19110006110110061918108110011101100111011011 00010111001

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.
- **x**550 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

	1
Products and software version that apply to this guide	2
Related documents	3
Starting Vista Manager mini	6
What does a wireless network look like?	7
What is Vista Manager mini?	7
Licensing	8
How many APs can a device manage?	8
What APs are supported?	8
Wi-Fi architectures	9
Configuring a multi channel wireless network	10
The Auto Setup feature	10
Manual setup	12
Configuring AWC Channel Blanket	18
Creating an AP profile	
Adding APs to an AP profile	21
The network map	22
The network map features	22
Viewing node information	23
Configuring the topology view	23
Customizing network node icon images	24
Access to device GUI by clicking on device icon	25
Heat maps	27
Adding a floor map	28
5	
Adding APs to a floor map	30
Adding APs to a floor map Configuring heat map coverage	30 32
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map	
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map Introduction to AWC Smart Connect	
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map Introduction to AWC Smart Connect The benefits of AWC-SC	
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map Introduction to AWC Smart Connect The benefits of AWC-SC Wireless AP roles	
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map Introduction to AWC Smart Connect The benefits of AWC-SC Wireless AP roles Wireless topology overview	
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map Introduction to AWC Smart Connect The benefits of AWC-SC Wireless AP roles Wireless topology overview AWC-SC configured VAPs	
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map Introduction to AWC Smart Connect The benefits of AWC-SC. Wireless AP roles Wireless topology overview AWC-SC configured VAPs Configuring AWC Smart Connect	
Adding APs to a floor map Configuring heat map coverage Re-naming a heat map Introduction to AWC Smart Connect The benefits of AWC-SC Wireless AP roles Wireless topology overview AWC-SC configured VAPs Configuring AWC Smart Connect Basic setup steps	

	42
Create an AP profile to use with Smart Connect	44
Configure the Root and Satellite APs	45
Connect Satellite APs to the Root AP	45
View the Smart Connect links	46
Introduction to Captive Portal	47
Configuring Captive Portal	48
Configuring the Page Proxy	50
Introduction to Passpoint	51
Configuring Passpoint: Basic Configuration	52
Configuring Passpoint: Customized Configuration	52
Enabling Passpoint on a new wireless network	53
Enabling Passpoint on an existing wireless network	62
Emergency mode	64
Set up a network for emergency mode	64
Use the Device GUI to enable emergency mode	65
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode	65 66
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled	65 66 67
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled Wireless network trigger	65 66 67 67
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled Wireless network trigger Create trigger	65 66 67 67 67
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled Wireless network trigger Create trigger for the network	65 66 67 67 67 68
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled Wireless network trigger Create trigger Set up the trigger for the network Assign network with trigger to VAP	65 67 67 67 67 68 69
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled Wireless network trigger Create trigger Set up the trigger for the network Assign network with trigger to VAP Activate the trigger	
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled Wireless network trigger Create trigger Set up the trigger for the network. Assign network with trigger to VAP Activate the trigger	
Use the Device GUI to enable emergency mode Use a pre-prepared USB stick to enable emergency mode See whether emergency mode is enabled Wireless network trigger Create trigger Set up the trigger for the network Assign network with trigger to VAP Activate the trigger Monitoring the wireless network	

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

-	Allied Tele	esis x	930-52GPX	-{
8 0	Dashboard Vista Manager mini Network MAP	^	Dashboard	
	🗢 Wireless	~	Port Status	
۲	Network Infrastructure	2 20	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51	3
۲	Network Services	1997) 1997)	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52	\$
-	User Management			
٠	System	~	Port Traffic	Ş
			Port 1.0.1 Traffic	
4	A start of the		Receive Transmit	1

Acronyms

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

Table 1: Acronyms used in Autonomous Wave Control

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 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 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:

Allied Telesis	AR4050S	AR	4050S Up time: 13 days 22:53	🛓 Admin 📑 Save
Dashboard Wizard	Wireless Setur	p		ON CON
Vista Manager mini Vista Manager mini Vista Manager mini Vireless Vireless Setup	Wireless Setup: enable wireless mane Use Auto-Setup to automatically discu Alternatively, use the Networks' and V Start Networks Ac	agement and set a management IP address over and set up your access points. Access Points' tabs to manually set up new ccess Points MAC Filter	to get started.	
Monitoring AWC Management AMF Security mini	Management IP Address	192.168.1.1 Failed Start Last run Auto-Setup: 202	1-06-14 11:10	
Licensed Features Network Infrastructure	Store Wireless Client/Neighbor AP logs	Disable 🍀 Configure		
Network Services Vetwork Services	Neighbor Managed AP Detection	ON		
💠 System 🗸 🗸				

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:

 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.

	Allied Telesis	AR4050S	AR4050S	Up time: 13 days 23:26	🛓 Admin 📄 Save
@24 >*	Dashboard Wizard ~	Wireless Setup			
	Vista Manager mini ~ Image: Strate	Auto Setup: Restart APs for DHCP Use Alter Please power on your APs. If they are already powered allow DHCP to provide them with an IP address for con Country Profile (Belect to apply to created profile)	on, please restart them to nectivity to the AWC mana United States Auto Cancel	ager.	
8	Security ~	🔒 Start Last run Au	to-Setup: 2021-06-14 11:1	10	
∎ ⊕ ⊕	Licensed Features ~ Network Infrastructure ~ Network Services ~	Store Wireless Client/Neighbor AP logs Disable 🍣 Configure	1		
45 0	User Management System ~	Neighbor Managed AP ON Detection			

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.

	Allied	Telesis	AR4050S		AR4050S	Up time: 8 days (
#	Dashboard Wizard	▲	Wireless Set	up		
6	Vista Manager m	nini A	Wireless Setup: enable wireless n Use Auto-Setup to automatically o Alternatively, use the 'Networks' a	nanagement and set a management IP address to get sta discover and set up your access points. Ind 'Access Points' tabs to manually set up new networks	rted.	
	🗢 Wireless	^	When you use "WPA-Enterprise", "	OSEN" or "Captive Portal", please configure [AAA] to s	pecify RADIUS Server.	
	Wireless Se	tup	Start Networks	Access Points MAC Filter		
	Monitoring AWC Manag	gement	Management IP Address	192.168.1.1		
	😚 AMF Securi	ty mini	Auto Setup	Failed		
e	Security	~				
C	Licensed Feature	es 🗸		Last run Auto-Setup: 2021-12	-06 09:33	
•	Network Infrastr	ucture 🗸	Store Wireless Client/Neig	hbor AP Disable		
	Network Service	s v	logs			

- 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):

Auto Setup	×
Click 'Start' to begin Auto Setup	
Country New Zealand	~
Profile (Select to apply to created profile) AUTO	~
Cancel	Start

- 5. Click Start again to proceed with auto discovery.
- 6. When the auto discovery is complete you will see this dialog:

