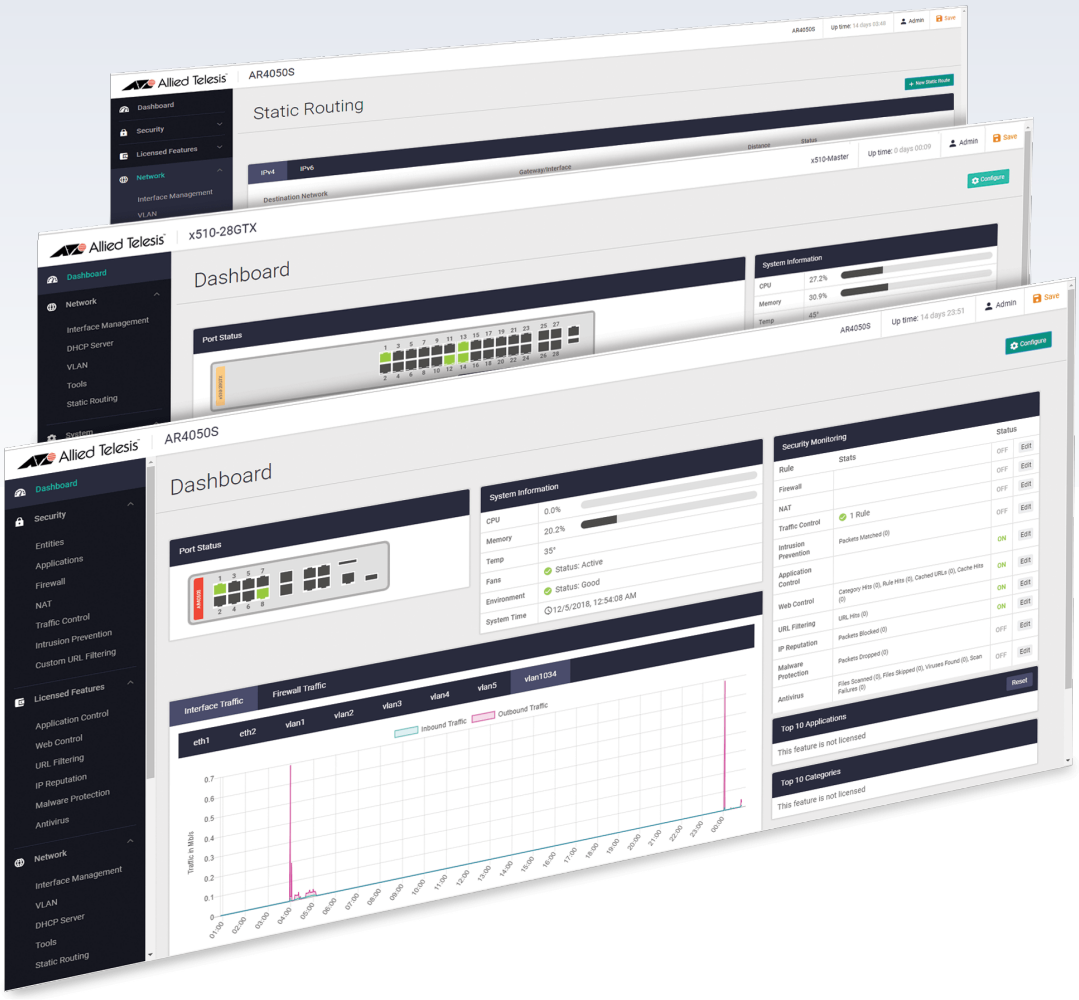
Release Note for Web-based Device GUI Version 2.20.x



» 2.20.0

AlliedWare Plus OPERATING SYSTEM

Acknowledgments

Getting the most from this Release Note

To get the best from this release note, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from **www.adobe.com/**

Contents

What's New in Version 2.20.0

Product families supported by this version:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 Series
x220 Series
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series[1]
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
ARX200S-GTX
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR2050V[2]
AR2010V[2]
AR1050V
TQ7403-R
TQ6702 GEN2-R

1. Not available in all regions
2. Does not support all of the latest features

Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.20.0. You can run 2.20.0 with AlliedWare Plus firmware versions 5.5.5-x.x, 5.5.4-x.x, or 5.5.3-x.x on your device, although the latest GUI features may only be supported with the latest firmware version.

For information on accessing and updating the Device GUI, see "Accessing and Updating the Web-based GUI" on page 21.

The following table lists model names that support this version:

Table 1: Models and software file names

Models	Family
AMF Plus Cloud	
SBx81CFC960	SBx8100
SBx908 GEN2	SBx908 GEN2
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950

Table 1: Models and software file names (cont.)

Models	Family
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
x540L-28XTm x540L-28XS	x540L
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330
x320-10GH x320-11GPT	x320
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250
x240-10GTXm x240-10GHXm x240-26GHXm	x240
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L
x220-28GS x220-52GT x220-52GP	x220
IE360-12GTX IE360-12GHX	IE360
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340
IE220-6GHX IE220-10GHX	IE220
IE210L-10GP IE210L-18GP	IE210L

Table 1: Models and software file names (cont.)

Models	Family
SE540L-28XTm SE540L-28XS	SE540L
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250
SE240-10GTXm SE240-10GHXm	SE240
XS916MXT XS916MXS	XS900MX
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX
GS980EM/10H GS980EM/11PT	GS980EM
GS980M/52 GS980M/52PS	GS980M
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
AR4000S-Cloud	
ARX200S-GTX	ARX200S
10GbE UTM Firewall	
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls
AR1050V AR2050V[1] AR2010V[1]	AR-Series VPN routers
TQ7403-R	Wireless AP Router
TQ6702 GEN2-R	Wireless AP Router

1. Does not support all of the latest features

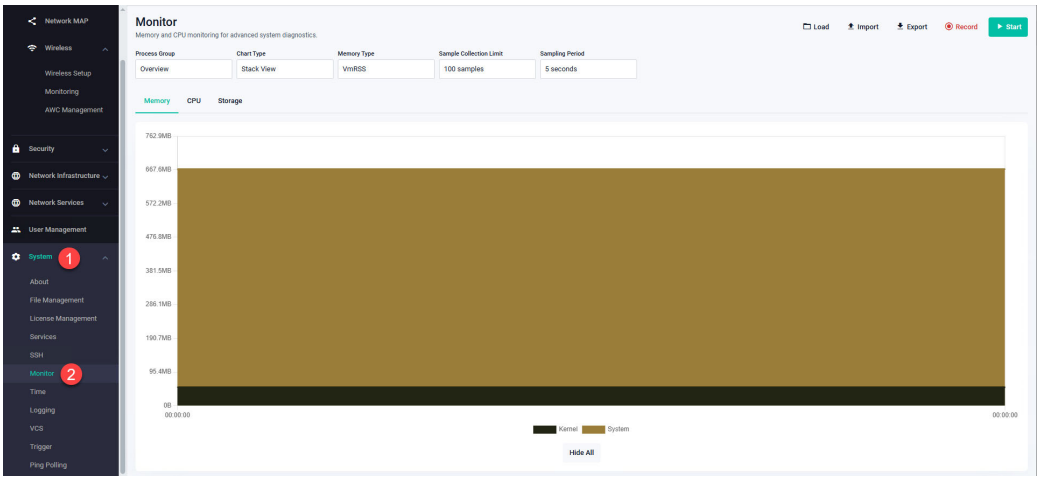
New Features and Enhancements

This section summarizes the new features in the Device GUI software version 2.20.0.

