Technical Guide

Wireless Management (AWC) with Vista Manager mini User Guide

Introduction

Vista Manager mini is useful for smaller wireless networks that may not need the capabilities of Vista Manager EX. It is a simplified version of Vista Manager EX and is integrated into the Device GUI. It provides network visibility of Allied Telesis Autonomous Management Framework (AMF) and Autonomous Wave Control (AWC) devices.

Autonomous Wave Control (AWC) allows you to set up and manage your wireless access points (APs) from the GUI of an AlliedWare Plus™ device that supports this functionality. AWC uses wireless intelligence to model where your APs are located and what their signal strength is.

Using this information, AWC automatically optimizes wireless output and channel selection. It minimizes coverage gaps and reduces AP interferences. This results in a high-quality wireless experience that responds to network configuration changes and bandwidth demands from user devices.

The Internet of Things (IoT) and Bring Your Own Device (BYOD) movements have created an exponential increase in the number of connected devices, all of which demand reliable and high-speed wireless network access. This unprecedented rise in the number of connections and the associated traffic puts a major strain on networks, many of which struggle to deliver the coverage, performance, and roaming access that today's users demand.

- AWC helps to address this complex and rapidly-evolving environment, by reducing the need for costly human involvement in the deployment and tuning of a wireless network.
- AWC uses game theory to model the continuously changing relationship between AP location and signal strength requirements, resulting in a more efficient, higher-performing wireless network environment.

This guide describes how to use AWC in Vista Manager mini to configure:

- A multi-channel wireless network
- AWC Channel Blanket for totally seamless roaming
- The network map
- Heatmaps
- AWC Smart Connect for cable-free wireless network expansion
- Captive portal
- Passpoint
- Emergency mode
- Wireless triggers

This is followed by information on using the AWC management and monitoring tools, and troubleshooting

Products and software version that apply to this guide

Vista Manager mini is built into the Device GUI, and is available for SwitchBlade x908 Generation 2, x950, x930, x550, and x530 series switches, and AR-Series UTM Firewalls and VPN Routers.

This guide applies to:

- AR-Series UTM Firewalls and VPN Routers running version **5.4.8-x.x** or later.
- SwitchBlade x908 Generation 2 and x950 series switches running version **5.4.9-0.1** or later.
- x930 and x530 series switches running version **5.4.9-1.3** or later.
- x550 series switches running version **5.5.0-0.1** or later
- From software release **5.4.8-1.2** onwards, on AR-Series UTM Firewalls and VPN Routers, you can set up your wireless network automatically using **Auto Setup**.
- From software release **5.4.9-2.1**, you can set up your wireless network APs to use **Channel Blanket**.
- From software release **5.5.0-0.1**, you can set up your wireless network APs to use **Smart Connect.**
- From software release **5.5.0-1.3**, you can set up your wireless network APs to use **Captive Portal**.
- From software release **5.5.0-2.3**, you can set up your wireless network APs to use **Passpoint**.
- From software release **5.5.0-1.0**, you can set up your wireless network APs to use **network triggers**.
- From software release **5.5.1-2.0**, and using Device GUI version 2.10.0, logging into the Device GUI with a privilege level of less than 15 gives you read-only access to device information and

network maps. In read-only access, you can click Refresh to update the device information and you can also view Network topology and Heat maps set by the Administrator.

- From software release **5.5.2-0.1**, and using Device GUI version 2.11.0, you can configure advanced Passpoint options including OSU (Online sign-up).
- From software release **5.5.2-0.1**, and using Device GUI version 2.11.0, TQ6602 APs support Smart Connect.
- From software release **5.5.2-2.1**, and using Device GUI version 2.13.0, TQ6702 GEN2 and TQ6602 GEN2 APs support Channel Blanket.

Related documents

You also may find the following alliedtelesis.com documents useful:

- AMF Feature Overview and Configuration Guide
- The product's Datasheet
- The product's Command Reference
- The Device GUI Release Note.

Content

Starting Vista Manager mini

Vista Manager mini is part of the web-based Device GUI, which ships on supported switches, firewalls, and VPN routers. To access the web-based GUI:

On SBx908 GEN2, x950, x930, x550 and x530 series switches:

1. Connect to any of the LAN switch ports
2. Open a web browser and browse to the default IP address for VLAN1

   The default IP address is 169.254.42.42. Alternatively, give VLAN1 an IP address of your choice and browse to that address.
3. Log in with the default username of **manager** and the default password of **friend**.

On AR4050S and AR3050S UTM firewalls and AR2050V VPN routers:

1. Connect to any of the LAN switch ports
2. Open a web browser and browse to the default IP address for VLAN1

   The default IP address is 192.168.1.1. Alternatively, give VLAN1 an IP address of your choice and browse to that address.
3. Log in with the default username of **manager** and the default password of **friend**.

On AR2010V VPN routers:

1. Connect to the eth1 interface
2. Open a web browser and browse to the default IP address for eth1

   The default IP address is 192.168.1.1. Alternatively, give eth1 an IP address of your choice and browse to that address.
3. Log in with the default username of **manager** and the default password of **friend**.

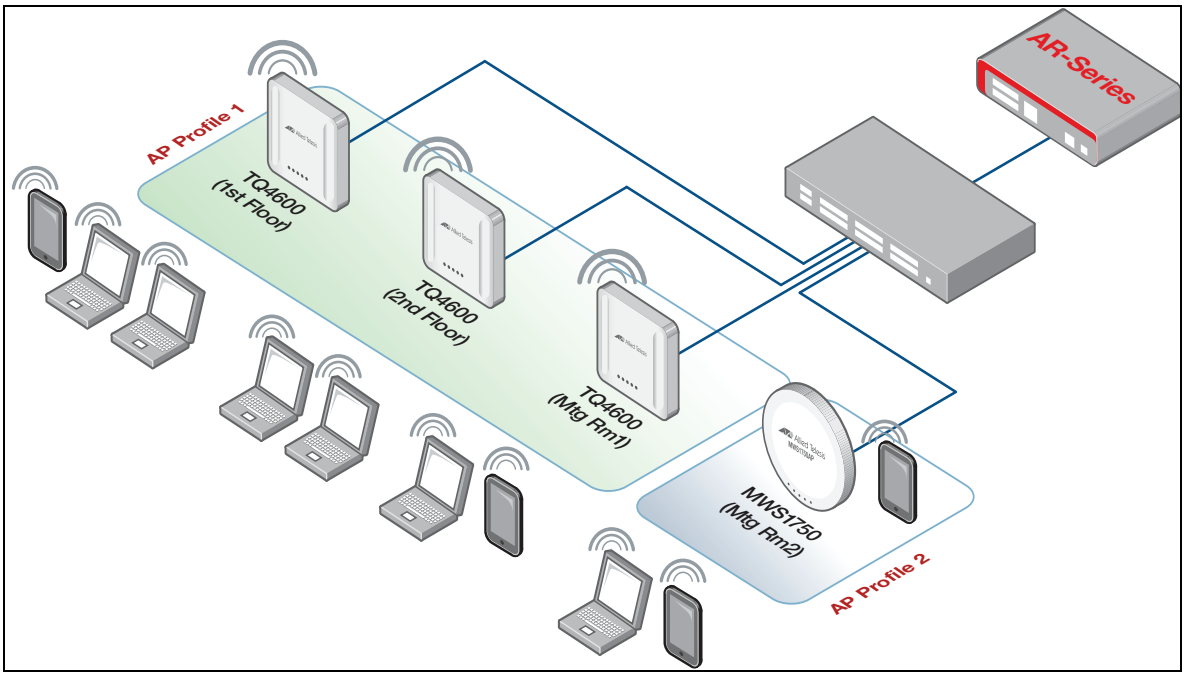
For more information about basic setup, see:

- Getting Started with the AlliedWare Plus Command Line Interface - for details about setting IP addresses
- Getting Started with the Device GUI on Switches
- Getting Started with the Device GUI for VPN Routers
- Getting Started with the Device GUI for UTM Firewalls

If you want Vista Manager mini to display other AlliedWare Plus devices in your network, you need to set up Allied Telesis Autonomous Management Framework (AMF) too. For step-by-step details, see the AMF Feature Overview and Configuration Guide. Without AMF, all your APs will appear as if they are connected to your AWC controller, even if they are physically connected through intermediary AlliedWare Plus devices.

What does a wireless network look like?

Here is an example of a typical wireless network setup with Autonomous Wave Control running from an AR-Series router or firewall:

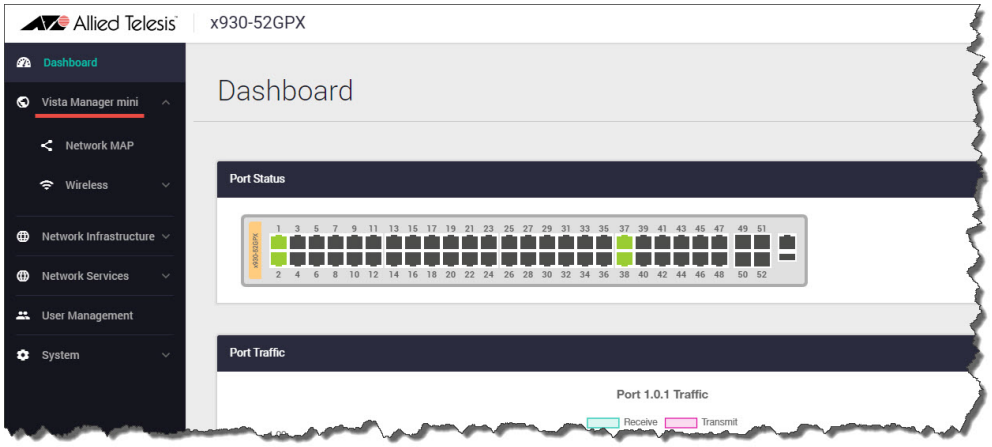


What is Vista Manager mini?

Vista Manager mini is a simplified version of Vista Manager EX. Vista Manager mini is integrated into the Device GUI, and provides full network visibility of AMF and AWC devices.

Vista Manager mini allows for:

- Wired and wireless network visibility
- AWC wireless network management
- AWC Channel Blanket hybrid wireless and AWC Smart Connect



Acronyms

Table 1: Acronyms used in Autonomous Wave Control

ACRONYM	DESCRIPTION
WAP or AP	Wireless Access Point is a networking hardware device that allows a Wi-Fi device to connect to a wired network.
AWC	Autonomous Wave Control is an advanced network technology that uses Artificial Intelligence (AI) to deliver significant improvements in wireless network connectivity and performance while reducing deployment and operating costs.
AWC Auto Setup	Autonomous Wave Control Auto Setup is a way of setting up a wireless network to automatically discovers access points.
VAP	Virtual Access Point is a concept of assigning multiple wireless networks to a wireless radio configuration.
BSSID	Basic Service Set Identifier - or the APs physical MAC address
SSID	Service Set Identifier - a unique name for the wireless network

Licensing

There is a range of wireless management licensing options available. For license information, see your device's Datasheet.

How many APs can a device manage?

The number of APs a device can manage is:

- A maximum of 5 APs for free.
- More than 5 APs requires a subscription-based feature license. For more information on licenses, see your device's Datasheet.

What APs are supported?

AWC on Vista Manager mini supports the following APs:

- ***TQ Series***: TQ6702 GEN2, TQm6702 GEN2, TQ6602 GEN2, TQm6602 GEN2, TQ6602, TQ5403, TQm5403, TQ5403e,TQ4600, TQ4400, TQ4400e, TQ3600, TQ3400, TQ3200, TQ2450 (must be running software version 4.0.5 or later), TQ1402, TQm1402.
- ***MWS Series***: MWS2533, MWS1750, MWS600

See the Allied Telesis website for the list of TQ datasheets.

Note: Not all AP models are available in all regions.

Wi-Fi architectures

There are three Wi-Fi architectures:

- Single channel - also known as channel blanket
- Multi channel
- Channel blanket hybrid

Single channel

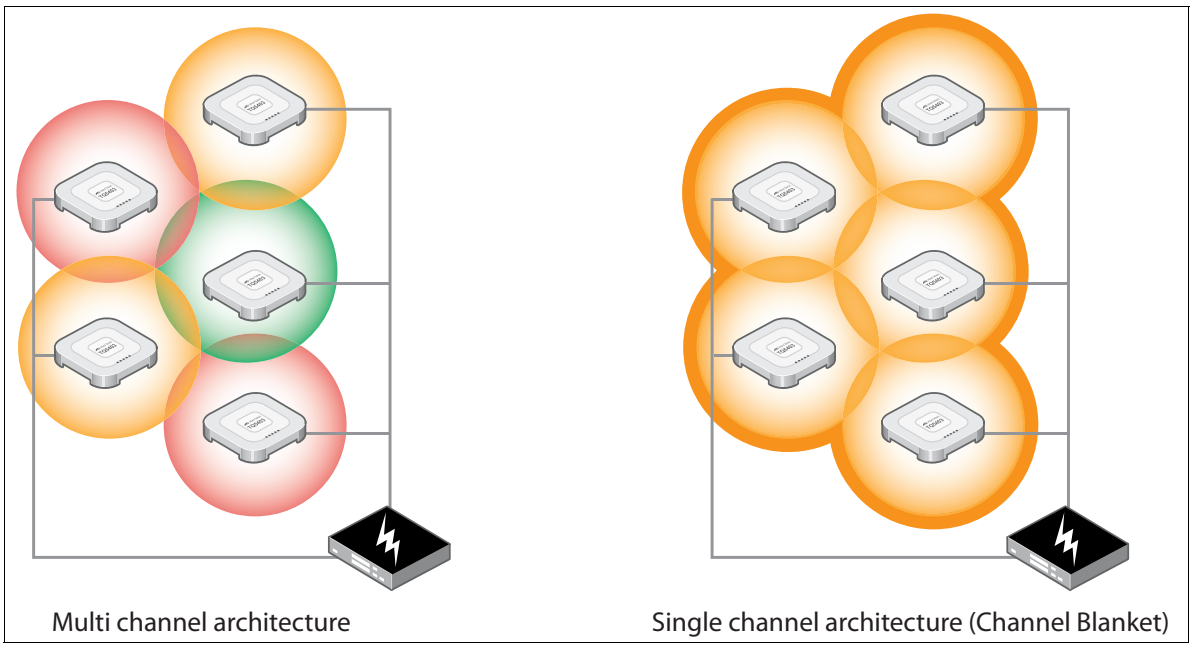
A **single** channel (i.e. channel blanket) setup operates all wireless APs on the same channel radio frequency. Because each AP operates on the same channel, any AP interference is avoided. This setup is reliable, stable, and has seamless connections, ideal for highly mobile devices. In this setup you need to consider the number of devices because the higher the number of APs using the single channel the lower the throughput will be.

Multi channel

A **multi** channel setup operates with a number of wireless APs working on different channel radio frequencies or cells. Because each AP operates on different frequencies in the same network, APs are forced to renegotiate a connection, and may drop off between connections to the different APs. This setup is ideal for stationary devices and has a higher throughput than a single channel setup.

Channel blanket hybrid

Channel blanket **hybrid** mode allows simultaneous multi channel and single channel WLAN connectivity from the same AP. Network administrators can combine the performance attributes of the two architectures to best suit their specific deployment requirements. The multi-cell architecture enables both high bandwidth and high data throughput, while single cell channel blanket enables stable data transactions with seamless roaming on a single Wi-Fi channel.

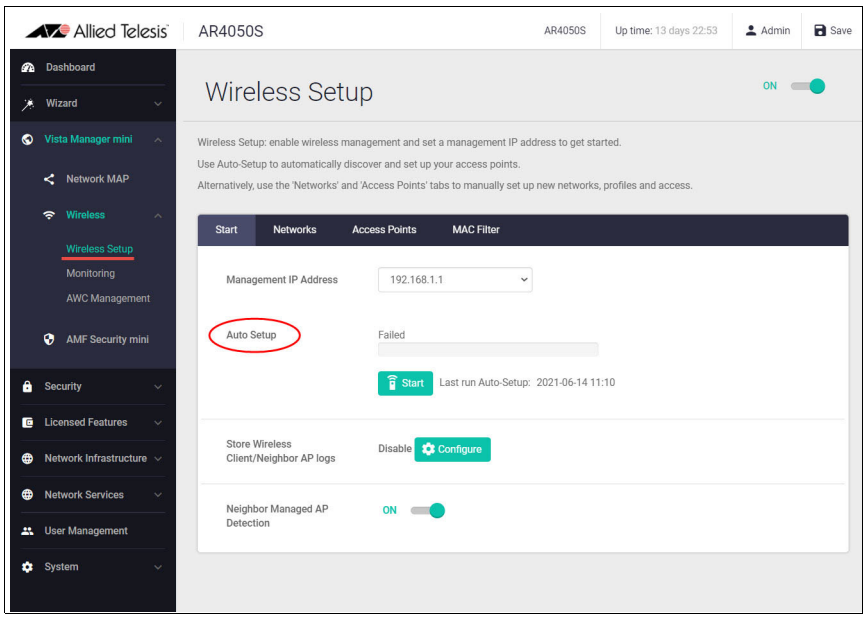


For a high-level video presentation about the AWC Channel Blanket (AWC-CB) wireless controller which enables both single and multi channel operation at the same time, see the Hybrid Wireless Technology video on the Allied Telesis website.

Configuring a multi channel wireless network

The Device GUI includes Vista Manger mini and a **Wireless Setup** menu, which allows you to set up your wireless network, monitor and configure the network, and manage AWC. You can set up AWC manually or use the Auto Setup feature.

These two methods are described next:



The Auto Setup feature

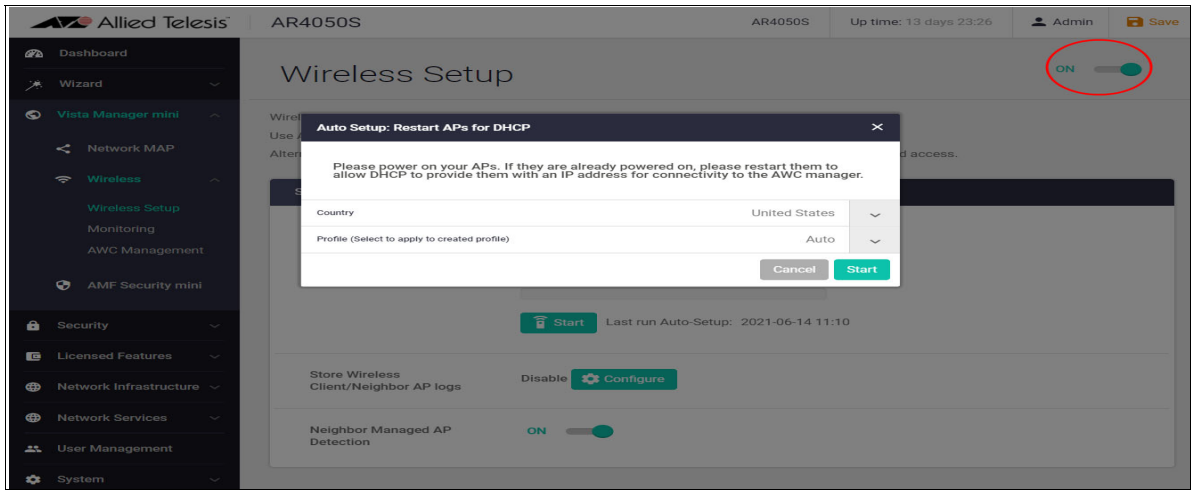
From release 5.4.8-1.2 onwards, you can set up your AWC managed network automatically using **Auto Setup**. Auto Setup makes wireless deployment simple. The Auto Setup feature is available on the AR2010V, AR2050V, AR3050S, and AR4050S devices.

The Auto Setup feature:

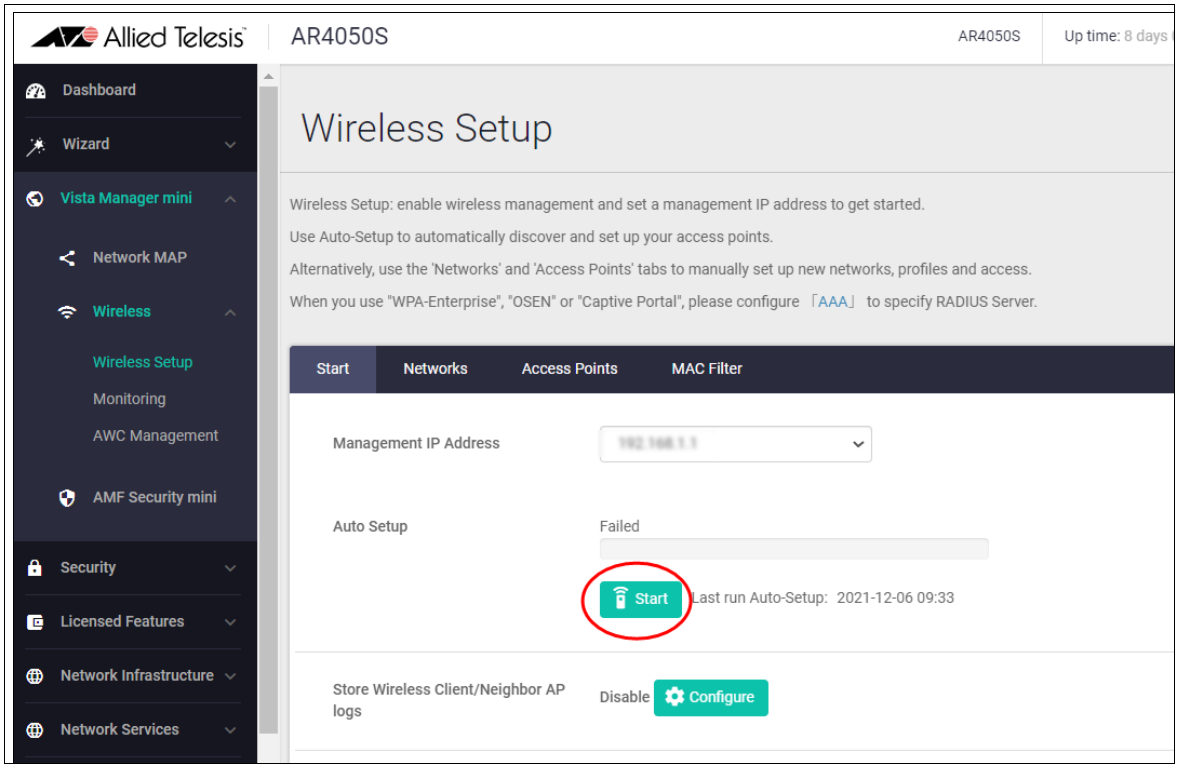
- discovers APs and automatically creates a configuration using their IP and MAC addresses.
- configures AP profiles based on the model name.
- creates the wireless network and security using defined default values.

Perform the following steps to automatically set up your AWC managed wireless network:

1. Click on **Wireless Setup** from the Vista Manger mini menu, then turn on wireless (**ON/OFF** button at top right of window) to enable wireless management. You may get a notification to power on your APs to allow DHCP to provide an IP address for connectivity to the AWC manager.

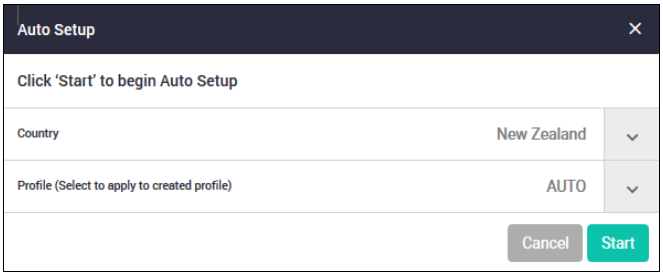


2. In the Wireless Setup **Start** tab, enter a **Management IP Address**. This is an IP address on the device you are on. AWC will use this IP address to communicate with APs in your network.



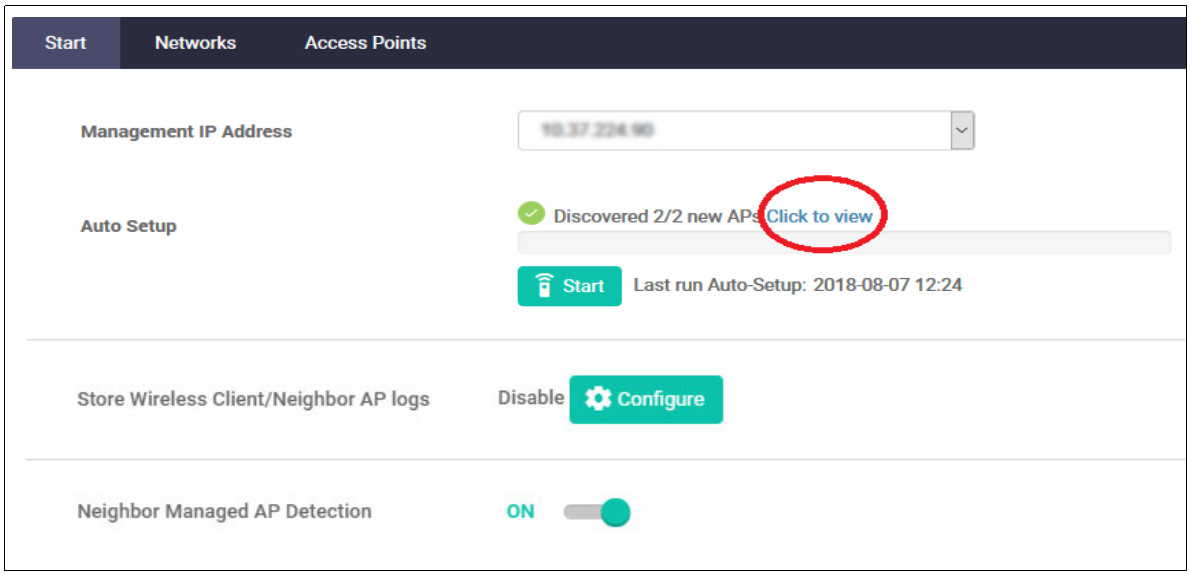
3. Use **Auto Setup** to automatically discover and set up your access points. Click the green **Start** button.

4. Select the country, for example New Zealand, and the Profile (you can use auto):



5. Click **Start** again to proceed with auto discovery.

6. When the auto discovery is complete you will see this dialog:



7. To see the automatically discovered APs, select **Click to view**.

8. This will take you to the **Monitoring** page, where you can select an AP and perform an action, such as **Refresh**, **Apply Config**, **Reboot** or **Update Firmware**. See "Monitoring the wireless network" on page 72.

Manual setup

There are a number of steps to manually set up a wireless system.

