TQ6000 GEN2

WIRELESS ACCESS POINTS

TQ6702 GEN2
TQm6702 GEN2
802.11ax Dual-radio 5G/2.4GHz 8x8+4x4 Access Points

TQ6602 GEN2
TQm6602 GEN2
802.11ax Dual-radio 5G/2.4GHz 4x4+4x4 Access Points

6007

Management Software User's Guide

613-003026 Rev.D

Contents

List of Figures

List of Tables

Preface

This guide contains instructions on how to manage the features of the TQ6000 GEN2 access points with the web browser management interface. The models included in this manual are:

- TQ6702 GEN2
- TQm6702 GEN2
- TQ6602 GEN2
- TQm6602 GEN2

This preface contains the following sections:

Safety Symbols Used in this Document

This document uses the following conventions.

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Warning
Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Services & Support section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- Helpdesk (Support Portal) - Log onto Allied Telesis interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorizations (RMAs), and contact Allied Telesis technical experts.
- Software Downloads - Download the latest software releases for your product.
- Licensing - Register and obtain your License key to activate your product.
- Product Documents - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- Warranty - View a list of products to see if Allied Telesis warranty applies to the product you purchased and register your warranty.
- Allied Telesis Helpdesk - Contact a support representative.

To contact a sales representative or find Allied Telesis office locations, go to **www.alliedtelesis.com/contact**.

Chapter 1

Getting Started

Here are the sections in this chapter:

Features

Hardware features include:

- One 2.4GHz radio
- One 5GHz radio
- Internal omni-directional antennas
- Two 100/1000Mbps/2.5G/5G Ethernet ports with RJ-45 connectors
- PoE+ Class 4 powered device
- One Reset button for restoring the default settings
- One AC power adapter connector
- LEDs for 2.4GHz and 5GHz radios, LAN1 and LAN2 ports, and power
- Kensington lock port
- Ceiling, wall, or table installation
- Installing on the Cisco or Fortimet mounting brackets using BRKT-CONV-AP1 converter bracket
- One Console RS232 RJ-45 port for factory use only

Features of the 2.4GHz and 5GHz radios include:

- IEEE802.11a/b/g/n/ac/ax
- Automatic channel selection
- Band steering
- Wi-Fi multimedia (WMM) for prioritizing traffic

Features of system power and Power over Ethernet (PoE):

- PoE+ (IEEE 802.3at)
- Maximum power consumption: 22.03W
- Power saving mode: support IEEE802.3af when either 2.5G or 5G is disabled.
- Redundant power by AC adapter and PoE+ ports

Software features include:

- Flow control (IEEE 802.3x)
- VLAN tagging (IEEE 802.1Q)
- Link aggregation
- On-board web browser management interface
- Virtual access points (VAPs)

- ❒ Network Time Protocol (NTP) client
- ❒ Dynamic Host Control Protocol (DHCP) client
- ❒ WPA Personal and WPA Enterprise security
- ❒ WPA and WPA2 encryption: CCMP (AES) and TKIP
- ❒ WPA3 encryption CCMP (AES/CNSA)
- ❒ Quality of Service (QoS) ingress and egress queues
- ❒ Fast roaming (IEEE802.11v/k/r)
- ❒ MAC address client filtering with the on-board filter
- ❒ MAC address client filtering with RADIUS servers
- ❒ Wireless Distribution System (WDS) bridges (Only one-to-one WDS connection is supported.)
- ❒ Quick Response codes for VAPs
- ❒ System log
- ❒ Syslog client
- ❒ SNMPv1, v2c, and v3

Software features with Vista Manager EX and the Autonomous Wave Controller (AWC) plug-in include:

- ❒ AWC Lite
- ❒ Combination use with Cell, AWC-SC, and AMF-SEC
- ❒ Autonomous Management Framework (AMF) Guest node

Table 1 indicates the maximum supported numbers of features:

Table 1. Maximum Supported Numbers

Feature	Item	Maximum Number
VAP	Virtual wireless interfaces per RF interface	8
	ESSID	32
	VLAN ID	4,094
WDS	WDS links	1
	WDS HOPs	1
AWC	Access points managed by AWC	3,000
Client Authentication	MAC address list	2,048

Management Tools

The access points support the following management tools.