Process Monitor

From version 2.20.0 onwards, the Device GUI supports a Process Monitor to visualize usage statistics like CPU, memory, and storage I/O. This can help identify processes that are consuming more (or less) resources than expected.

To use the Process Monitor, go to **System** > **Monitor** in the left-hand menu.



GeoIP support in firewall entities

Applies to all UTM firewalls and VPN routers running AlliedWare Plus

From version 2.20.0 onwards, the GeoIP (Geographic IP) feature is supported.

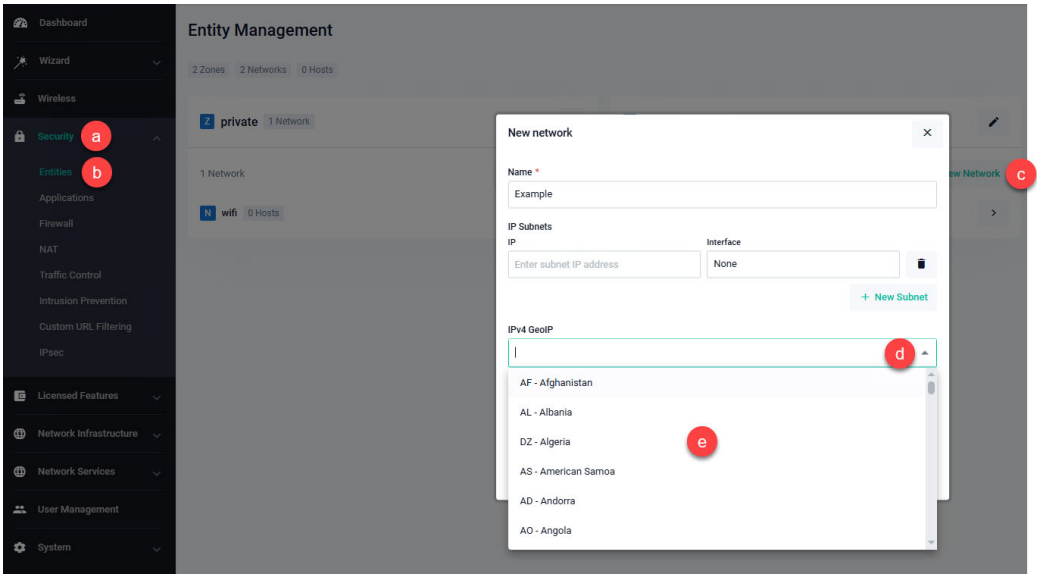
The GeoIP feature is a network security and traffic management tool. It uses IP address geolocation to identify the approximate geographic location of clients or servers by mapping IP address blocks to specific countries or regions.

GeoIP is widely used for purposes such as security, access control, and traffic optimization. For instance, it can restrict access to a service to only those with source IP addresses from a specific region. Similarly, it can block all traffic originating from regions known for frequent malicious or nuisance network activities.

The feature enables you to dynamically add all networks assigned to a specific country to an entity with a single command. These networks are sourced from a third-party provider and updated automatically on a regular basis.

GeoIP is a best-effort service designed to conveniently limit or block traffic based on expected sources or destinations. However, it does not guarantee that all traffic associated with these locations will be detected, nor does it prevent parties from obscuring their true location. Users are encouraged to utilize additional features, such as Advanced IPS, IP Reputation, and Web Categorization, to enhance protection against malicious activity.

To use GeoIP, go to **Security** > **Entities** in the left-hand menu, then select the desired country in the **New Network** or **Edit Network** dialog box.



RFScan Improvements on TQ-R Series

Available on: TQ6702 GEN2-R and TQ7403-R

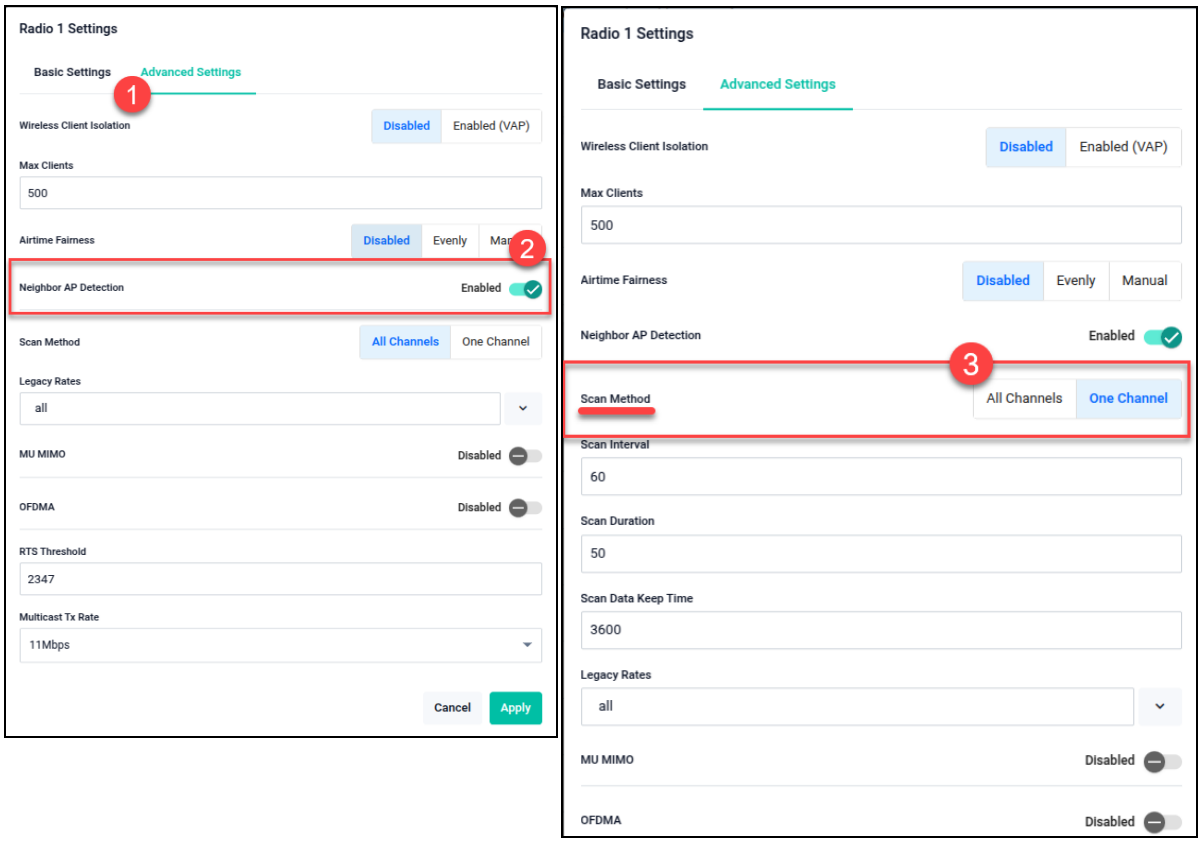
From version 2.20.0 onwards, RFScan functionality has been improved on TQ-R Series wireless AP routers. RFScan detects neighboring APs.

The previous method of scanning all channels on a radio simultaneously, which could lead to prolonged communication loss, has been replaced. You can now select between two scan methods:

- **All-Channel Scan**: Scans all channels at once (behavior similar to the initially improved 5 GHz, 4 channels at a time approach).
- **Single-Channel Scan**: Scans one channel at a time, allowing configuration of scan interval, duration, and data retention.