In brief, the order is as follows:

- Set a management IP address
- Add a network
- Create an access point profile for the AP series (e.g. TQ5403 Series)
- Add APs to the access point profile

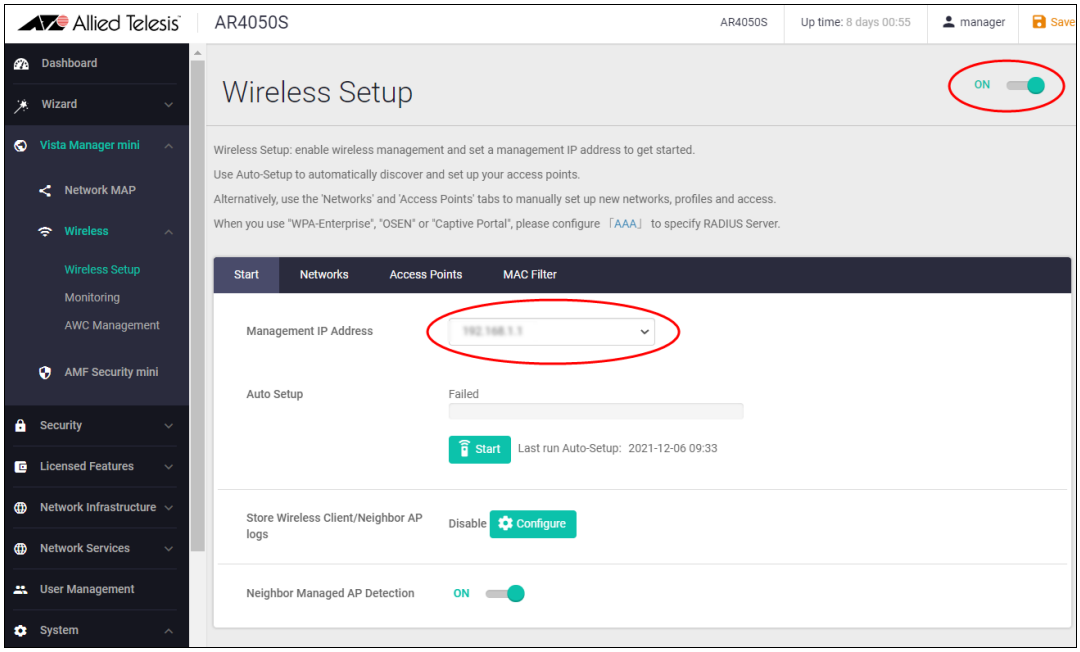
The detailed steps follow:

Set a management IP address

To manually set up your network, go to the **Wireless Setup** menu:

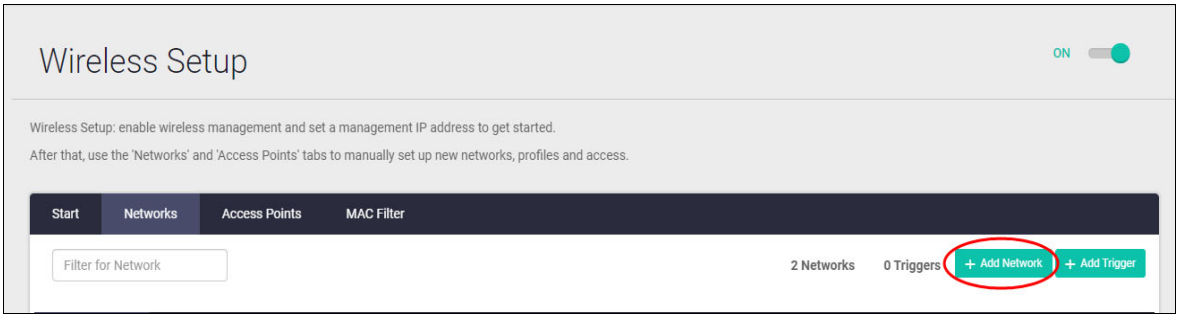
1. Click on **Wireless Setup**, then click the **ON/OFF** button to enable wireless management.

2. In the **Start** tab, select a **Management IP Address**. This is an IP address on the device you are on. AWC will use this IP address to communicate with APs in your network:

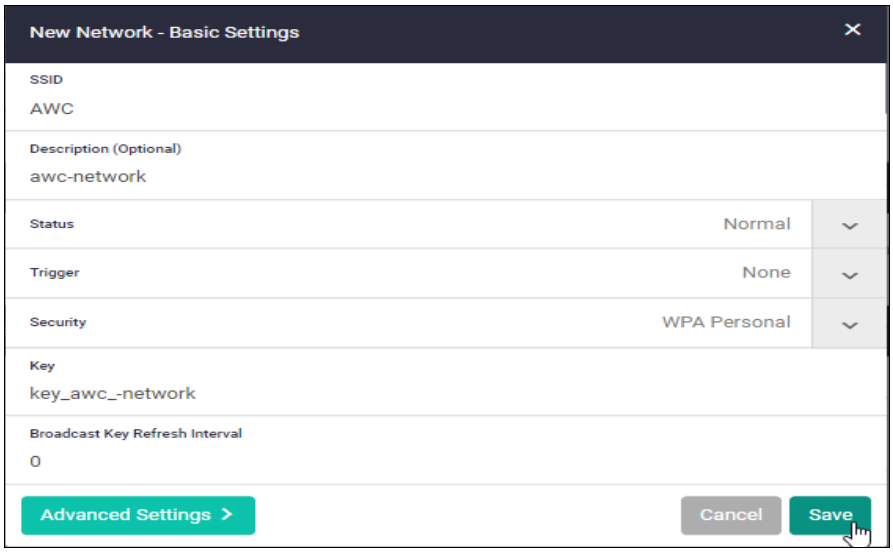


Add a network

1. From the **Networks** tab, click **+Add Network**:

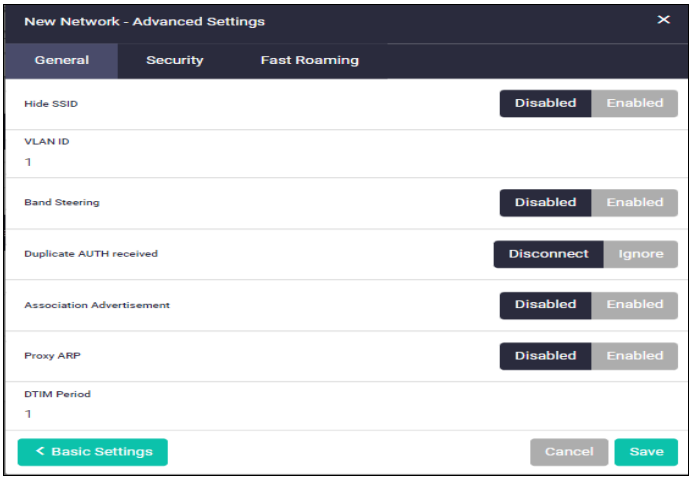


2. Add an **SSID Name**, and **Description**, and select the desired security type for your wireless network. Each **Security** type provides various fields for you to complete, for example - Key, RADIUS Authentication Group and Dynamic VLAN.



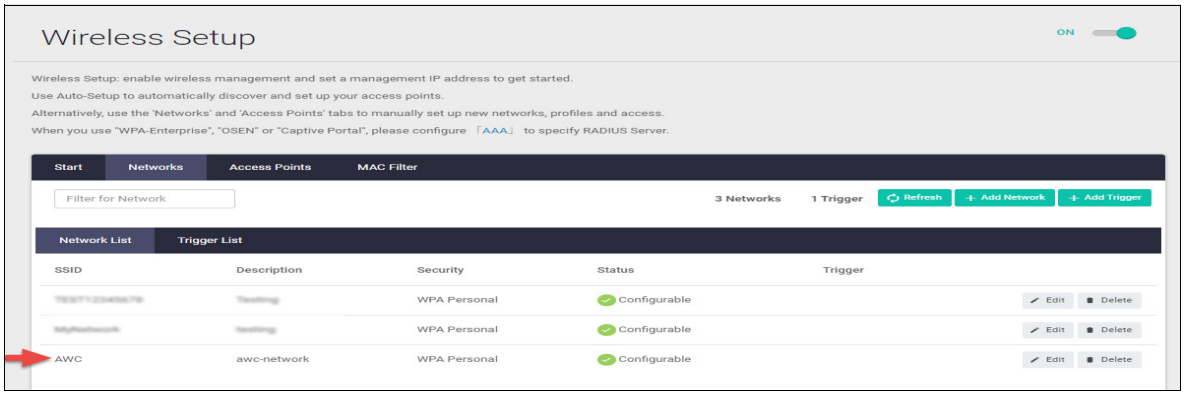
3. Click **Save**.

4. The **Advanced Settings** button provides network **General**, **Security**, and **Fast Roaming** configuration. Use the Security tab to configure **Captive Portal**. For information on configuring Captive Portal, see "Introduction to Captive Portal" on page 47.



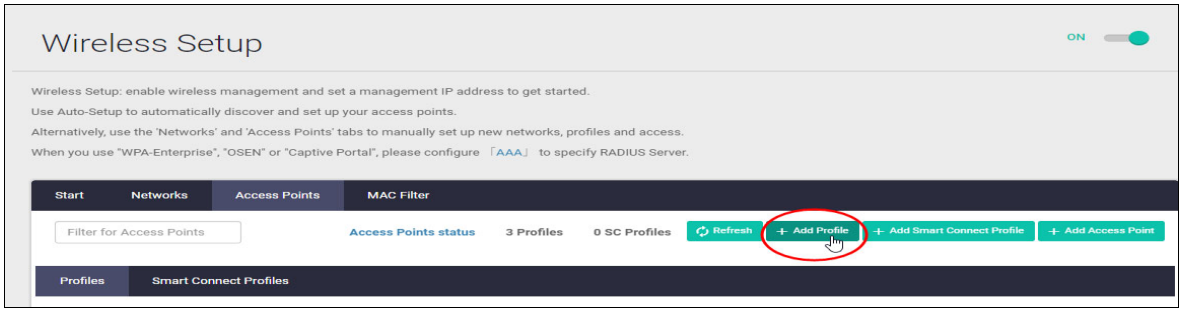
5. Click **Save** to complete this step.

6. The **Network List** tab, **SSID** column, contains a list of configured networks and their status.



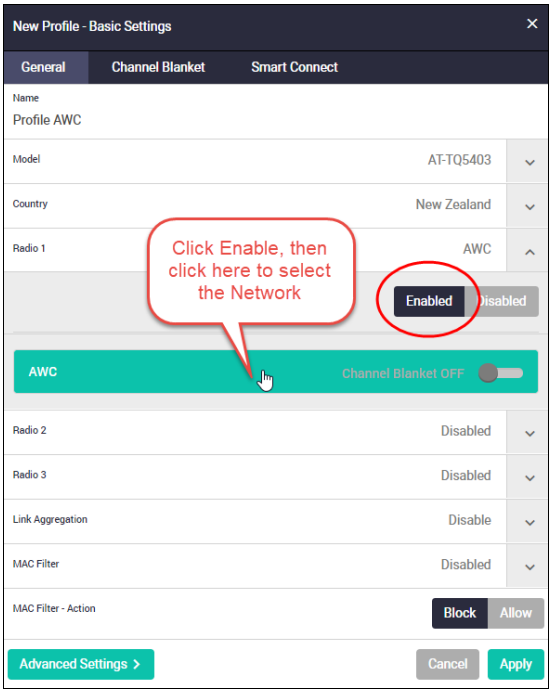
Create an access point profile for the AP series

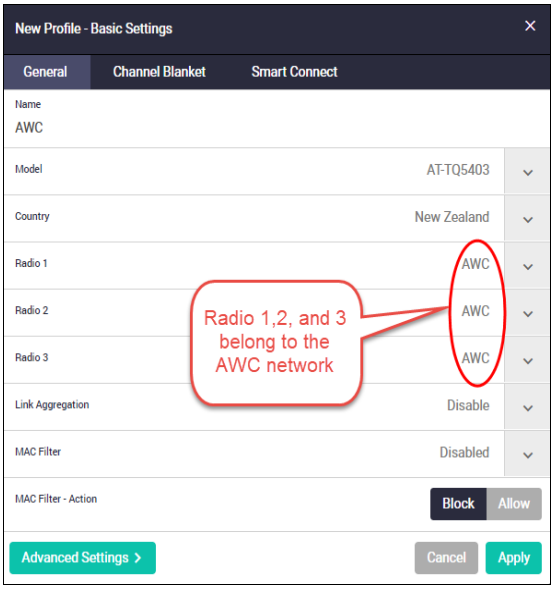
1. Click on the **Access Points** tab, then click **+Add Profile**:



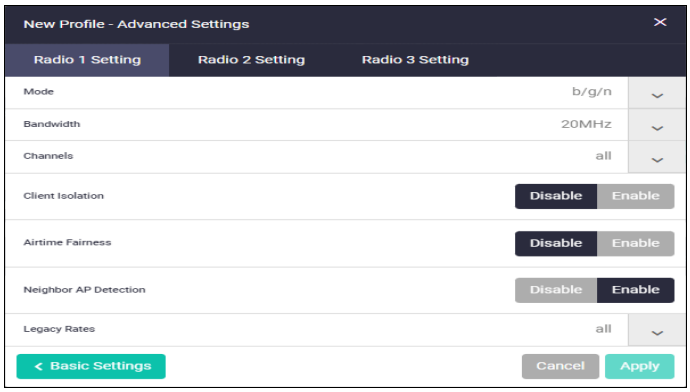
2. Create a profile for each series of AP being used:

- In the **New Profile Basic Settings** dialog, add a **Profile Name**, select the **AP model**, **Country, then Enable each internal radio (Radio1, 2, and 3).**
- Our example uses the TQm5403 AP, which contains three IEEE 802.11 2ss internal radios to enable concurrent Wi-Fi communications: one at 2.4GHz band, and two at 5GHz band.
- Make sure you click on the network name (the network is 'AWC' in our example below). The field will turn green in color when selected correctly.



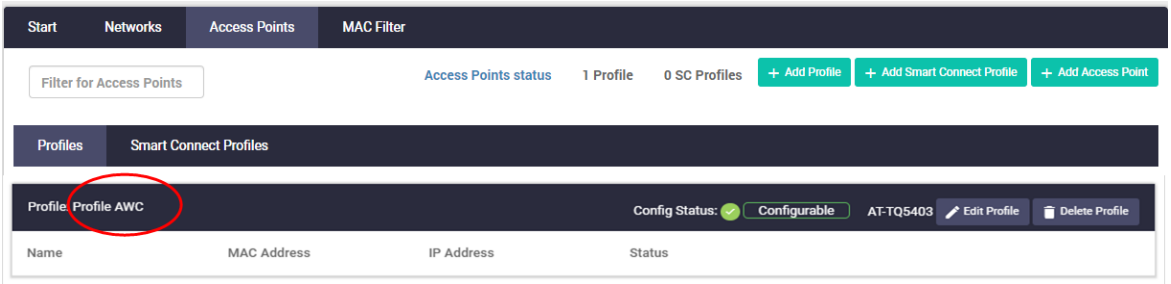


3. Use the **Advanced Settings** to configure: **Mode**, **Bandwidth**, **Channels**, **Client Isolation**, **Neighbor AP Detection** and **Legacy Rates** options for each radio.



4. Click **Apply** to save your selections.

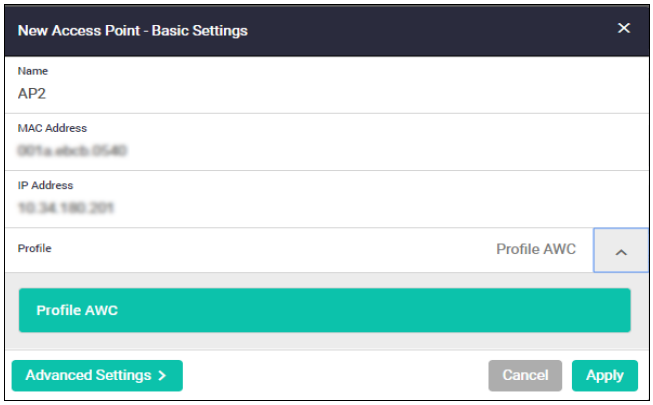
5. You can now see the newly created AP profile (‘Profile AWC’ in our example below):



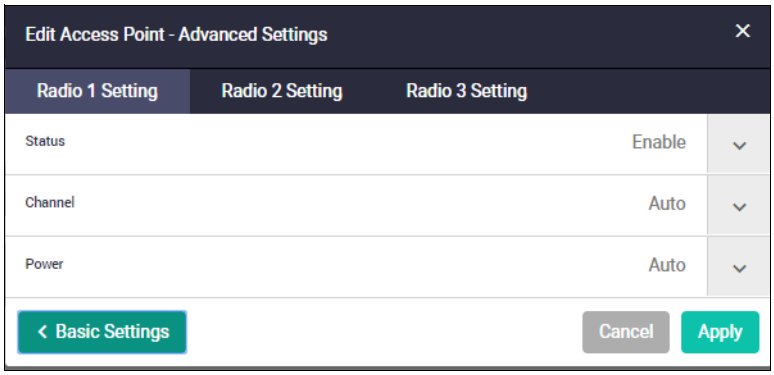
Add APs to the access point profile

1. Click on the **Access Points** tab, then click **+Add Access Point**.

2. Enter the AP **Name**, **MAC Address**, and **IP Address**, and then select the **Profile** for your AP:

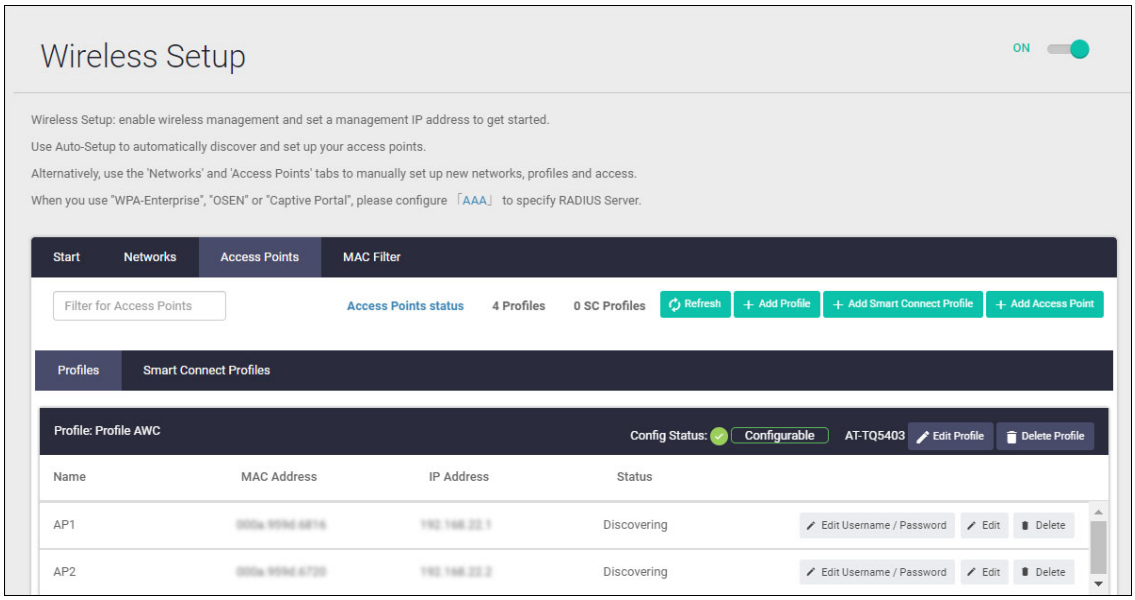


3. The **Advanced Settings** button provides additional internal radio settings: **Status**, **Channel** and **Power**:



4. Click **Apply** to complete this step.

5. You can now see our newly added access points listed under the AP profile they have been assigned to. In the example below, AP1 and AP2 are assigned to: ***Profile AWC***.



Configuring AWC Channel Blanket

AWC Channel Blanket is a wireless feature where groups of access points are configured to use the same wireless settings including WLAN channel, BSSID, SSID, and Country.

License requirements and Vista Manager mini

You need an AWC-CB license and an AWC license for Channel Blanket to operate. The channel-blanket setting can only be used with APs that support channel blanket. If this is set for other APs, you will not be able to manage those APs. See your AP's datasheet to see if it supports channel blanket.

You can configure and manage AWC Channel Blanket using Vista Manager mini. Integrated into the Device GUI, Vista Manager mini provides full network visibility of AMF and AWC devices.

First you need to set up a multi channel wireless network (see "Configuring a multi channel wireless network" on page 10). Then, there are two more steps to configure AWC Channel Blanket:

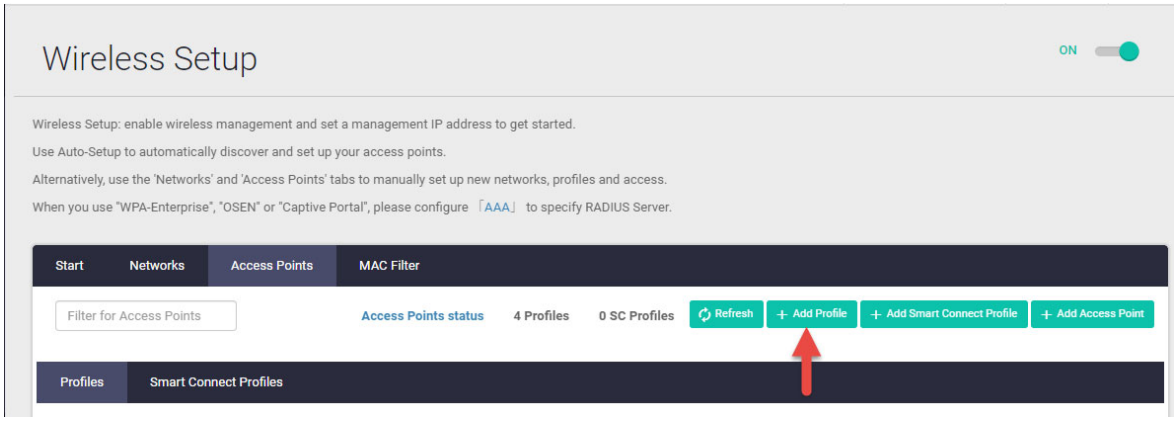
- Create an AP profile
- Add APs to the profile

Creating an AP profile

An access point profile groups together APs of the same model type, enabling you to manage multiple wireless APs. You can easily apply a Channel Blanket configuration by turning on Channel Blanket in the AP profile settings.

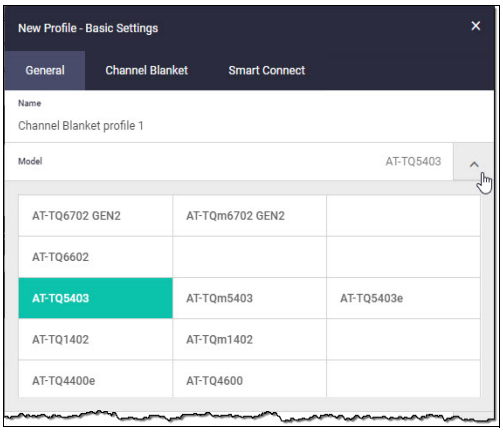
To create an AP profile:

1. Select the **Access Points** tab, then click the **+Add Profile** button:



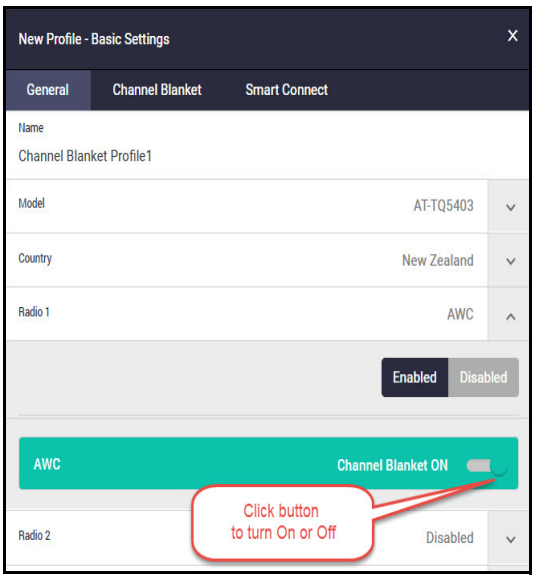
2. In **New Profile -Basic Settings** select the **General** tab.

3. Enter a Profile **Name**, select the AP **Model**, and **Country**.

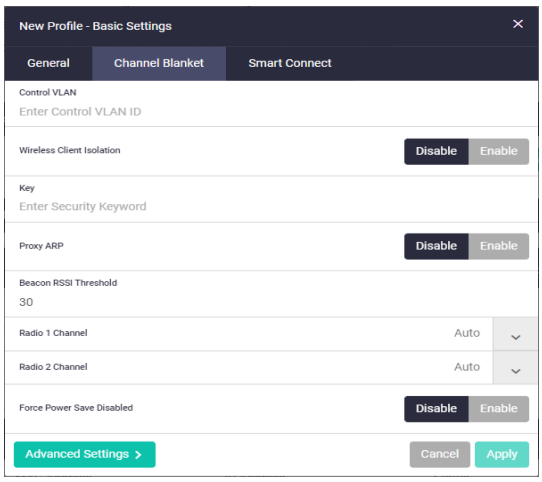


4. Enable each internal radio. Our example uses the TQm5403 AP, which contains three internal radios: one at the 2.4GHz band, and two at the 5GHz band.

5. Turn on **Channel Blanket**.



6. Select the **Channel Blanket** tab.

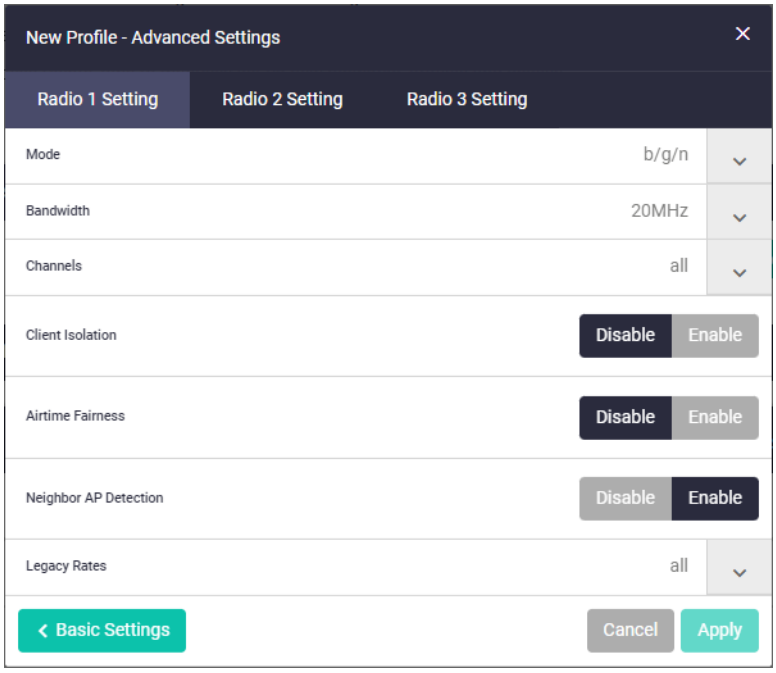


7. Enter the **Control VLAN** number.

8. Nominate the **Designated AP**. The Designated AP's BSSID (i.e. the AP's physical MAC address) will be advertised as the channel blanket BSSID.

