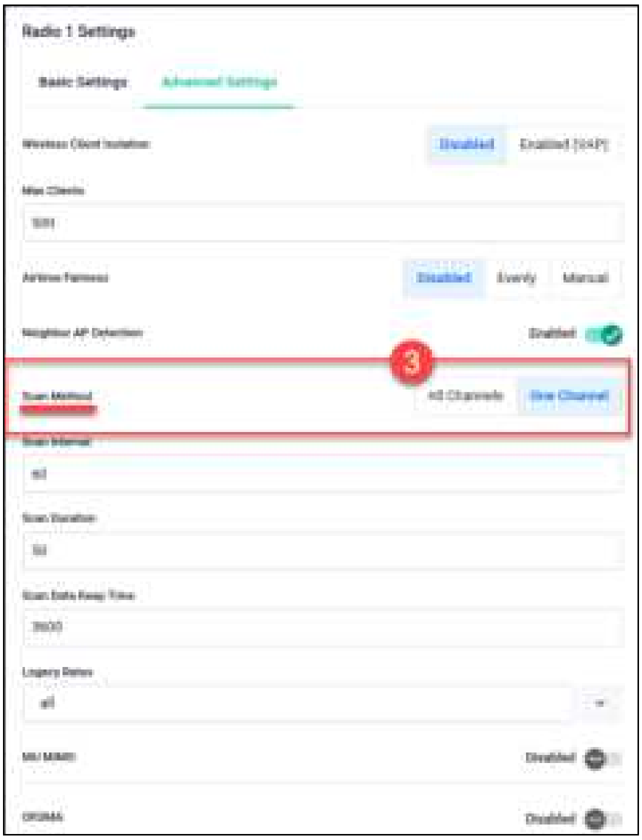
MU MIMO: Disabled

OFDMA: Disabled

RTS Threshold: 2347

Multicast Tx Rate: 11Mbps

Cancel | Apply



Radio 1 Settings

Basic Settings | Advanced Settings

Wireless Client Isolation: Disabled | Enabled (SAP)

Max Clients: 500

Airtime Fairness: Disabled | Evenly | Manual

Neighbor AP Detection: Enabled

Scan Method: All Channels | One Channel

Scan Interval: 60

Scan Duration: 50

Scan Data Keep Time: 3600

Legacy Rates: all

MU MIMO: Disabled

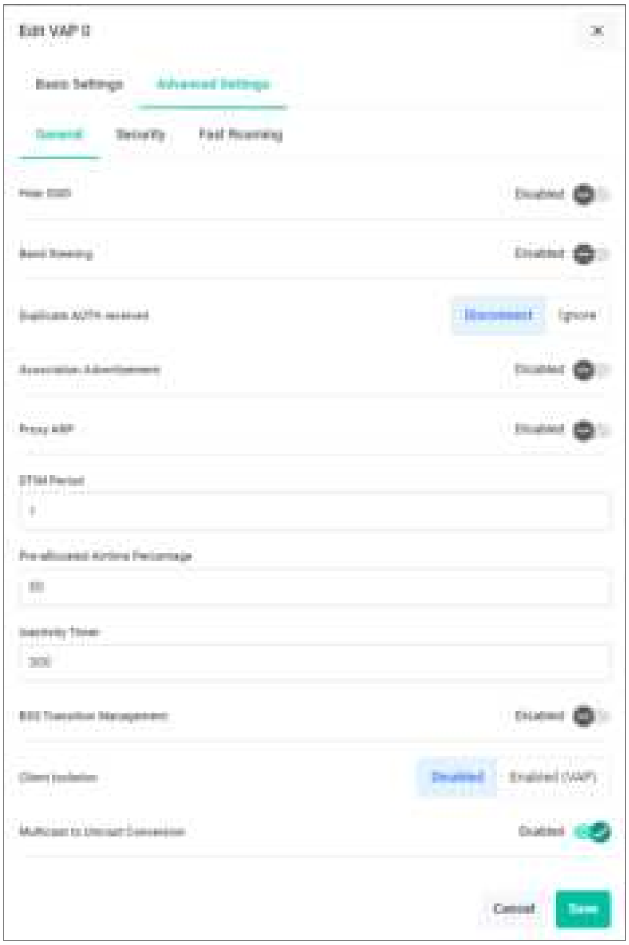
OFDMA: Disabled

VAP settings

The following optional advanced settings are available from the **Edit VAP 0** dialog **Advanced Settings** tab.

General settings

From the **General** tab:



Edit VAP 0

Basic Settings | Advanced Settings

General | Security | Fast Roaming

Hide SSID: Disabled

Band Steering: Disabled

Duplicate AUTH received: Disconnect | Ignore

Association Advertisement: Disabled

Proxy ARP: Disabled

DTIM Period: 1

Pre-allocated Airtime Percentage: 30

Inactivity Timer: 300

BSS Transition Management: Disabled

Client Isolation: Disabled | Enabled (VAP)

Multicast to Unicast Conversion: Disabled

Cancel | Save

Table 11: Edit VAP 0 - Advanced Settings General

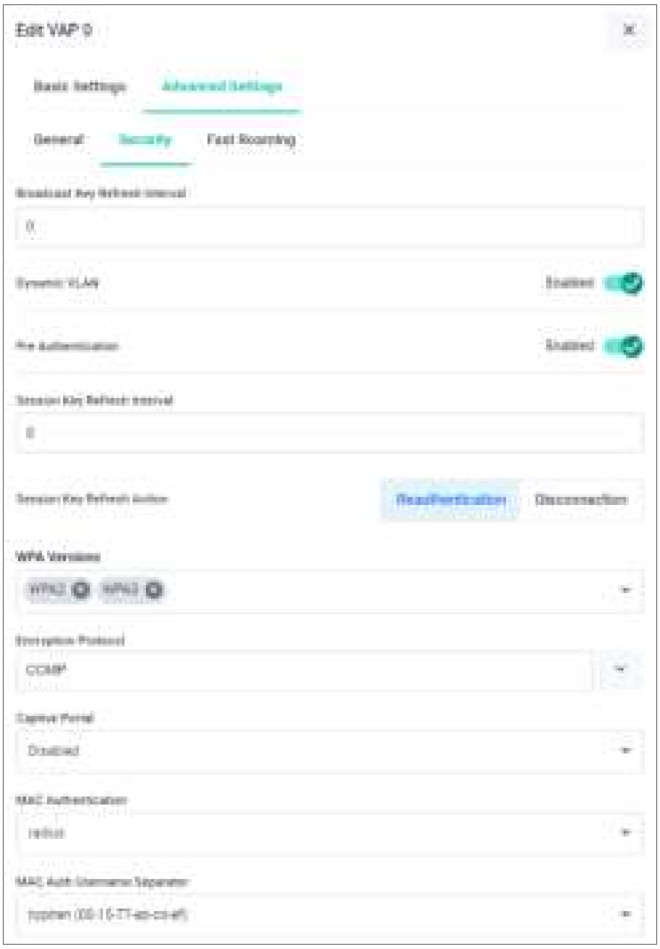
FIELD	DESCRIPTION
Hide SSID	You can enable or disable the SSID from view.
Band Steering	You can enable or disable band steering. Band steering automatically connects your devices to the best available WiFi frequency. For this to work you must have matching configuration between a VAP on Radio 1 (2.4 GHz) and a VAP on Radio 2 (5 GHz).
Duplicate AUTH received	You can disconnect clients on reception or ignore duplicate authentication messages.
Association Advertisement	You can enable or disable advertisements. Notify the previously connected AP that a wireless client has roamed away from it to another AP. This feature must be enabled on all APs in the network.
Proxy ARP	You can enable or disable proxy ARP. The AP will respond to ARP requests on behalf of the wireless client.