Start	Networks	Access Points	
Mai	Management IP Address Auto Setup		10.37.224.90 ×
Aut			Discovered 2/2 new APs Click to view
			Start Last run Auto-Setup: 2018-08-07 12:24
Stor	re Wireless Client/I	Neighbor AP logs	Disable 🏼 🗱 Configure
Nei	ghbor Managed AF	Detection	ON

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

	Allied Telesis	AR4050S AR4050S	Up time: 8 days 00:55	💄 manager 🛛 🗟 Save
@ a **	Dashboard Wizard v	Wireless Setup		
0	Vista Manager mini > Image: Manager mini > Image: Mireless > Image: Mireless > Monitoring > AWC Management > Image: Mireless >	Wireless Setup: enable wireless management and set a management IP address to get started. Use Auto-Setup to automatically discover and set up your access points. Alternatively, use the 'Networks' and 'Access Points' tabs to manually set up new networks, profiles and access. When you use "WPA-Enterprise", 'OSEN' or 'Captive Portal', please configure [AAA] to specify RADIUS Server. Start Networks Access Points MAC Filter Management IP Address IP Address IP Address IP Address IP Address 		
A	Security ~	G Start Last run Auto-Setup: 2021-12-06 09:33		
C	Licensed Features V	_		
۲	Network Infrastructure 🗸	Store Wireless Client/Neighbor AP Disable Configure		
۲	Network Services \lor	lugs		
*	User Management	Neighbor Managed AP Detection ON		
٥	System ^			

Add a network

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

Wireless S	etup			ON CON
Wireless Setup: enable wirele After that, use the 'Networks	ess management and set and 'Access Points' tabe	a management IP address to get started. to manually set up new networks, profiles and access.		
Start Networks	Access Points	MAC Filter		
Filter for Network			2 Networks	0 Triggers + Add Network + Add Trigger

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.

New Network - Basic Settings	×
SSID	
AWC	
Description (Optional)	
awc-network	
Status Normal	~
Trigger None	~
Security WPA Personal	~
Key	
key_awcnetwork	
Broadcast Key Refresh Interval	
0	
Advanced Settings > Cancel	Save

- 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.

New Network	k - Advanced Set	ttings		×
General	Security	Fast Roaming		
Hide SSID			Disabled	Enabled
VLAN ID				
1				
Band Steering			Disabled	Enabled
Duplicate AUTH	received		Disconnect	Ignore
Association Adv	ertisement		Disabled	Enabled
Proxy ARP			Disabled	Enabled
DTIM Period				
1				
< Basic Se	ttings		Cancel	Save

- 5. Click **Save** to complete this step.
- 6. The Network List tab, SSID column, contains a list of configured networks and their status.

Wireless S	Setup						0	N -
eless Setup: enable wire	less management and set a ma	anagement IP address to get sta	rted.					
e Auto-Setup to automati	cally discover and set up your	access points.						
ernatively, use the 'Netwo	orks' and 'Access Points' tabs to	o manually set up new networks,	profiles and access.					
ien you use "WPA-Enterpr	rise", "OSEN" or "Captive Portal	, please configure 「AAA」 to sp	pecify RADIUS Server.					
Start Networks	Access Points N	AC Filter						
Eilter for Network				2 Notworks	1 Triggor	C Refresh	- Add Network	- Add Trior
The for Network				5 Networks	i niggei			
Network List Tr	igger List							
	Description	Security	Statue		Televen			
SSID	Description	ocounty	olutuo		ingger			
SSID	Description	WPA Personal	Configurable		Ingger		Edit	Delete
SSID	Description	WPA Personal	Configurable		Ingger		 Edit Edit 	DeleteDelete

Create an access point profile for the AP series

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

Wire	less Set	tup						ON	•
Wireless Setu Use Auto-Set Alternatively, When you use	up: enable wireless up to automatically use the 'Networks' e "WPA-Enterprise",	management and set discover and set up and 'Access Points' , "OSEN" or "Captive	et a management IP addre o your access points. tabs to manually set up no Portal", please configure	ess to get starte ew networks, pr 「AAA」 to spe	rd. ofiles and access cify RADIUS Serve	К.			
Start	Networks	Access Points	MAC Filter						
Filter fo	or Access Points		Access Points status	3 Profiles	0 SC Profiles	🗘 Refresh 🛛 + Add	+ Add Smart Connect Prof	ile 🛛 🕂 Add Access P	loint
Profiles	Smart Conr	nect Profiles							

- 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.

New Profile - Basic Sett	tings		×	New Profile -	Basic Settings			×
General Chanr	nel Blanket Smart Connect			General	Channel Blanket	Smart Connect		
Name Profile AWC				Name AWC				
Model		AT-TQ5403	~	Model			AT-TQ5403	~
Country		New Zealand	~	Country			New Zealand	~
Radio 1	Click Enable, then click here to select	AWC	^	Radio 1	_		AWC	~
		Enabled	led	Radio 2	Ra	dio 1,2, and 3	AWC	~
AWC	L Chan	nnel Blanket OFF 🛛 🛑		Radio 3	A A	WC network	AWC	~
Radio 2		Disabled	~	Link Aggregation			Disable	~
Radio 3		Disabled	~	MAC Filter			Disabled	~
Link Aggregation		Disable	~	MAC Filter - Actio	n		Block	Allow
MAC Filter		Disabled	~	Advanced S	ettings >		Cancel	Apply
MAC Filter - Action		Block A	llow					
Advanced Settings >		Cancel	pply					

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

New Profile - Advanc	ed Settings			×
Radio 1 Setting	Radio 2 Setting	Radio 3 Setting		
Mode			b/g/n	~
Bandwidth			20MHz	~
Channels			all	~
Client Isolation			Disable Er	able
Airtime Fairness			Disable Er	able
Neighbor AP Detection			Disable Er	able
Legacy Rates			all	~
< Basic Settings			Cancel	pply

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

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

Start	Networks	Access Points	MAC Filter							
Filter fo	r Access Points			Access Points status	1 Profile	0 SC Profiles	+ Add Profile	+ Add Smart	Connect Profile	+ Add Access Point
Profiles	Smart Co	nnect Profiles								
Profile. Pro	ofile AWC				C	onfig Status: 🔗 (Configurable	AT-TQ5403	💉 Edit Profile	盲 Delete Profile
Name		MAC Address		IP Address	St	atus				

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:

New Access Point - Basic Settings		×
Name AP2		
MAC Address		
IP Address		
Profile	Profile AWC	^
Profile AWC		
Advanced Settings >	Cancel	pply

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

Edit Access Point - A	dvanced Settings			×
Radio 1 Setting	Radio 2 Setting	Radio 3 Setting		
Status			Enable	~
Channel			Auto	~
Power			Auto	~
< Basic Settings			Cancel	pply

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*.