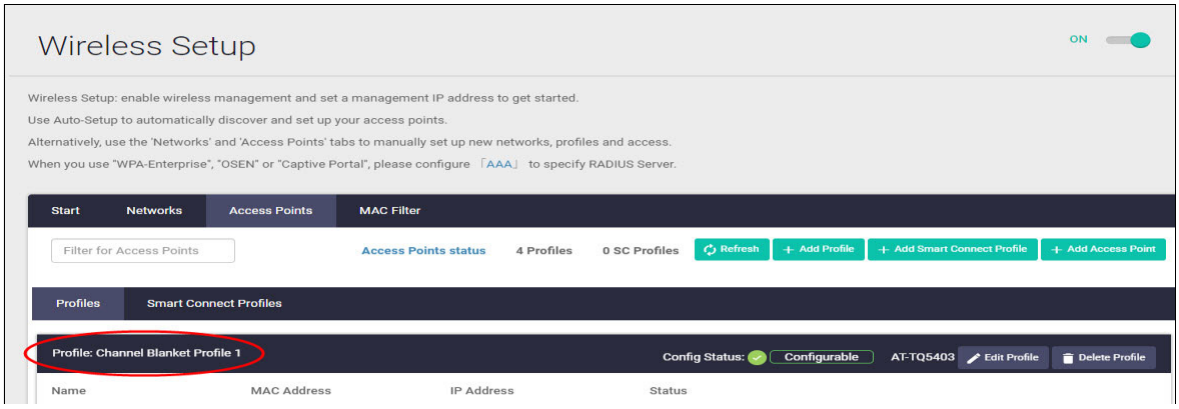
9. You can also configure **Wireless Client Isolation**, **Key** (this will be automatically set up if left blank), **Radio 1 Channel** and **Radio 2 Channel** settings (auto is the default setting). The **Force Power Save Disabled** setting will prevent clients from changing to power saving mode (only available for certain models).

10. The **Advanced Settings** button provides additional Profile settings: **Mode**, **Bandwidth**, **Channels**, **Client Isolation**, **Airtime Fairness**, **Neighbor AP Detection**, and **Legacy Rates** options for each of the internal radios.



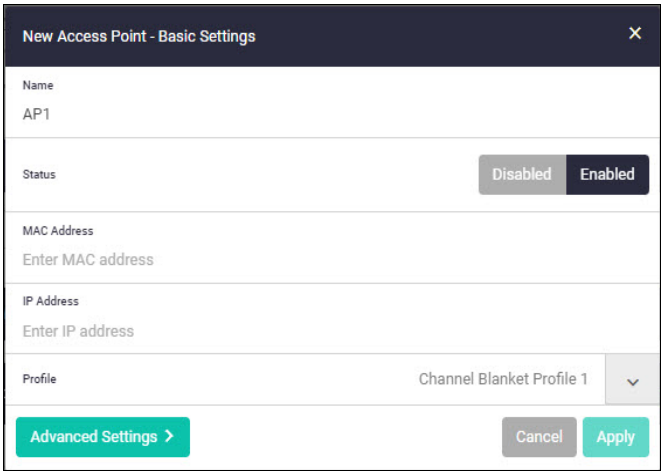
11. Click **Apply** to complete this step.

12. You can now see the newly created profile.

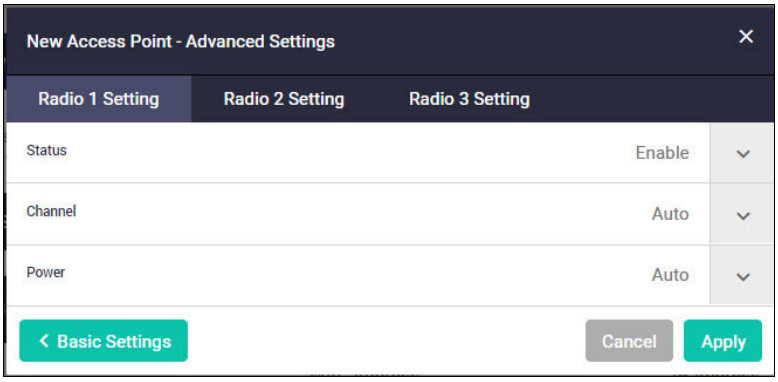


Adding APs to an AP profile

1. Click **+Add Access Point**, and enter the access point **Name**, **MAC address**, **IP Address**, and select the Channel Blanket **Profile**:

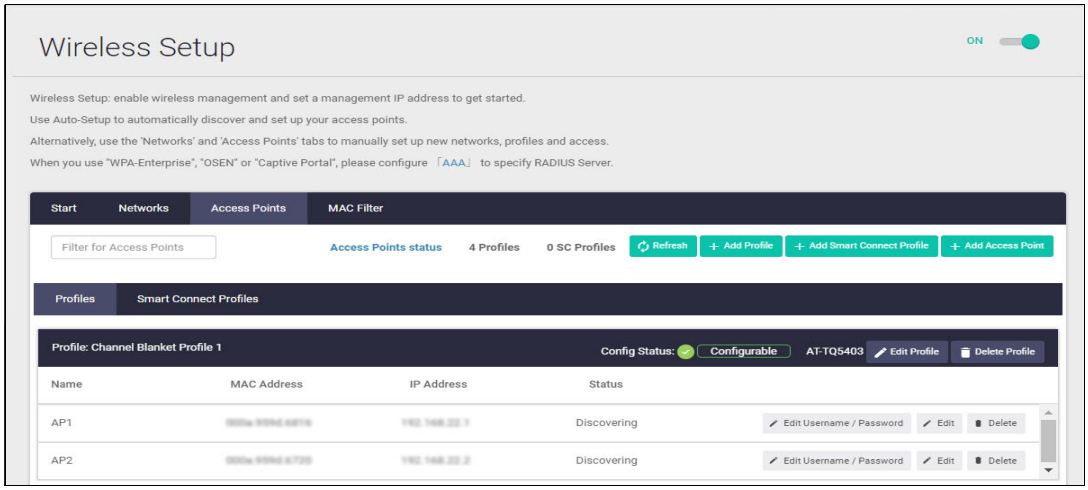


2. The **Advanced Settings** window provides **Status**, **Channel** and **Power** settings for the AP's internal radios. Change these as required.



3. Click **Apply** to complete this step.

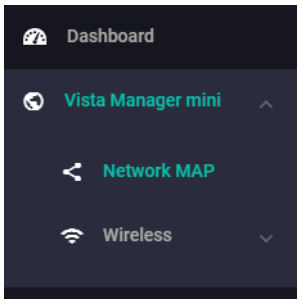
4. You can now see the Profiles, APs, and Networks that you have added in your wireless network.



You can come back to the **Wireless Setup** anytime to add, edit, or delete profiles, APs, and networks.

The network map

Under the Vista Manager mini menu, there is a network topology map:



This map shows details of the devices connected to the switch or firewall. You can use it to see your:

- wired devices
- APs
- wireless deployment and coverage.

This section begins with a brief description of the network map window and the tasks you can perform there. The section ends with a look at configuring the network topology view and customizing node icon images.

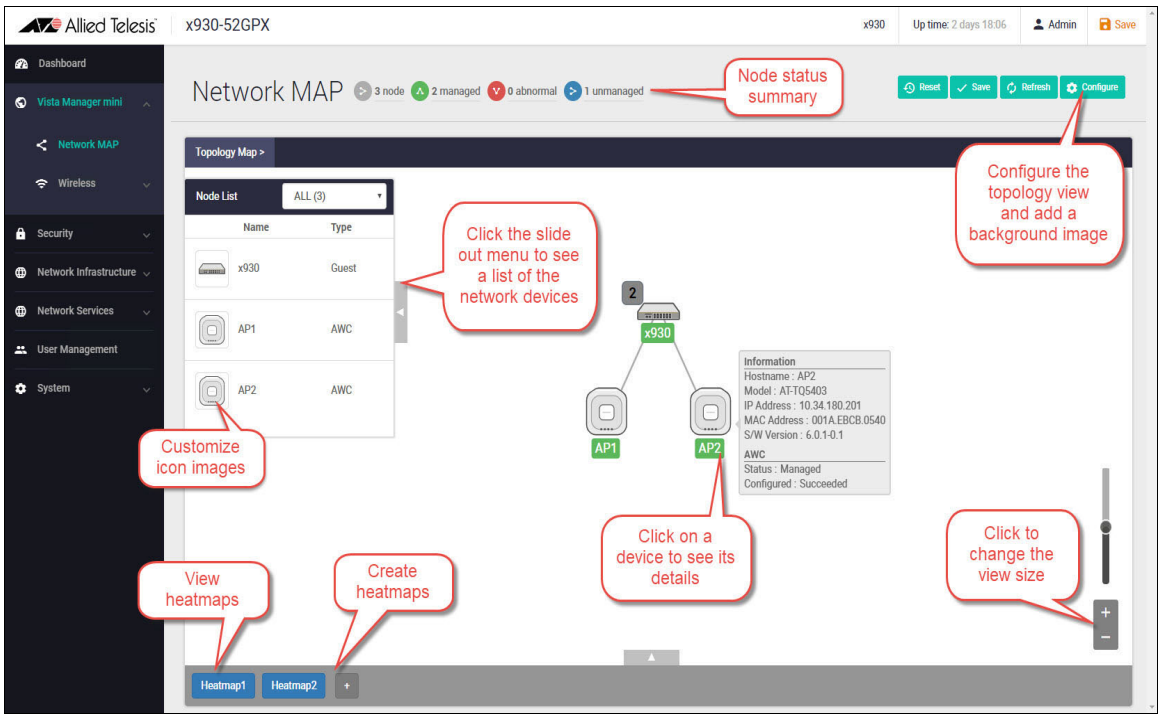
Note that the screenshots in this section show an x930 Series switch, but the functionality is the same for all models that include Vista Manager mini.

The network map features

The network map displays details of a network configuration. Double click on an area to see all the nodes in that area. Use the network map to check the status of a node at a glance. Node status is indicated by the node title background color. Abnormal is red, managed is green, and blue indicates an unmanaged node.

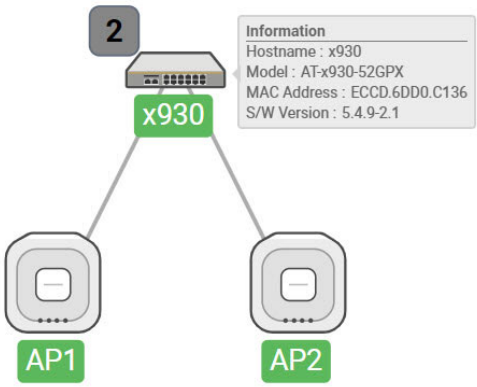
From the **network MAP** page, you can:

- customize network icon images
- view individual node details
- see a list of network nodes
- configure the topology view
- create a heat map
- view stored heat maps



Viewing node information

In the network topology map view, click on a device to see information about the Hostname, Model, MAC address, and software version.



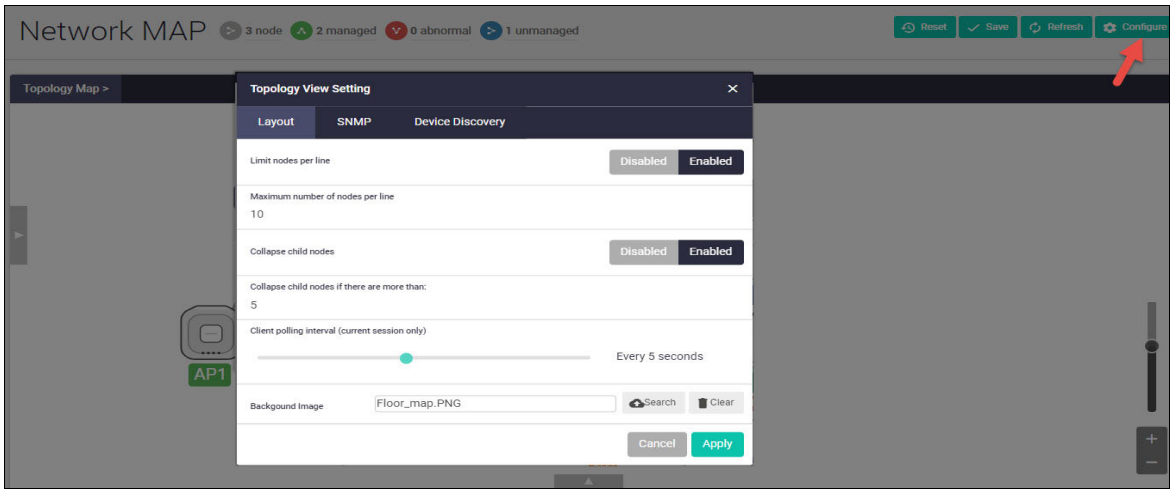
Configuring the topology view

Vista Manager mini automatically creates a complete topology map from an AMF network of switches, firewalls, and wireless access points (APs), showing areas and multiple levels of connected nodes and devices.

To change the topology view settings:

- In the Topology Map view, select **Configure** - the menu is located at top right corner.

- In the **Topology View Settings** window, you can choose to:
  - limit nodes per line
  - collapse child nodes
  - select a background image
- **Save** your changes.



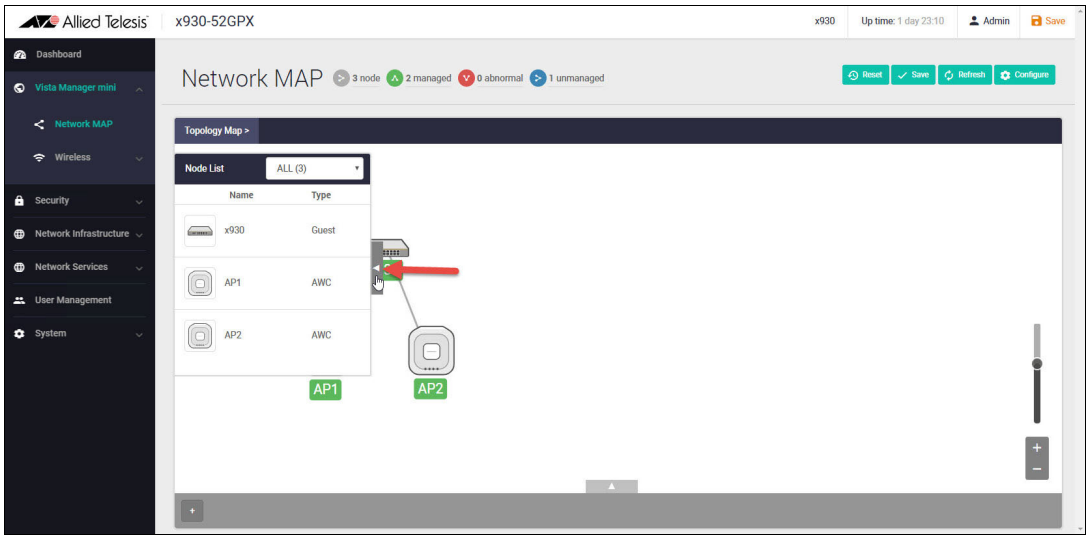
Customizing network node icon images

You can customize the look of your network nodes with icon images. For example, you can add access point, switch, and router images to make the network map easier to understand at a glance.

You can create an icon library to help store, organize, and find images.

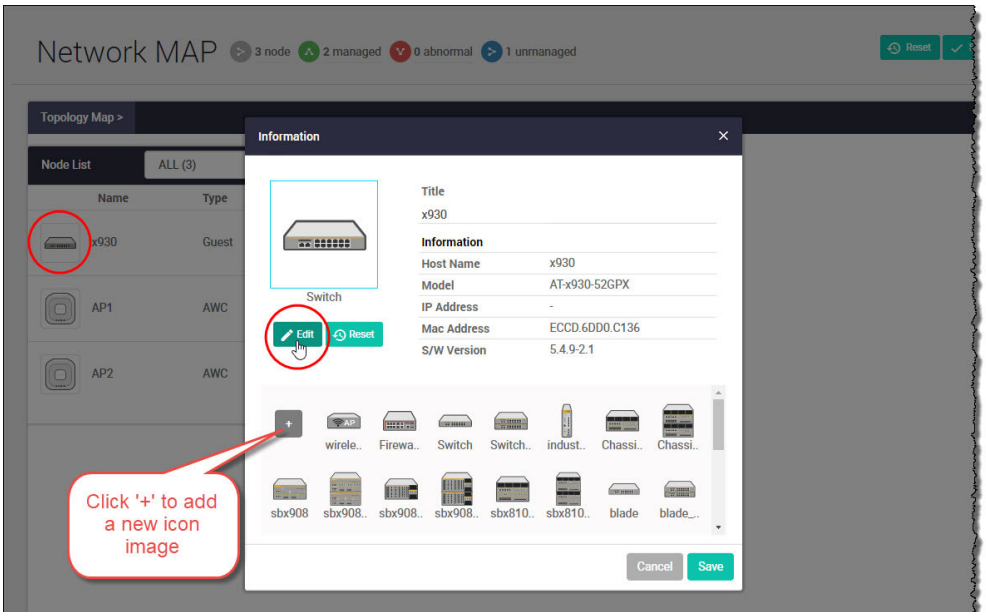
To customize a network node icon:

1. In the Topology Map view, open the **Node List** (slide-out menu)



2. Click on a node's icon image.

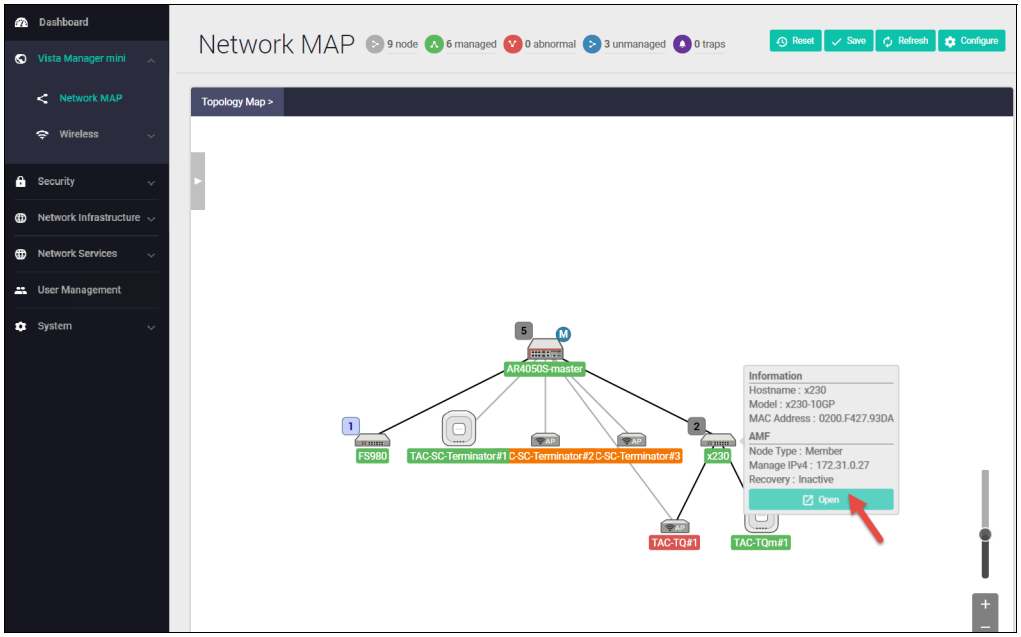
3. Click **Edit**.
4. Select an image from the library or click the '+' sign to add a new one.
5. Click **Save**.



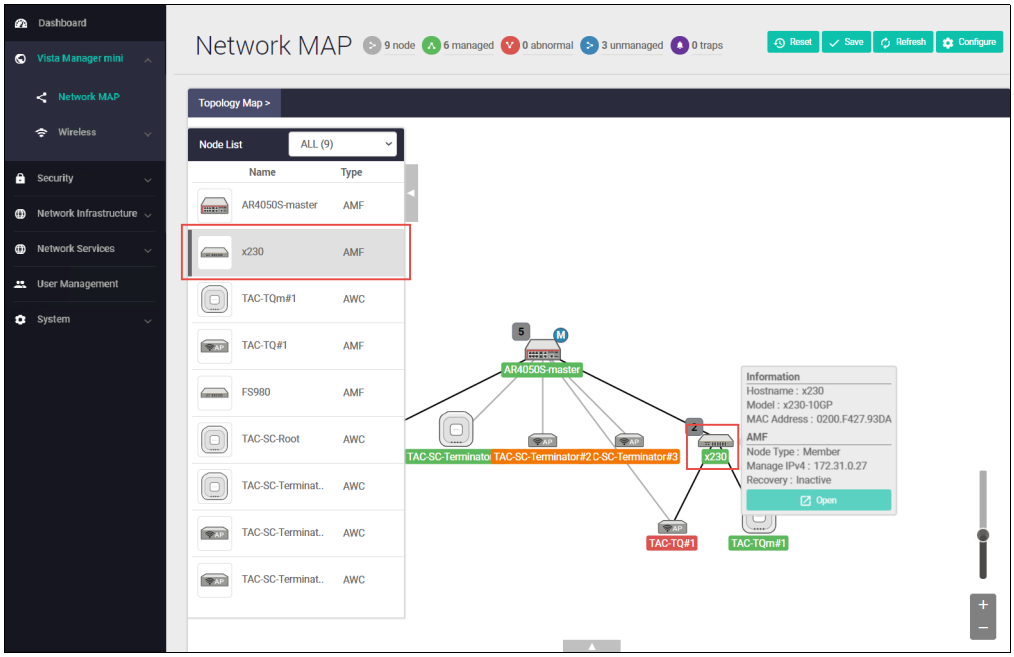
Access to device GUI by clicking on device icon

From version 2.5.2 onwards, you can open the GUI for a device in your network (e.g. an x230) from the network map in the GUI of another device in your network (e.g. an AR4050S).

When you click a node icon on the Network Map, the node information is displayed. In the node information window, click on the **Open** button to access the device's GUI.



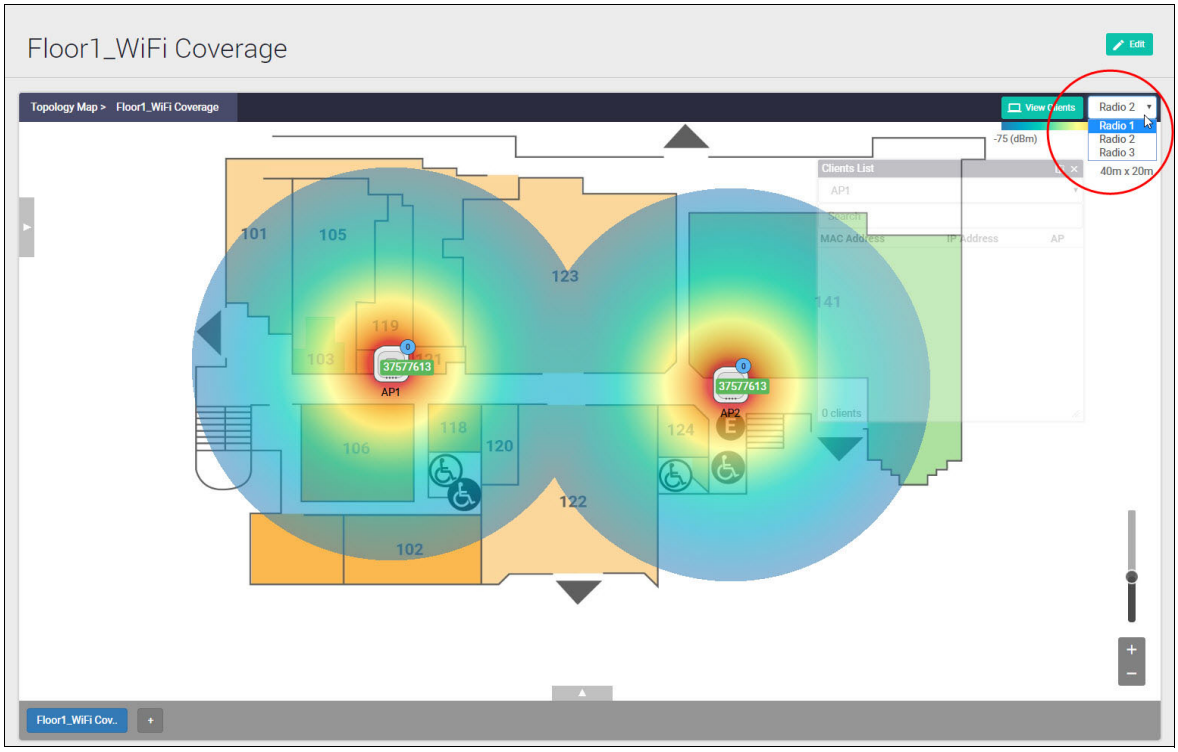
You can use the **Node List** to help you locate a device in the network map. Simply click the device in the Node List to see its **Information** details.



Heat maps

Heat maps show wireless deployment and coverage. Heat maps use colors that immediately show the spots with stronger and weaker Wi-Fi signal strength. Red indicates the strongest signal strength and as the signal attenuates the circle color changes to become shades of orange, yellow, green, and then blue at the weakest signal strength.

AWC creates heat maps using wireless intelligence models based on AP location and signal strength information. Heat maps let you see exactly what quality of coverage your Wi-Fi access point provides, and whether you should move it, or add another AP.



To create a heat map you need to perform two tasks:

- Add a floor map
- Add APs to the floor map.

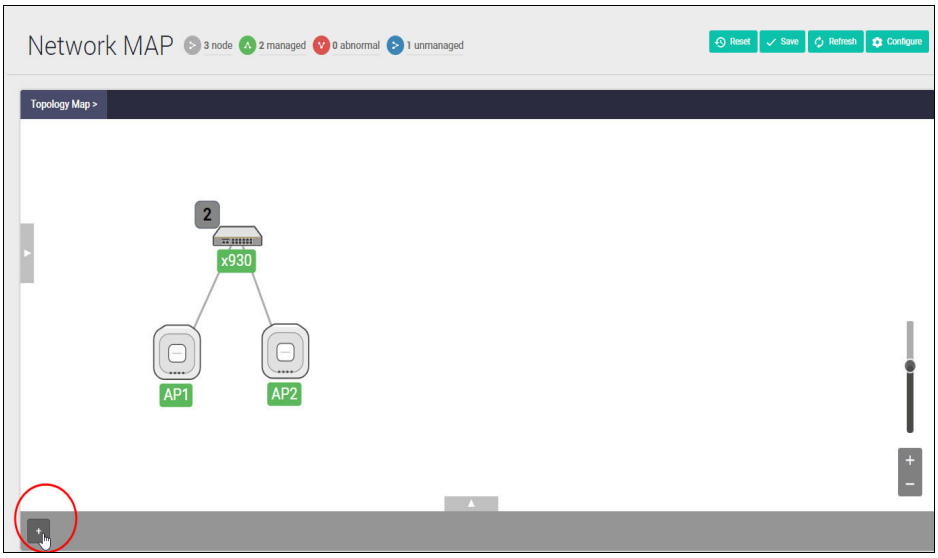
These two tasks are described next.