To configure these settings through the GUI:

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



Additional Proxy ARP option on TQ-R Series

Available on: TQ6702 GEN2-R and TQ7403-R

From version 2.20.0 onwards, TQ-R Series wireless AP routers have a new option to allow ARP packets from unknown addresses for Proxy ARP, rather than dropping the packets.

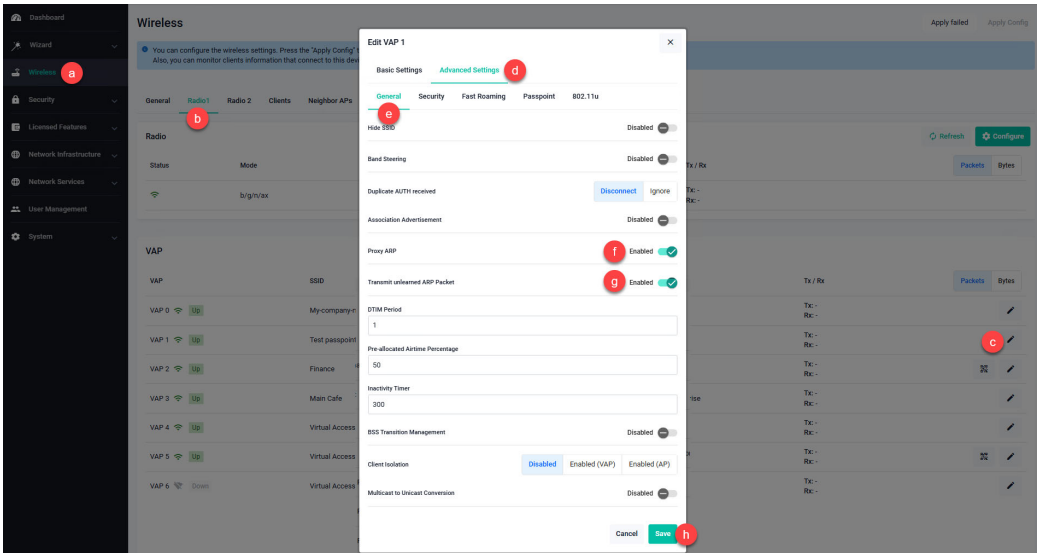
How it works

Some stations, such as IP phones, do not send packets for Proxy ARP learning. This means that the Proxy ARP drops any ARP packets that the TQ-R cannot respond to by proxy, which causes delayed IP resolution.

This feature implements an option to allow ARP packets from unknown addresses for Proxy ARP, rather than dropping them. This speeds up IP resolution for stations such as IP phones.

To configure this:

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



Vista Manager mini enhancements

Vista Manager mini uses Allied Telesis Autonomous Wave Control (AWC) for setting up and managing your wireless access points (APs). By minimizing coverage gaps and reducing AP interference, AWC automatically reconfigures access points to meet user demand.

For more information about Vista Manager mini, see the User Guide for Wireless management (AWC) with Vista Manager Mini.

Use Vista Manager mini to control TQ7403 Access Points

From version 2.20.0 onwards, you can use Vista Manager mini as a wireless controller to control TQ7403 access points.

Use Vista Manager mini on ARX200S-GTX to configure Channel Blanket

Available when managing APs that support Channel Blanket

From version 2.20.0 onwards, you can use Vista Manager mini on ARX200S-GTX to configure Channel Blanket.

Channel Blanket uses one wireless channel to create a single 'blanket' of wireless coverage. It solves some of the main challenges of Wi-Fi networks: co-channel and adjacent channel interference, and roaming.

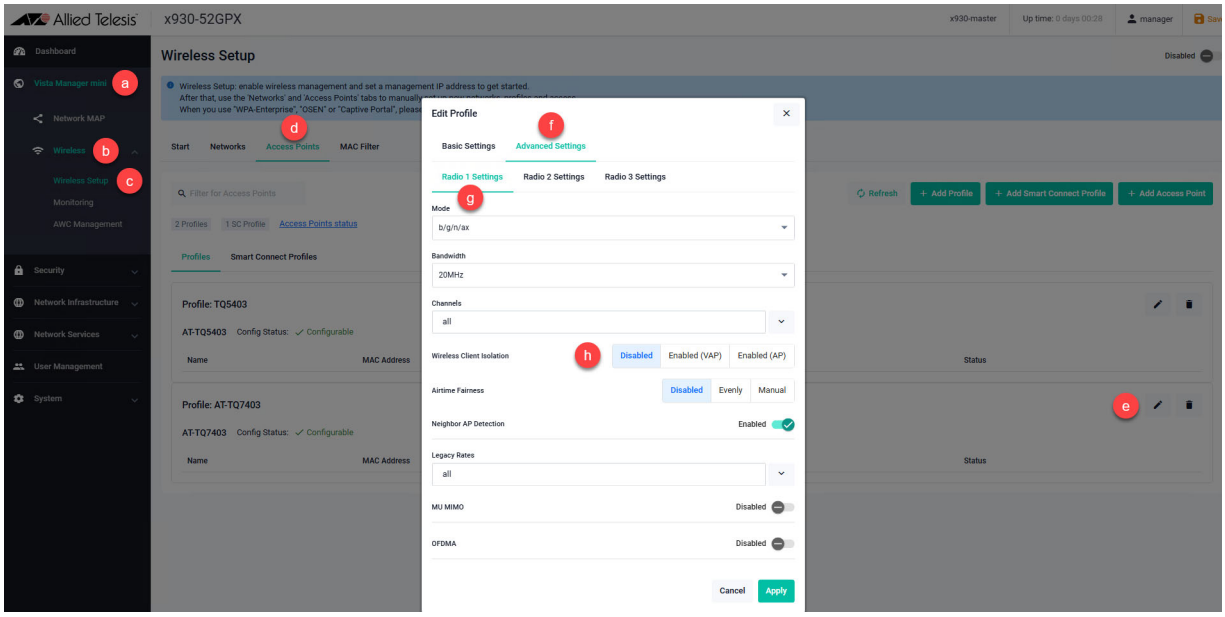
Wireless Client Isolation

Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2

From version 2.20.0 onwards, you can enable or disable client isolation per AP or per VAP. Per VAP client isolation blocks communication between wireless clients that connect to the same VAP.

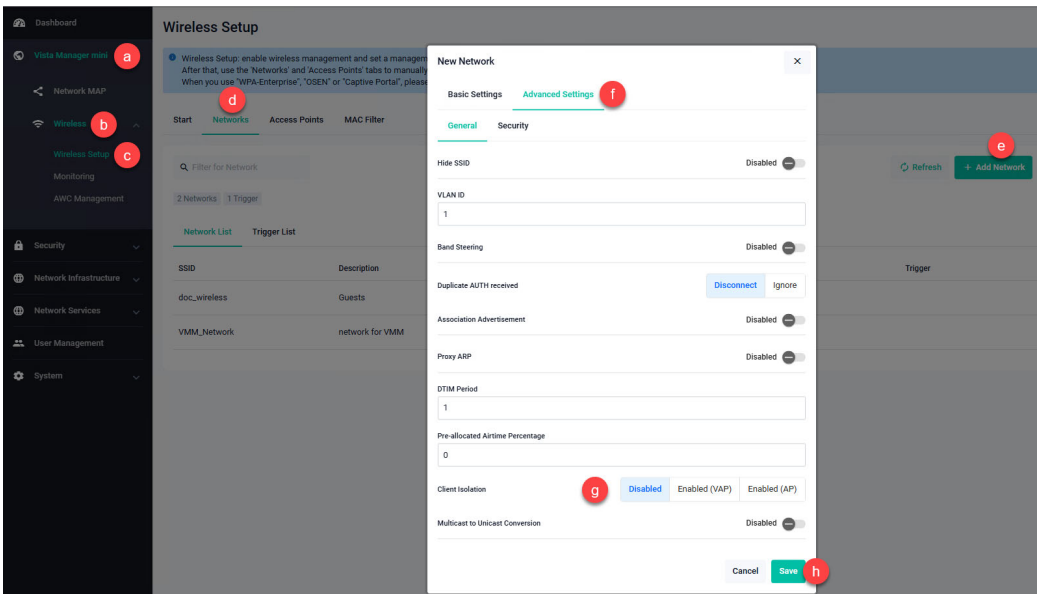
In AP Profile To set this in an AP Profile:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Access Points** and add or edit a profile.
3. Select **Advanced Settings** > **Radio X Settings** > **Wireless Client Isolation.**



In network To set this in a network:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Advanced Settings** > **General** > **Client Isolation**.