Wireless	Setup				on 🛑
/ireless Setup: enable v se Auto-Setup to autor Iternatively, use the 'Ne /hen you use "WPA-Ent	wireless management and set a man matically discover and set up your ac stworks' and 'Access Points' tabs to n erprise", "OSEN" or "Captive Portal", p	gement IP address to get started. ess points. aanually set up new networks, prof lease configure 「AAA」 to specif	iles and access. fy RADIUS Server.		
Start Networ	rks Access Points MA Points Ac	C Filter cess Points status 4 Profiles	0 SC Profiles 🗘 Refres	h + Add Profile + Add Smart Connect Profile	+ Add Access Point
Profiles Sm	art Connect Profiles				
Profile: Profile AWC	MAC Address	IP Address	Config Status:	Configurable AT-TQ5403 🖌 Edit Profile	e 🧃 Delete Profile
AP1	000a 9594 6816	192.168.22.1	Discovering	✓ Edit Username / Password	Edit 🔋 Delete
AP2	000a 999d 4720	192.168.22.2	Discovering	Edit Username / Password	Edit 🛢 Delete 🔻

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 channelblanket 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:

Wire	less Se	tup						ON	-•
Wireless Setu Use Auto-Set Alternatively, When you use	/ireless Setup: enable wireless management and set a management IP address to get started. Ise Auto-Setup to automatically discover and set up your access points. Iternatively, use the 'Networks' and 'Access Points' tabs to manually set up new networks, profiles and access. Yhen you use "WPA-Enterprise", "OSEN" or "Captive Portal", please configure 「AAA」 to specify RADIUS Server.								
Start	Networks	Access Points	MAC Filter						
Filter fo	or Access Points		Access Points status	4 Profiles	0 SC Profiles	C Refresh + Add Profile	+ Add Smart Connect Profile	+ Add Acc	cess Point
Profiles	Smart Con	nect Profiles							

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

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

General Chanr	el Blanket Smart Connect	tę.
ame hannel Blanket profile	1	
odel		AT-TQ5403
AT-TQ6702 GEN2	AT-TQm6702 GEN2	
AT-TQ6602		
AT-TQ5403	AT-TQm5403	AT-TQ5403e
AT-TQ1402	AT-TQm1402	
AT-TQ4400e	AT-TQ4600	

- 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.

New Profile -	Basic Settings		×
General	Channel Blanket	Smart Connect	
Name Channel Blan	ket Profile1		
Model		AT-TQ5403	~
Country		New Zealand	~
Radio 1		AWC	^
		Enabled Disal	bled
AWC		Channel Blanket ON	\cup
Radio 2		Click button to turn On or Off Disabled	~

6. Select the Channel Blanket tab.

New Profile -	Basic Settings			×
General	Channel Blanket	Smart Connect		
Control VLAN Enter Contro	I VLAN ID			
Wireless Client I	colation		Disable Er	able
Key				
Enter Securit	y Keyword			
Proxy ARP			Disable Er	able
Beacon RSSI Thr 30	eshold			
Radio 1 Channel			Auto	~
Radio 2 Channel			Auto	~
Force Power Sav	e Disabled		Disable En	able
Advanced S	ettings >		Cancel	pply

- 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.
- 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).
- 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.

New Profile - Advance	ed Settings			×
Radio 1 Setting	Radio 2 Setting	Radio 3 Setting		
Mode			b/g/n	~
Bandwidth			20MHz	~
Channels			all	~
Client Isolation			Disable Er	able
Airtime Fairness			Disable Er	nable
Neighbor AP Detection			Disable Er	able
Legacy Rates			all	~
< Basic Settings			Cancel	pply

- 11. Click **Apply** to complete this step.
- 12. You can now see the newly created profile.

	Wireles	ss Set	up								ON	•
W	Vireless Setup: enable wireless management and set a management IP address to get started.											
U	se Auto-Setup to automatically discover and set up your access points.											
A	ternatively, use th	tively, use the 'Networks' and 'Access Points' tabs to manually set up new networks, profiles and access.										
V	'hen you use "WP	A-Enterprise*, *	'OSEN" or "Captive Po	rtal", please configure 「🗛	A to specify	RADIUS Server.						
	Start N	etworks	Access Points	MAC Filter								
	Filter for Acc	ess Points		Access Points status	4 Profiles	0 SC Profiles	🇘 Refresh	+ Add Profile	+ Add Smart Co	nnect Profile	+ Add Acc	ess Point
J	Profiles	Smart Conne	ect Profiles									
<	Profile: Channe	el Blanket Profi	ile 1			Cont	fig Status: 📀	Configurable	AT-TQ5403	🖋 Edit Profile	👕 Delete	Profile
	Name		MAC Address	IP Addre	SS	Status						

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:

Name	
AP1	
Status	Disabled Enabled
MAC Address	
Enter MAC address	
IP Address	
Enter IP address	
Profile	Channel Blanket Profile 1

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

dvanced Settings		×
Radio 2 Setting	Radio 3 Setting	
	Enable	~
	Auto	~
	Auto	~
	dvanced Settings Radio 2 Setting	dvanced Settings Radio 2 Setting Radio 3 Setting Enable Auto Auto Auto

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.

Vireless	Setup			ON C		
eless Setup: enable v	wireless management and set a mana	gement IP address to get starte	d.			
Auto-Setup to automatically discover and set up your access points.						
ernatively, use the 'Networks' and 'Access Points' tabs to manually set up new networks, profiles and access.						
en you use "WPA-Ent	terprise", "OSEN" or "Captive Portal", pl	ease configure 「AAA」 to spec	cify RADIUS Server.			
Start Netwo	rks Access Points MAC	Filter				
Filter for Access I	Points	ess Points status 4 Profiles	s 0 SC Profiles CRefresh	+ Add Profile + Add Smart Connect Profile + Add Access P		
Profiles Sm	part Connect Profiles					
Thomas Chi	an connect romes					
Profile: Channel Bla	inket Profile 1		Config Status: 🧔 🤇	Configurable AT-TQ5403 🖋 Edit Profile 🝵 Delete Profi		
	MAC Address	IP Address	Status			
Name						
Name AP1	CODA VOId care	192,768,22.1	Discovering	✓ Edit Username / Password ✓ Edit ● Delete		

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.

Network MAP	3 node 🔥 2 manag	jed 📀 0 abnormal 🕞 1 unm	anaged	🔊 Reset 🧹 Save	🗘 Refresh	Configure
Topology Map >	Topology View Settin	ng	×	_		/
	Layout SNN	IP Device Discovery				
	Limit nodes per line		Disabled Enabled			
	Maximum number of node: 10	per line				
	Collapse child nodes		Disabled Enabled			
	Collapse child nodes if the	e are more than:				
	Client polling interval (curre	ent session only)				
AP1		•	Every 5 seconds			Ĭ
	Backgound Image	Floor_map.PNG	Search Tear			
			Cancel Apply			+

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)

Allied Telesis	x930-52GPX			x930	Up time: 1 day 23:10	2 Admin	Save
 Dashboard Vista Manager mini 	Network I	MAP 🖸 3 nc	ide 🐼 2 managed 🦁 0 abnormal 📀 1 unmanaged	ſ	⊙ Reset 🗸 Save 🗘	Refresh 😰 C	onfigure
< Network MAP	Topology Map >						
🗢 Wireless 🗸 🗸	Node List	ALL (3) •					
🔒 Security 🗸	Name	Туре					
Network Infrastructure ~	x930	Guest					
Network Services ~	AP1	AWC					
🚢 User Management							
😍 System 🗸	AP2	AWC	AP2				
							+
	•						

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.