Adding a floor map

The first step in creating a heat map is to add a floor map. The floor map provides a background for your heat map. The floor map must be based on the actual physical layout of a building floor and you will need to know the floor area size. This is so AWC can correctly calculate the Wi-Fi coverage that any given AP will produce.

To add a floor map:

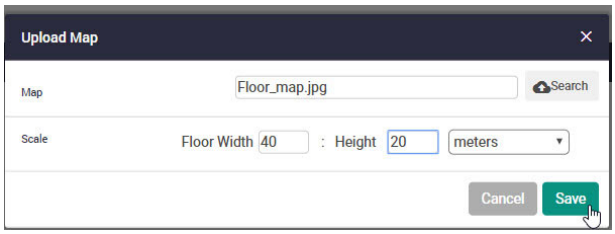
1. In the network topology map view, click the '+' sign at the bottom of the window.



2. Click **Upload Map**.

3. Browse to select a floor map and enter its physical dimensions, for example: 40m x 20m.

   Note: Enter the actual floor size because signal strength information is automatically retrieved based on AP model specifications.



4. Click **Save**.

5. The floor map is displayed.

6. Click the pencil icon to change the heat map name from the default, if desired.

7. Repeat this process to create additional floor maps as required.

You are now ready to add APs to the floor map. For more information on working with or editing heat maps, see "Configuring heat map coverage" on page 32.

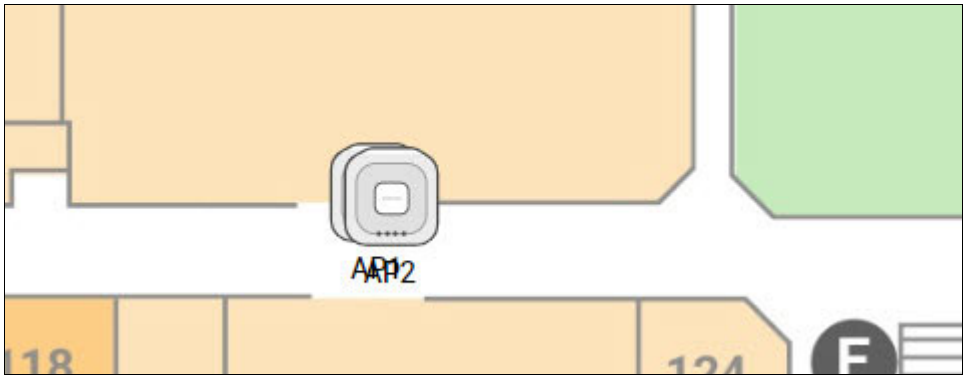
Adding APs to a floor map

The second step in creating a heat map is to add APs to the floor map. In this step, you place each AP in the position you consider appropriate or as they are physically installed.

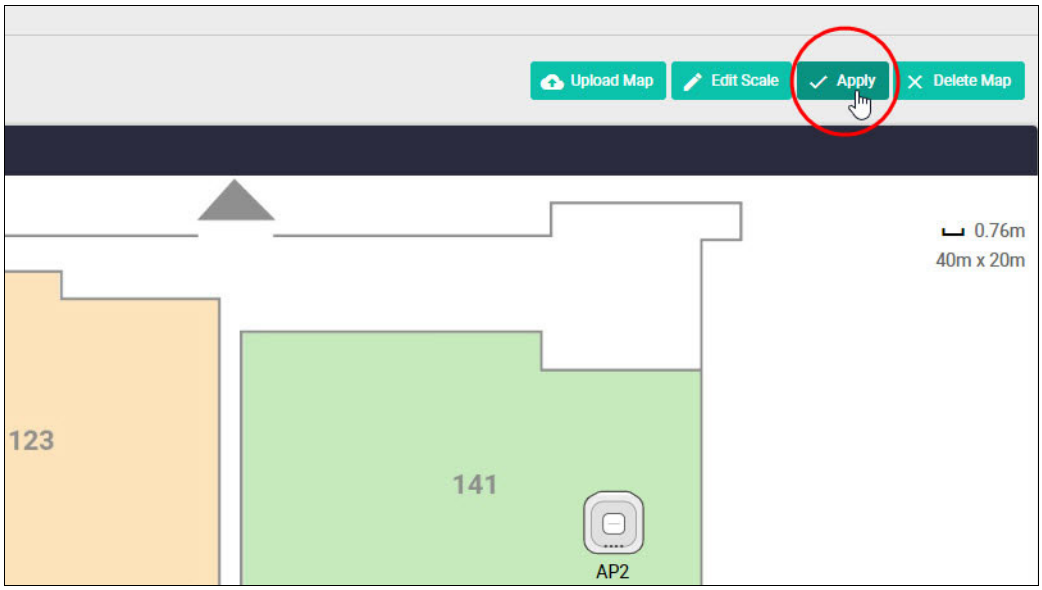
To add APs to a floor map:

1. In the Network MAP view, open the **Node List**.
2. Click the AP **Name** (not the icon).

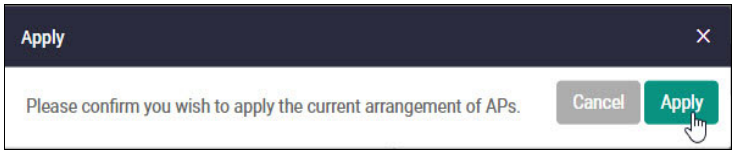
3. The AP icon is added to the centre of the map. Note: If you can't see one of the newly added icon images, look behind one that you can see. Sometimes the icons are hiding behind each other.



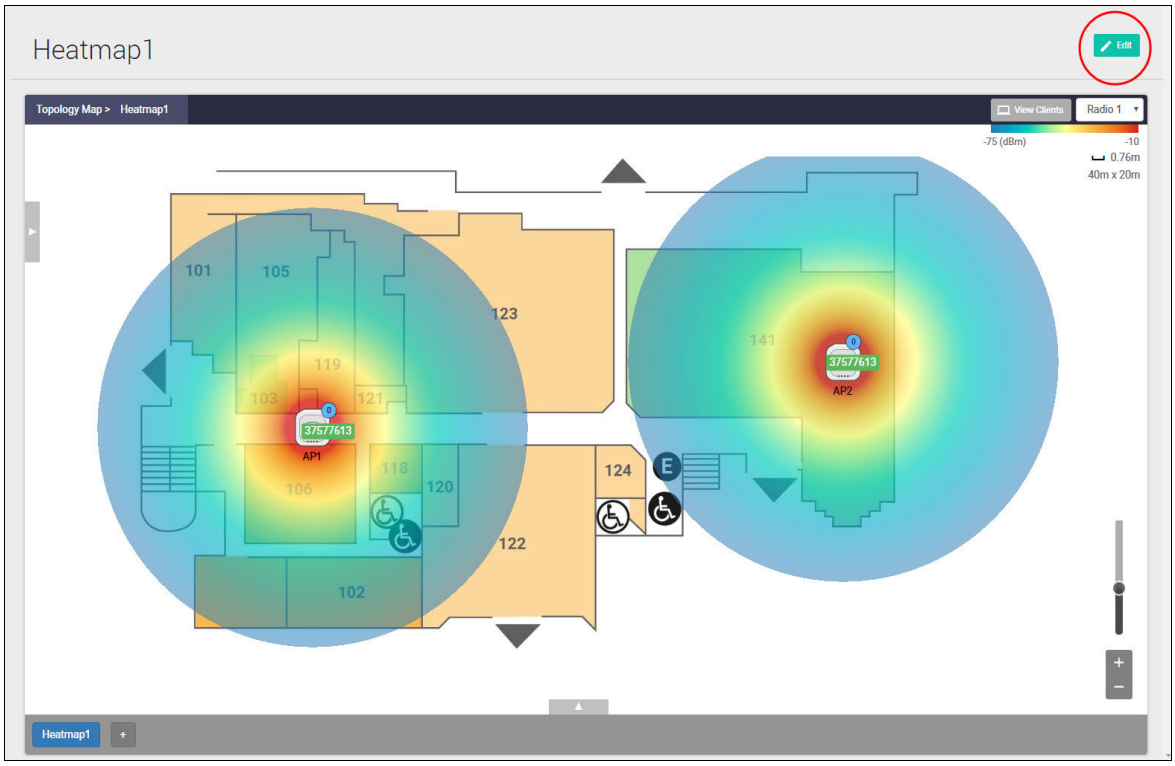
4. Drag the AP(s) to the desired position(s) on the floor map.
5. Once the APs are in place, click **Apply**.



6. To save and confirm the current AP arrangement, click **Apply** a second time.



7. The heat map automatically displays.

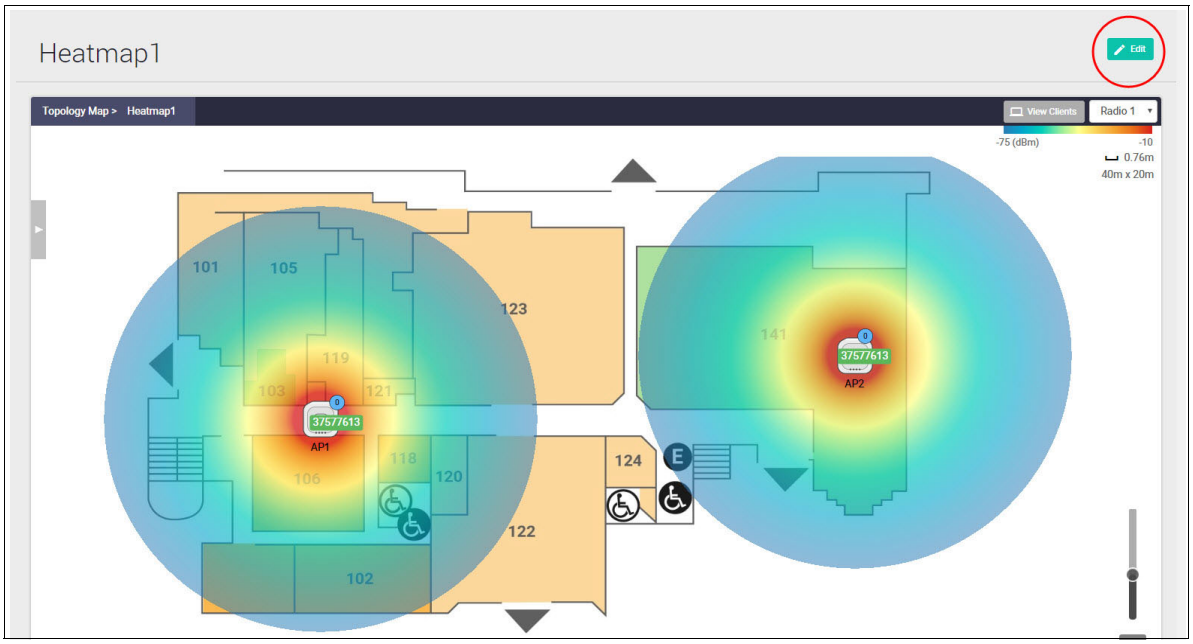


8. Edit the heat map if coverage needs to be improved. We discuss how to do this next.

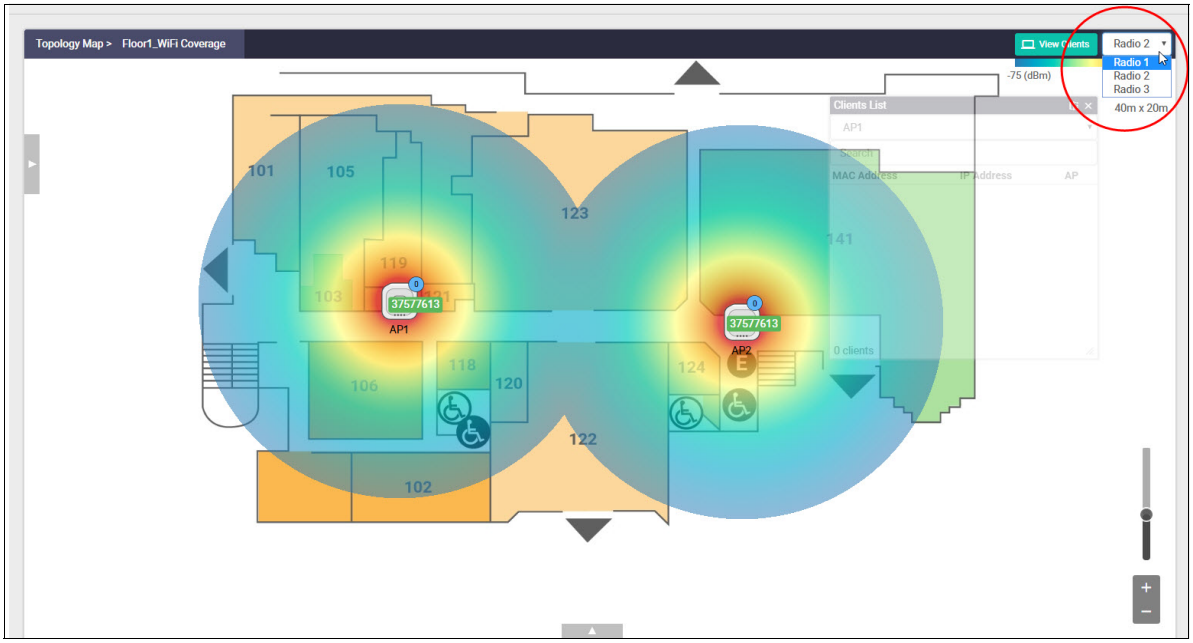
Configuring heat map coverage

Heat maps use colored rings to indicate the radio signal strength and range. You can see in the example below, the heat map rings do not cover the entire floor map. This isn't ideal as some floor areas will have weak, limited, or even no Wi-Fi signal strength.

To remedy this, move one or more of the APs to a different physical location. Then **Edit** the heat map, re-position the APs, and re-save the heat map.



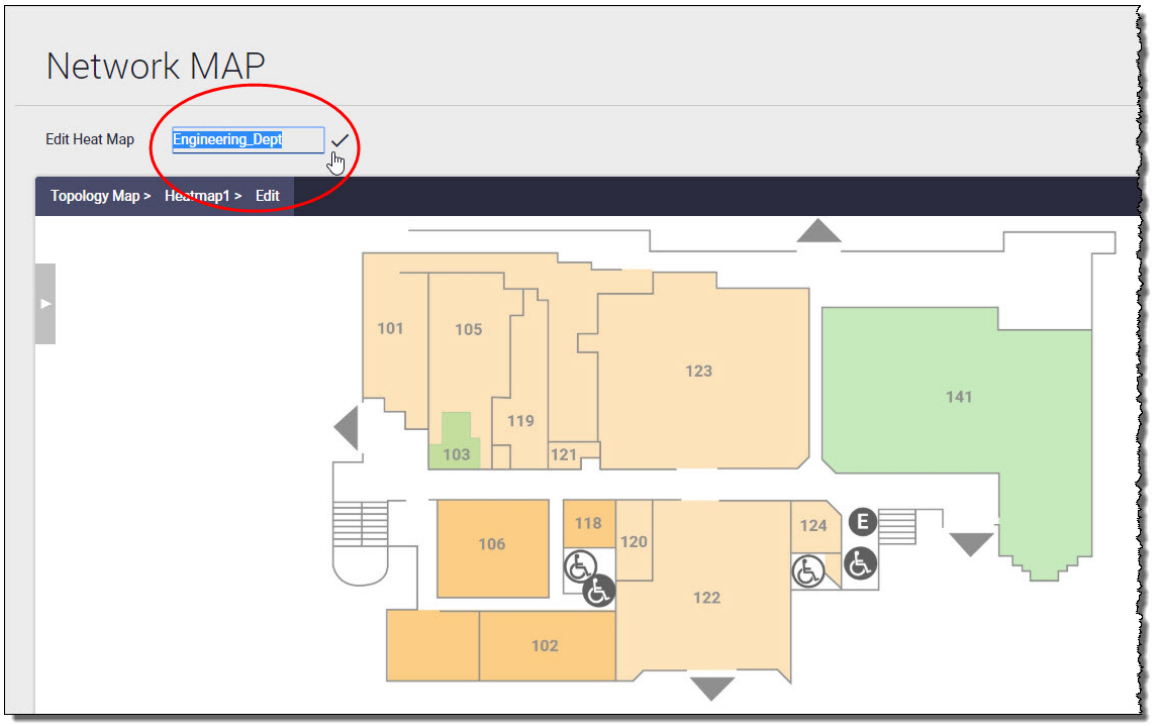
After re-positioning one or more APs, and saving the configuration, the new heat map shows improved coverage.



Re-naming a heat map

Use the **Edit** function to re-name a heat map.

- In the **Edit Heat Map** view, enter the new heat map name.
- Click the ‘check mark’ to **save**.



Introduction to AWC Smart Connect

Based on a plug-and-play concept, AWC Smart Connect (AWC-SC) is a wireless feature that allows you to expand your wireless network without the complexity of added cables.

Software and license requirements

You can configure and manage AWC-SC using Vista Manager mini. Integrated into the Device GUI, Vista Manager mini provides full network visibility of AMF and AWC devices.

You need an AWC license and an AWC-SC license for Smart Connect to operate.

The AWC-SC feature is supported by AP models:

- TQ6602 with firmware version 7.0.2-0.1 or later, with Device GUI 2.11.0 or later
- TQ5403,TQm5403, and TQ5403e with firmware version 6.0.1-0.1 or later, with Device GUI 2.4.0 or later.

You can build an AWC-SC network using the following AP model combinations:

- TQ6602 only
- TQ5403 only
- TQ5403e only
- TQ5403 as the Root, and TQm5403 in a Connector or Terminator role

For more information on AP roles, see "Wireless AP roles" on page 35.

The benefits of AWC-SC

Managing a wireless LAN can be challenging with environments constantly changing. Some of the most common tasks associated with changing wireless environments include:

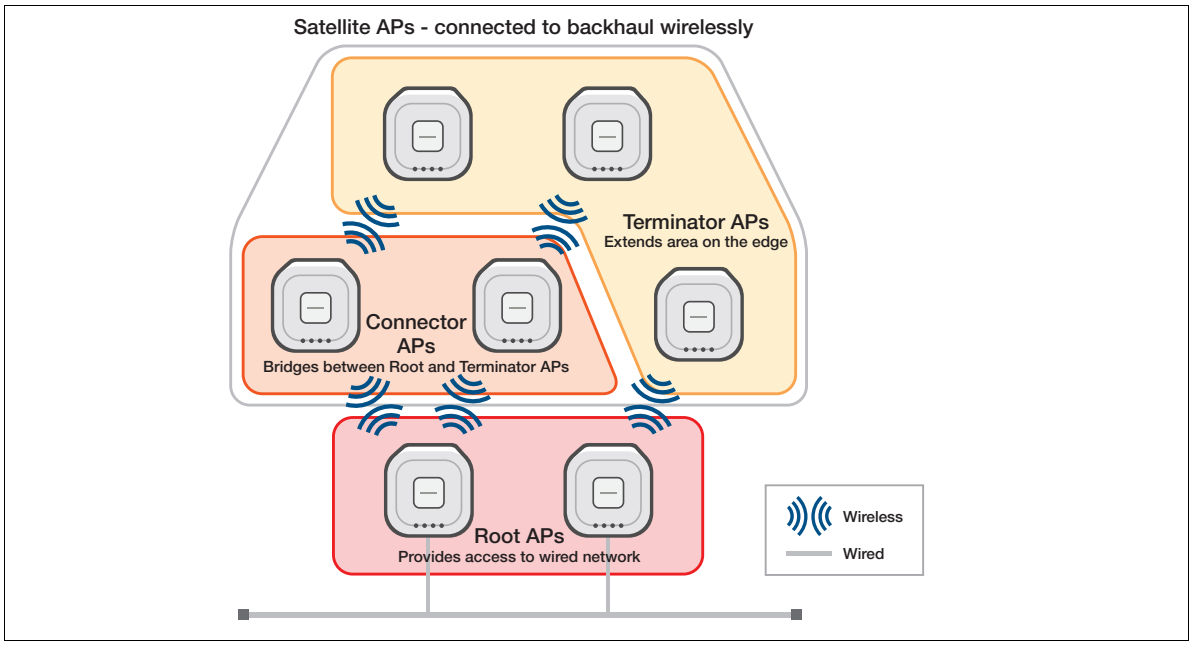
- Modifying a floor layout
- Expanding the wireless area
- Deploying a new wireless LAN

Modifying, expanding, and deploying wireless LANs can be costly when you factor in device purchases, cabling, configuration costs, and possible site surveys. Site surveys consider how best to achieve a redundant, stable, and loop free wireless environment using the available range of AP radio channels. However, using AWC-SC in combination with AWC Channel Blanket eliminates the need for site surveys as all existing and additional APs operate on the same channel. The cost benefits are obvious.

In an AWC-SC network, the wireless connection path between APs is dynamically changed according to the surrounding conditions. In this way a redundant, stable, and loop free wireless network is achieved.

Wireless AP roles

A wireless access point (AP), is the hardware device that allows other wireless devices to connect with each other and to a wired network.



APs support the connection of multiple wireless devices through a wired connection. APs can have different roles, and these are generally classified as follows:

Root AP

Root APs are located at the very top of a Smart Connect network. They are connected to the **wired** network and bridge packets between the Satellite APs connected wirelessly and the wired network. Root APs provide both Wi-Fi connectivity to client devices as well as providing a wireless backhaul connection to one or more wired APs.

Satellite AP

Satellite APs are located downstream and wirelessly connected to other APs in a Smart Connect network. Wireless connection paths between Satellite APs are automatically constructed and changed according to the surrounding conditions. Satellite APs can be further classified as Connector or Terminator APs:

Connector APs

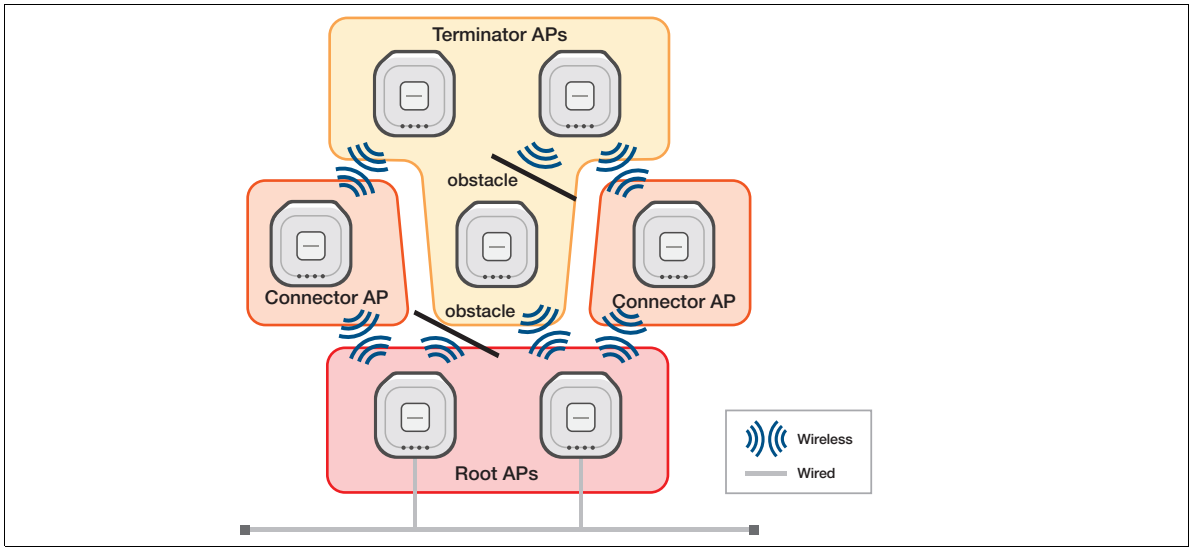
- are located in the middle of the AWC-SC's multi-tier wireless connection.
- bridge packets from the Root AP to the Terminator AP and clients, and from the Terminator AP and clients to the Root AP.
- support only one bridge connection - (2 hops as Root-Connector-Terminator APs.)

Terminator APs

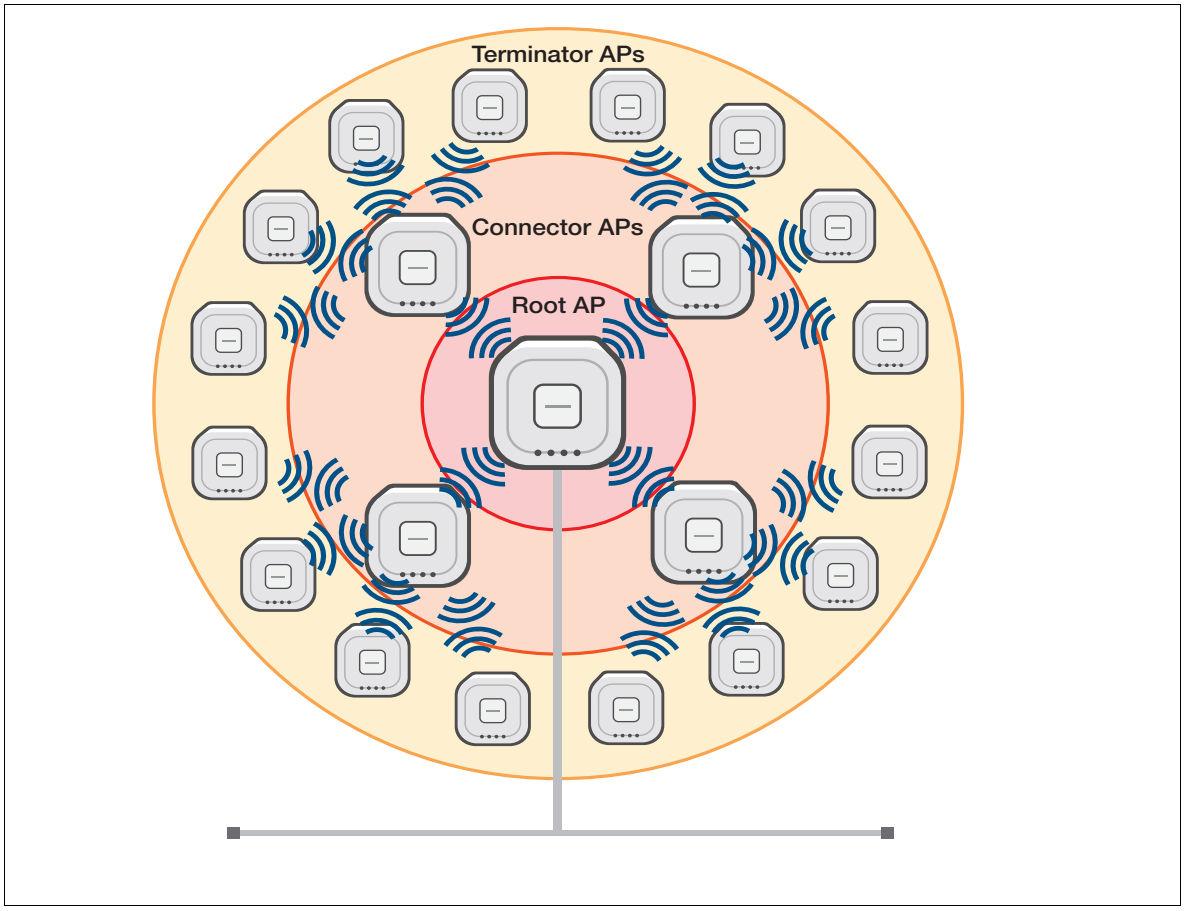
- are located on the edge of the AWC's multi-tier wireless connection.