Airtime Fairness

Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2

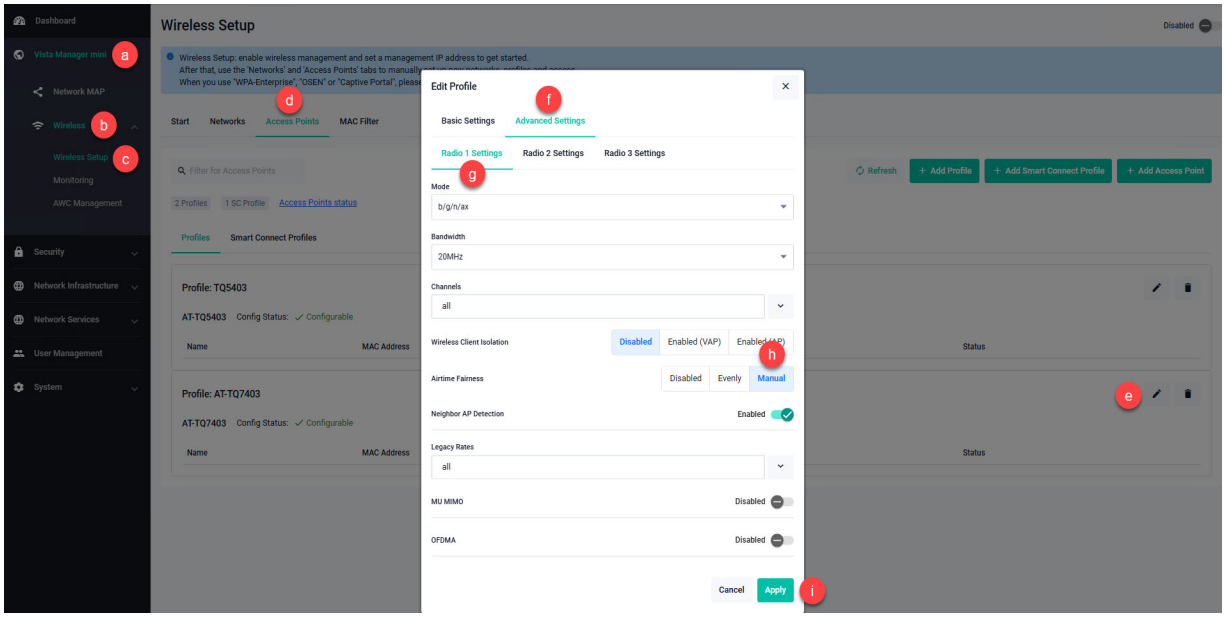
Airtime fairness ensures that all devices on a wireless network receive a fair share of the available airtime. This is particularly important in environments where devices with varying capabilities and data rates are connected to the same wireless access point.

From version 2.20.0 onwards, you can set the Airtime Fairness percentage manually in an AP Profile or a network.

In AP Profile

To set this in an AP Profile:

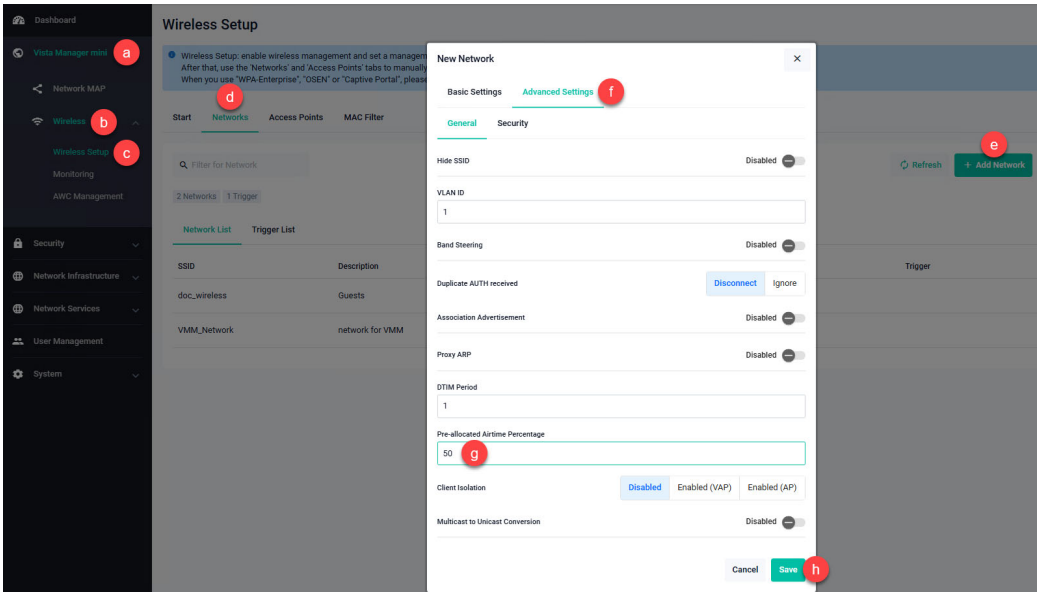
1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Access Points** and add or edit a profile.
3. Select **Advanced Settings** > **Radio X Settings** > **Airtime Fairness.**
4. Go to the VAP and specify the desired **Pre-allocated Airtime Percentage.**



In network

To set this in a network:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Advanced Settings** > **General** > **Pre-allocated Airtime Percentage**.



Removal of requirement to specify a basic rate

Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2

From version 2.20.0 onwards, you are no longer required to specify a basic rate for Radio 1, when you specify the legacy rates to use.