Web Browser

The access point has a web browser management interface for configuring the device from your management workstations. The web browser interface allows you to manage one unit at a time and supports both non-secure HTTP and secure HTTPS management sessions. The default is HTTP.

Note
The product has been tested with Microsoft Edge and Google Chrome.

Vista Manager EX and AWC Plug-in

The access point is supported with Vista Manager (version 3.9.0 or later) and the Autonomous Wave Control (AWC) plug-in. Configuring and monitoring large numbers of devices is simplified with AWC because you can add multiple devices to management groups and manage them as one unit. The application can also monitor the operations of the access points and automatically adjust operating properties to optimize the performance of your wireless network.

You cannot configure the following access point settings with Vista Manager EX and the AWC plug-in. These settings require the web browser interface:

- Hostname
- DHCP client or static IP address
- Domain Name Server name
- System date or time
- HTTP and HTTPS modes
- System name, location, and contact
- LLDP PoE negotiation
- Enable or disable the Reset button
- Management VLAN

SNMPv1, SNMPv2c, and SNMPv3

You can use SNMPv1, SNMPv2c, and SNMPv3 to view the parameter settings of the access point. The MIB is available from Allied Telesis website. For instructions on how to configure the access point for SNMP, see “Configuring SNMPv1, SNMPv2, and SNMPv3” on page 53.

Note
You cannot change the parameter settings on the access point with SNMP.

Starting the First Management Session

After you install and power on the access point, it queries the subnet on the LAN1 port for a DHCP server. If a DHCP server responds to its query, the unit uses the IP address the server assigns to it. If there is no DHCP server, the access point uses the default IP address.

The default IP address of the access point: **192.168.1.230**

If your network has a DHCP server, use the IP address that the server assigns to the access point to start the management session. For directions, see “Starting a Management Session” on page 21.

If your network does not have a DHCP server, you can start the first management session by establishing a connection between your computer and the unit.

Connecting the Access Point to a Computer

If you have an AC/DC adapter to supply power to the access point, you can connect your computer and access point directly with an Ethernet cable. This procedure requires changing the IP address on your computer to make it a member of the same subnet as the default IP address on the access point.

Connecting the Access Point to a Network

The first management session can also be performed while the device is connected to your network. However, If your network does not have a DHCP server, you still have to change the IP address of your computer to match the subnet of the default address of the access point. Furthermore, if your network is divided into virtual LANs (VLANs), you have to be sure to connect the access point and your computer to ports on an Ethernet switch that are members of the same VLAN.

The instructions for starting the first management session are found in the following sections:

- “Starting the First Management Session with a Direct Connection” on page 19.
- “Starting the First Management Session without a DHCP Server” on page 20

Starting the First Management Session with a Direct Connection

To start the management session with a direct Ethernet connection between your computer and the LAN1 port on the access point, perform the following procedure:

Note
If the access point uses PoE as a power source, you cannot perform this procedure because it requires a direct connection between your computer and the LAN1 port on the access point. This procedure works when you have the optional power supply for the access point. Without the optional power supply, perform “Starting the First Management Session without a DHCP Server” .

1. Connect one end of a network cable to the LAN1 port on the access point and the other end to the Ethernet network port on your computer.
2. Change the IP address on your computer to 192.168.1.*n*, where *n* is a number from 1 to 254, but not 230.

   See the documentation that accompanies your computer for instructions on how to set the IP address.
3. Set the subnet mask on your computer to 255.255.255.0.
4. Power on the access point.
5. Start the web browser on your computer.
6. Enter the IP address 192.168.1.230 in the URL field of the browser and press the Enter key.

   You should now see the login window, shown in Figure 1 on page 21.
7. Enter the user name and password.
   - ❒ User name: **manager**
   - ❒ Password: **friend**

   Note
   The user name and password are case-sensitive.
8. Click the Login button.