Wireless topology overview

In an actual environment, the signal sensitivity also changes depending on the movement of people and objects between wireless APs, and if communication is poor, the satellite APs attempt to switch the backhaul connection destination.



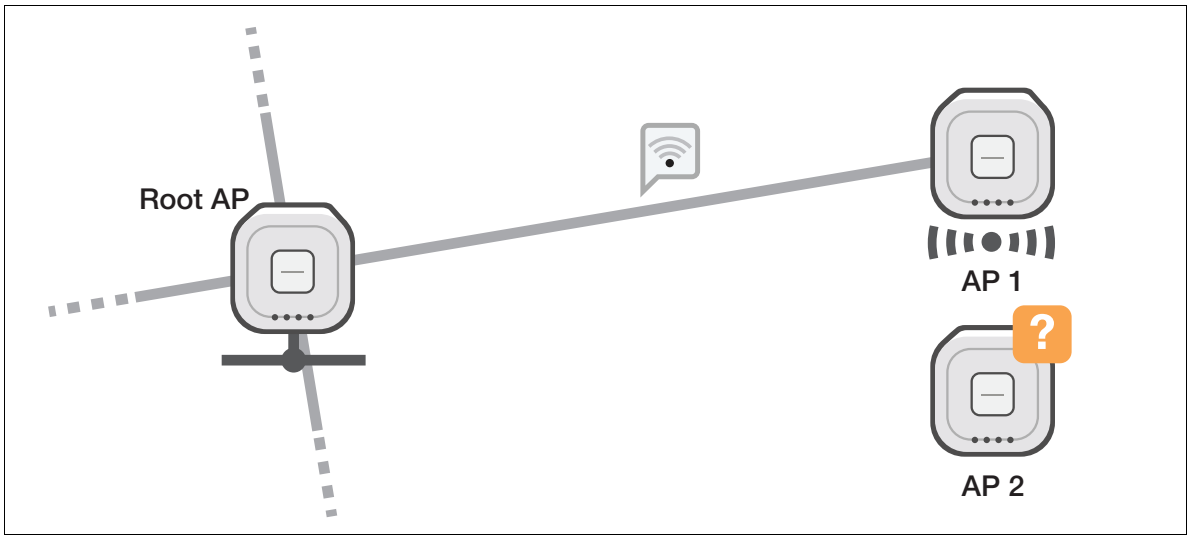
Up to four fronthaul wireless APs can be connected directly to each of the Root APs and Connector APs. In the most congested situation, up to 4 Connector APs and 16 Terminator APs can be connected to a single Root AP.



Wireless topology design suggestions

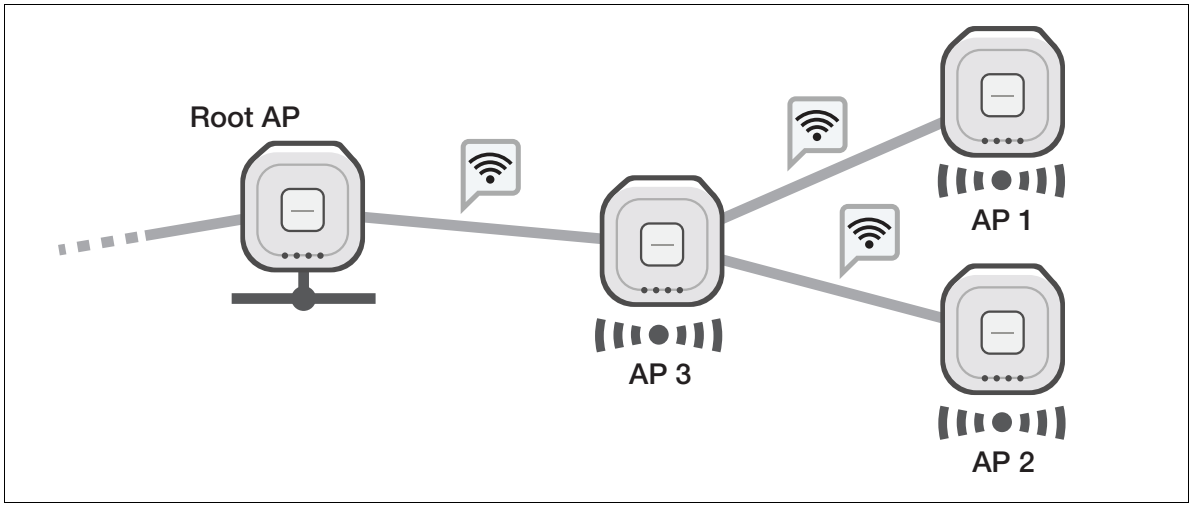
It is recommended that you design your wireless network with a margin for the number of Root APs to the number of Satellite APs. If there are not enough Root APs, the path may not be as optimal as expected, depending on the order in which the Satellite APs are installed.

For example, if the communication condition between the Root AP and the Satellite AP (hereinafter, AP1) is stable, but the radio wave is very weak, then AP1 is unable to be a Connector AP and accept a Smart Connect connection request from another wireless AP (hereinafter, AP2).

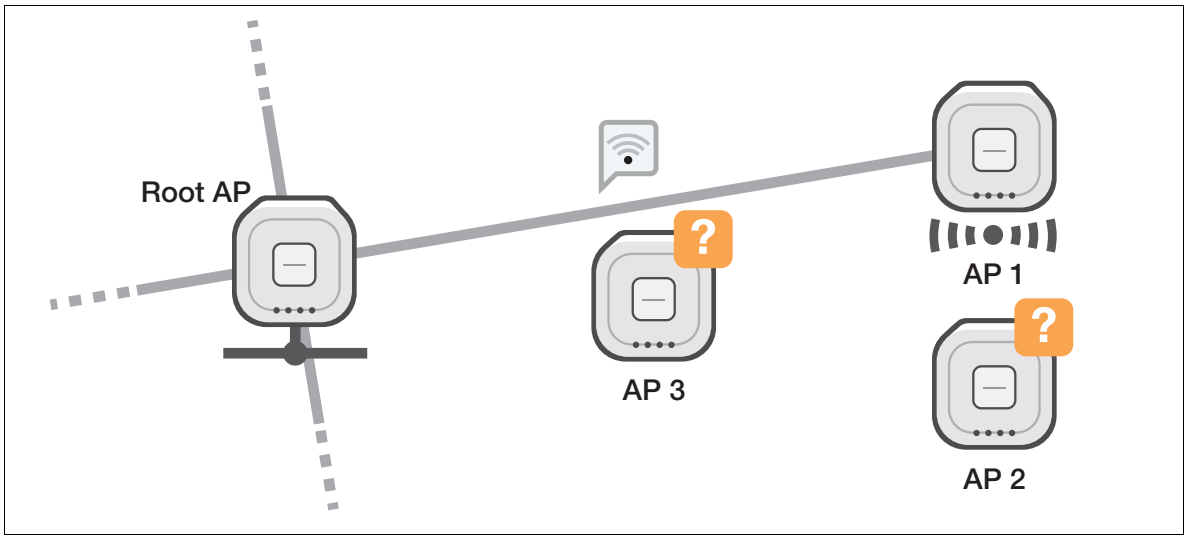


In this case, install a new wireless AP (AP3) between the Root AP and AP1.

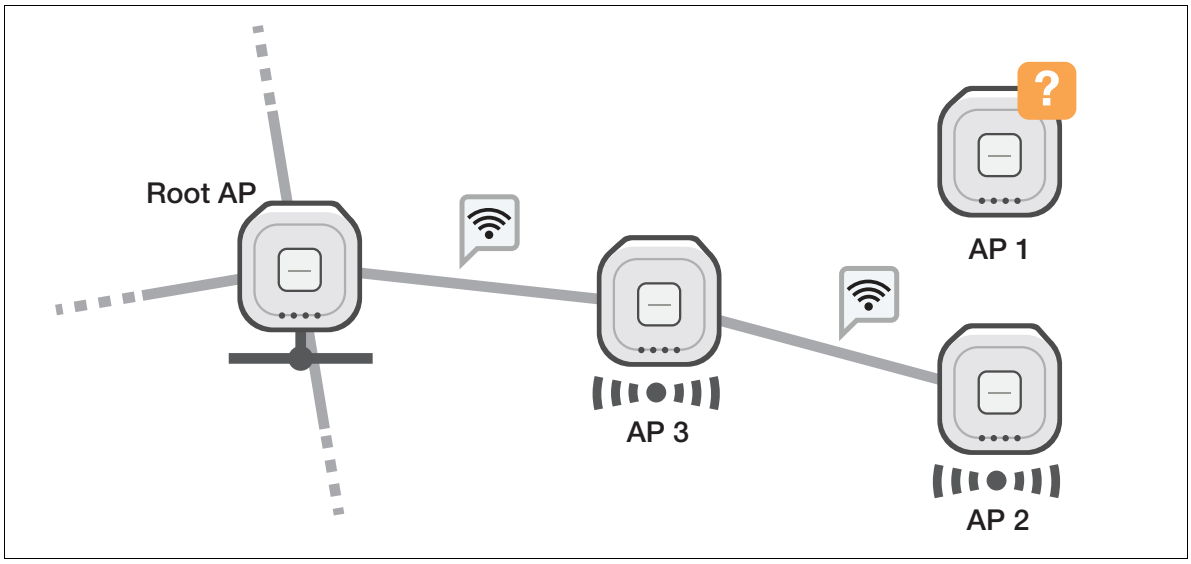
When the Root AP has enough margin to accept Satellites, first, the Root AP and AP3 establish the Smart Connect link with a strong radio wave. Next, by using path optimization, AP3 will bridge between AP1 and AP2 to the Root AP, as a Connector AP.



However, if the Root AP has connections with four Satellite APs already, and the Root AP and AP1 is still connected with weak but stable radio, AP3 can not join the Smart Connect Network.



In this case, the weak radio connection between AP1 is stopped temporarily. This allows the Root AP to have AP3 joined under it. Performing as a connector AP, AP3 can join AP2 to the Smart Connect Network, and also AP1 after it has been rebooted.



Note: When installing Satellite APs, pay attention to the number and distance of adjacent wireless APs. If a large number of Satellite APs are arranged so that the distance between wireless APs becomes too short, the throughput of the entire Smart Connect network may be significantly reduced.

AWC-SC configured VAPs

AWC-SC uses two VAPs as an alternative to wired networks between wireless APs.

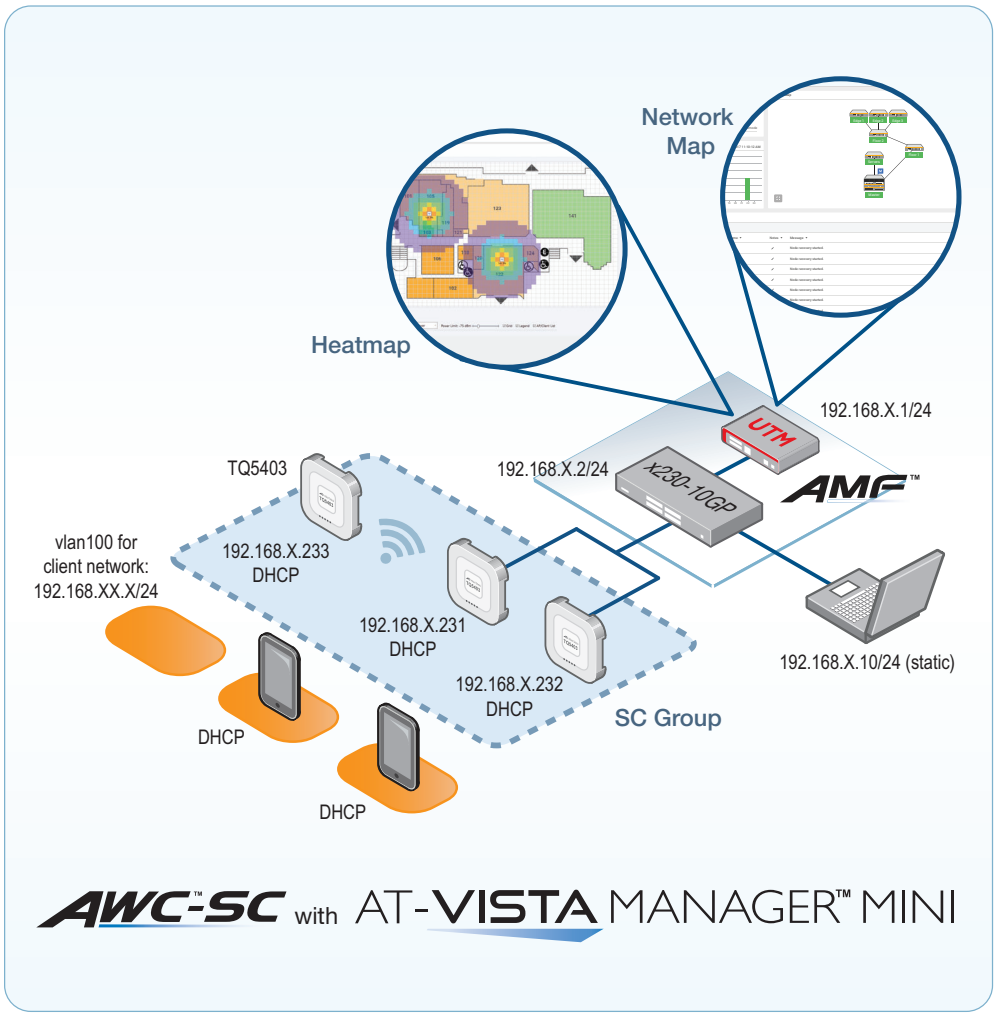
- **SC management VAP**
  - A VAP used to communicate between wireless APs in a wireless network established with AWC-SC.
  - Operates by overwriting VAP1 of AP Profile in the radio band selected as ‘Frequency’ of SC Profile.
  - SSID can be set arbitrarily, but will not be broadcast. The encryption method is fixed to ‘WPA2 Personal’, and the security key (WPA2-PSK) can be set arbitrarily.
- **SC provisioning VAP**
  - A VAP that allows factory default APs to find a Root AP and join to the Smart Connect Network.
  - Operates by overwriting VAP2 of AP Profile in the radio band selected as ‘Frequency’ of SC Profile.
  - SSID is fixed to ‘sc-initial-provisioning’ and will not be broadcast.
  - The encryption method is fixed to ‘WPA2 Personal’. The Security Key (WPA2-PSK) is hidden and can not be changed.

Note: In the radio band used by AWC-SC, the other VAPs will be disabled automatically

Configuring AWC Smart Connect

Once the initial wireless configuration is complete, when you plug your AP into the AWC-SC network:

- The AP will find the nearest AWC-SC Root or Connector AP and try to connect.
- The AWC-SC Root or Connector AP will ask the Centralised Wireless Manager (CWM) whether to allow the AP join the topology.
- If the AP is valid, the CWM will distribute a configuration for the AP and allow it to join the topology.



Basic setup steps

Here are the basic steps to configure Smart Connect:

- Pre-configuration
- Create a Smart Connect profile
- Create an AP profile to use with Smart Connect
- Add APs to the Smart Connect profile

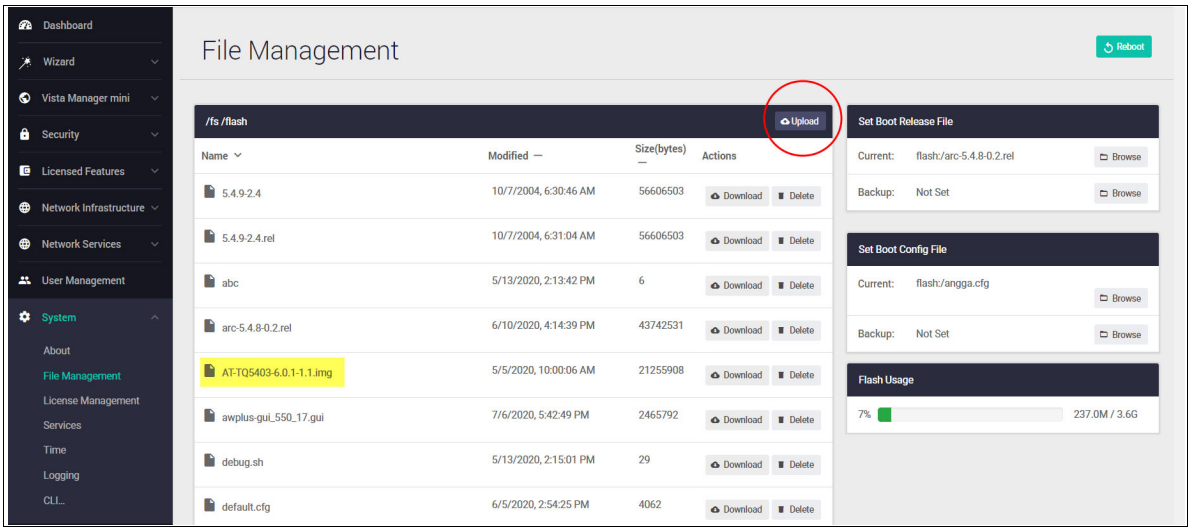
Pre-configuration

Obtain a valid AWC-SC license.

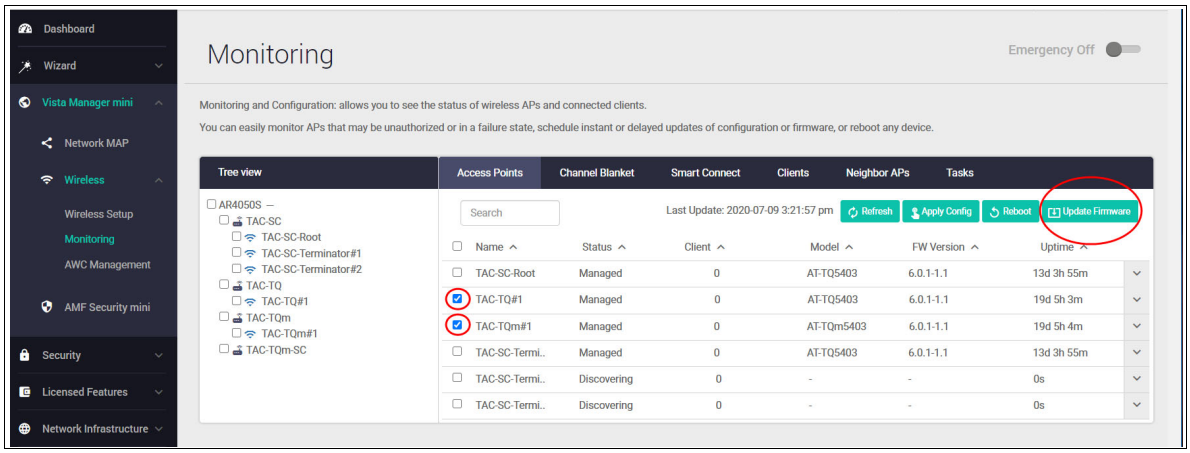
Upgrade the AP firmware

In the **System** > **File Management** window, upload the correct firmware on each of the APs. The version must be:

- TQ5403, TQ5403e, TQm5403: 6.0.1-0.1 or later
- TQ6602: 7.0.2-0.1 or later



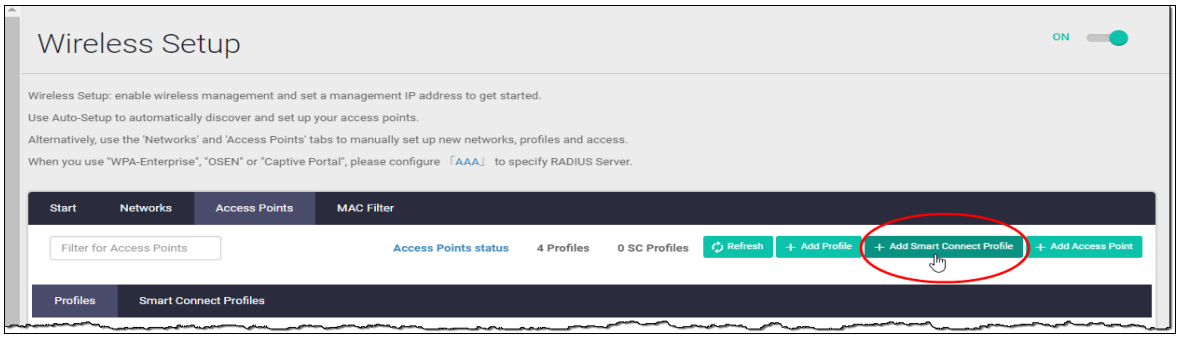
In the **Wireless** > **Monitoring** - **Access Points** tab, select the AP(s) and click **Update Firmware**:



Create a Smart Connect profile

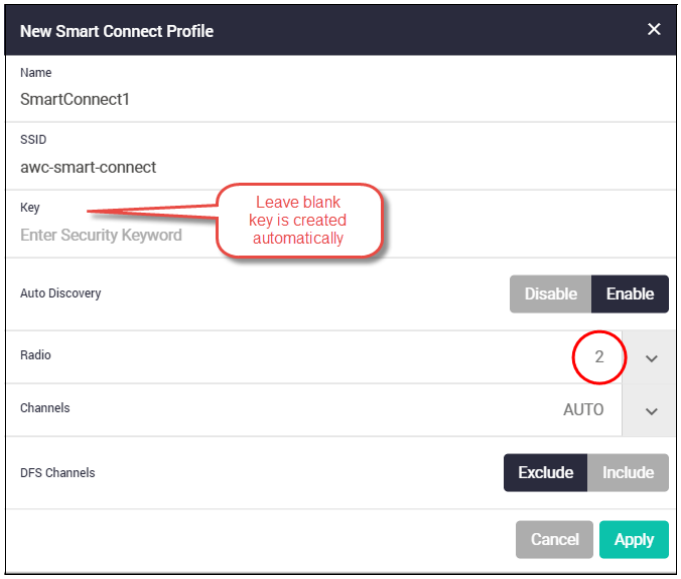
This section describes how to create an AWC-SC profile.

- From **Wireless** > **Wireless Setup** - **Access Points** tab, click **+Add Smart Connect Profile**:



In the **New Smart Connect Profile** window:

- Enter a **Name** for the Smart Connect profile. Max 100 characters (mandatory).
- Enter the **SSID** (descriptive name)
- Leave the **Key** ‘blank’
- Enable **Auto Discovery**
- Select the **Radio** you wish to configure (radio 2 in our example)
- Leave **Channels** at the default Auto

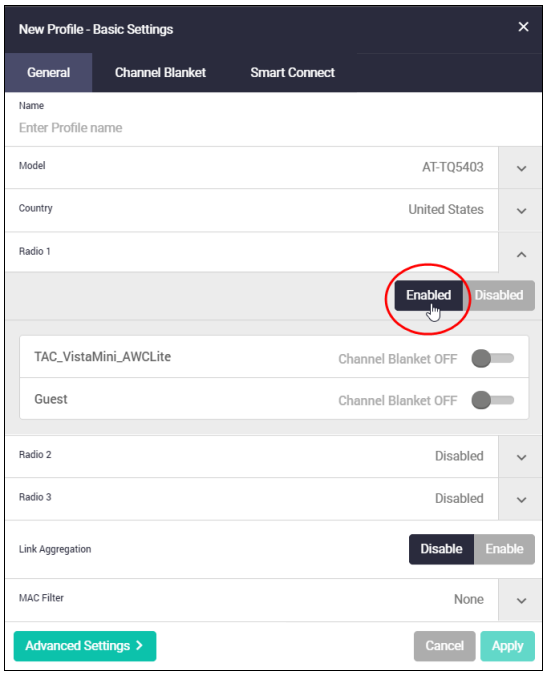

New Smart Connect Profile
Name
SmartConnect1
SSID
awc-smart-connect
Key
Enter Security Keyword
Leave blank key is created automatically
Auto Discovery
Disable
Enable
Radio
2
Channels
AUTO
DFS Channels
Exclude
Include
Cancel
Apply

- Click **Apply**

Create an AP profile to use with Smart Connect

Next, create an AP profile to use with Smart Connect.

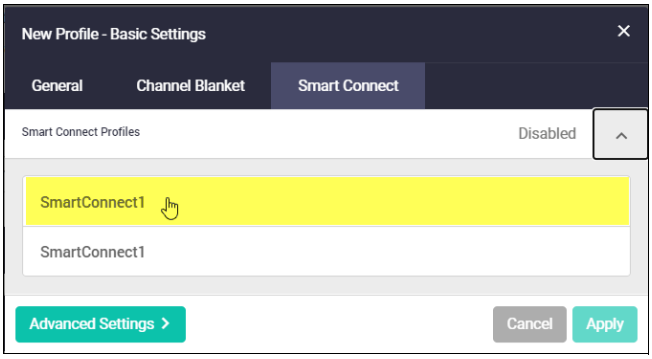
- Select **+Add Profile**



From here:

- Enter the profile **Name**
- Select the AP **Model** and **Country**
- Enable **Radios** as required.

Before applying the configuration, go to the **Smart Connect** tab, click the drop down box at right, and select the Smart Connect Profile that you just configured. In this example it would be 'SmartConnect1', as described in "Create a Smart Connect profile" on page 42.



- Click **Apply**.

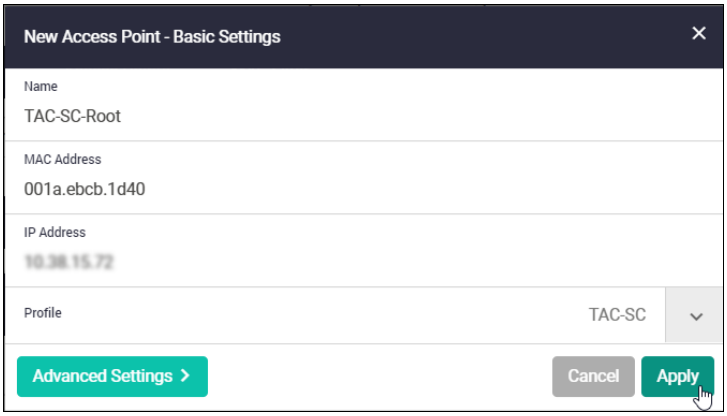
We have now created a SC Profile and a new AP profile with Smart Connect attached.