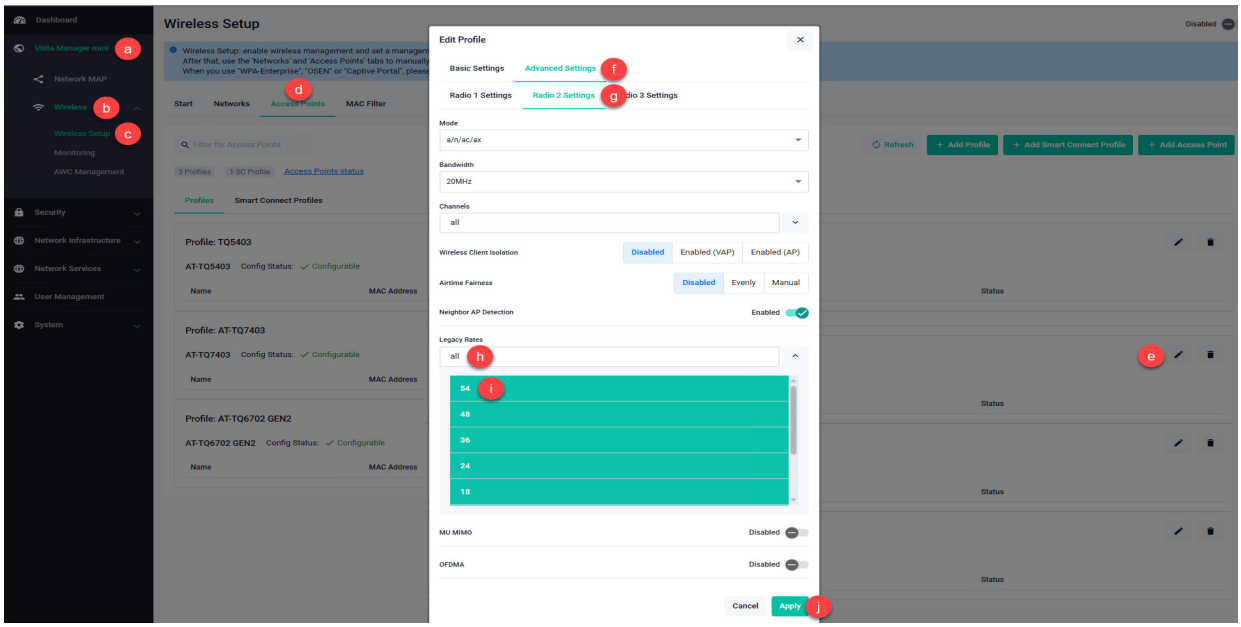
Basic rates are the most backward compatible rates in a Wi-Fi network - rates that will work with the oldest Wi-Fi standards. For 2.4Ghz, the basic rates are: 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps. For 5Ghz, the basic rates are: 6Mbps, 12Mbps, and 24Mbps.

The rates can be one or more of 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, or 1.

If none of the basic rates is specified, the device will use the lowest selected legacy rate as the basic rate. Note that the beacon frame and management frame must use this lowest rate.

To set the legacy rates:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Access Points** and add or edit a profile.
3. Select **Advanced Settings** > **Radio 1 Settings** > **Legacy Rates.**
4. Click on a rate to add or remove it.



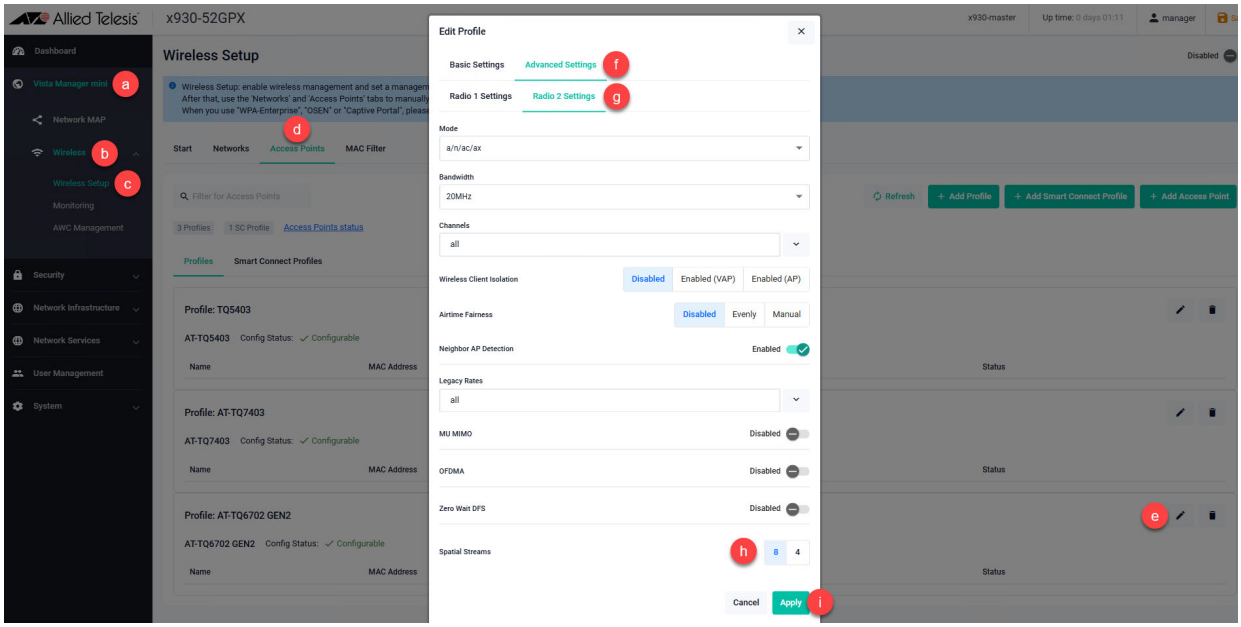
Reducing the number of spatial streams

Available when managing the following APs: TQ6702 GEN2, TQm6702 GEN2

From version 2.20.0 onwards, you can reduce the number of spatial streams from 8 to 4.

To change the number of spatial streams:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Access Points** and add or edit a profile.
3. Select **Advanced Settings** > **Radio 2 Settings** > **Spatial Streams.**



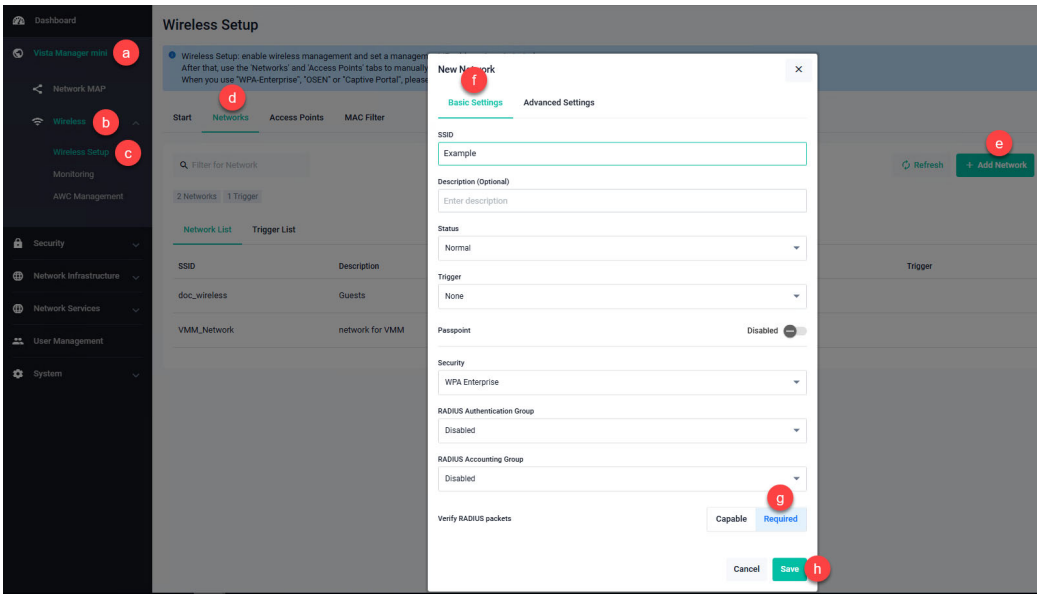
Verifying RADIUS Packets

Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2

From version 2.20.0 onwards, you can require verification of RADIUS packets. Verification can be set to **Required** on WPA Enterprise, Captive Portal, and MAC Authentication.