Table 11: Edit VAP 0 - Advanced Settings General (continued)

FIELD	DESCRIPTION
DTIM Period	A delivery traffic indication message (DTIM) period value is a number that determines how often a beacon frame includes a DTIM, and this number is included in each beacon frame. The default is 1.
Inactivity Timer	The inactivity timer functionality closes client sessions that have been idle for a specified period of time. This feature is enabled by default and the default time-out value is 300 seconds.
BSS Transition Management	You can enable or disable BSS transmission management. BSS transition management enables an AP to request non-AP wireless client to transition to a specific AP, or to indicate to a non-AP wireless client a set of preferred APs due to network load balancing or BSS Termination.
Client Isolation	You can enable or disable per VAP client isolation. Per VAP client isolation blocks communication between wireless clients that connect to the same VAP.

Security settings

From the **Security** tab:



Broadcast Key Refresh Interval: 0

Dynamic VLAN: Enabled

Pre Authentication: Enabled

Session Key Refresh Interval: 0

Session Key Refresh Action: ReAuthentication | Disconnection

WPA Versions: WPA2, WPA3

Encryption Protocol: CCMP

Captive Portal: Disabled

MAC Authentication: radius

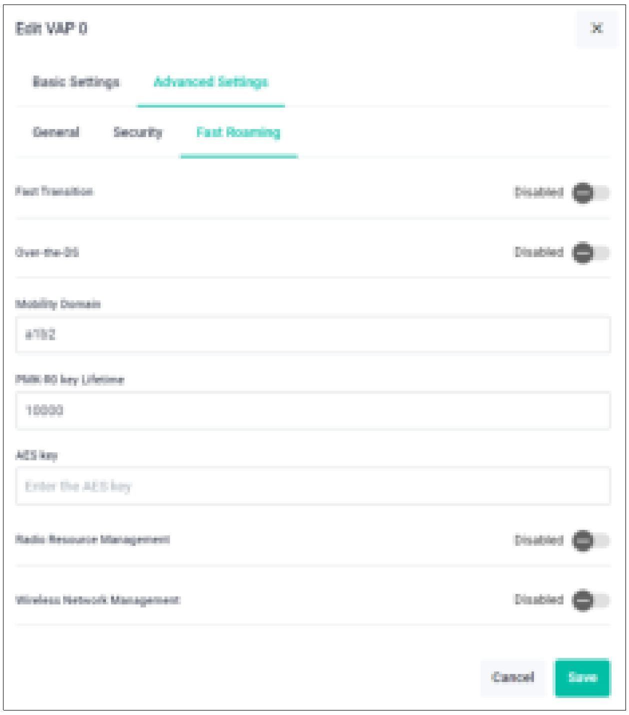
MAC Auth Username Separator: hyphen (00-15-77-ab-cd-ef)

Table 12: Edit VAP 0 - Advanced Settings Security

FIELD	DESCRIPTION
Broadcast Key Refresh Interval	The interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 0 seconds. The valid range is from 0 to 86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
WPA Versions	You can select the WPA version you want to use. WPA3 is the latest WPA standard. The default is WPA2. WAP3/WPA2 can be selected together and WPA2/WPA can be selected together. The wireless device will connect using the highest version it supports out of the selection.
Encryption Protocol	The default is the GCMP cipher. From version 5.4.4-2.3 onwards, you can select the CCMP cipher for WPA Enterprise version WPA3.
Captive Portal	You can disable captive portal if you do not use it. If you want to use the captive portal feature see "Captive Portal" on page 21.
MAC Authentication	Select from **Disabled**, **radius**, **MAC Filter**, **External Radius + MAC Filter**, or **AMF Application Proxy**.
Management Frame Protection	Select from **Enable (Capable)** or **Disabled**.

Fast Roaming settings

From the **Fast Roaming** tab:



Edit VAP 0

Fast Transition: Disabled

Over-the-DS: Disabled

Mobility Domain: a1b2

PMK-R0 key Lifetime: 10000

AES key: Enter the AES key

Radio Resource Management: Disabled

Wireless Network Management: Disabled

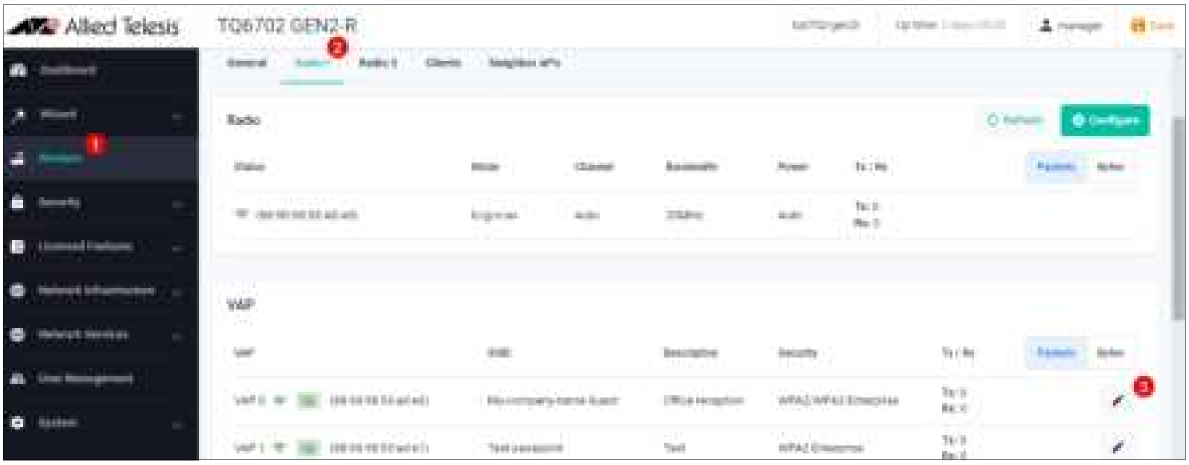
Table 13: Edit VAP 0 - Advanced Settings Fast Roaming

FIELD	DESCRIPTION
Fast Transition	You can enable or disable this feature. Fast BSS Transition (often abbreviated to Fast Transition or FT) describes mechanisms by which a mobile device can reestablish existing security and/or QoS parameters prior to re-associating to a new AP.
Over-the-DS	You can enable or disable this feature. When Over-the-DS is enabled and a client's data needs to go from this AP to another AP, then the data travels over the wired network between the two APs.
AES key	The encryption key that will be shared with all participating APs.
Radio Resource Management	You can enable or disable this feature. RRM involves sharing of the scarce spectrum among all users of the system. It includes performance gains in terms of efficient energy usage, higher throughput, lower delays, and decreased packet loss.
Wireless Network Management	Enables wireless clients to exchange information for the purpose of improving the overall performance of the wireless network.

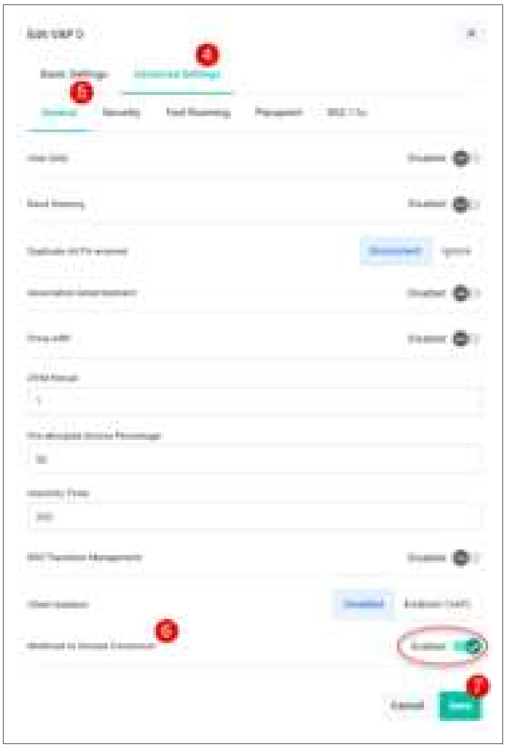
Multicast to Unicast conversion

From Device GUI version 2.18.0 onwards and AlliedWare Plus software version 5.5.4-1.1 or later, you can configure an Access Point (AP) to convert multicast packets into unicast packets. These unicast packets are destined for the client connected to the VAP. This conversion allows each client to receive data at the highest possible rate it supports. To configure this feature:

1. Click **Wireless** from the Menu bar.
2. Select the Radio tab to configure (The default is Radio1).
3. Click on the **Edit** button to select a VAP to configure (The default is VAP0).