Configure the Root and Satellite APs

Before you configure these APs, configure your DHCP server with a static binding for the MAC address of the Root and Satellite APs.

For the Root and Satellite APs, repeat the following steps:

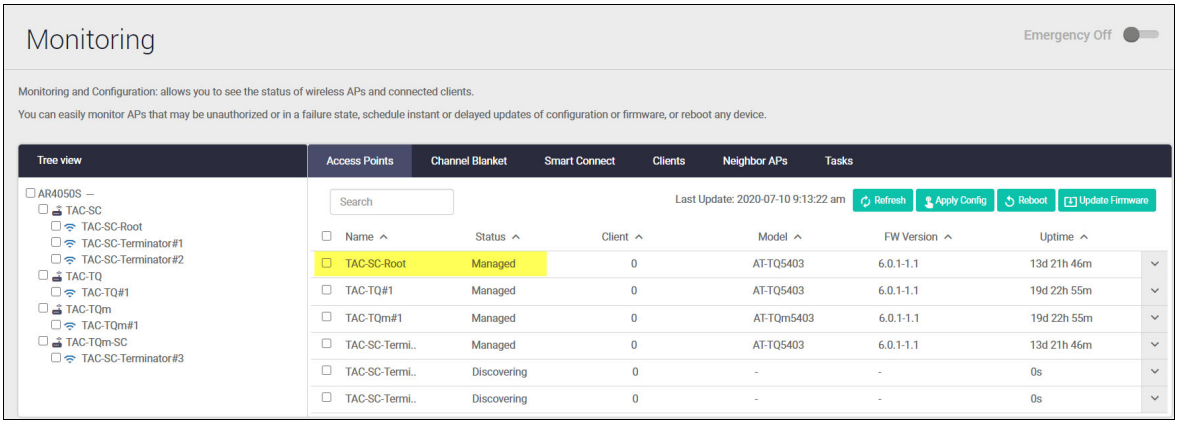
- Select **+Add Access Point**.
- Enter a **Name**, e.g. for the Root, 'TAC-SC-Root' and for the Terminator(s), 'TAC-SC-Terminator#1'
- Enter the **MAC** and **IP Address** for each AP you configure.
- Select the **Profile** containing the Smart Connect settings.
- Click **Apply**.



Connect Satellite APs to the Root AP

Use the **Monitoring** page **Access Points** tab to see if the Root AP is in the **Managed** state. You may need to refresh the Monitoring page to see this status change, sometimes it can take a few minutes to update any new configuration.

Once the Root AP is in the **Managed** state, then turn on the Satellite AP(s).

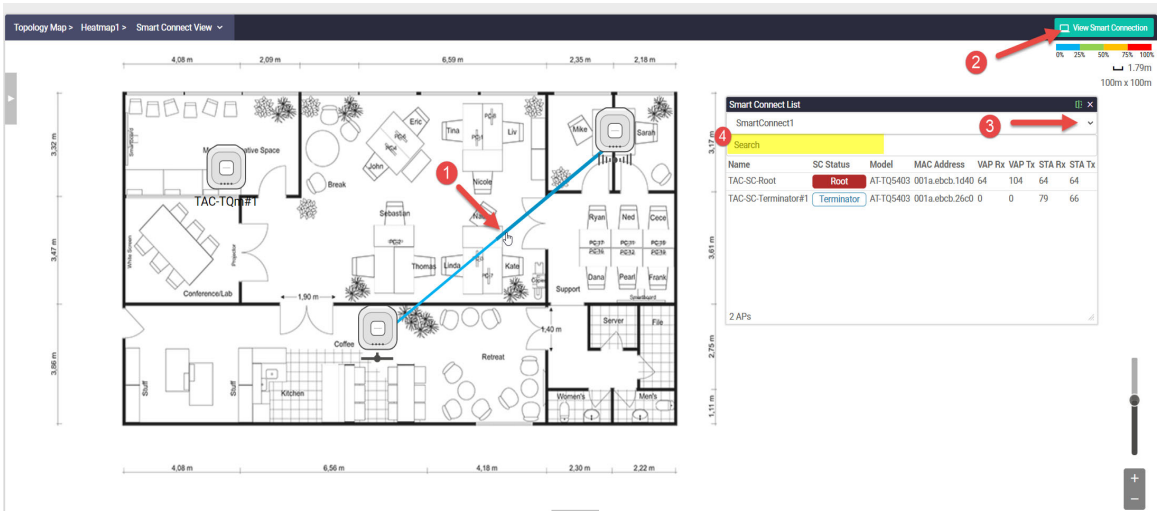


View the Smart Connect links

From the **Topology** > **Heatmap**, select **Smart Connect View** to see the Smart Connect links.

To see more details on the Smart Connect links, click the:

1. blue connection link to open the **Smart Connection List** window.
2. green **View Smart Connection** button
3. drop down list to select a Smart Connect Profile.
4. ‘Search’ window to locate a specific Smart Connect Profile.



Introduction to Captive Portal

Captive Portal is a mechanism to let wireless clients authenticate themselves before they are granted Wi-Fi access or external web access.

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 APs monitor traffic from wireless clients and 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:

- **External 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. You will need to store the username and password on a RADIUS server and use AlliedWare Plus to specify the RADIUS server.
- **Click-through** - this method only asks users 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 users 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 through the AlliedWare Plus CLI. See the RADIUS Feature Overview and Configuration Guide.

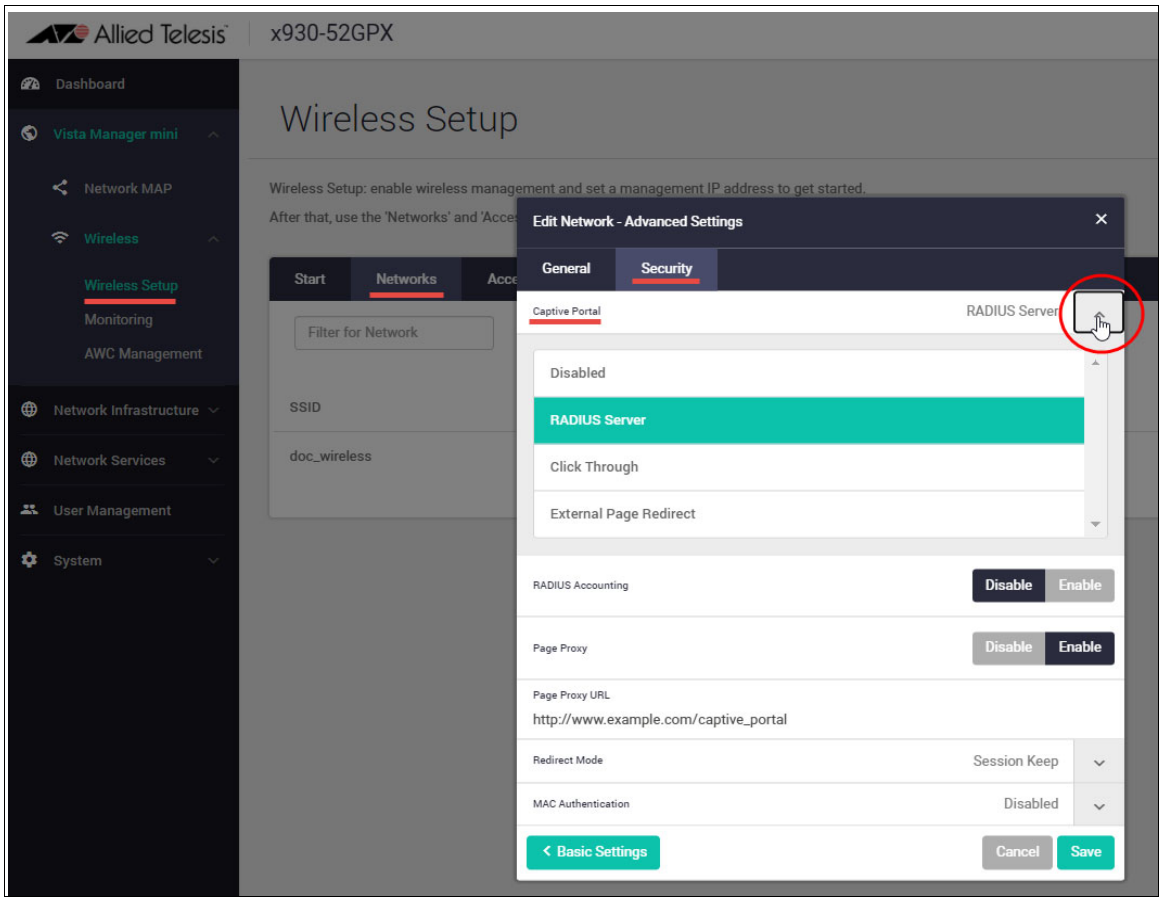
1. Select **Wireless** > **Wireless Setup** > **Networks**

   Either create a new network by clicking **+ Add Network** or **edit** an existing network. For this example we will edit an existing network (doc_wireless).

2. Click **Advanced Settings**.

3. Select the **Security** tab.

4. Select the **Captive Portal** type: RADIUS Server, Click Through, or External Page Redirect, and then complete the configuration fields provided.



The configuration fields are described in the table below.

Table 2: The configuration fields vary with each Captive Portal type

CONFIGURATION FIELD/TYPE	DESCRIPTION
External Page URL ■ For type: External Page Redirect	Specify the URL of the third-party Captive Portal vendor's web page.
RADIUS Server ■ For type: External Page Redirect	Select the RADIUS server setting.
RADIUS Accounting ■ For type: RADIUS Server, External Page Redirect	Enable or Disable Enable this option to enable accounting on the Captive Portal with an external RADIUS server. RADIUS Accounting collects a variety of information that can be used for accounting and for reporting on network activity. ■ You must set the RADIUS server setting in advance. ■ Captive Portal RADIUS accounting uses the same RADIUS server as Captive Portal RADIUS authentication.
Page Proxy ■ For type: RADIUS Server, Click Through ■ This field may be present for External Page Redirect, but has no effect.	Specify whether to use an external authentication page or not. Enable: Shows the external portal page. Disable: Shows the authentication page that is embedded in the APs. For information on configuring the Page Proxy, See "Configuring the Page Proxy" on page 50.
Page Proxy URL ■ For type: RADIUS Server, Click Through ■ This field may be present for External Page Redirect, but has no effect.	If you set a Page Proxy URL: ■ Specify the base URL of the external web authentication page. ■ The HTML filename of the external authentication page must be "radius_login.html". ■ The AP's proxy will get the page from "Page Proxy URL/ radius_login.html" and send it back to clients.
Redirect Mode ■ For type: RADIUS Server, External Page Redirect	Specify what page the user will be shown after passing web authentication. Session Keep: Shows the original URL page that was entered in the client's browser before web authentication. For example, if the user is trying to access the airport URL from the airport Wi-Fi network, the browser will redirected to the RADIUS user URL and after it is authenticated, it will be redirected back to airport URL page. Fixed: Always shows a fixed URL that you specify. Disable: Does not redirect the browser after successful web authentication.
MAC Authentication ■ For type: RADIUS Server, Click Through, External Page Redirect	Specify whether to use MAC Address Authentication on the VAP, so that the Captive Portal only allows approved devices to access the guest network. RADIUS: The APs will query the RADIUS server. MAC Filter: Filtering is performed using the MAC address filter list which is managed via the **Wireless Setup** > **MAC Filter** tab. AMF Application Proxy: Filtering is performed using the AMF Application Proxy managed via the **Wireless Setup** > **Start** tab. Disabled: No MAC address authentication is performed.
Walled Garden ■ For type: RADIUS Server, Click Through, External Page Redirect	Specify the IP, network, or FQDN address of the walled garden. A walled garden limits users to accessing only a selection of web pages. A common example could be a hotel environment where unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

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 filename of the external authentication failure page must be ‘radius_login_fail.html’. For example, if 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_fail.html’ to connecting 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.

Introduction to Passpoint

You can enable Passpoint on your wireless networks from GUI version 2.7.0 and AlliedWare Plus software version 5.5.0-2.2 or later. Passpoint is available on Access Points: TQ5403, TQm5403, TQ5403e.

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.

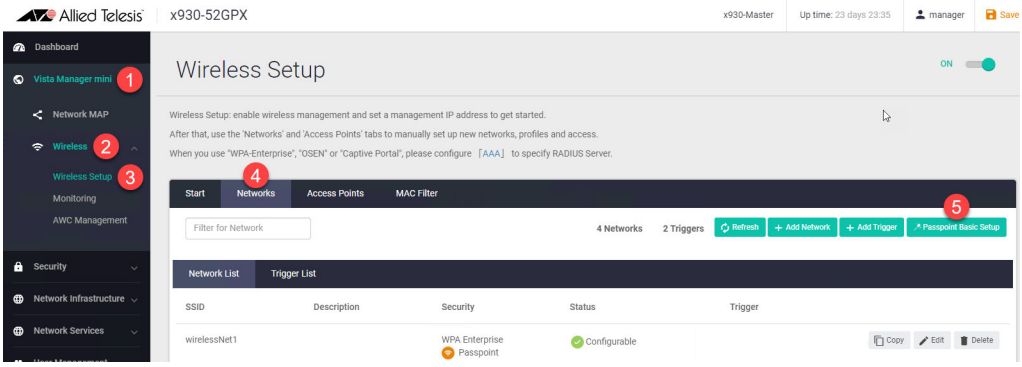
Passpoint improves the mobile user experience by offering:

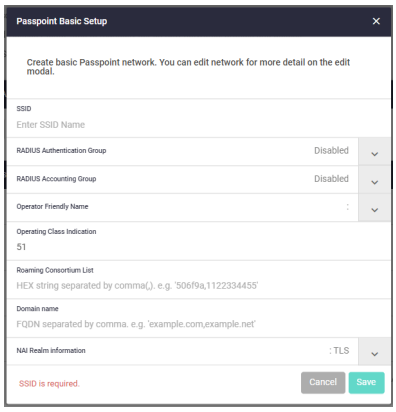
- Automatic network discovery and selection
- Simplified online sign-up and instant account provisioning
- Seamless network access and cellular-like roaming between hotspots
- Enhanced security

Configuring Passpoint: Basic Configuration

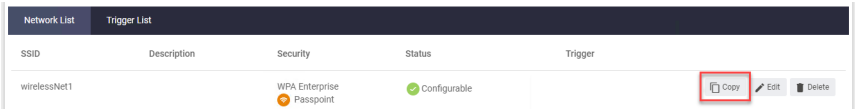
From Device GUI 2.12.0 onwards, you can use the **Passpoint Basic Setup** option to create a Passpoint network quickly and easily. To do this:

- Select **Vista Manager mini** > **Wireless** > **Wireless Setup** > **Networks.**
- Click the **Passpoint Basic Setup** button
- Fill out the required fields in the dialog box.





You can also copy an existing network. To do this, click on the Copy button on that network's row:



Configuring Passpoint: Customized Configuration

This section describes how to enable and customize Passpoint on:

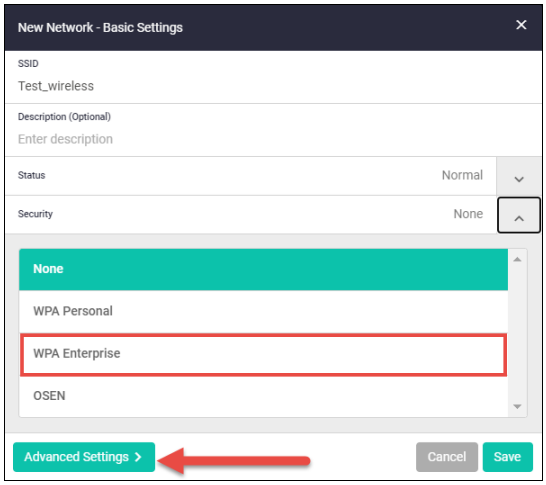
- a new wireless network
- an existing wireless network

Enabling Passpoint on a new wireless network

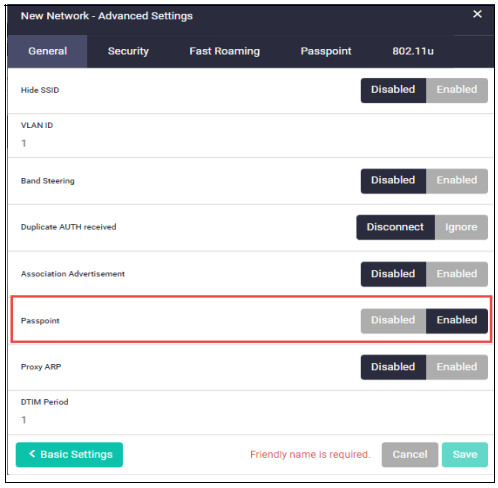
To create a new wireless network and enable Passpoint on it:

- Select **Vista Manager mini** > **Wireless** > **Wireless Setup** > **Networks.**
- Click **+ Add Network**.
- The **Network - Basic Settings** window opens. From here you can:

1. Enter the **SSID**, **Description**, **Status**, and **Security** details.
2. For **Security** type, select **WPA Enterprise**.



3. Go to the **Advanced settings**.
4. Select the **General** tab and **Enable** Passpoint.



Configuring Passpoint

5. In the **Advanced Settings**, select the **Passpoint** tab.
6. Complete the **Passpoint** configuration fields: Table 3 below describes these fields.

Note: From GUI version 2.11.0 onwards, you can use Passpoint **OSU** options to register a mobile device with a service provider and choose a plan to gain network access. When you sign up, your device will send you user credentials to connect to the network.

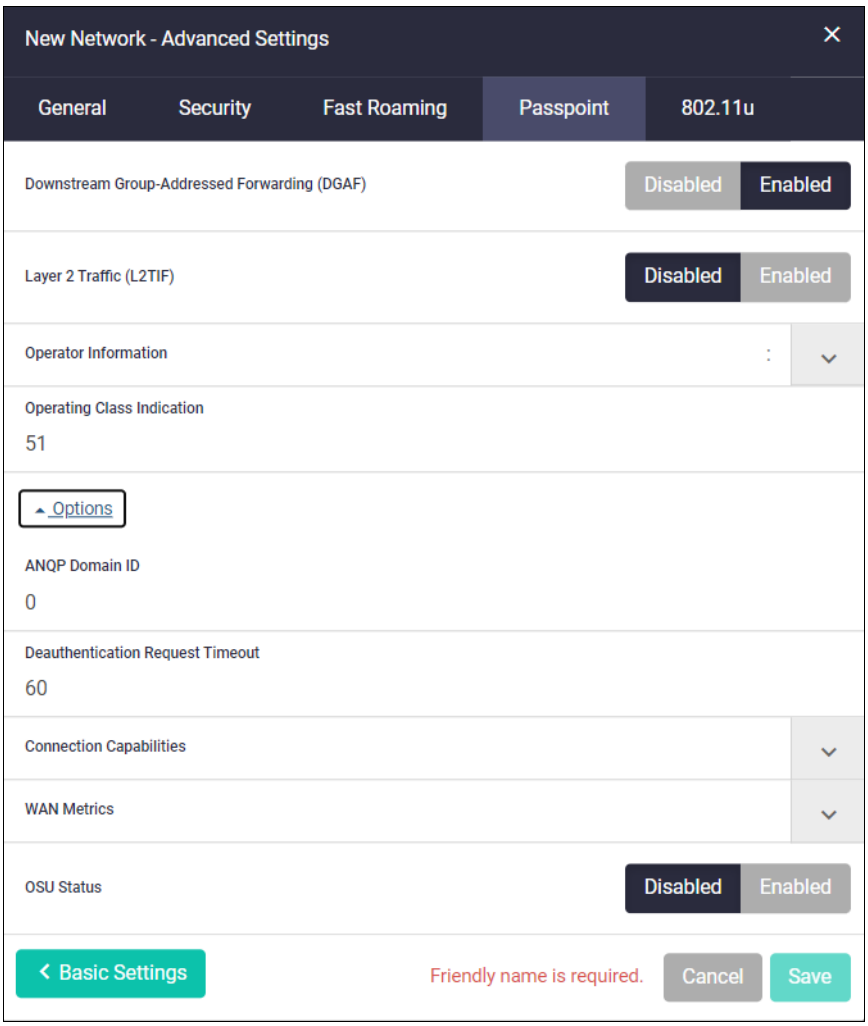


Table 3: Passpoint configuration fields

FIELD	DESCRIPTION
Downstream Group-Address Forwarding (DGAF)	Select 'Enable' to disable Downstream Group-Addressed Forwarding, change Disable Downtown Group-Addressed Forwarding (DGAF).
L2 Traffic Inspection and Filtering (L2TIF)	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 Information	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

Table 3: Passpoint configuration fields (continued)

<table>
<tr><th>FIELD</th><th>DESCRIPTION</th></tr>
<tr><td>Operating Class Indication</td><td>The HEX number of the radio information. For example, ‘517376’ means using 1-13ch and 36-64ch(20MHz).
The default is ‘51’ (2.4GHz) 1-13channels
See Table E-4 of IEEE Std 802.11-2020 Annex E for more detail.

<table><tr><th>Hex</th><th>Channels</th></tr><tr><td>51</td><td>(2.4GHz) 1-13ch</td></tr><tr><td>73</td><td>(5GHz) 36,40,44,48ch</td></tr><tr><td>76</td><td>(5GHz) 52,56,60,64ch</td></tr><tr><td>79</td><td>(5GHz) 100,104,108,112,116,120,124,128,132,136,140,144ch</td></tr><tr><td>7D</td><td>(5GHz) 149,153,157,161,165,169,173ch</td></tr></table></td></tr>
<tr><td>ANQP Domain ID</td><td>Configures the Hotspot 2.0 ANQP (Access Network Query Protocol) domain identifier.
Optional - If you don’t configure this, the default ‘0’ is set.</td></tr>
<tr><td>Deauthentication Request Timeout</td><td>Optional - If you don’t configure this, the default ‘60’ is set.</td></tr>
<tr><td>Connection Capabilities</td><td>Optional, and includes the following fields:
■ IP Protocol Number
■ Port Number
■ Port Status</td></tr>
<tr><td>WAN Metrics</td><td>Optional, and includes the following fields:
■ At Capacity
■ Symmetric Link
■ Link Status
■ Uplink Load
■ Downlink Load
■ Uplink Speed
■ Downlink Speed
■ Load Measure Duration</td></tr>
<tr><td>OSU Status</td><td>Optional - Enable/Disable
Disabled by default</td></tr>
<tr><td>OSU SSID</td><td>Configures the SSID that wireless clients will use for OSU.</td></tr>
<tr><td>OSU Providers Server URI</td><td>Uniform Resource Identifier (URI) of the OSU server, for example:
osu-server.example.com</td></tr>
<tr><td>OSU Providers NAI</td><td>Optional - The OSU Providers NAI (Network Access Identifier)
This is in an email address format, for example:
fred.smith@example.com</td></tr>
<tr><td>OSU Providers Method</td><td>Select one of the OSU provider provisioning methods:
■ OMA-DM: Open Mobile Alliance (OMA) Device Management (DM)
■ SOAP-XML SSP: Simple Object Access Protocol/Extensible Markup Language</td></tr>
</table>

Table 3: Passpoint configuration fields (continued)

FIELD	DESCRIPTION
OSU Providers Friendly Name	Optional - User-friendly name of a service provider in the OSU providers list. Enter a Name - e.g. Allied Telesis Inc. Enter a language code - e.g. "jpn", "eng"
OSU Providers Service Description	Optional - The description for the OSU service provider. Enter a Name - e.g. Allied Telesis Inc. Enter a language code - e.g. "jpn", "eng"
OSU Icons	Optional - If the user elects to sign up, they will be presented with a list of the available Online Signup providers. The list is typically displayed as an icon, title, and description for each operator. The icon is actually embedded within the certificate issued to the OSU server, thus ensuring that clients don't connect to "rogue" provisioning systems. Select a file (.png) Enter a language code - e.g. "jpn", "eng"

Configuring 802-11u

7. Select the **802.11u** tab.
8. Complete the 802.11u configuration fields and click **Save**.

Table 4 on page 58 below describes these configuration fields.