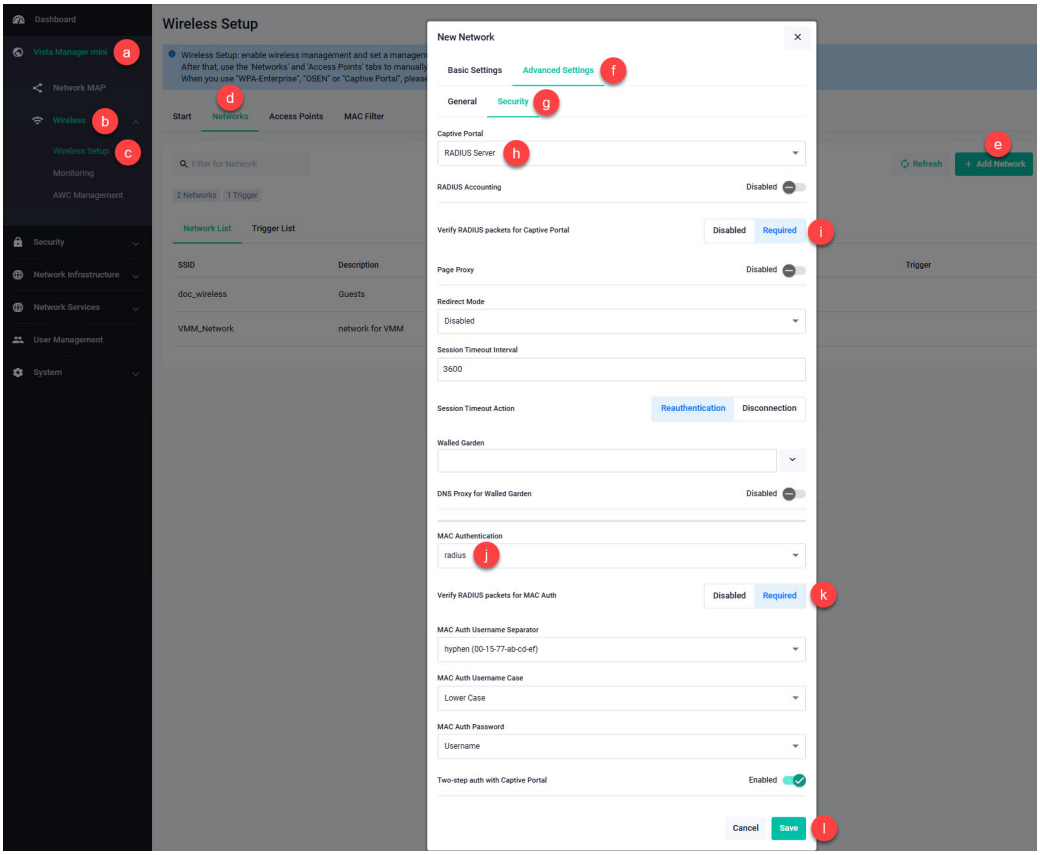
To set this for WPA Enterprise:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Basic Settings** > **Security.**
4. Choose **WPA Enterprise.**
5. Change **Verify RADIUS Packets** to **Required.**



To set this for Captive Portal or MAC Authentication:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Advanced Settings** > **Security.**
4. Choose the desired settings for Captive Portal or MAC Authentication. The Verify fields only appear after you have done this.
5. Change **Verify RADIUS Packets for Captive Portal** or **Verify RADIUS Packets for MAC Auth** to **Required.**



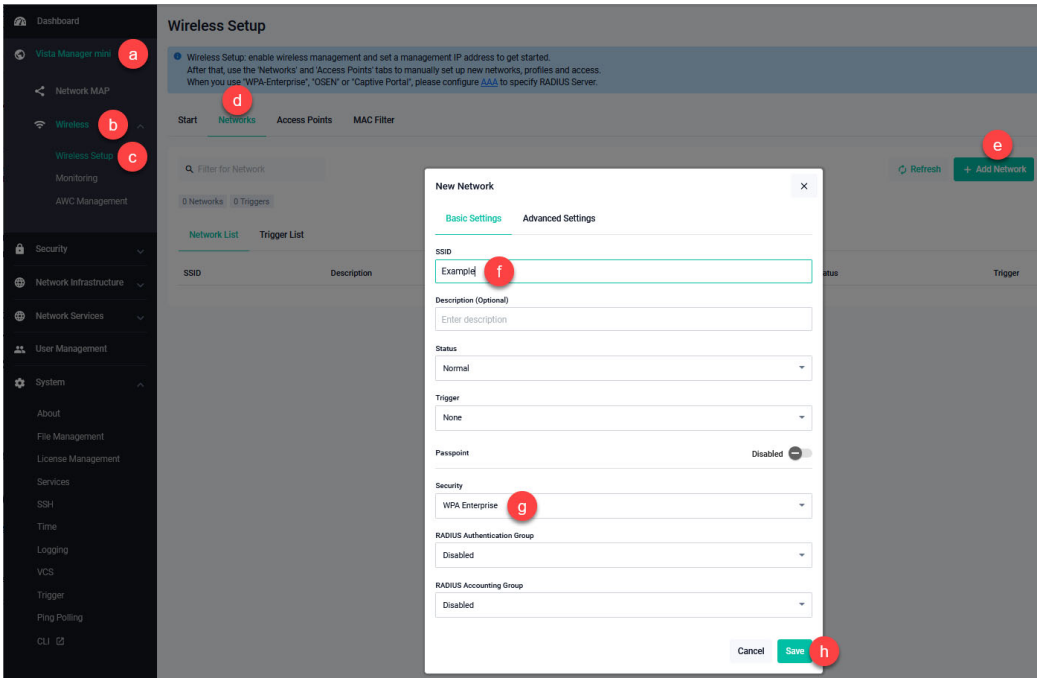
Support for CCMP cipher with WPA3 encryption

Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2

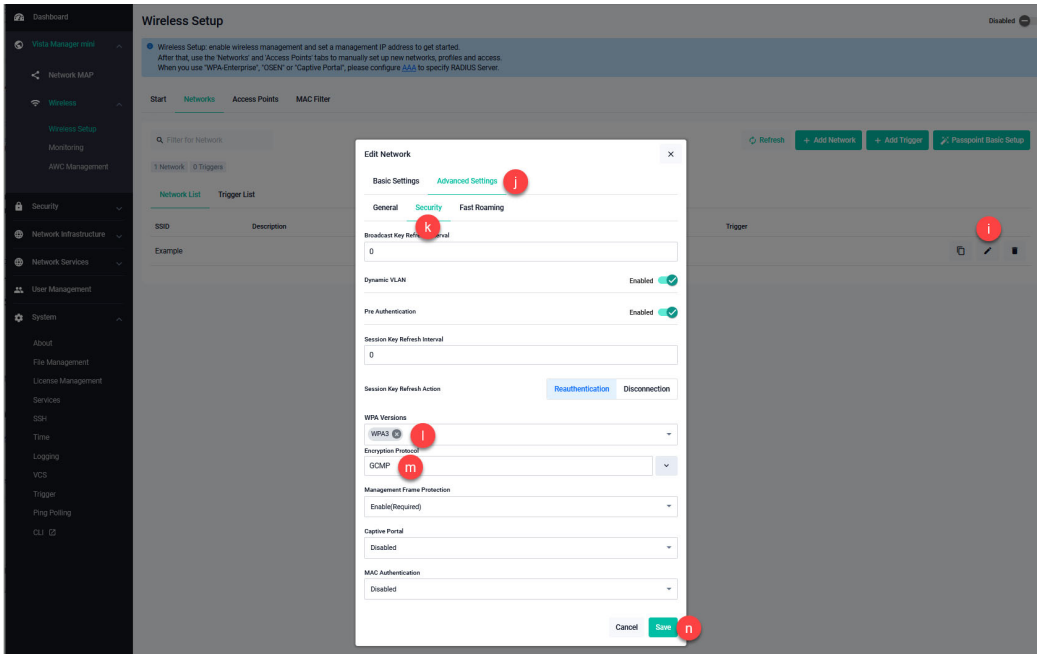
From version 2.20.0 onwards, the CCMP cipher is supported for WPA Enterprise version WPA3.