4. Click **Advanced Settings**.
5. Select the **General** tab.
6. Enable **Multicast to Unicast Conversion**.
7. Click **Save**.



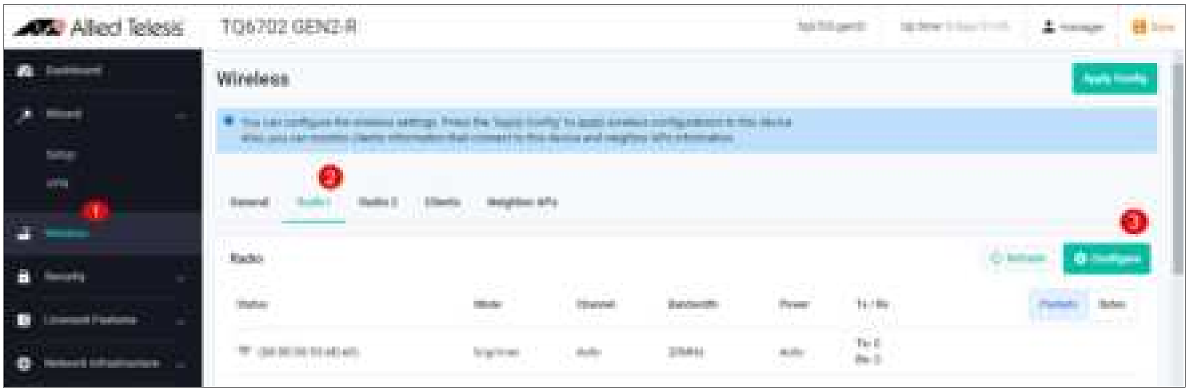
Airtime Fairness for each VAP

From Device GUI version 2.18.0 onwards and AlliedWare Plus software version 5.5.4-1.1 or later, you can configure each VAP’s Airtime Fairness percentage manually.

Airtime fairness is a concept and feature designed to ensure that all devices on a wireless network receive a fair share of the available airtime. This is particularly important in environments where devices with varying capabilities and data rates are connected to the same wireless access point.

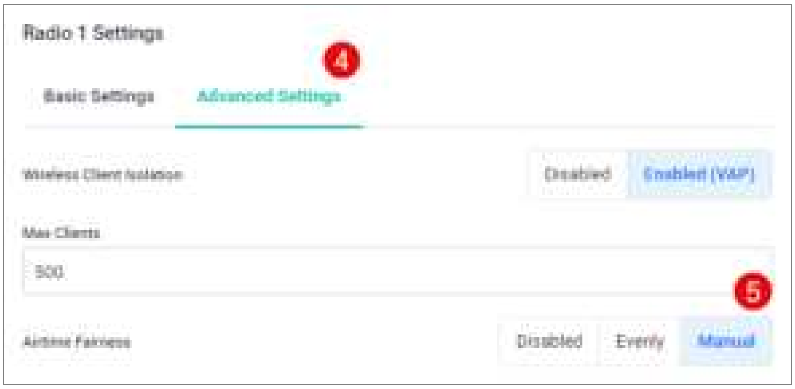
To set Airtime Fairness manually:

1. Click on **Wireless** from the Menu bar.
2. Select the Radio tab to configure (the default is Radio1).
3. Click the **Configure** button from the **Radio** settings.



4. Click on the **Advanced Settings** tab.
5. Click **Manual** from the Airtime Fairness options.

The other options available are to disable Airtime Fairness completely, or to automatically allocate it evenly between VAP’s.


Radio 1 Settings

Basic Settings | Advanced Settings

Wireless Client Isolation: Disabled [✓ Enabled (VAP)]

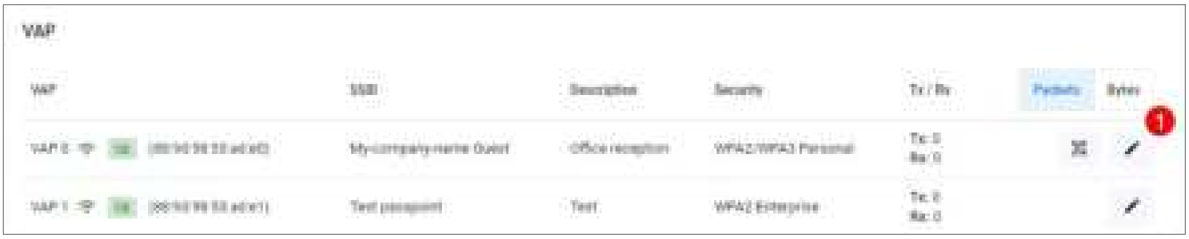
Max Clients: 500

Airtime Fairness: Disabled Evenly [✓ Manual]

6. Click **Apply**.

You can now configure the **Pre-allocated Airtime Percentage** for each VAP individually. For example, you could allocate 60% for VAP 0 and 40% for VAP 1.

1. Click the **Edit** button for the VAP you want to configure.



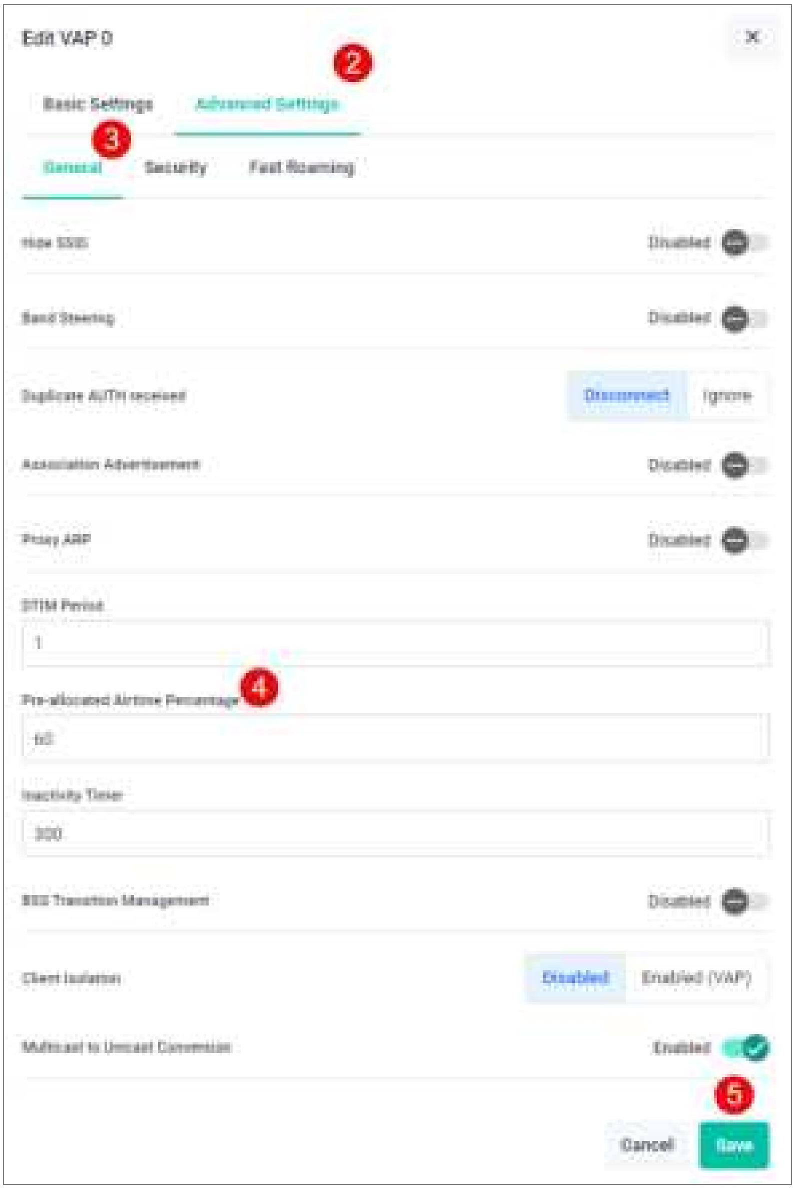
VAP

VAP	SSID	Description	Security	Tx / Rx	Packets	Bytes
VAP 0 [illegible] (00:50:99:33:ad:e0)	My-company-name Guest	Office reception	WPA2/WPA3 Personal	Tx: 0 Rx: 0		
VAP 1 [illegible] (00:50:99:33:ad:e1)	Test passpoint	Test	WPA2 Enterprise	Tx: 0 Rx: 0		