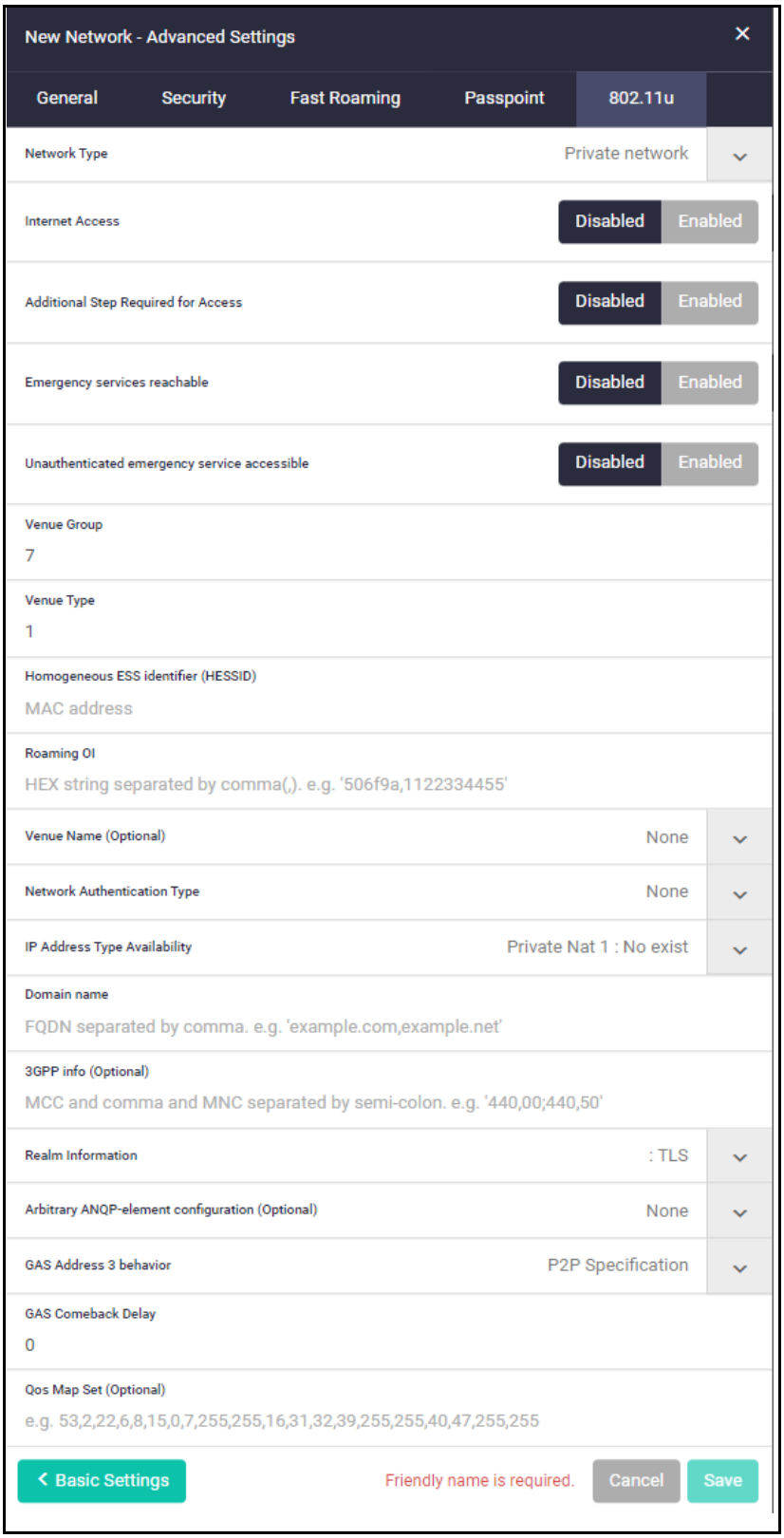

New Network - Advanced Settings
General
Security
Fast Roaming
Passpoint
802.11u
Network Type
Private network
Internet Access
Disabled
Enabled
Additional Step Required for Access
Disabled
Enabled
Emergency services reachable
Disabled
Enabled
Unauthenticated emergency service accessible
Disabled
Enabled
Venue Group
7
Venue Type
1
Homogeneous ESS identifier (HESSID)
MAC address
Roaming OI
HEX string separated by comma(,). e.g. '506f9a,1122334455'
Venue Name (Optional)
None
Network Authentication Type
None
IP Address Type Availability
Private Nat 1 : No exist
Domain name
FQDN separated by comma. e.g. 'example.com,example.net'
3GPP info (Optional)
MCC and comma and MNC separated by semi-colon. e.g. '440,00;440,50'
Realm Information
: TLS
Arbitrary ANQP-element configuration (Optional)
None
GAS Address 3 behavior
P2P Specification
GAS Comeback Delay
0
Qos Map Set (Optional)
e.g. 53,2,22,6,8,15,0,7,255,255,16,31,32,39,255,255,40,47,255,255
Basic Settings
Friendly name is required.
Cancel
Save

Table 4: 802.11u configuration fields

FIELD	DESCRIPTION
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.
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.
Venue Group	The general class of venue, such as: ■ Assembly ■ Business ■ Educational ■ Industrial ■ Residential ■ Vehicular ■ Outdoor
Venue Type	The specific type of venue within each group. For example venue types in the 'Assembly' group include: ■ Arena ■ Stadium ■ Place of Worship ■ Library ■ Restaurant

Table 4: 802.11u configuration fields (continued)

FIELD	DESCRIPTION
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.
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
Roaming OI	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'
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: { } | \ ^ [ ]
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
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'
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

Table 4: 802.11u configuration fields (continued)

FIELD	DESCRIPTION
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 EAP method is the method that this NAI realm uses for authentication: ■ TLS ■ TTLS ■ SIM
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)

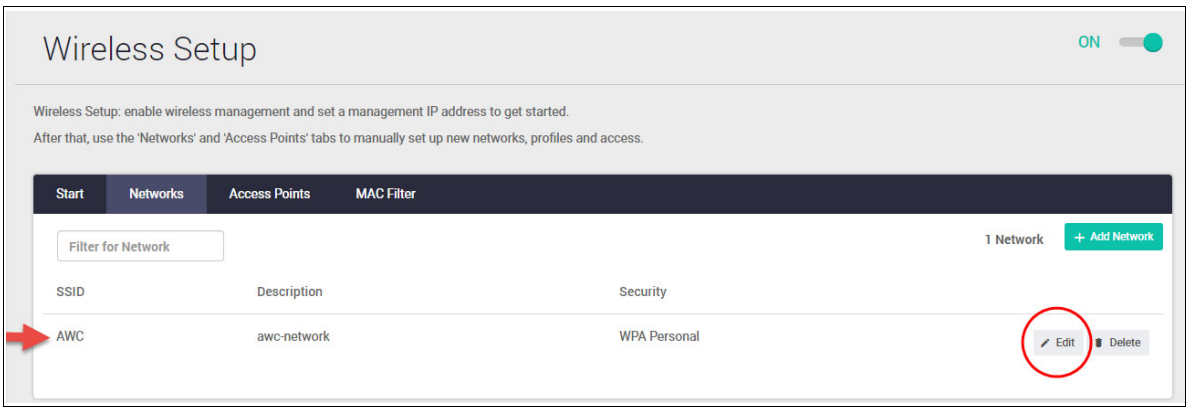
Table 4: 802.11u configuration fields (continued)

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)

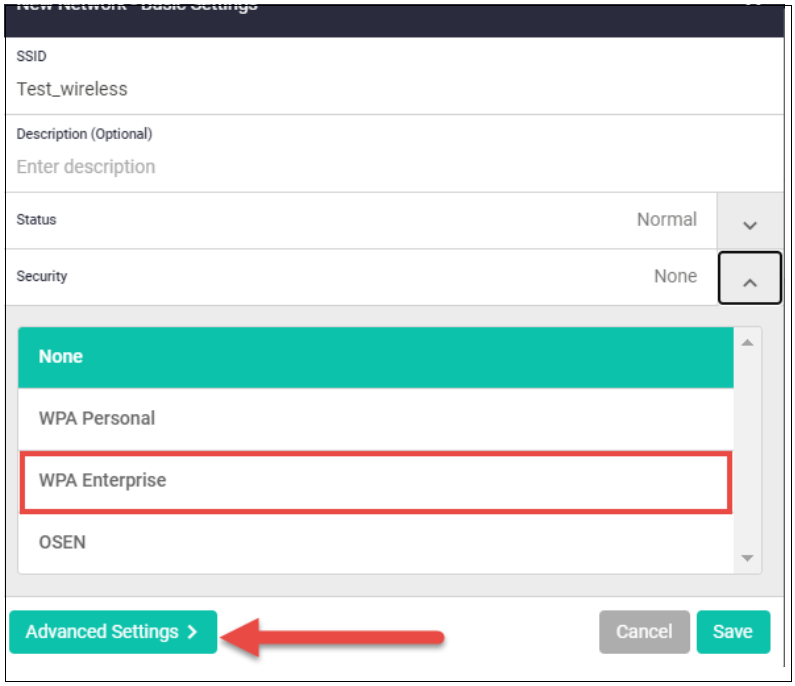
Enabling Passpoint on an existing wireless network

To enable Passpoint on an existing wireless network:

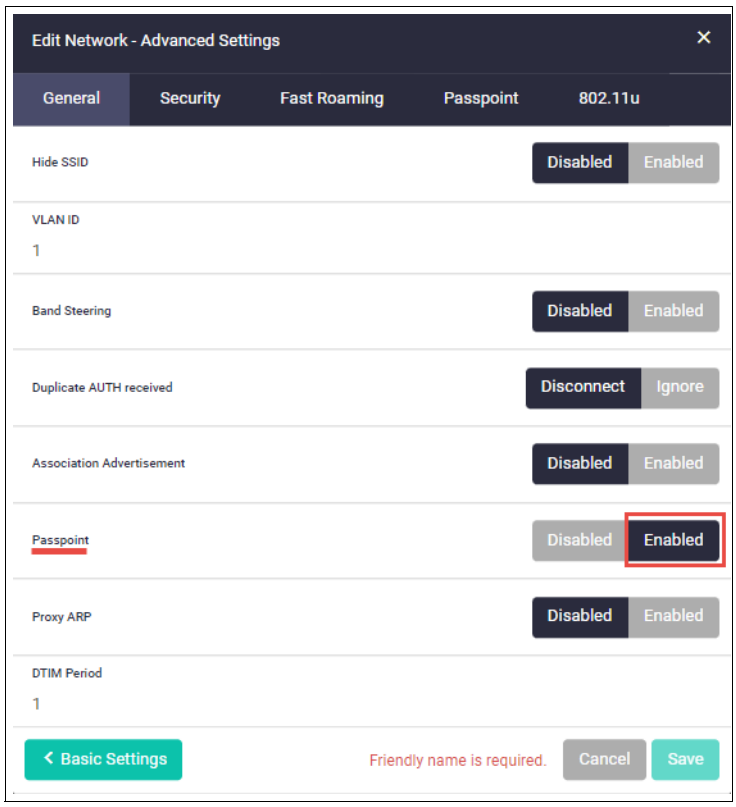
1. Select **Wireless** > **Wireless Setup** > **Networks**
2. Select a network and click **Edit**.



3. For **Security** type, select **WPA Enterprise**
4. Go to the Network's **Advanced settings**.



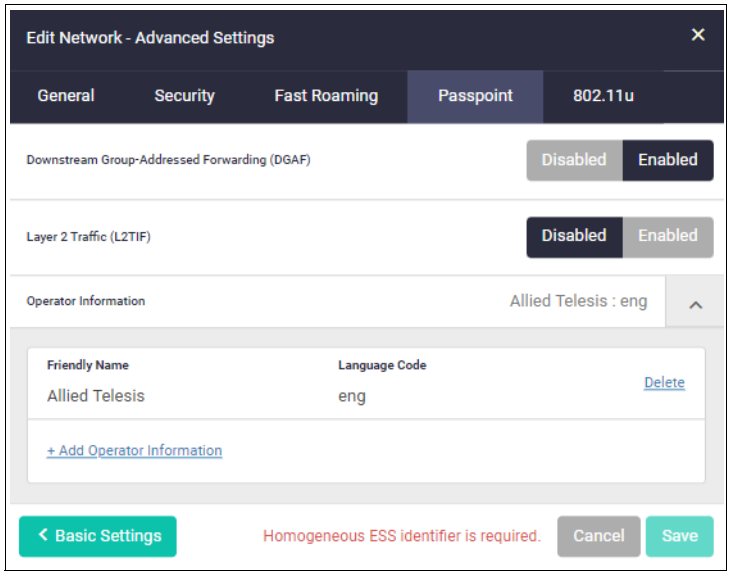
5. Select the **General** tab and **Enable** Passpoint.



Configuring Passpoint

6. Now select the **Passpoint** tab.

7. Complete the Passpoint configuration fields as shown in Table 3 on page 54.



8. Click **Save** to complete.

Emergency mode

From Device GUI 2.5.2 onwards, you can set one or more wireless networks to emergency mode. Emergency mode makes those wireless networks available to the public in an emergency, such as a natural disaster.

You can set up the emergency mode network or networks in advance — see “Set up a network for emergency mode” below. Then if there is an emergency, you just have to enable emergency mode globally. Wireless networks in emergency mode are only active when emergency mode is enabled.

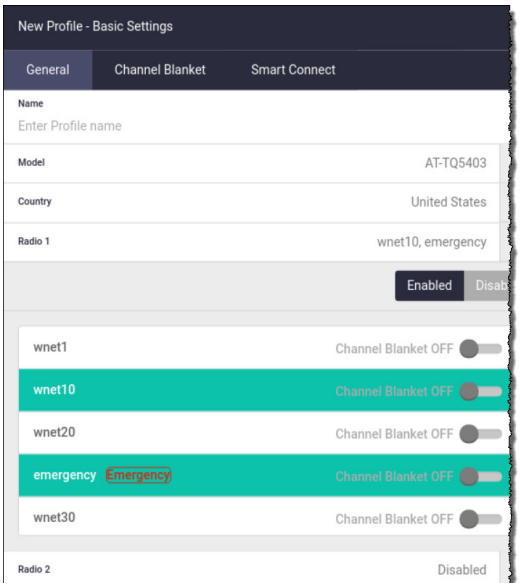
There are two ways to enable emergency mode globally:

- From version 2.5.2 onwards, you can use the Device GUI to enable emergency mode — see "Use the Device GUI to enable emergency mode" on page 65
- From version 2.12.0 onwards, you can insert a pre-prepared USB stick into the AlliedWare Plus device that is the wireless controller — see "Use a pre-prepared USB stick to enable emergency mode" on page 66. This makes it easier to enable emergency mode, because you don’t have to log into the Device GUI to do so.

Set up a network for emergency mode

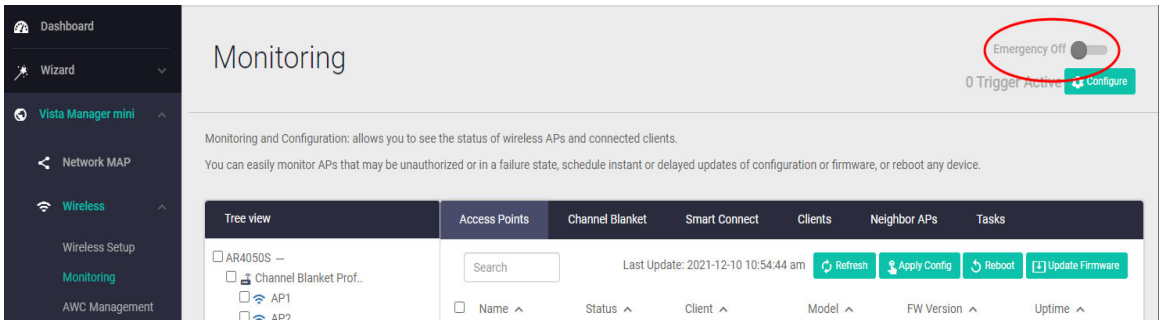
- Go to **Wireless** > **Wireless Setup** > **Networks > Basic Settings**
- Set the network **Status** to **Emergency**

- Go to **Wireless** > **Access Points** > **Profiles** > **General > Radio 1 (or 2 or 3)**
- Enable the Radio and select the Emergency network.
- Click **Apply**.

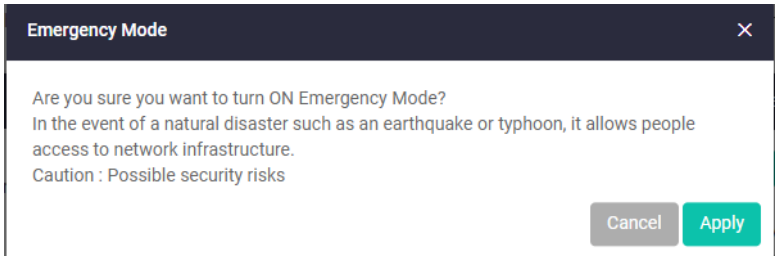


Use the Device GUI to enable emergency mode

- Go to **Wireless** > **Monitoring**
- Turn **Emergency** mode to **ON** - use the button at top right of window



- Click **Apply** to confirm.

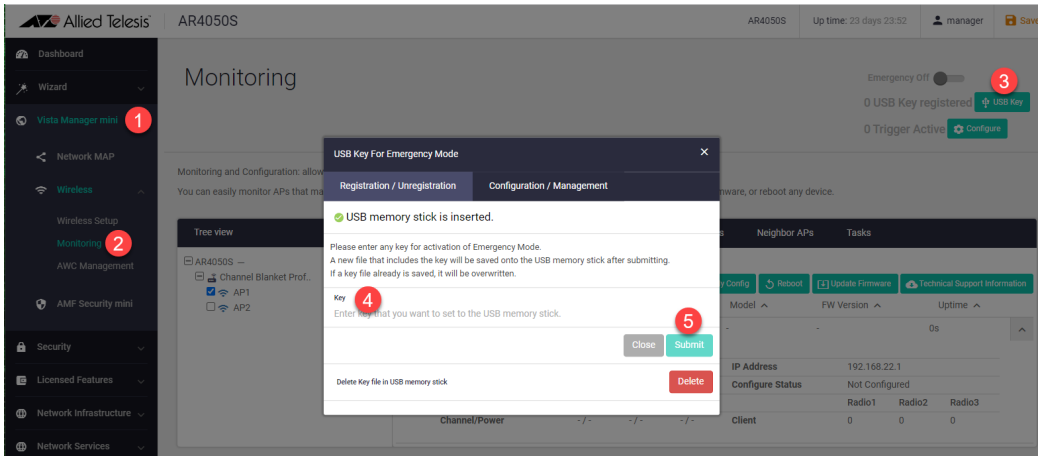


Use a pre-prepared USB stick to enable emergency mode

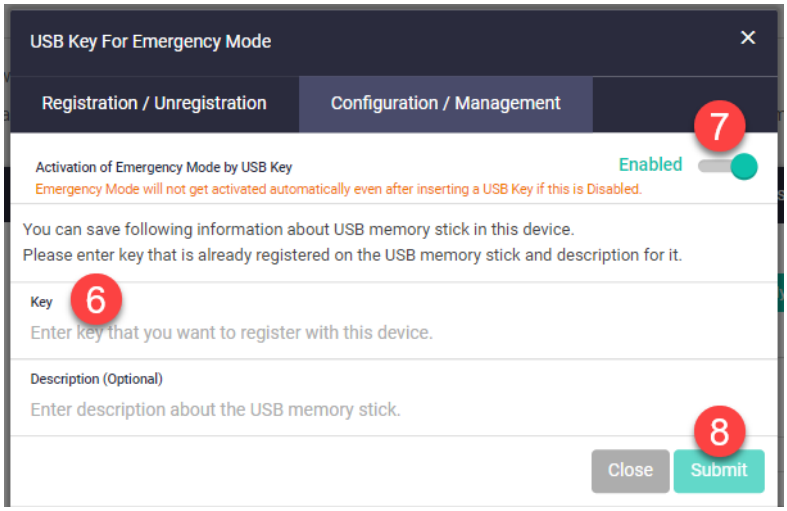
From version 2.12.0, the Device GUI lets you enable emergency mode by simply inserting a pre-prepared USB stick into the AlliedWare Plus device that is the wireless controller. This makes it easier to start emergency mode, because you don't have log into the Device GUI to do so.

To set this up:

- Insert an empty USB stick into the AlliedWare Plus device
- Go to **Wireless** > **Monitoring**
- Click on the **USB Key** button.
- On the **Registration/Unregistration** tab, enter a key and click **Submit**.



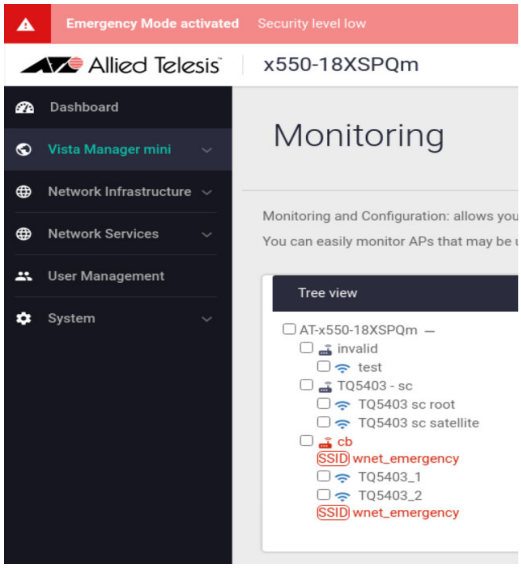
- On the **Configuration/Management** tab, set **Activation of Emergency Mode by USB Key** to enabled if it is disabled. Enter the key again, and a description of this USB stick, and click **Submit.**



- Remove the USB stick and keep it somewhere convenient.
- To put the network into Emergency Mode, just insert the USB stick into the AlliedWare Plus device. As long as the keys on the device and the stick match, emergency mode will automatically activate.

See whether emergency mode is enabled

- The device's port LEDs will blink to indicate it is in emergency mode.
- On **Wireless** > **Monitoring**, the top bar displays a warning of **Emergency mode activated Security level low**.
- The **Tree view** shows all the APs that are in an emergency network.



Wireless network trigger

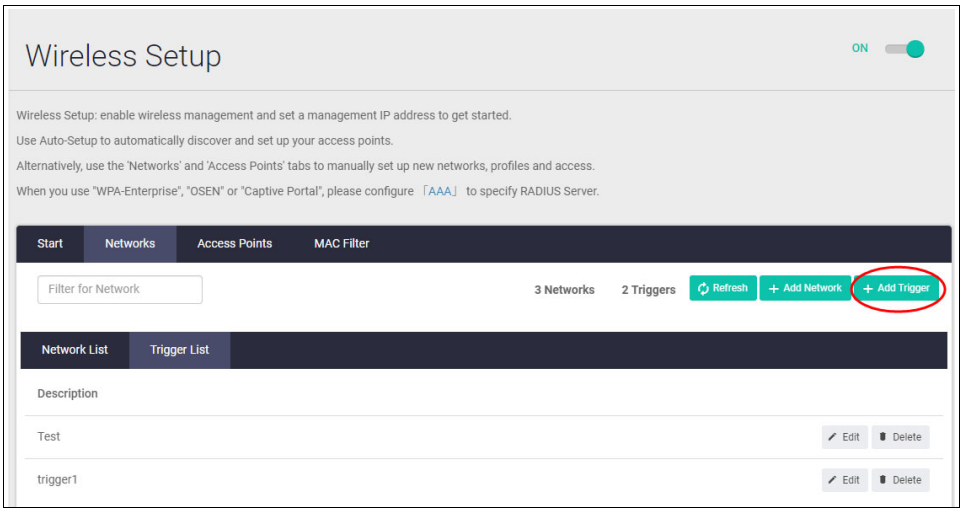
From Device GUI version 2.8.0 onwards, you can configure up to eight wireless network triggers on a VAP. Network triggers are used to enable/disable multiple VAPs at once.

To configure a wireless network trigger, follow these steps:

- Create trigger
- Set up the trigger for the network
- Assign network with trigger to VAP
- Activate the trigger

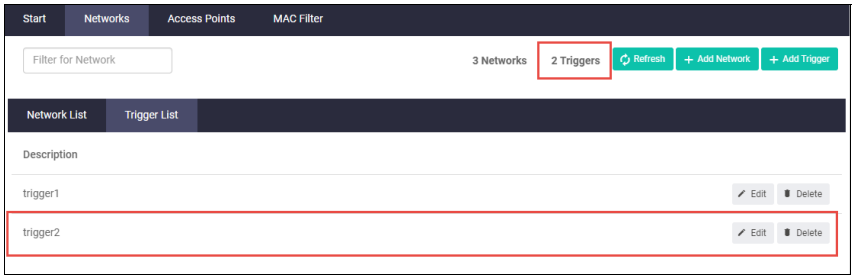
Create trigger

1. Select **Wireless** > **Wireless Setup** > **Networks**
2. Click **+Add trigger**.



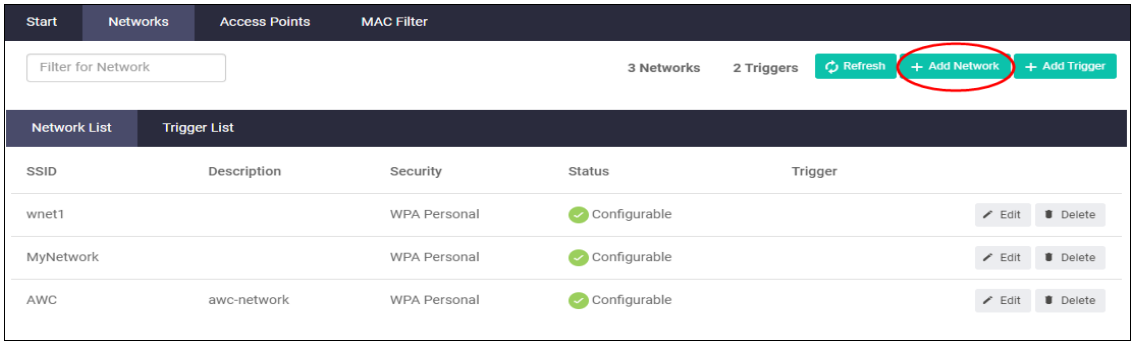
3. Enter a description and click **Save**.

4. The **Trigger List** is updated.



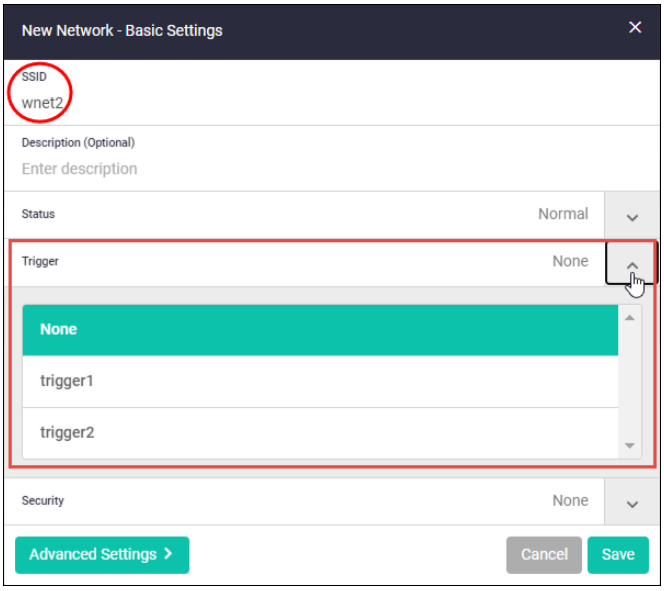
Set up the trigger for the network

1. Click **+ Add Network**.



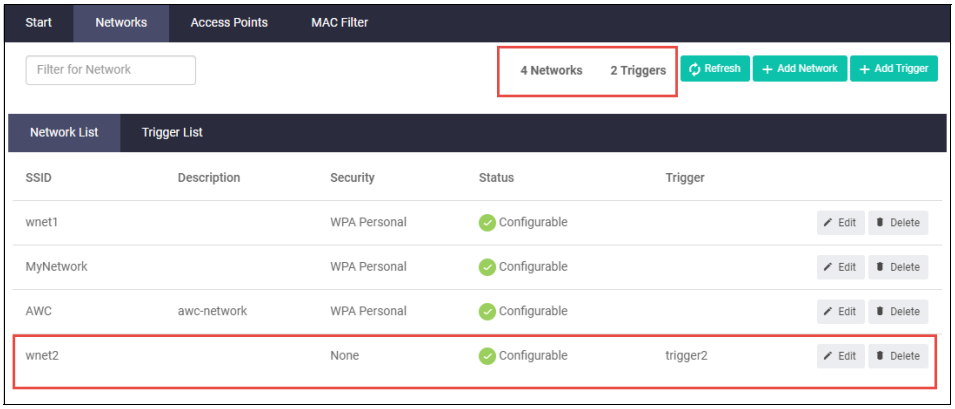
2. Enter the **SSID** and optional description.

3. Select the **Trigger**.



4. Click **Save**.

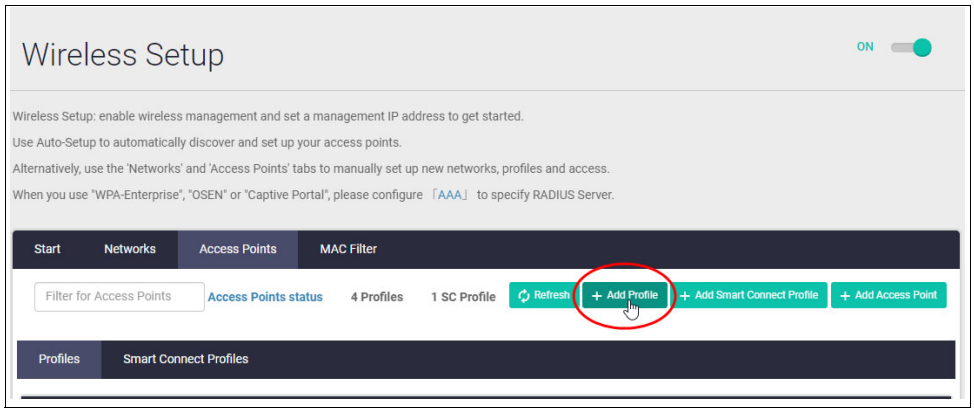
5. The **Network List** is updated.