Network MAP 🛛	3 node 🔕 2 managed 🤨 0 abnormal 📀 1 unmanaged	🕘 Reset 🖉 🗸 Save 🧳 Refresh 🔹 🗘 Contigure
Topology Map >		
L AP1	2 x930 AP2	
\frown		+ _

2. Click Upload Map.

Network MAP	
Edit Heat Map 🔰 Heatmap3 🖍	G Upload Map ✓ Edit Scale ✓ Appty X Delete Map
Topology Map > Heatmap3 > Edit	
	∟ 1m 1mx1m
	المراجع

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.

Upload Map		×
Мар	Floor_map.jpg	Search
Scale	Floor Width 40 : Height 20 meters	٣
	Canc	el Save

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**.

Network MAP
Edit Heat Map
Topology Map > Hectmap1 > Edit

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

A	Dashboard						_
*	Wizard ~	File Management					S Reboot
0	Vista Manager mini 🛛 🗸						
ô	Security ~	/fs /flash			🛆 Upload	Set Boot Release File	
C	Licensed Features 🛛 🗸	Name ~	Modified —	Size(bytes)	Actions	Current: flash:/arc-5.4.8-0.2.rel	D Browse
•	Network Infrastructure 🗸	5.4.9-2.4	10/7/2004, 6:30:46 AM	56606503	▲ Download ■ Delete	Backup: Not Set	🗅 Browse
۲	Network Services 🗸 🗸	5.4.9-2.4.rel	10/7/2004, 6:31:04 AM	56606503	Download II Delete	Set Boot Config File	
**	User Management	abc	5/13/2020, 2:13:42 PM	6	Download I Delete	Current: flash:/angga.cfg	D Browse
٠	System ^	arc-5.4.8-0.2.rel	6/10/2020, 4:14:39 PM	43742531	✿ Download ■ Delete	Backup: Not Set	D Browse
	About File Management	AT-TQ5403-6.0.1-1.1.img	5/5/2020, 10:00:06 AM	21255908	▲ Download ■ Delete	Flash Usage	
	License Management Services	awplus-gui_550_17.gui	7/6/2020, 5:42:49 PM	2465792	Download II Delete	7% 2	37.0M / 3.6G
	Time Logging	ebug.sh	5/13/2020, 2:15:01 PM	29	Download II Delete		
	CLI	default.cfg	6/5/2020, 2:54:25 PM	4062	Download I Delete		

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

🕰 Dashboard	Monitoring						Emergency Off	
 Vista Manager mini Network MAP 	Monitoring and Configuration: allows you to see You can easily monitor APs that may be unauth	e the status of wireless APs and norized or in a failure state, sche	l connected clients. dule instant or delay	ed updates of configural	tion or firmware, or reboot an	y device.		
🗢 Wireless 🛛 🔨	Tree view	Access Points	Channel Blanket	Smart Connect	Clients Neighbor	APs Tasks		
Wireless Setup	□ AR4050S □ ♣ TAC-SC	Search]	Last Update: 2020-07	7-09 3:21:57 pm 🧳 Refresh	S Apply Config	Reboot	ware
Monitoring	□	Name	Status ^	Client ^	Model ^	FW Version A	Uptime A	
AWC Management	G ⇒ TAC-SC-Terminator#1 ⇒ TAC-SC-Terminator#2 a TAC-TQ G ⇒ TAC-TQ G ⇒ TAC-TQ#1	TAC-SC-Root	Managed	0	AT-TQ5403	6.0.1-1.1	13d 3h 55m	~
AMF Security mini		TAC-TQ#1	Managed	0	AT-TQ5403	6.0.1-1.1	19d 5h 3m	~
	□ 🚔 TAC-TQm □ 🗢 TAC-TQm#1	TAC-TQm#1	Managed	0	AT-TQm5403	6.0.1-1.1	19d 5h 4m	~
Security ~	🗆 🚢 TAC-TQm-SC	TAC-SC-Termi	Managed	0	AT-TQ5403	6.0.1-1.1	13d 3h 55m	~
G Licensed Features		TAC-SC-Termi	Discovering	0	-	-	0s	~
		TAC-SC-Termi	Discovering	0		-	0s	~
Network Infrastructure $ imes $								

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 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

New Profile -	Basic Settings		×
General	Channel Blanket	Smart Connect	
Name Enter Profile	name		
Model		AT-TQ5403	~
Country		United States	~
Radio 1		\frown	^
		Enabled Disa	bled
TAC_Vista	aMini_AWCLite	Channel Blanket OFF	
Guest		Channel Blanket OFF	
Radio 2		Disabled	~
Radio 3		Disabled	~
Link Aggregatior	1	Disable En	able
MAC Filter		None	~
Advanced S	Settings >	Cancel	pply

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.

New Profile - Basic Settings						
General	Channel Blanket	Smart Connect	_			
Smart Connect P	rofiles		Disabled	、 、		
SmartCon	nect1 🐣					
SmartCon	nect1					
Advanced S	ettings >		Cancel			

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**.

New Access Point - Basic Settings		×
Name TAC-SC-Root		
MAC Address 001a.ebcb.1d40		
IP Address		
Profile	TAC-SC	~
Advanced Settings >	Cancel	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).

Monitoring						Emergency Off	
Monitoring and Configuration: allows you to see the status of You can easily monitor APs that may be unauthorized or in a	f wireless APs and connecte failure state, schedule insta	ed clients. ant or delayed updates o	configuration or firmware, or r	eboot any device.			
Tree view	Access Points	Channel Blanket	Smart Connect Clients	Neighbor APs Tasl	KS		
□ AR4050S □ 🚔 TAC-SC	Search		La	ast Update: 2020-07-10 9:13:22 am	🗘 Refresh 🙎 Apply Config	S Reboot Update Fin	mware
□	□ Name ∧	Status 🔨	Client ^	Model ^	FW Version A	Uptime 🔺	
TAC-SC-Terminator#2	TAC-SC-Root	Managed	0	AT-TQ5403	6.0.1-1.1	13d 21h 46m	~
□	TAC-TQ#1	Managed	0	AT-TQ5403	6.0.1-1.1	19d 22h 55m	~
□ 🚔 TAC-TQm □ 🗢 TAC-TQm#1	TAC-TQm#1	Managed	0	AT-TQm5403	6.0.1-1.1	19d 22h 55m	~
TAC-TQM-SC	TAC-SC-Termi	Managed	0	AT-TQ5403	6.0.1-1.1	13d 21h 46m	~
□ 🗢 TAC-SC-Terminator#3	TAC-SC-Termi	Discovering	0	-	-	0s	~
	TAC-SC-Termi	Discovering	0	-	-	0s	~

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.