2. Click on the **Advanced Settings** tab.

3. Click on the **General** tab.

4. Enter the **Pre-allocated Airtime Percentage** number.



Edit VAP 0

Basic Settings | Advanced Settings

General | Security | Fast Roaming

Hide SSID: Disabled

Band Steering: Disabled

Duplicate AUTH received: [✓ Disconnect] Ignore

Association Advertisement: Disabled

Proxy ARP: Disabled

DTIM Period: 1

Pre-allocated Airtime Percentage: 60

Inactivity Timer: 300

BSS Transition Management: Disabled

Client Isolation: [✓ Disabled] Enabled (VAP)

Multicast to Unicast Conversion: Enabled

5. Click **Save**.

Proxy ARP handling

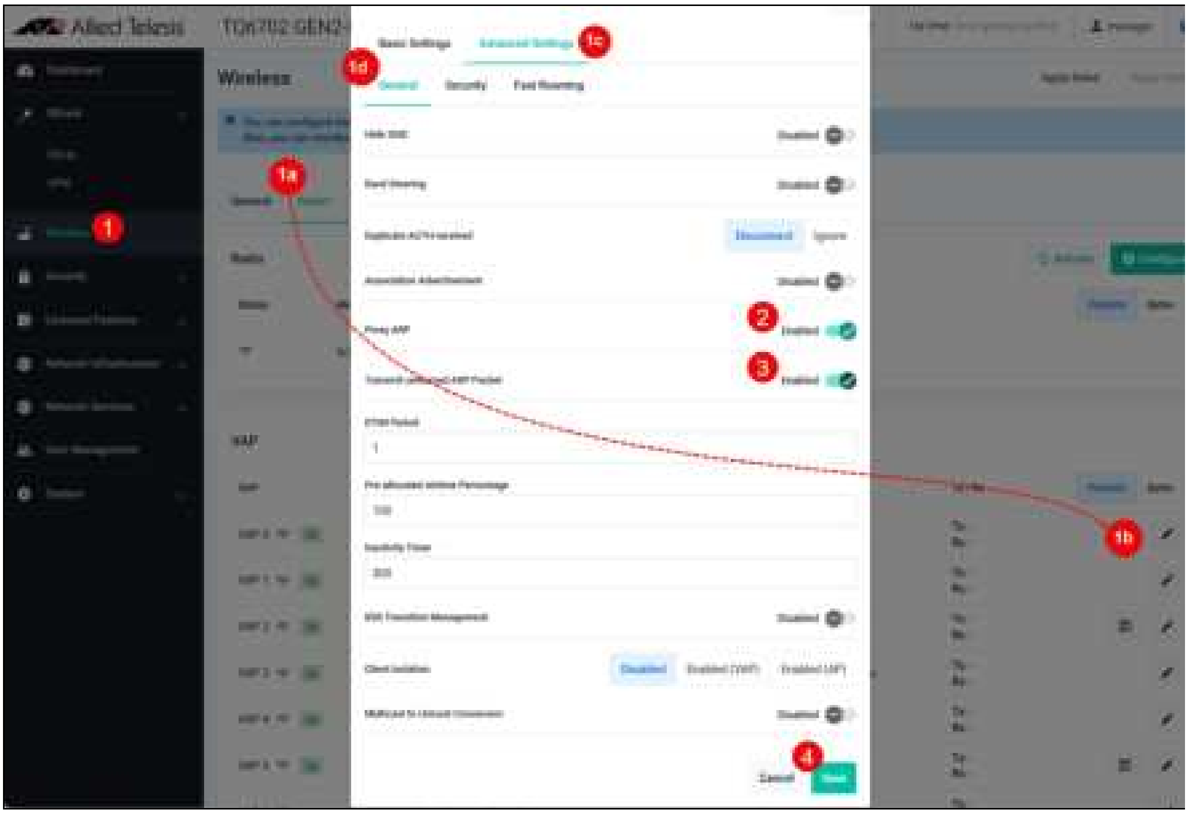
TQR Series wireless AP routers include an option to allow ARP packets from unknown addresses for Proxy ARP instead of dropping them.

How it works

Some devices, such as IP phones, don’t send the packets needed for Proxy ARP learning. As a result, the AP may drop ARP requests it can't answer by proxy, causing delays in IP resolution. Enabling this option allows the AP to accept those ARP packets, improving connectivity for such devices.

To configure this:

1. Go to **Wireless** > **Radio X** > **Edit VAP Y** > **Advanced Settings** > **General**.
2. In that dialog box, enable **Proxy ARP**.
3. The **Transmit unlearned ARP Packet** is displayed. Toggle it to **Enabled**.
4. Click **Save**.



Hide SSID Disabled
Band Steering Disabled
Duplicate AUTH received Disconnect Ignore
Association Advertisement Disabled
Proxy ARP Enabled
Transmit unlearned ARP Packet Enabled
DTIM Period
1
Pre-allocated airtime Percentage
100
Inactivity Timer
300
BSS Transition Management Disabled
Client Isolation Disabled Enabled (VAP) Enabled (AP)
Multicast to Unicast Conversion Disabled

Two-step authentication with MAC authentication and Captive Portal

From AlliedWare Plus version 5.5.5-0.2 onwards two-step authentication allows STAs (stations) to connect using either MAC authentication or Captive Portal authentication.

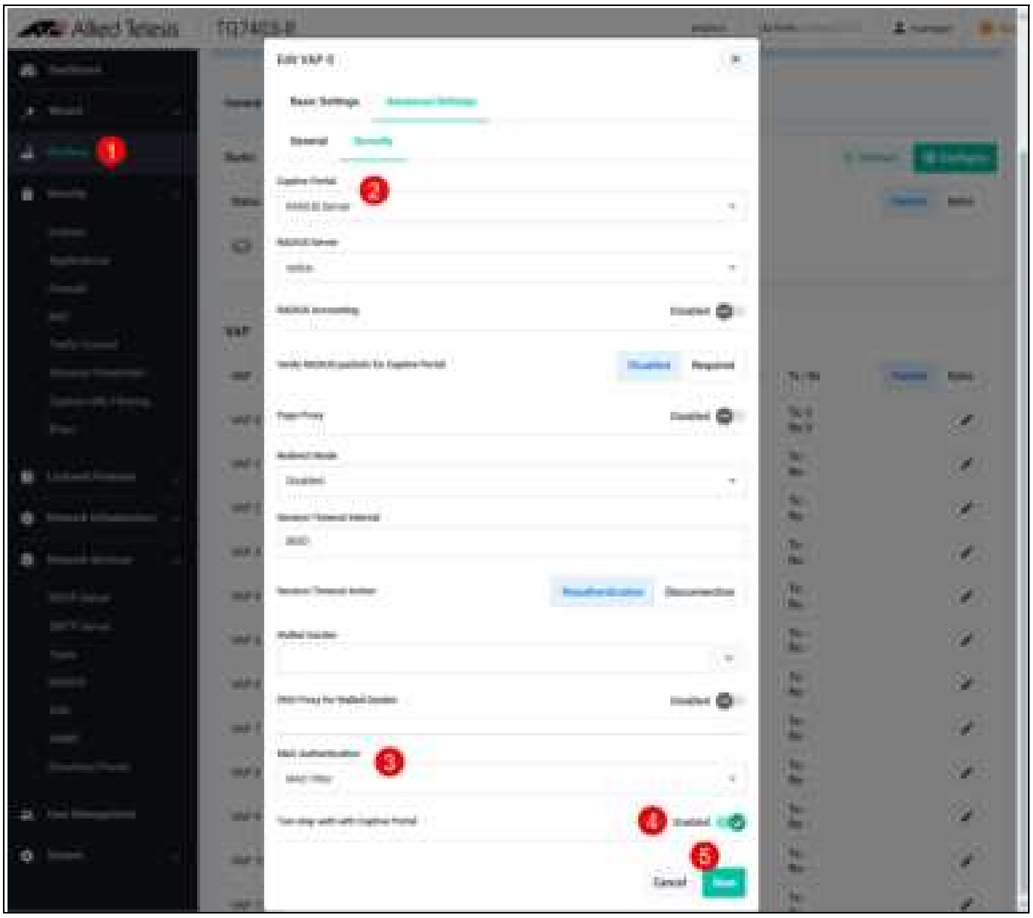
This means that if MAC authentication:

- fails, the STA can still connect using the Captive Portal.
- succeeds, the STA can connect without needing Captive Portal authentication.