To select the cipher:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Basic Settings.**
4. Give it as SSID (if creating a new network) and choose **WPA Enterprise** under **Security.**
5. Save the network.



6. Edit the network.
7. Select **Advanced Settings** > **Security.**
8. Select the desired cipher in **Encryption Protocol.**



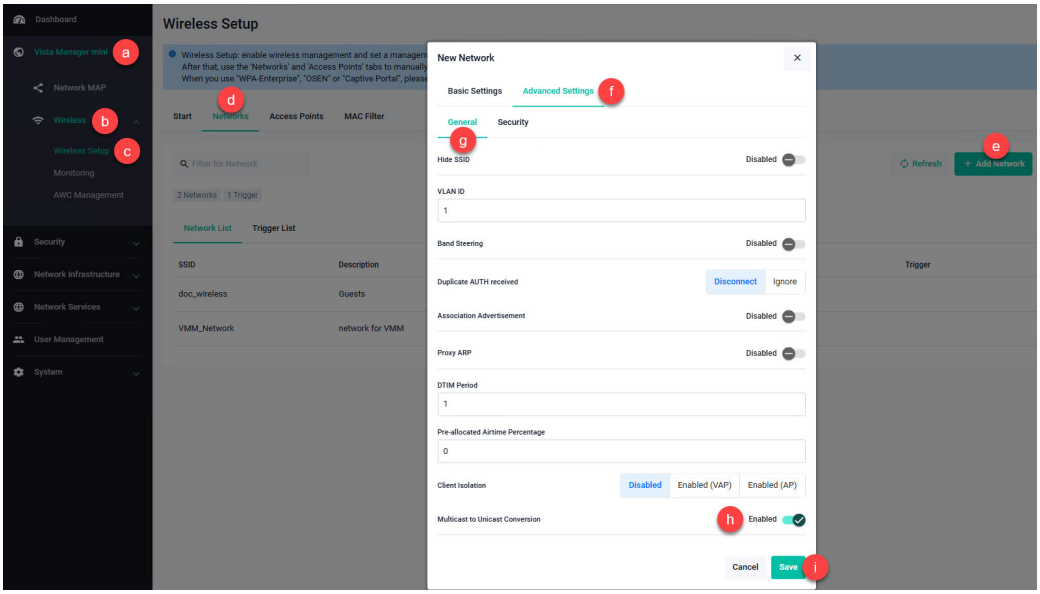
Multicast to Unicast conversion

Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2

From version 2.20.0 onwards, you can configure an Access Point to convert multicast packets into unicast packets destined for the client connected to the VAP. This conversion allows each client to receive data at the highest possible rate it supports.

To select Multicast to Unicast conversion:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Advanced Settings** > **General.**
4. Select **Multicast to Unicast Conversion.**



DNS Proxy for Walled Garden

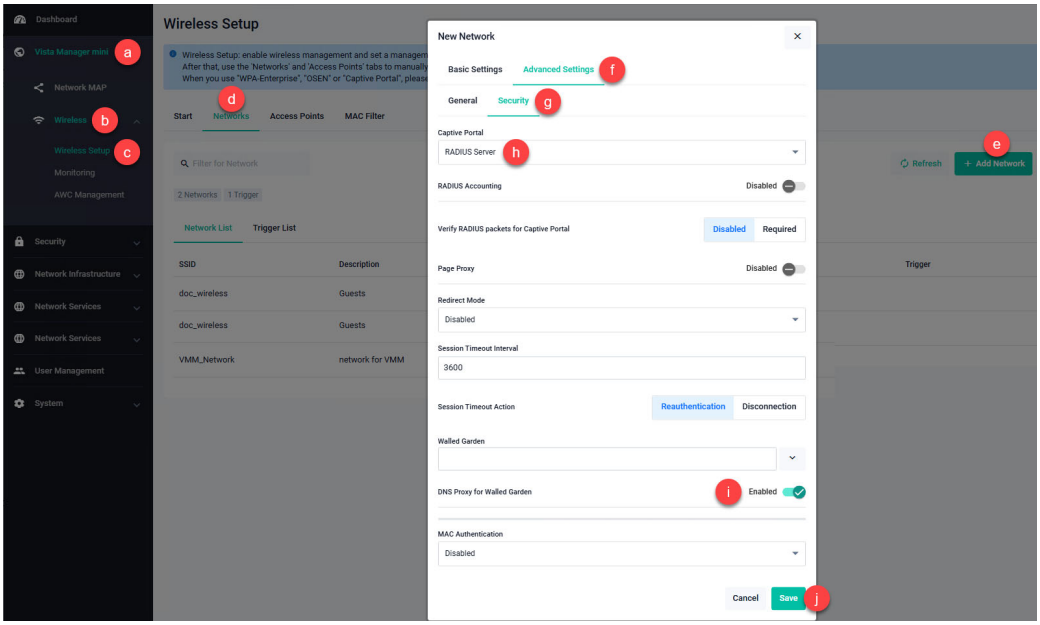
Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2

From version 2.20.0 onwards, you can configure DNS Proxy for a walled garden with Captive Portal. A walled garden limits clients to accessing only a selection of web pages.

To enable this:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Advanced Settings** > **Security.**
4. Under **Captive Portal,** choose **RADIUS Server** or **External Page Redirect**

5. Enable **DNS Proxy for Walled Garden**.



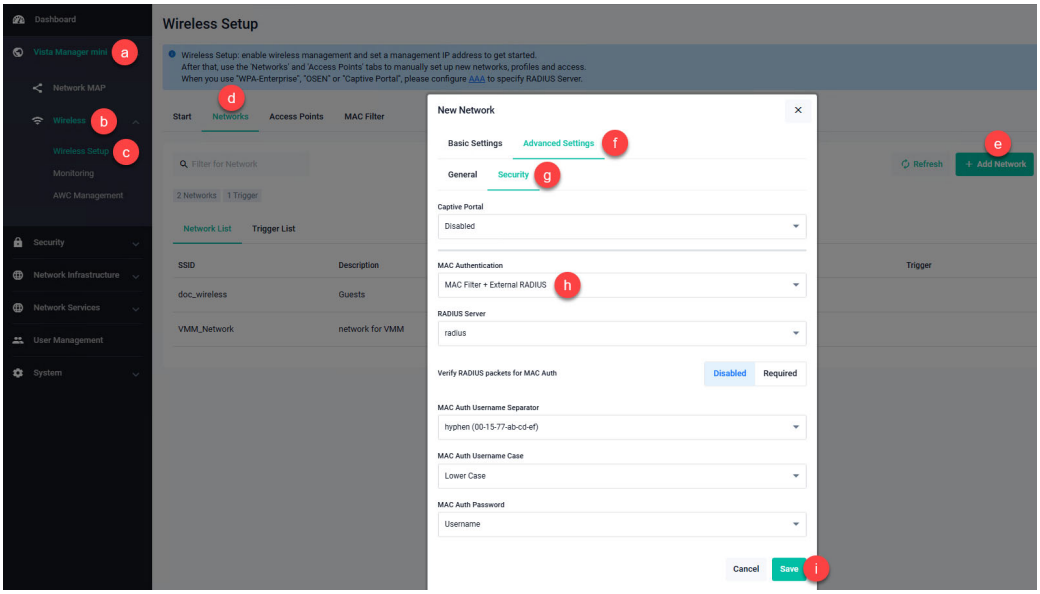
New option for MAC Authentication

Available when managing the following APs: TQ7403, TQ6702 GEN2, TQm6702 GEN2, TQ6702e GEN2, TQ6602 GEN2, TQm6602 GEN2, TQ5403, TQm5403, TQ5403e, TQ1402, TQm1402

From version 2.20.0 onwards, you can specify **External Radius + MAC Filter** as the method for MAC Authentication.