Allied Telesis	x930-52GPX		
 Dashboard Viete Manager mini 	Wireless Setup		
Vista Manager mini	Vireless Setup: enable wireless manag	ement and set a management IP address to get started.	_
 Wireless Wireless Setup Monitoring 	Start Networks Acce	Edit Network - Advanced Settings General Security Captive Portal	RADIUS Server
AWC Management	SSID	Disabled RADIUS Server	<u>_</u>
Network Services Vetwork Services	doc_wireless	Click Through External Page Redirect	
🗘 System 🗸 🗸		RADIUS Accounting	Disable Enable
		Page Proxy	Disable Enable
		Page Proxy URL http://www.example.com/captive_portal	
		Redirect Mode	Session Keep 🗸 🗸
		MAC Authentication	Disabled 🗸
		< Basic Settings	Cancel Save

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.

	Allied Telesis	x930-5	52GPX				x930-Maste	r Up time: 23 days 23:35	1 manager	Save	
ଜ୍ଜ ତ	Dashboard Vista Manager mini	Wir	Wireless Setup								
	 Network MAP Wireless 2 Wireless Setup 3 Monitoring AWC Management 	Wireless S After that, When you Start Filte	Setup: enable w , use the 'Network use "WPA-Ente Network Network	ireless management and set a rrks' and 'Access Points' tabs t rprise', "OSEN" or "Captive Por ts Access Points	2 Triggers 💋 Refresh	Ş gers ⊈ Refixeb + Add Network + Add Trigger 2*Pecspecifi Balic Setue					
â	Security ~	Netw	vork List	Trigger List							
•	Network Infrastructure \lor	SSID		Description	Security	Status	Trigger				
•	Network Services	wirele	essNet1		WPA Enterprise Passpoint	Configurable		Cop	y 🎤 Edit 🖠	Delete	

Passpoint Basic Setup		×
Create basic Passpoint network. You can edit network for more deta modal.	il on the edit	
SSID		
Enter SSID Name		
RADIUS Authentication Group	Disabled	~
RADIUS Accounting Group	Disabled	~
Operator Friendly Name		~
Operating Class Indication 51		
Roaming Consortium List		
HEX string separated by comma(,). e.g. '506f9a,1122334455'		
Domain name		
FQDN separated by comma. e.g. 'example.com,example.net'		
NAI Realm information	: TLS	~
SSID is required.	Cancel	Save

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

l	Network List	Trigger List				
	SSID	Description	Security	Status	Trigger	
	wirelessNet1		WPA Enterprise Passpoint	Configurable		Copy 🖍 Edit 👔 Delete

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.

New Network - Basic Settings		×
SSID		
Test_wireless		
Description (Optional)		
Enter description		
Status	Normal	~
Security	None	^
None		^
WPA Personal		
WPA Enterprise		
OSEN		Ŧ
Advanced Settings >	Cancel	Save

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

New Network	k - Advanced Sett	ings			×
General	Security	Fast Roaming	Passpoint	802.11	u
Hide SSID			l	Disabled	Enabled
VLAN ID 1					
Band Steering			l	Disabled	Enabled
Duplicate AUTH	received			Disconnect	Ignore
Association Adv	ertisement		l	Disabled	Enabled
Passpoint				Disabled	Enabled
Proxy ARP				Disabled	Enabled
DTIM Period					
< Basic Set	ttings	Friendly	y name is required	. Cancel	Save

Passpoint

- **Configuring** 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.

New Network - Advanced Settings ×					
General	Security	Fast Roaming	Passpoint	802.11ı	ı
Downstream Grou	p-Addressed Forward	ling (DGAF)		Disabled	Enabled
Layer 2 Traffic (L2	TIF)			Disabled	Enabled
Operator Informat	ion				: 🗸
Operating Class In 51	dication				
<u> Options</u>					
ANQP Domain ID O					
Deauthentication I 60	Request Timeout				
Connection Capab	bilities				~
WAN Metrics					~
OSU Status				Disabled	Enabled
Basic Sett	tings	Friend	lly name is required.	Cancel	Save

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</language></friendly>

Table 3: Passpoint configuration fields (continued)

FIELD	DESCRIPTION			
Operating Class Indication	The HEX number of the radio information. For example, '517376' means using 1-13ch and 36-64ch(20MHz). The default is '51' (2.4GHz) 1-13channels See Table E-4 of IEEE Std 802.11-2020 Annex E for more detail.			
	Hex Channels			
	51 (2.4GHz) 1-13ch			
	73 (5GHz) 36,40,44,48ch			
	76 (5GHz) 52,56,60,64ch			
	79 (5GHz) 100,104,108,112,116,120,124,128,132,136,140,144ch			
	7D (5GHz) 149,153,157,161,165,169,173ch			
ANQP Domain ID	Configures the Hotspot 2.0 ANQP (Access Network Query Protocol) domain identifier. Optional - If you don't configure this, the default '0' is set.			
Deauthentication Request Timeout	Optional - If you don't configure this, the default '60' is set.			
Connection Capabilities	Optional, and includes the following fields:			
	IP Protocol Number			
	Port Number			
	Port Status			
WAN Metrics	Optional, and includes the following fields:			
	At Capacity			
	Symmetric Link			
	■ Link Status			
	Uplink Load			
	Downlink Load			
	Uplink Speed			
	 Downlink Speed 			
	Load Measure Duration			
OSU Status	Optional - Enable/Disable Disabled by default			
OSU SSID	Configures the SSID that wireless clients will use for OSU.			
OSU Providers Server URI	Uniform Resource Identifier (URI) of the OSU server, for example: osu-server.example.com			
OSU Providers NAI	Optional - The OSU Providers NAI (Network Access Identifier) This is in an email address format, for example: fred.smith@example.com			
OSU Providers Method	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 			

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 7. Select the 802.11u tab.

802-11u

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

Table 4 on page 58 below describes these configuration fields.