This allows web-authenticated devices to stay authenticated, even if they move between different switches.

To configure this:

1. Go to **Wireless** > **Radio X** > **VAP X** > **Advanced Settings** > **Security**
2. Enable **Captive Portal**
3. Select **MAC Authentication > MAC Filter**
4. Enable **Two-step auth with Captive Portal**
5. Click **Save**.



Edit VAP 0

Captive Portal: RADIUS Server

RADIUS Server

RADIUS accounting: Disabled

Verify RADIUS packets for Captive Portal: Disabled | Required

Page Proxy: Disabled

Redirect Mode: Disabled

Session Timeout Interval: 3600

Session Timeout Action: Reauthentication | Disconnection

Walled Garden

DNS Proxy for Walled Garden: Disabled

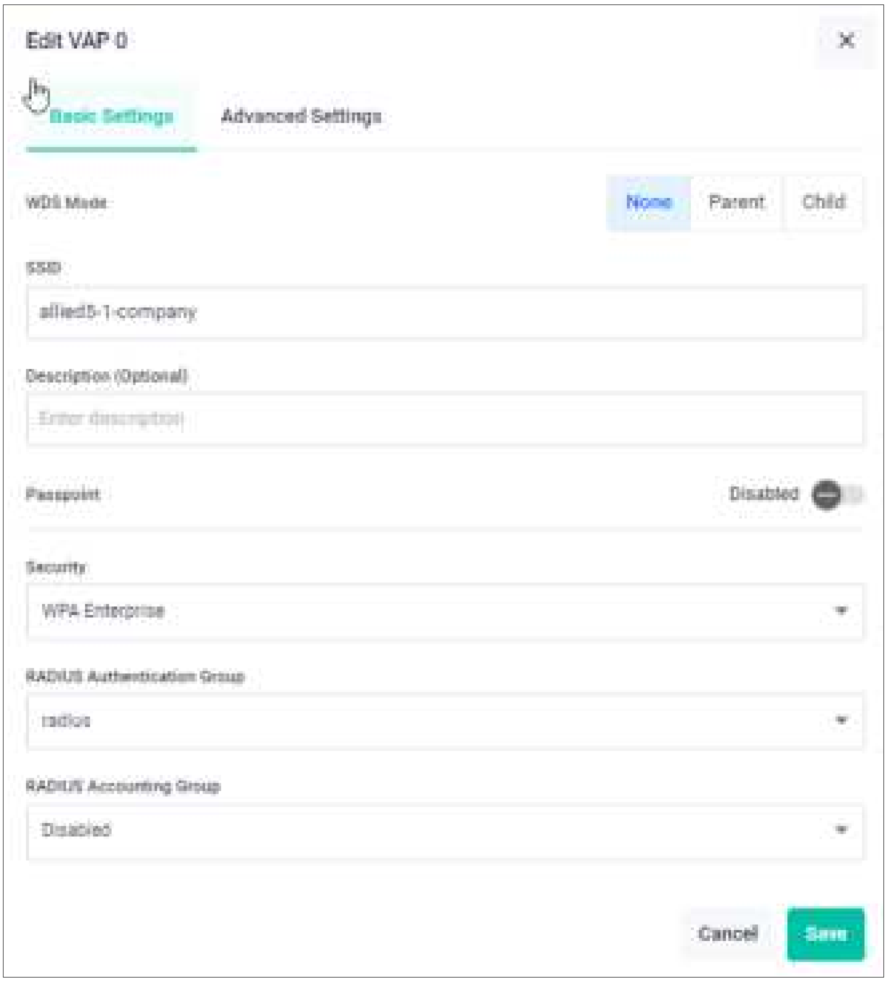
MAC Authentication: MAC Filter

Two-step auth with Captive Portal: Enabled

Configuration examples

The following two examples show VAP configuration for a company wireless network and VAP configuration for a guest wireless network.

Example 1 This example shows VAP configuration for a company wireless network called allied5-1-company, using WPA Enterprise security. First configure the recommended Basic Settings:



Edit VAP 0

Basic Settings | Advanced Settings

WDS Mode: None | Parent | Child

SSID: allied5-1-company

Description (Optional): Enter description

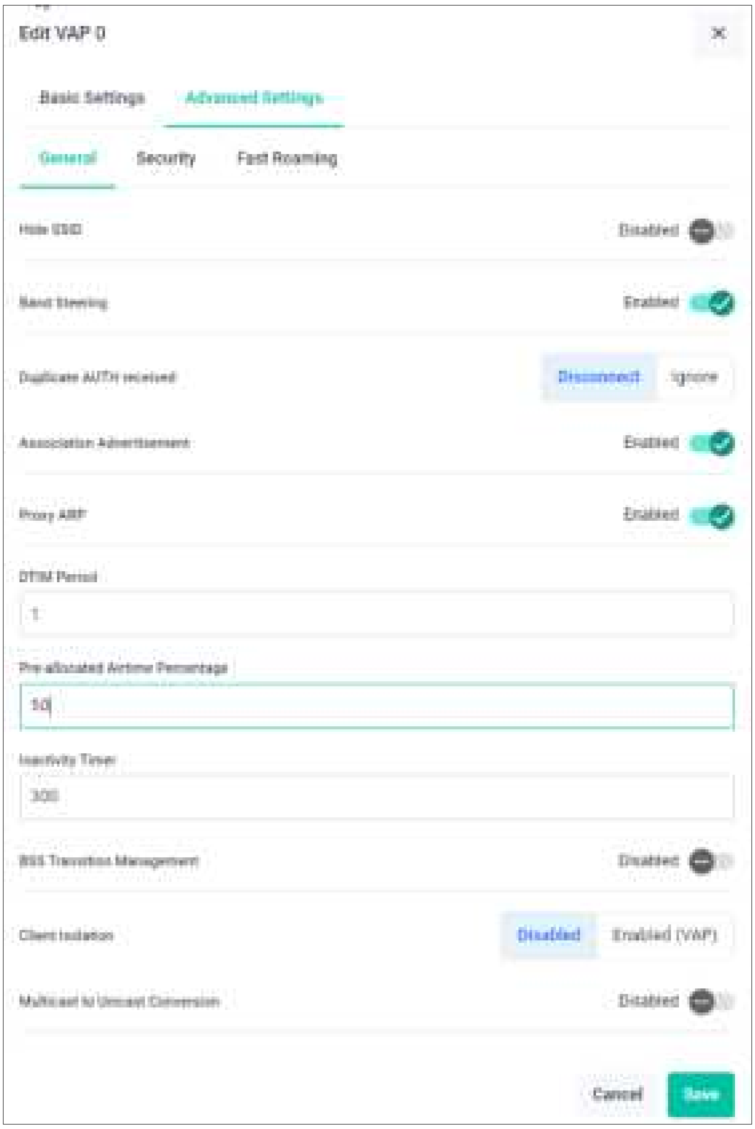
Passpoint: Disabled

Security: WPA Enterprise

RADIUS Authentication Group: radius

RADIUS Accounting Group: Disabled

Next, configure advanced settings. The following example shows the recommended VAP General Advanced Settings for this company wireless network:



Hide SSID: Disabled

Band Steering: Enabled

Duplicate AUTH received: Disconnect | Ignore

Association Advertisement: Enabled

Proxy ARP: Enabled

DTIM Period: 1

Pre-allocated Airtime Percentage: 50

Inactivity Timer: 300

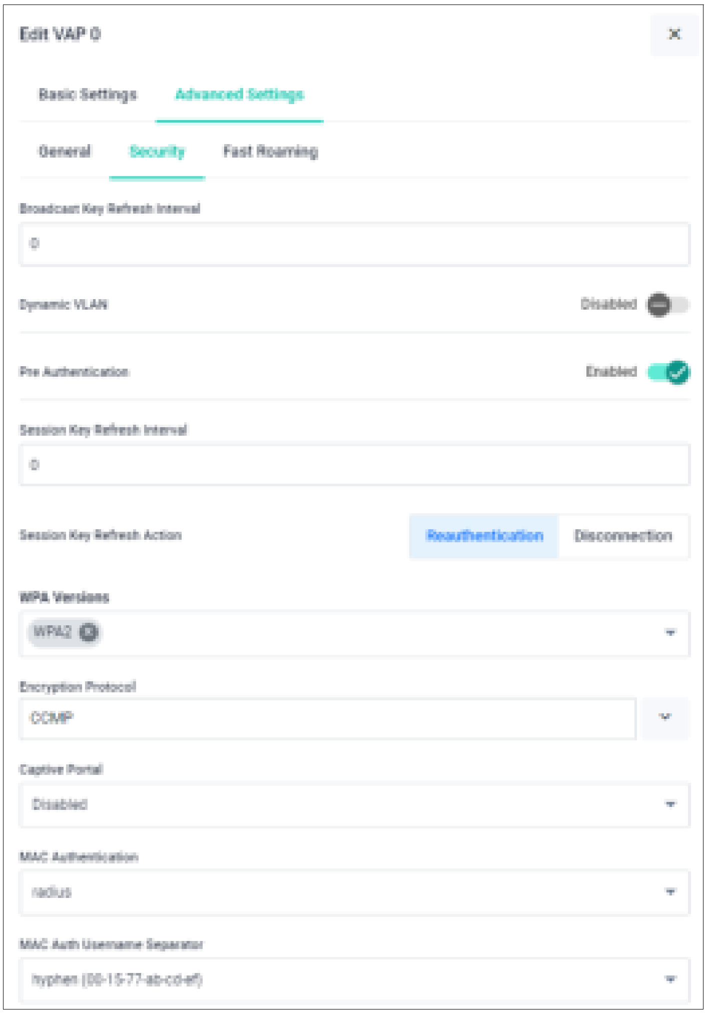
BSS Transition Management: Disabled

Client Isolation: Disabled | Enabled (VAP)

Multicast to Unicast Conversion: Disabled

In this example above, Band Steering, Association Advertisement and Proxy ARP are enabled.

In this example MAC Authentication is enabled using a RADIUS server:



Broadcast Key Refresh Interval
0

Dynamic VLAN Disabled

Pre Authentication Enabled

Session Key Refresh Interval
0

Session Key Refresh Action Reauthentication Disconnection

WPA Versions
WPA2

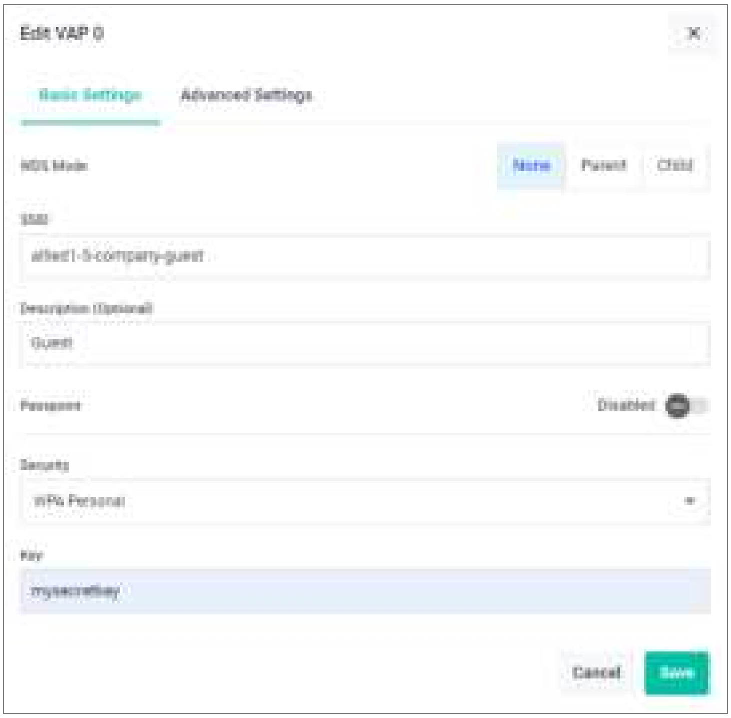
Encryption Protocol
CCMP

Captive Portal
Disabled

MAC Authentication
radius

MAC Auth Username Separator
hyphen (00-15-77-ab-cd-ef)

Example 2 This example shows VAP configuration for a guest wireless network called allied1-5-company-guest, using WPA Personal security. First configure the recommended Basic Settings:



Edit VAP 0

WDS Mode: None | Parent | Child

SSID: allied1-5-company-guest

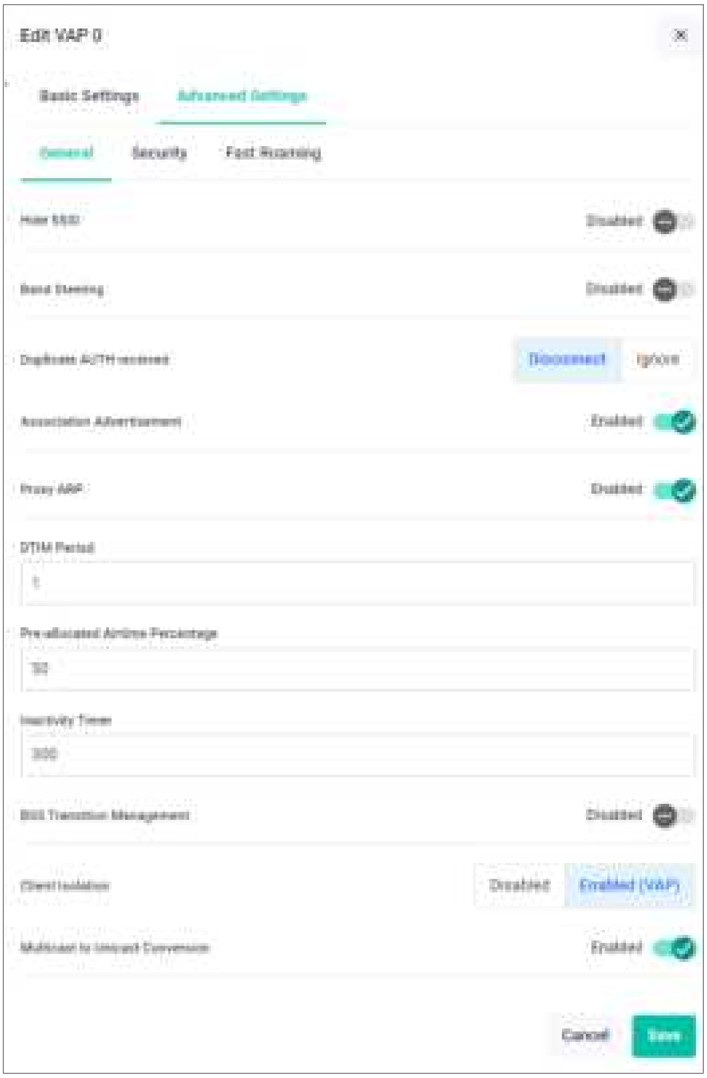
Description (Optional): Guest

Passpoint: Disabled

Security: WPA Personal

Key: mysecretkey

Next, configure advanced settings. The following example shows the recommended VAP General Advanced Settings for this guest network:



Hide SSID Disabled

Band Steering Disabled

Duplicate AUTH received Disconnect Ignore

Association Advertisement Enabled

Proxy ARP Enabled

DTIM Period

1

Pre-allocated Airtime Percentage

50

Inactivity Timer

300

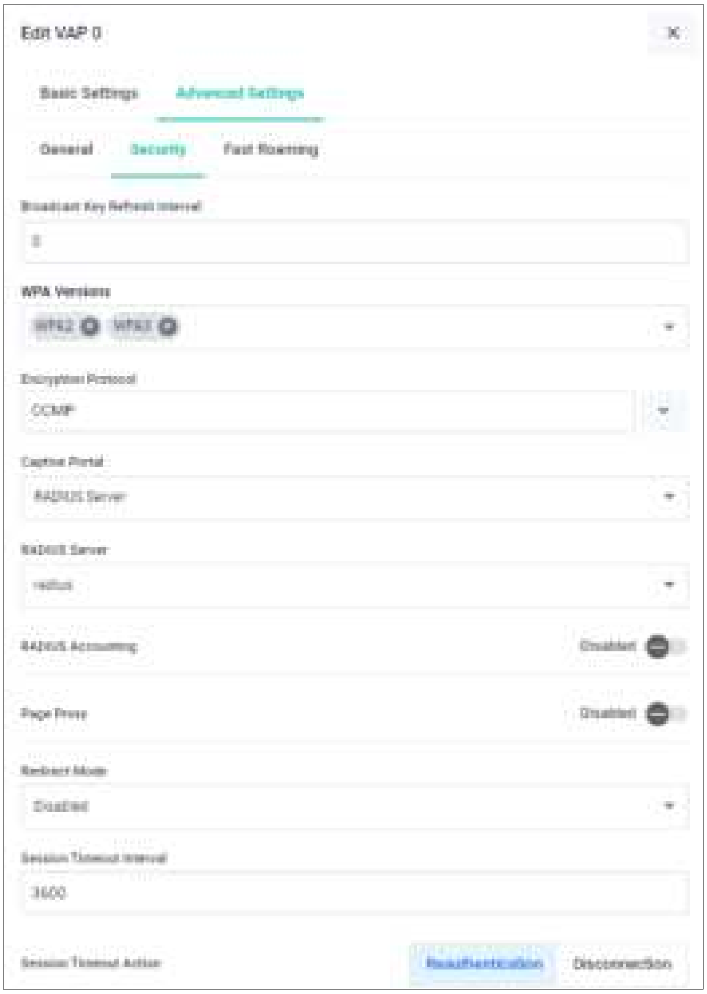
BSS Transition Management Disabled

Client Isolation Disabled Enabled (VAP)

Multicast to Unicast Conversion Enabled

In this example Association Advertisement, Proxy ARP and Client Isolation are enabled.

The following example shows the recommended VAP Security Advanced Settings for a guest network:



Broadcast Key Refresh Interval: 0

WPA Versions: WPA2, WPA3

Encryption Protocol: CCMP

Captive Portal: RADIUS Server

RADIUS Server: radius

RADIUS Accounting: Disabled

Page Proxy: Disabled

Redirect Mode: Disabled

Session Timeout Interval: 3600

Session Timeout Action: Reauthentication | Disconnection

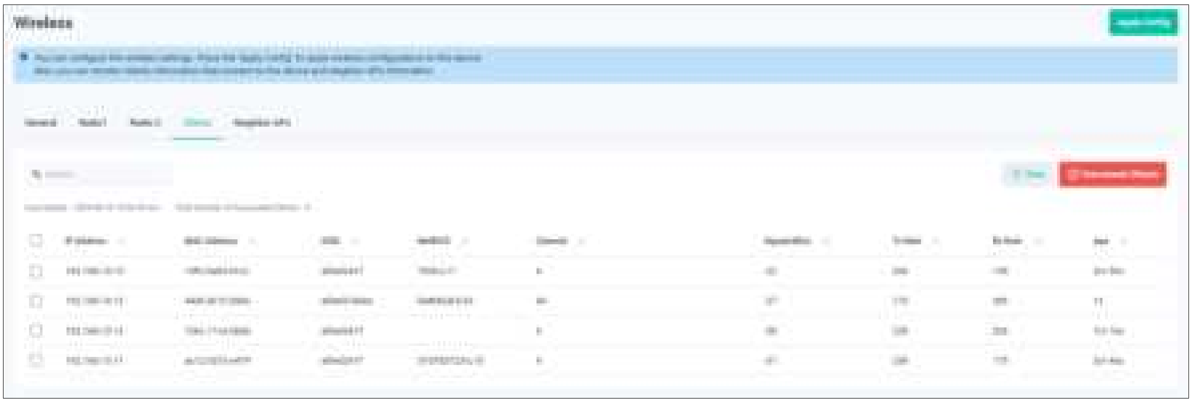
In this example Captive Portal is enabled using a RADIUS server.

Monitoring your wireless network

From the **Wireless** menu you can see the status of wireless APs and connected clients. You can display this information from the **Clients** and **Neighbor APs** tabs.

Clients

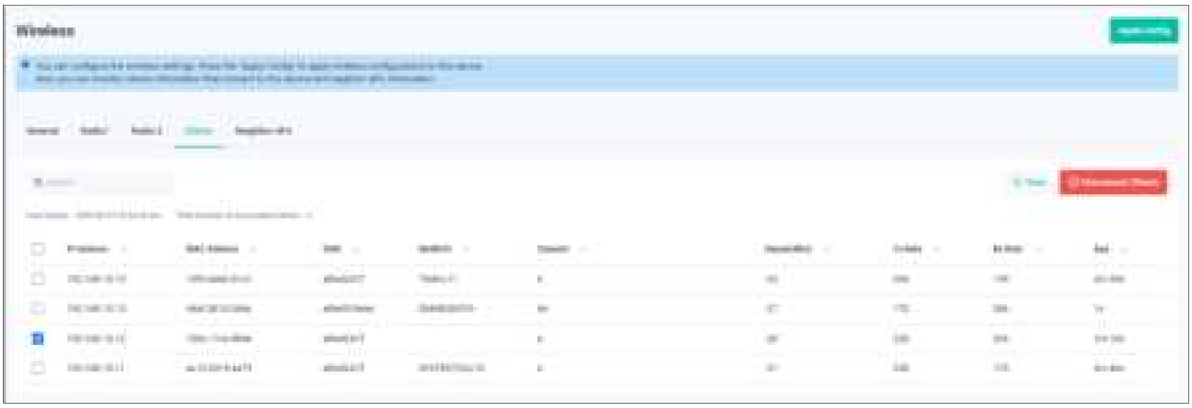
1. Click on the **Clients** tab to display information about your clients.
2. Click on the **View** button to display the up-to-date current detail.



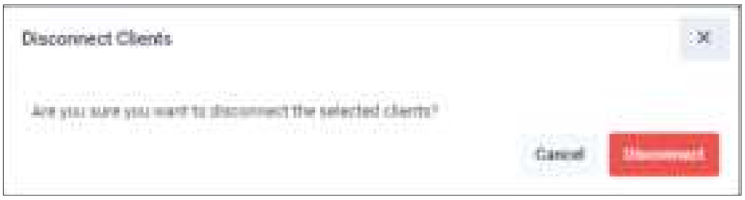
This updates the client status including the following: IP Address, MAC Address, SSID, netBIOS, Channel, Signal (dBm), Tx Rate (transmitted rate), Tr Rate (received rate) and Age for each client.

3. Click on the **down arrow** beside the field that you want to sort by in ascending or descending order.

The example below shows a selected client 192.168.1.4 with the default sorting which is by IP address:



4. Click the **Disconnect Clients** button to disconnect a selected client.


Disconnect Clients

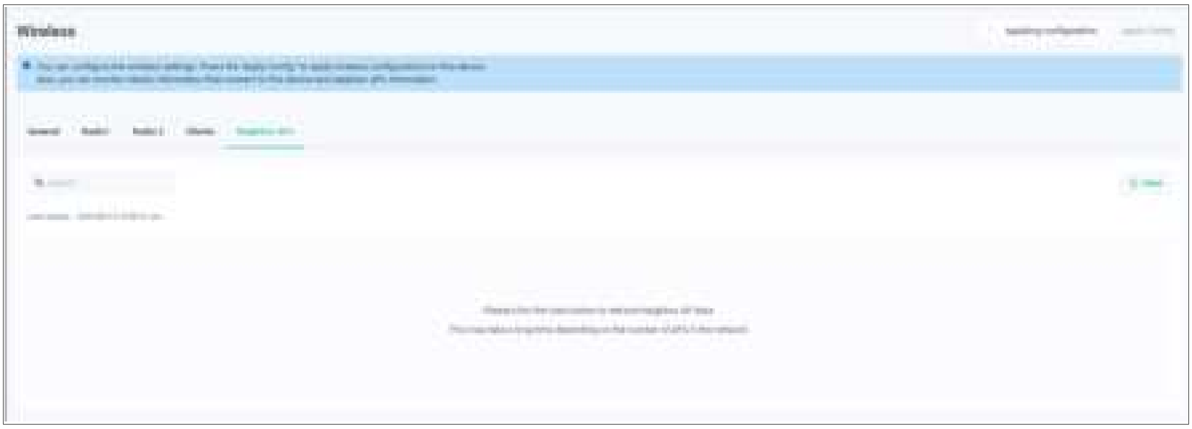
Are you sure you want to disconnect the selected clients?