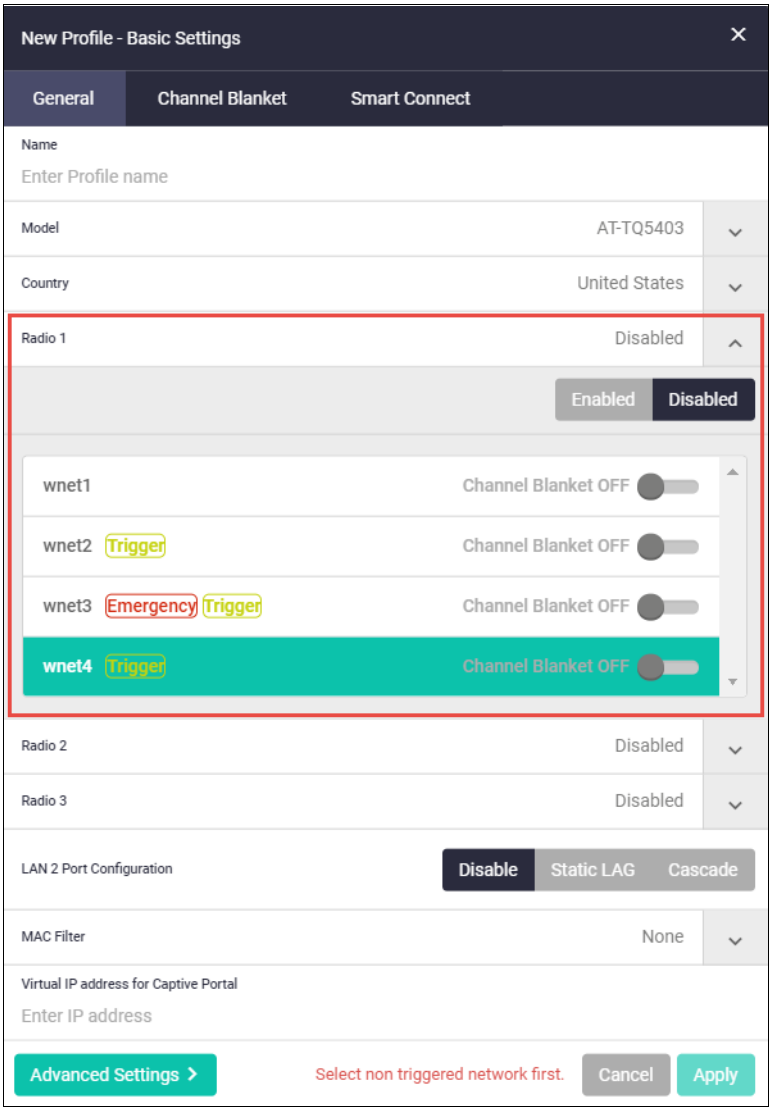
Assign network with trigger to VAP

1. Select **Wireless** > **Wireless Setup** > **Access Points**

2. Click **+Add Profile**.



3. In the New Profile **General** tab, **Radio** settings, enable the Radio and select the network.

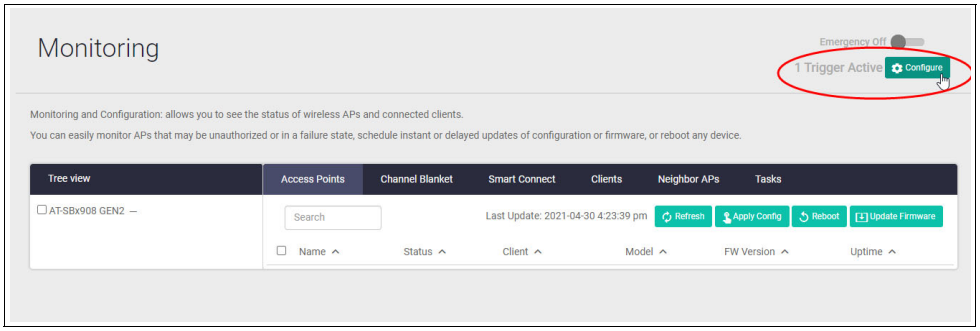


4. Click **Apply**.

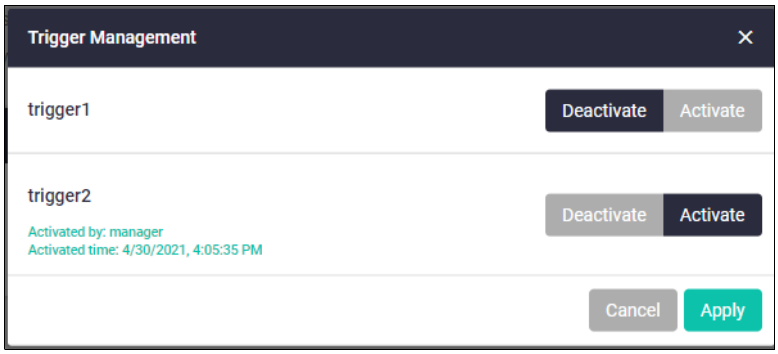
Activate the trigger

To choose which trigger is activated:

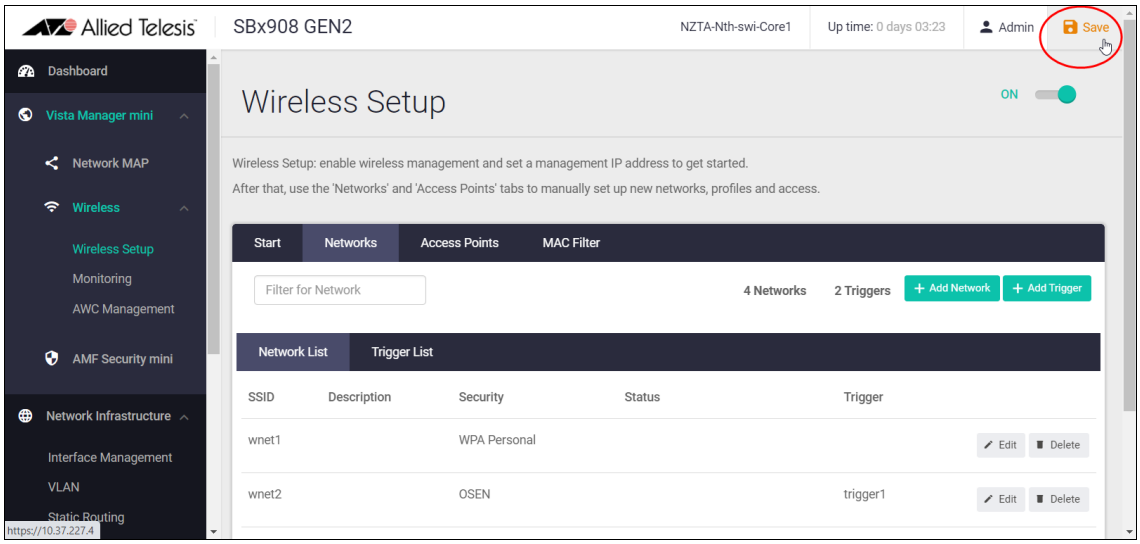
1. Select **Wireless** > **Monitoring** > **Access Points**
2. Select the **Access Points** tab.
3. Click **Configure**.



4. Select the trigger and click **Activate** or **Deactivate** as required.
5. Click **Apply**.



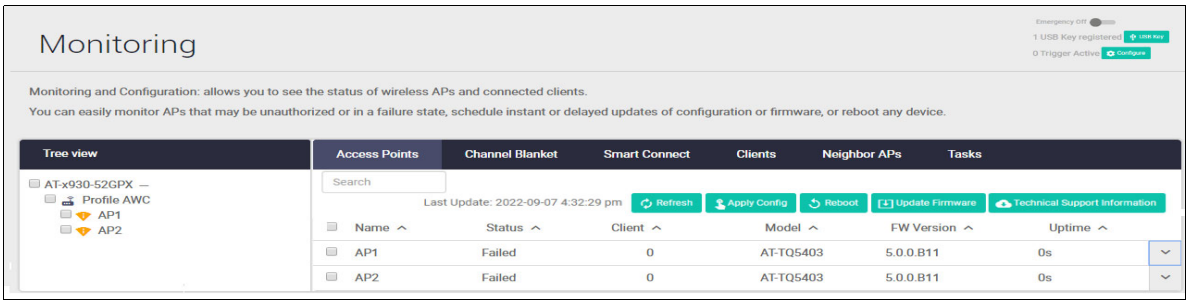
6. Click **Save** to save your configuration to the running configuration.



Monitoring the wireless network

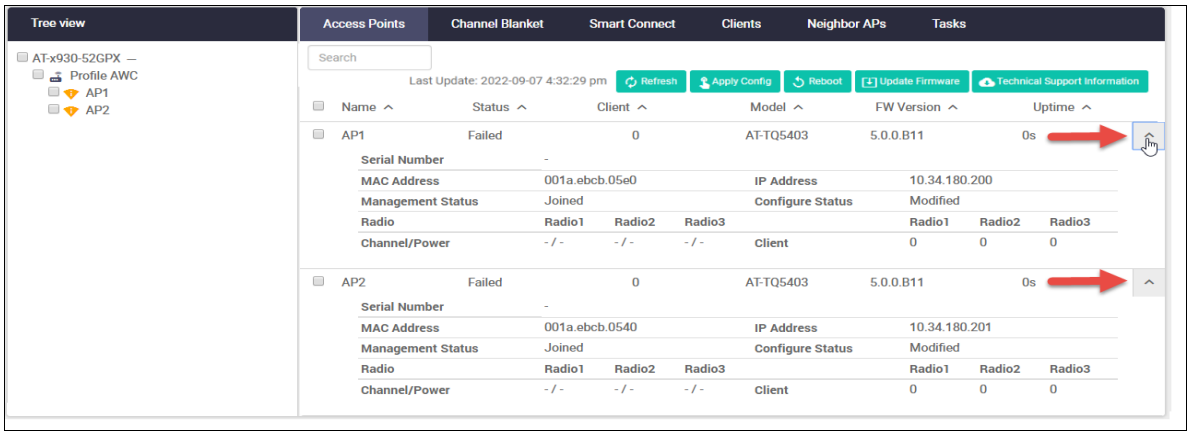
Use the **Monitoring** menu to:

- see the status of wireless APs and connected clients.
- use the expand ^ tool to sort columns by Name, Status, Client, Model, FW Version, and Uptime.
- configure your APs, monitor clients, neighbor APs, and schedule wireless management tasks.
- reboot any device.

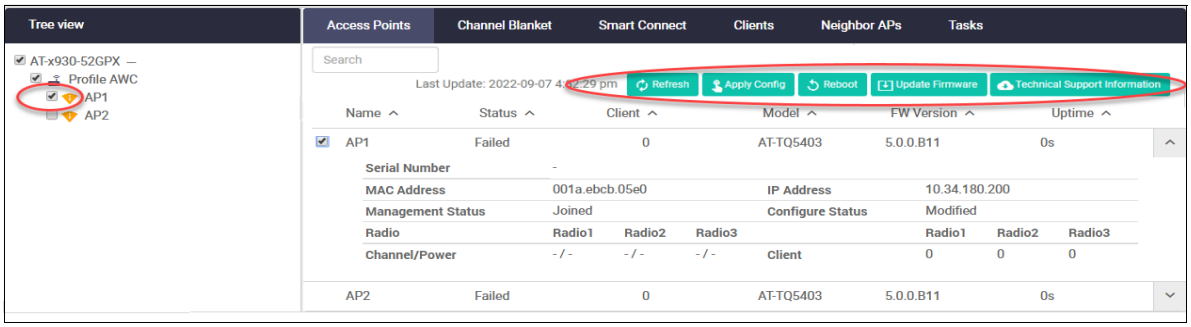


Access Points tab

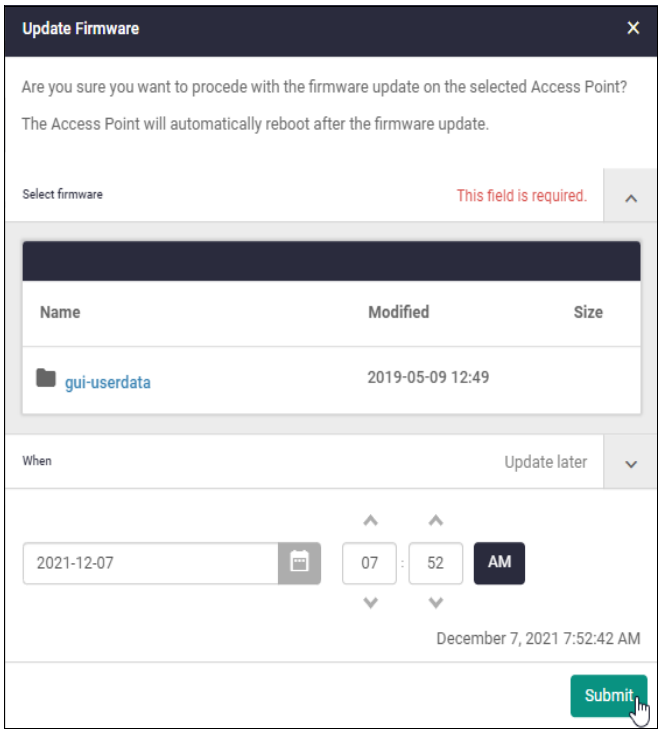
- On the **Access Points** tab, click the ^ tool to view additional details:



- Select an AP, then use the green action buttons to **Refresh**, **Apply Configuration**, **Reboot**, **Update Firmware** immediately or at a scheduled time, or get **Technical Support Information**.

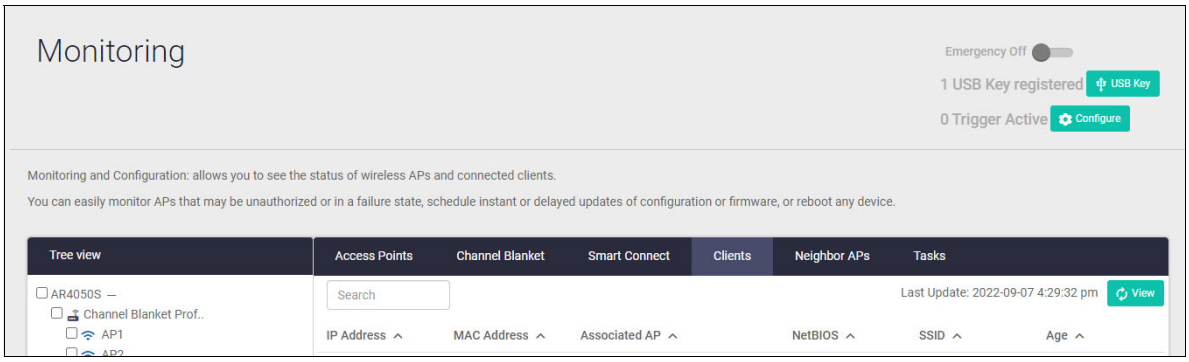


For example, you can schedule a firmware upgrade for a specific date and time:



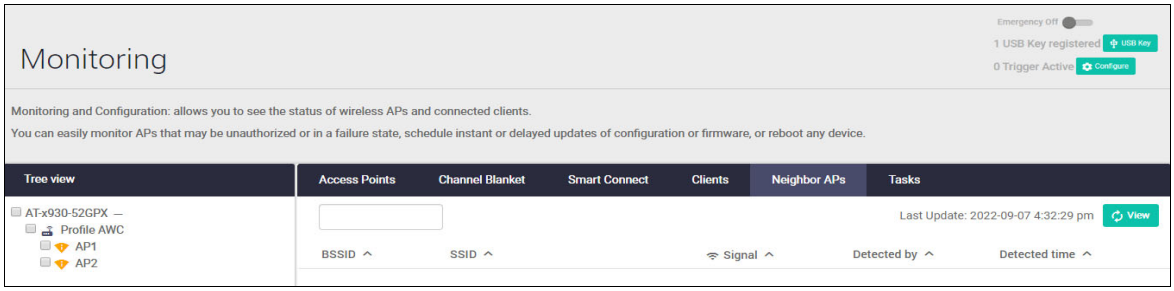
Clients tab

- The **Clients** tab shows clients that are currently connected to your wireless APs, including how long they have been connected for (the 'Age'). Click **View** to display the client information:



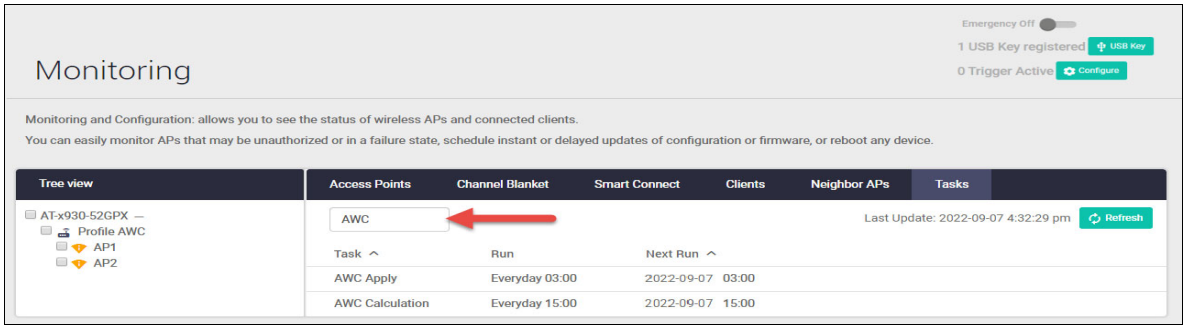
Neighbor APs tab

- The **Neighbor APs** tab shows other access points that can be seen, their signal strength, and which AP detected them.Click **View** to display the neighbor information.



Tasks tab

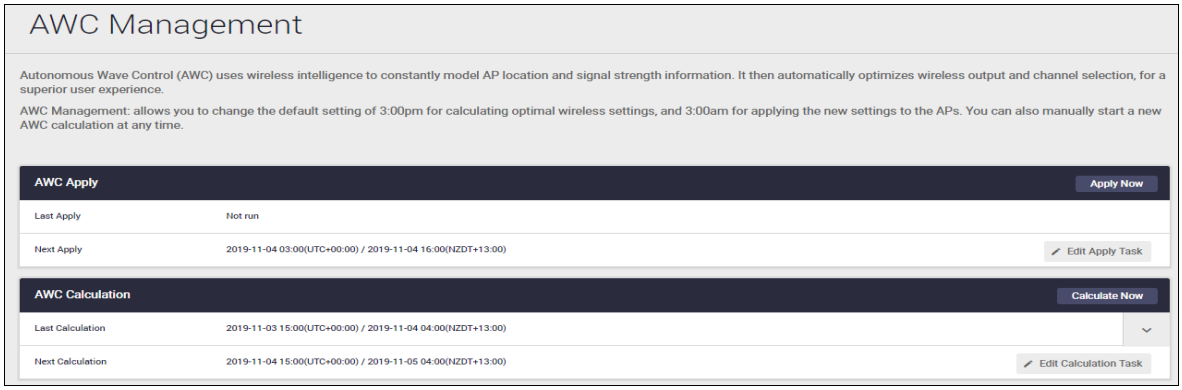
- The **Tasks** tab shows any scheduled wireless management tasks (for example a firmware update or applying new AWC settings to improve performance), and when they will next be run. Use the search window to locate tasks by name.



AWC management

AWC uses wireless intelligence to constantly model AP location and signal strength information. It then automatically optimizes wireless output and channel selection.

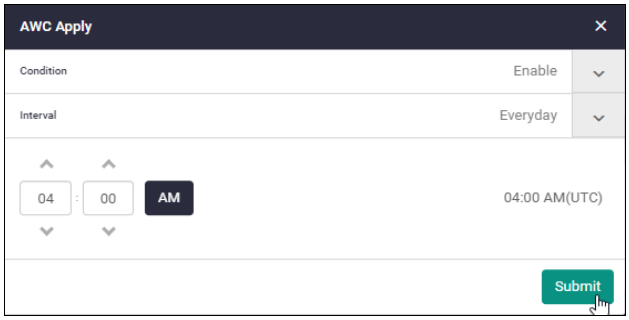
By default, AWC runs a calculation to optimize signal strength and channel settings at 15:00 hours each day. The new settings are then applied to all APs at 03:00 hours to avoid user disruption, as applying new settings disables the APs (approximately 30 seconds for the TQ Series, and 1–4 minutes for the MWS Series).



To change the **AWC Apply** settings:

1. Click **Apply Now** to manually apply a configuration change at any time
2. Click **Edit Apply Task** to change the current configuration.

3. Set the **Condition**, **Interval** and **Time**, and click **Submit**:



To change the **AWC Calculation** settings:

1. Click **Calculate Now** to manually start a new calculation at any time.
2. Click **Edit Calculation Task** to change the current configuration.
3. Set the **Condition**, **Interval** and **Time**, and click **Submit**:

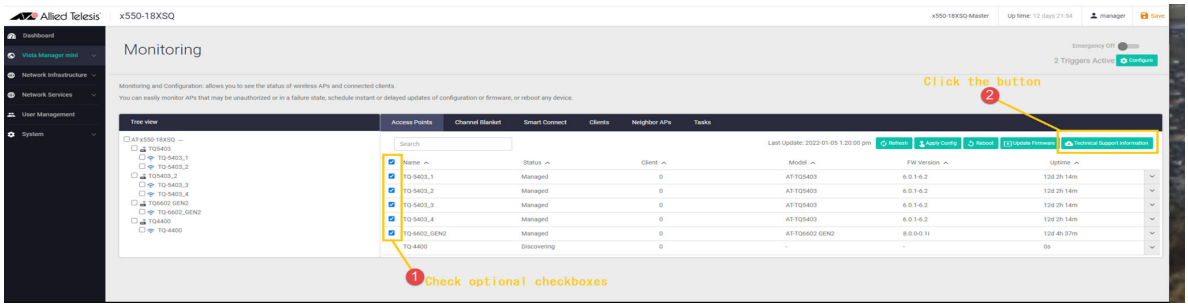
Troubleshooting

Available on the following AP models:

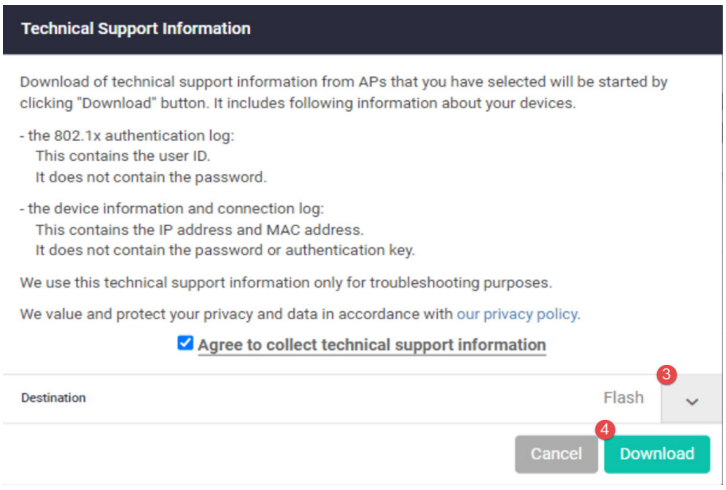
Model	Firmware version
TQ6702 GEN2, TQm6702 GEN2	8.0.0-1.1 or later
TQ6602 GEN2, TQm6602 GEN2	8.0.1-1.1 or later
TQ6602	7.0.1-2.1 or later
TQ5403 GEN2, TQm5403, TQ5403e, TQ1402, TQm1402	6.0.1-4.1 or later
TQ4600, TQ4400e	4.3.0 or later

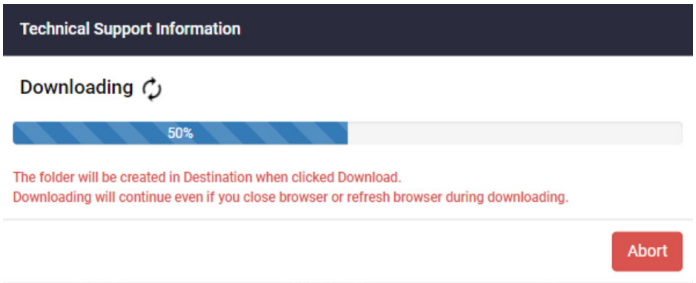
From version **5.5.2-0.1** onwards, and Device GUI **2.11.0** onwards, you can get a tech-support file via Vista Manager mini from every single managed AP or all of the APs that belong to an AWC-CB or AWC-SC group. Tech-support files contain debug information and are used for trouble shooting customer environments. To access this feature, go to **Vista Manager mini** > **Monitoring**:

1. Select AP(s).
2. Click **Technical Support Information** in either the Access Points, Channel Blanket, or Smart Connect tab.

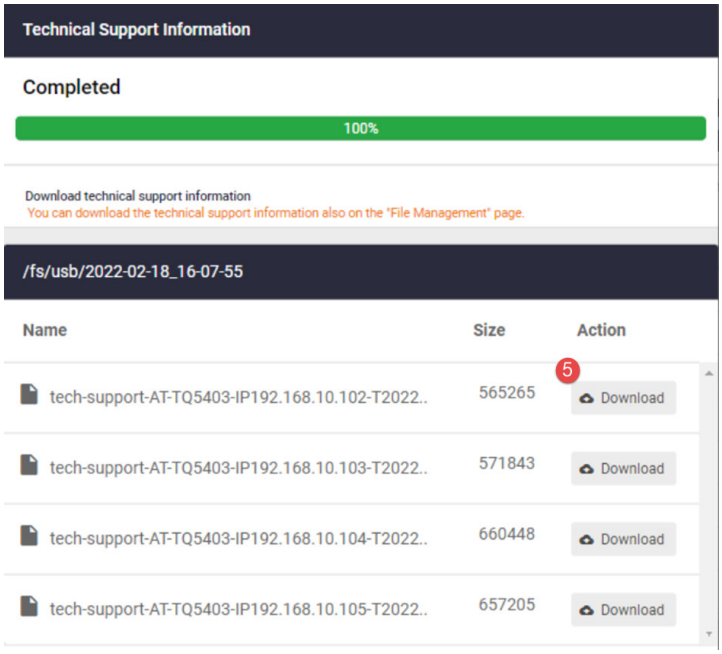


3. Select the download **Destination**.
4. Click **Download** to continue.





5. Click **Download** to complete the process.



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