New Network	- Advanced Setti	ngs			×
General	Security	Fast Roaming	Passpoint	802.11u	
Network Type			F	Private network	~
Internet Access				Disabled Ena	bled
Additional Step Re	equired for Access			Disabled Ena	abled
Emergency service	es reachable			Disabled Ena	abled
Unauthenticated e	mergency service acc	essible		Disabled Ena	bled
Venue Group					
/					
Venue Type 1					
Homogeneous ES	S identifier (HESSID)				
MAC address					
Roaming 01 HEX string se	parated by comn	na(,). e.g. '506f9a,1122	2334455'		
Venue Name (Opti	ional)			None	~
Network Authentic	cation Type			None	~
IP Address Type A	wailability		Private	Nat 1 : No exist	~
Domain name					
FQDN separat	ted by comma. e.	.g. 'example.com,exan	nple.neť		
3GPP info (Option MCC and corr	al) nma and MNC se	parated by semi-color	1. e.g. '440,00;44	0,50'	
Realm Information	n			: TLS	~
Arbitrary ANQP-el	ement configuration (0	Optional)		None	~
GAS Address 3 be	havior		P2	P Specification	~
GAS Comeback De	elay				
0					
Qos Map Set (Opti	ional)				
e.g. 53,2,22,6,	8,15,0,7,255,255,	16,31,32,39,255,255,4	0,47,255,255		
Sasic Sett	tings	Friendly	y name is required	I. 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 network 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 Ol	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	Network Authentication Type Information — if this is an unsecured network, specify the additional steps required for access (ASRA):			
Туре	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	The cellular network identifier.			
Network Information	 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]=""></up></up></dscp>
	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.

Wireless	Setup		0N -
Wireless Setup: enable w After that, use the 'Netwo	vireless management and set a management IP orks' and 'Access Points' tabs to manually set up	address to get started. new networks, profiles and access.	
Start Network	ks Access Points MAC Filter		1 Network + Add Network
SSID	Description	Security	
AWC	awc-network	WPA Personal	Fdit Delete

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

New Network - Dasie Settings	
SSID	
Test_wireless	
Description (Optional)	
Enter description	
Status Normal	~
Security None	^
None	•
WPA Personal	
WPA Enterprise	
OSEN	-
Advanced Settings > Cancel	Save

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

Edit Network	Edit Network - Advanced Settings							
General	Security	Fast Roaming	Passpoint	802.11u				
Hide SSID				Disabled Enabled				
VLAN ID 1								
Band Steering				Disabled Enabled				
Duplicate AUTH r	received		D	isconnect Ignore				
Association Adve	ertisement			Disabled Enabled				
Passpoint				Disabled Enabled				
Proxy ARP				Disabled Enabled				
DTIM Period								
Basic Set	ttings	Friend	lly name is required.	Cancel Save				

Configuring Passpoint

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

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

Edit Network - Advanced Settings							
General	Security	Fast Roaming	Passpoint	802.11	u		
Downstream Grou	p-Addressed Forwa	rding (DGAF)		Disabled	Enabled		
Layer 2 Traffic (L2	TIF)			Disabled	Enabled		
Operator Informati	ion		Allie	ed Telesis : e	ng 🔨		
Friendly Name Allied Teles	sis	Language Co eng	ode		<u>Delete</u>		
+ Add Operat	tor Information						
< Basic Sett	lings	Homogeneous ESS io	dentifier is required.	Cancel	Save		

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**

Edit Network - Basic Settings	x
SSID	
wnet1	
Description (Optional)	
Enter description	
Status Normal	^
Normal	*
Emergency	v
Trigger None	~
Security WPA Personal	~

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

New Profile -	Basic Settings	
General	Channel Blanket	Smart Connect
Name Enter Profile i	name	
Model		AT-TQ5403
Country		United States
Radio 1		wnet10, emergency
		Enabled Disa
wnet1		Channel Blanket OFF
wnet10		Channel Blanket OFF 🛑
wnet20		Channel Blanket OFF
emergenc	Emergency	Channel Blanket OFF
wnet30		Channel Blanket OFF
Radio 2		Disabled

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

A	Dashboard		N.A. 11. 1	Monitoring				Emergency Off		
*	Wizard	~	Monitoring					0 Trigger Active Configure		
ତ	Vista Manager mini		Manitoring and Configuration: allows you to a	on the status of wirelass /	Do and connected alien	to				
3	< Network MAP		You can easily monitor APs that may be unau	thorized or in a failure sta	te, schedule instant or de	elayed updates of config	juration or firmw	are, or reboot any devi	ce.	
	🗢 Wireless		Tree view	Access Points	Channel Blanket	Smart Connect	Clients	Neighbor APs	Tasks	
	Wireless Setup		AR4050S -							
			🗆 🚔 Channel Blanket Prof	Search	Last Upd	ate: 2021-12-10 10:54:4	4 am	an Apply Config	3 Reboot	
	AWC Managemer	ıt	□ 奈 AP1 □ 奈 AP2	Name 🔨	Status 🔨	Client 🔨	Model 🔨	FW Version	∧ Uptime ∧	

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 preprepared 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.

Wireless Setup					on 🛑	
Wireless Setup: enable wireless management and set a management IP addre	ess to get started.					
Use Auto-Setup to automatically discover and set up your access points.						
Atternatively, use the Networks and Access Points tabs to manually set up n When you use "WPA-Enterprise", "OSEN" or "Captive Portal", please configure	AAA to specify RADIUS Server.					
Start Networks Access Points MAC Filter						
Filter for Network	3 Networks	2 Triggers	🗘 Refresh	+ Add Network	+ Add Trigge	
Network List Trigger List						
Description						
Test				✓ Ec	dit 🔋 Delete	
trigger1				🖌 Ed	iit 🔋 Delete	

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

New Trigger	×
Description trigger2	
	Cancel Save

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

Start	Networks	Access Points	MAC Filter					
Filter fo	r Network			3 Networks	2 Triggers	🗘 Refresh	+ Add Network	+ Add Trigger
Network	List Trigg	ger List						
Descripti	DN							
trigger1							🖉 Ec	lit 🛢 Delete
trigger2							✓ Ec	iit 🔋 Delete

Set up the trigger for the network

1. Click + Add Network.

Start	Networks	Access Points	MAC Filter			
Filter f	or Network			3 Networks	2 Triggers 🗘 Refresh +	Add Network + Add Trigger
Network	c List Trigg	ger List				
SSID		Description	Security	Status	Trigger	
wnet1			WPA Personal	Configurable		🖍 Edit 🗯 Delete
MyNetwo	ork		WPA Personal	Configurable		🖍 Edit 🛢 Delete
AWC		awc-network	WPA Personal	Configurable		🖌 Edit 🔋 Delete

- 2. Enter the **SSID** and optional description.
- 3. Select the Trigger.

New Network - Basic Settings	×
wnet2	
Description (Optional)	
Enter description	
Status Normal	~
Trigger None	L _{îm}
None	
trigger1	
trigger2	-
Security None	~
Advanced Settings > Cancel	Save

- 4. Click Save.
- 5. The **Network List** is updated.

Start	Networks	Access Points	MAC Filter					
Filter for	Network			4 Netw	vorks 2 Triggers	🗘 Refresh	+ Add Network	+ Add Trigger
Network L	ist Trigg	ger List						
SSID		Description	Security	Status	1	Trigger		
wnet1			WPA Personal	🕑 Configurat	ble		🖍 Ed	it 🛡 Delete
MyNetwork			WPA Personal	🕗 Configurat	le		🖌 Ed	it 🔋 Delete
AWC		awc-network	WPA Personal	🕑 Configurat	ble		🖍 Ed	it 🛢 Delete
wnet2			None	Configurat	ile t	trigger2	🖍 Ed	it 🛢 Delete
L								

Assign network with trigger to VAP

- 1. Select Wireless > Wireless Setup > Access Points
- 2. Click +Add Profile.