To select this:

1. Go to **Vista Manager mini > Wireless** > **Wireless Setup.**
2. Select **Networks** and add or edit a network.
3. Select **Advanced Settings** > **Security.**
4. Select **MAC Authentication.**
5. Select **External Radius + MAC Filter.**


Dashboard
Vista Manager mini
a
Network MAP
Wireless
b
Wireless Setup
c
Monitoring
AWC Management
Security
Network Infrastructure
Network Services
User Management
System
Wireless Setup
Wireless Setup: enable wireless management and set a management IP address to get started.
After that, 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
d
Networks
Access Points
MAC Filter
Filter for Network
2 Networks
1 Trigger
Network List
Trigger List
SSID
Description
doc_wireless
Guests
VMM_Network
network for VMM
Refresh
e
Add Network
Trigger
New Network
Basic Settings
Advanced Settings
f
General
Security
g
Captive Portal
Disabled
MAC Authentication
MAC Filter + External RADIUS
h
RADIUS Server
radius
Verify RADIUS packets for MAC Auth
Disabled
Required
MAC Auth Username Separator
hyphen (00-15-77-ab-cd-ef)
MAC Auth Username Case
Lower Case
MAC Auth Password
Username
Cancel
Save
i

Accessing and Updating the Web-based GUI

This section describes how to access the GUI, check the version, and update it.

Important Note: Very old browsers may not be able to access the Device GUI. From AlliedWare Plus version 5.5.2-2.1 onwards, to improve the security of the communication for the Device GUI, ciphersuites which use RSA or CBC based algorithms have been disabled, as they are no longer considered secure. Note that the removal of ciphersuites using those algorithms may prevent some old versions of browsers from communicating with the device using HTTPS.

Browse to the GUI

Perform the following steps to browse to the GUI.

1. If you haven't already, add an IP address to an interface. For example:

   ```
   awplus> enable
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)# ip address 192.168.1.1/24
   ```

   Alternatively, on unconfigured devices you can use the default address, which is:

   - on switches: 169.254.42.42
   - on AR-Series and TQ6702 GEN2-R: 192.168.1.1

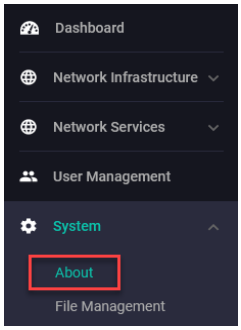
2. Open a web browser and browse to the IP address from step 1.

3. The GUI starts up and displays a login screen. Log in with your username and password. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the System > About page in the GUI and check the field called **GUI version**.

If you have an earlier version than 2.20.0, update it as described in "Update the GUI on switches" on page 22 or "Update the GUI on AR-Series devices" on page 23.



Update the GUI on switches

Perform the following steps through the Device GUI and command-line interface if you have been running an earlier version of the GUI and need to update it.

1. Obtain the GUI file from the Allied Telesis Support Portal.

   The filename for v2.20.0 of the GUI is:

   - awplus-gui_555_38.gui,
   - awplus-gui_554_38.gui, or
   - awplus-gui_553_38.gui

   Make sure that the version string in the filename (e.g. 555) matches the version of AlliedWare Plus running on the switch (e.g. 5.5.5-x.x). The file is not device-specific; the same file works on all devices.

2. Log into the GUI:

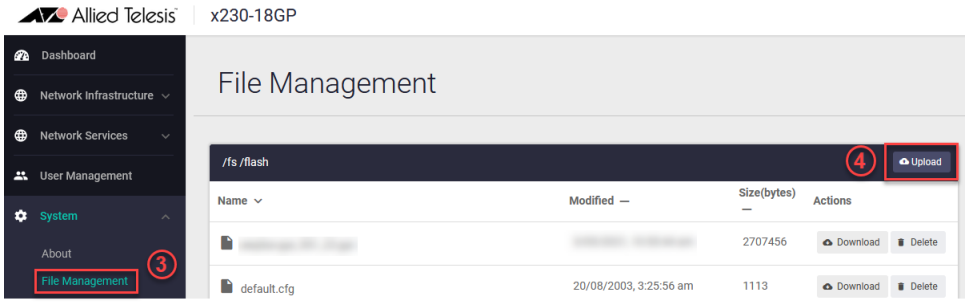
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   The GUI starts up and displays a login screen. Log in with your username and password.

   The default username is *manager* and the default password is *friend*.

3. Go to **System** > **File Management**

4. Click **Upload**.



5. Locate and select the GUI file you downloaded from our Software Download center. The new GUI file is added to the **File Management** window.

   You can delete older GUI files, but you do not have to.

6. Reboot the switch. Or alternatively, use a Serial console connection or SSH to access the CLI, then use the following commands to stop and restart the HTTP service:

   ```
   awplus> enable
   awplus# configure terminal
   awplus(config)# no service http
   awplus(config)# service http
   ```

   To confirm that the correct file is now in use, use the commands:

   ```
   awplus(config)# exit
   awplus# show http
   ```

Update the GUI on AR-Series devices

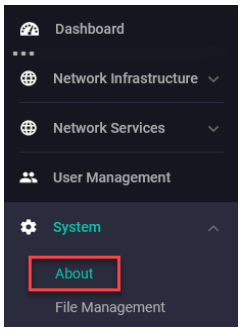
Prerequisite: On AR-Series devices, if the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

Perform the following steps if you have been running an earlier version of the GUI and need to update it.

1. Use a Serial console connection or SSH to access the CLI, then use the following commands to download the new GUI:

```
awplus> enable
awplus# update webgui now
```

2. Browse to the GUI and check that you have the latest version now, on the **System** > **About** page. You should have v2.20.0 or later.



Verifying the GUI File

On devices that support crypto secure mode, to ensure that the GUI file has not been corrupted or interfered with during download, you can verify the GUI file. To do this, enter Global Configuration mode and use the command:

```
awplus(config)#crypto verify gui <hash-value>
```

Where <*hash-value*> is the known correct hash of the file.

This command compares the SHA256 hash of the release file with the correct hash for the file.

The correct hash is listed in the table of Hash values below.

Caution

If the verification fails, the following error message will be generated:
"% Verification Failed"
In the case of verification failure, please delete the release file and contact Allied Telesis support.

If you want the device to re-verify the file when it boots up, add the **crypto verify** command to the boot configuration file.

Table: Hash values

Firmware Version	GUI File	Hash
5.5.5-x.x	awplus-gui_555_38.gui	b785918ca3acfa33afe8b16cc52adb27cfb281452e047fe6fb32f085eb2ff695
5.5.4-x.x	awplus-gui_554_38.gui	b785918ca3acfa33afe8b16cc52adb27cfb281452e047fe6fb32f085eb2ff695
5.5.3-x.x	awplus-gui_553_38.gui	b785918ca3acfa33afe8b16cc52adb27cfb281452e047fe6fb32f085eb2ff695