You cannot use the AP to reconnect a client. Instead, the client has to initiate reconnecting from the client device.

Neighbor APs

To display information about neighboring APs in your wireless network:

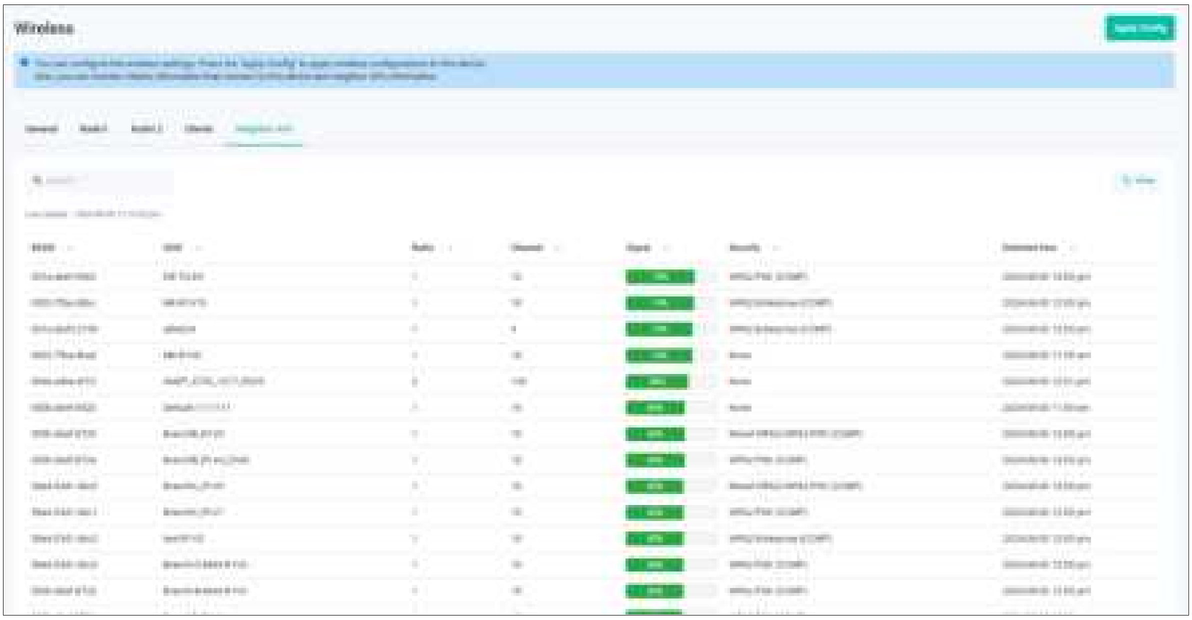
1. Click on the **Neighbor APs** tab to display information about your neighboring APs.
2. Click on the **View** button to display up to date current detail:



The BSSID, SSID, Radio, Channel, Signal, Security and Detected time are displayed in a list that you can sort in ascending or descending order.

3. Click on the **down arrow** beside the field that you want to sort by in ascending or descending order.

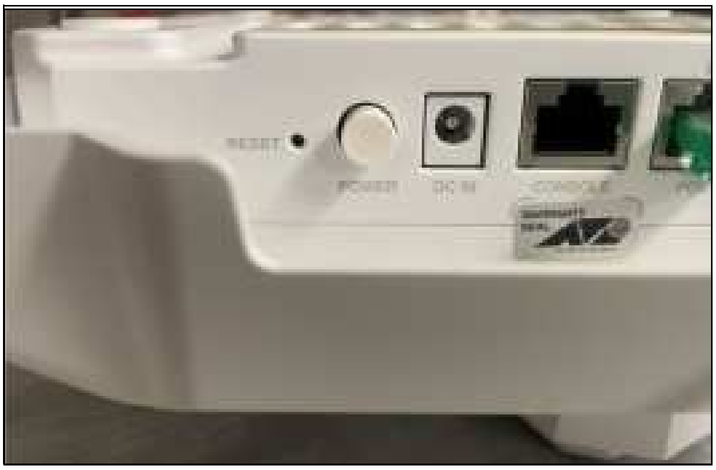
The example below shows the Neighbor APs sorted by channel strength:



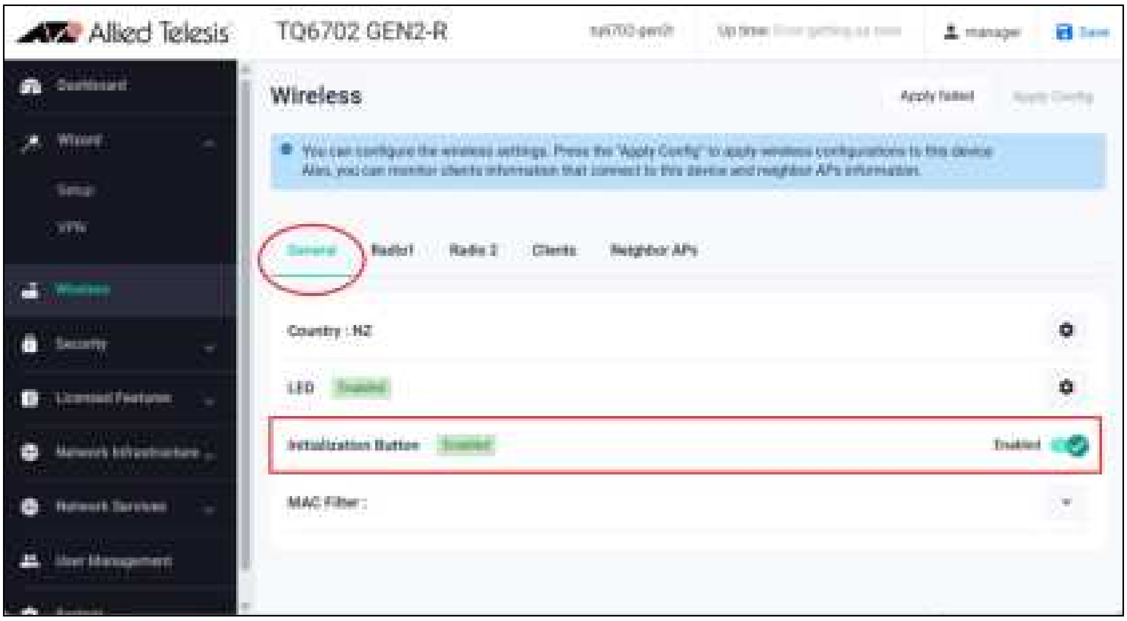
Reset button

The Reset button is recessed and located to the left of the Power button. To press it, use a small pointed tool, such as a metal pin. Pressing it for:

- **over five seconds**, results in a reboot that will restore the configuration back to the equivalent of a factory reset (ready for an AMF Plus recovery). **This means you will lose your configuration and any files stored on your device.**
- **less than five seconds** reboots your device.



The **Initialization Button** displayed in the Device GUI **Wireless** page performs the same function as the Reset button, (factory reset). By default it is enabled.



Wireless

You can configure the wireless settings. Press the "Apply Config" to apply wireless configurations to this device. Also, you can monitor clients information that connect to this device and neighbor APs information.

Country : NZ

LED Enabled

Initialization Button Enabled Enabled

MAC Filter :

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com