Wire	less Se	tup						ON 🛑			
Wireless Setu Use Auto-Set Alternatively, When you us	Vireless Setup: enable wireless management and set a management IP address to get started. Use Auto-Setup to automatically discover and set up your access points. Alternatively, use the 'Networks' and 'Access Points' tabs to manually set up new networks, profiles and access. When you use "WPA-Enterprise", "OSEN" or 'Captive Portal", please configure [AAA] to specify RADIUS Server.										
Start	Networks	Access Points	MAC Filter								
Filter fo	Filter for Access Points Status 4 Profiles 1 SC Profile C Refresh + Add Profile + Add Smart Connect Profile							ile + Add Access Point			
Profiles	Profiles Smart Connect Profiles										

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

New Profile - Basic Settings		×
General Channel Blanket	Smart Connect	
Name Enter Profile name		
Model	AT-TQ5403	~
Country	United States	~
Radio 1	Disabled	^
	Enabled Disa	bled
wnet1	Channel Blanket OFF	
wnet2 Trigger	Channel Blanket OFF	
wnet3 Emergency Trigger	Channel Blanket OFF	
wnet4 (Trigger)	Channel Blanket OFF	v
Radio 2	Disabled	~
Radio 3	Disabled	~
LAN 2 Port Configuration	Disable Static LAG Case	cade
MAC Filter	None	~
Virtual IP address for Captive Portal Enter IP address		
Advanced Settings > S	elect non triggered network first. Cancel	pply

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.

Monitoring						\langle	Emergency Off
Monitoring and Configuration: allows you to see the You can easily monitor APs that may be unauthorize	status of wireless APs a d or in a failure state, so	and connected clients. chedule instant or delaye	d updates of configur	ation or firmware, o	r reboot any dev	ice.	
Tree view	Access Points	Channel Blanket	Smart Connect	Clients	Neighbor APs	Tasks	
□ AT-SBX908 GEN2 -	Search		Last Update: 2021-	-04-30 4:23:39 pm	🗘 Refresh	Apply Config	S Reboot Update Firmware
	□ Name ヘ	Status 🔨	Client ^	Model	^	FW Version 🔺	Uptime 🔨

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

Trigger Management	×
trigger1	Deactivate Activate
trigger2 Activated by: manager Activated time: 4/30/2021, 4:05:35 PM	Deactivate Activate
	Cancel

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

	Allied Telesis	SBx908 GEN2		NZTA-Nth-swi-Core1	Up time: 0 days 03:23	Admin Save
# 4	Dashboard Vista Manager mini	Wireless	s Setup			ON
	Network MAP Wireless ^	Wireless Setup: enabl After that, use the 'Ne	e wireless management and set tworks' and 'Access Points' tabs	a management IP address to get started. s to manually set up new networks, profiles and acce	SS.	
	Wireless Setup Monitoring AWC Management	Start Netw	vorks Access Points	MAC Filter 4 Networks	2 Triggers + Add I	Network + Add Trigger
	AMF Security mini	Network List	Trigger List			
(Network Infrastructure A	wnet1	wPA Persor	Status	Trigger	✓ Edit ■ Delete
https:/	VLAN Static Routing /10.37.227.4	wnet2	OSEN		trigger1	✓ Edit ■ Delete

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.

Monitoring	Emergency Off										
Monitoring and Configuration: allows you to see the status of wireless APs and connected clients. You can easily monitor APs that may be unauthorized or in a failure state, schedule instant or delayed updates of configuration or firmware, or reboot any device.											
Tree view	Access Points	Channel Blanket	Smart Connect	Clients Neig	hbor APs Tasks						
AT-x930-52GPX —	Search										
Profile AWC AP1	La:	st Update: 2022-09-07 4:32	2:29 pm 🗘 Refresh	SApply Config 5 Rebo	ot Update Firmware	Technical Support Informati	on				
□	Name ^	Status ^	Client ^	Model ^	FW Version A	Uptime 🔨					
	AP1	Failed	0	AT-TQ5403	5.0.0.B11	0s	~				
	AP2	Failed	0	AT-TQ5403 5.0.0.B11		0s					

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

Tree view	Access Po	oints Ch	annel Blanket	Sn	nart Connect	Clie	ents	Neighbo	r APs	Tasks			
AT-x930-52GPX –	Search												
 ♀ AP1 ♀ AP2 	Name	Last Updat	te: 2022-09-07 Status ^	4:32:29 pm C	lient ^	Apply	Model A	Reboot	FW V	ersion 🛧	Technic	uptime 🔨	ition
	AP1	ial Number	Failed	-	0		AT-TQ5403		5.0.0.8	311	0:	s >	, în
	MA	C Address		001a.ebcb.05e0 Joined		IP Address		10.34.180.2		200			
	Mar	nagement State	us				Configure Status		Modified				
	Rad	dio		Radio1	Radio2	Radio3				Radio1	Radio2	Radio3	
	Cha	annel/Power		-/-	-/-	-/-	Client			0	0	0	
	AP2		Failed		0		AT-TQ5403		5.0.0.8	311	0:	s 🔫	^
	Seri	ial Number		-									
	MAG	C Address		001a.ebcb	.0540		IP Addres	ss		10.34.180.	201		
	Mar	nagement State	us	Joined			Configure	e Status		Modified			
	Rad	lio		Radio1	Radio2	Radio3				Radio1	Radio2	Radio3	
	Cha	annel/Power		-/-	-/-	-/-	Client			0	0	0	

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.

Tree view	Acc	ess Points	Channel Blank	et S	mart Connec	t Cl	lients	Neighbo	or APs	Tasks			
☑ AT-x930-52GPX —	Sear	ch											
Profile AWC		Last	Update: 2022-09-0)7 4: 02:29 p	m 🗘 Refres	sh 🙎 App	ly Config	👌 Reboot	L Update	e Firmware	🕢 Technic	al Support Informa	tion
AP2		Name 🔨	Status 🔨	Client ^			Model A		FW Version 🔿		Uptime 🔨		
		AP1	Failed		0		AT-TQ5	403	5.0.0.B	11	0s		^
		Serial Numbe	er	-									
		MAC Address	S	001a.ebc	b.05e0		IP Ad	dress		10.34.180.	200		
		Management	t Status	Joined			Confi	gure Status		Modified			
		Radio		Radio1	Radio2	Radio3				Radio1	Radio2	Radio3	
		Channel/Pow	/er	-/-	-/-	-/-	Client	t		0	0	0	
		AP2	Failed		0		AT-TQ5	403	5.0.0.B	11	05	\$	~
For example, you can schedule a firmware upgrade for a specific date and time:

Update Firmware		×
Are you sure you want to procede with The Access Point will automatically re	h the firmware update on the selecter eboot after the firmware update.	d Access Point?
Select firmware	This field i	is required.
Name	Modified	Size
gui-userdata	2019-05-09 12:49	
When	Uŗ	odate later 🗸 🗸
2021-12-07	 ▲ ▲ ● ●]
	December 7,	2021 7:52:42 AM

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:

Monitoring						Emergency 1 USB Key 0 Trigger	off O III y registered t USB Key Active Configure
Monitoring and Configuration: allows you to see the status of wireless APs and connected clients. You can easily monitor APs that may be unauthorized or in a failure state, schedule instant or delayed updates of configuration or firmware, or reboot any device.							
Tree view	Access Points	Channel Blanket	Smart Connect	Clients	Neighbor APs	Tasks	
AR4050S —	Search	MAC Address	Associated AP		NetBIOS A	Last Update: 2022-0	09-07 4:29:32 pm 🗘 View

APs tab

Neighbor 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.

Monitoring							Emergency Off
Monitoring and Configuration: allows you to see the s You can easily monitor APs that may be unauthorized	tatus of wireless APs a I or in a failure state, sc	and connected clients. hedule instant or delaye	ed updates of configurat	ion or firmware	, or reboot any dev	ice.	
Tree view	Access Points	Channel Blanket	Smart Connect	Clients	Neighbor APs	Tasks	
AT-x930-52GPX Profile AWC Profile AW1 AP1 P2	BSSID ^	ssid ^		হু Sign	al A	Last Updat	:e: 2022-09-07 4:32:29 pm ♀ View Detected time ^

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.

Monitoring						Emergency Off
Monitoring and Configuration: allows you to see the You can easily monitor APs that may be unauthority	ne status of wireless APs zed or in a failure state,	s and connected clients. schedule instant or delay	ed updates of config	uration or firmv	vare, or reboot any dev	vice.
Tree view	Access Points	Channel Blanket	Smart Connect	Clients	Neighbor APs	Tasks
AT-x930-52GPX —	AWC				Last Upo	date: 2022-09-07 4:32:29 pm 🗘 Refresh
	Task 🔿	Run	Next Run	^		
- • / / / /	AWC Apply	Everyday 03:00	2022-09-0	07 03:00		
	AWC Calculation	Everyday 15:00	2022-09-0	07 15:00		

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).

AWC Manag	jement	
Autonomous Wave Control (AW superior user experience.	C) uses wireless intelligence to constantly model AP location and signal strength information. It then automatically optimizes wireless output	t and channel selection, for a
AWC Management: allows you t AWC calculation at any time.	o change the default setting of 3:00pm for calculating optimal wireless settings, and 3:00am for applying the new settings to the APs. You ca	n also manually start a new
AWC Apply		Apply Now
Last Apply	Not run	
Next Apply	2019-11-04 03:00(UTC+00:00) / 2019-11-04 16:00(NZDT+13:00)	Edit Apply Task
AWC Calculation		Calculate Now
Last Calculation	2019-11-03 15:00(UTC+00:00) / 2019-11-04 04:00(NZDT+13:00)	~
Next Calculation	2019-11-04 15:00(UTC+00:00) / 2019-11-05 04:00(NZDT+13:00)	Edit Calculation Task

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.

AWC Apply		Apply Now
Last Apply	Not run	
Next Apply	2021-12-07 04:00(UTC+00:00) / 2021-12-07 17:00(NZDT+13:00)	Edit Apply Task

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

AWC Apply		×
Condition	Enable	~
Interval	Everyday	~
04 : 00 AM	04:00 AM(UTC)
	Su	bmit

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:

AWC Calculation		Calculate Now
Last Calculation	Not run	~
Next Calculation	2021-12-07 15:00(UTC+00:00) / 2021-12-08 04:00(NZDT+13:00)	✓ Edit Calculation Task

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.

Allied Telesis	x550-18XSQ								x550-18X5Q-Master	Up time: 12 days 21:54	1 manager	B Save
Deshboard Visla Manager mini	Monitoring 2 Tinggers Actin								afgare .			
Network Intrastructure Network Services User Management	sentoring with Carling and Carling and Carling and the model of the state of workers APs and connected clients.											
System ~	Tere we □ \$1000 H000 = □ \$1000 H000 =	Access Points Search Aname A TO 5403,1 TO 5403,2 TO 5403,2 TO 5403,2 TO 5403,2 TO 5403,4 TO 5403,2 TO 5403,4 TO 5403,2 TO 540,	Channel Blanket	Status ~ Managed Managed Managed Managed Discovering	Cilents P	Client APs 0 0 0 0 0 0	Tasks	Lest Update: 2022 01-05 1-20.00 pm Model A A 71 05403 A 71 705403 A 71 705403 A 71 705403 A 71 705403 A 71 705403 A 71 705403 -	Image: Second	C Lipscold Friendard Image: C Lipscold Friendard Uptime ^ 12d 2h 14m 12d 2h 14m 12d 2h 14m 12d 3h 14m 12d 3h 14m 12d 3h 14m 12d 3h 14m 12d 3h 14m 12d 3h 14m	nical Gapport Inform	
		1 Che	ck option	al checkb	oxes							

3. Select the download **Destination**.

4. Click **Download** to continue.

Technical Support Information	
- Jownload of technical support information from APs that you have selected will be started by clicking "Download" button. It includes following information about your devices.	
the 802.1x authentication log: This contains the user ID. It does not contain the password.	
the device information and connection log: This contains the IP address and MAC address. It does not contain the password or authentication key.	
Ne use this technical support information only for troubleshooting purposes.	
Ne value and protect your privacy and data in accordance with our privacy policy.	
Agree to collect technical support information	
Oestination Flash	~
Cancel Downloa	d



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

Technical Support Information			
Completed			
100%			
Download technical support information You can download the technical support information also on the 'File Manag	ement" page.		
/fs/usb/2022-02-18_16-07-55			
Name	Size	Action	
tech-support-AT-TQ5403-IP192.168.10.102-T2022	565265	5 Download	^
tech-support-AT-TQ5403-IP192.168.10.103-T2022	571843	Download	
tech-support-AT-TQ5403-IP192.168.10.104-T2022	660448	Download	
tech-support-AT-TQ5403-IP192.168.10.105-T2022	657205	Download	Ŧ

C613-22121-00 REV N

🔨 🖉 Allied Telesis

 North America Headquarters
 19800 North Creek Parkway
 Suite 100
 Bothell
 WA 98011
 USA
 T: +1
 +1
 425
 481
 3895

 Asia-Pacific Headquarters
 11
 Tai Seng Link
 Singapore
 534182
 T: +65
 6383
 3830

 EMEA & CSA Operations
 Incheonweg 7
 1437
 EK Rozenburg
 The Netherlands
 T: +31
 20
 7950020
 F: +31
 20
 7950021

alliedtelesis.com

© 2023 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.

NETWORK SMARTER