Starting the First Management Session without a DHCP Server

This procedure explains how to start the first management session on the access point when the LAN port is connected to an Ethernet switch on a network that does not have a DHCP server. To start the management session, perform the following procedure:

1. To use the PoE feature on the access point, be sure to connect the LAN port to a PoE source device.

2. Connect one end of network cable to the LAN port on the access point and the other end to a port on an Ethernet switch.

   If your network has VLANs, check to be sure that your computer and the access point are connected to ports on the Ethernet switch that are members of the same VLAN. This might require accessing the management software on the switch and listing the VLANS and their port assignments.

   For example, if the access point is connected to a port that is a member of the Sales VLAN, your computer must be connected to a port that is also a member of that VLAN. If your network is small and does not have VLANs or routers, you can connect your computer to any port on the Ethernet switch.

3. Change the IP address on your computer to 192.168.1.*n*, where *n* is a number from 1 to 254, but not 230.

   See the documentation that accompanies your computer for instructions on how to set the IP address.

4. Set the subnet mask on your computer to 255.255.255.0.

5. Power on the access point by pressing on the Power button.

6. Start the web browser on your computer.

7. Enter the IP address 192.168.1.230 in the URL field of the browser and press the Return key.

   You should now see the logon window, shown in Figure 1 on page 21.

8. Enter the user name and password.

   - ❒ User name: manager
   - ❒ Password: friend

   Note
   The user name and password are case-sensitive.

9. Click the Login button.

Starting a Management Session

This section explains how to start a management session on the access point from your management workstation, using a web browser. The procedure assumes that the access point has already been assigned an IP address, either manually or from a DHCP server.

Note
If the access point is using its default address 192.168.1.230, see “Starting the First Management Session” on page 18 for instructions.

To start a management session on the access point, perform the following procedure:

1. Open the web browser on your management workstation.
2. Enter the IP address of the access point in the URL field of the web browser.

Note
Precede the IP address with HTTPS:// if the access point is already configured for HTTPS management. The default is HTTP management.

See the log on window shown in Figure 1 as an example.

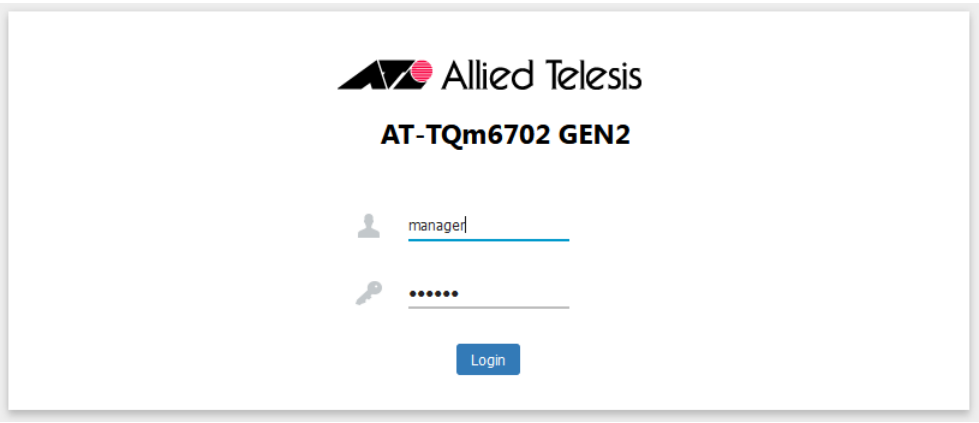

Figure 1. Log On Window

Note
If you use HTTPS management, your web browser might display a warning message stating that the site certificate is invalid. If this occurs, select an appropriate option to continue to the web site. To avoid the message in future management sessions, make the web site a trusted site in your web browser.

3. Enter the user name and password for the unit.

   The default values are:

   - User name: **manager**
   - Password: **friend**

   Note
   The user name and password are case-sensitive.

4. Click the Login button.

Management Windows

This section has a brief overview of the management windows and menus. The main parts of the management windows are identified in Figure 2.

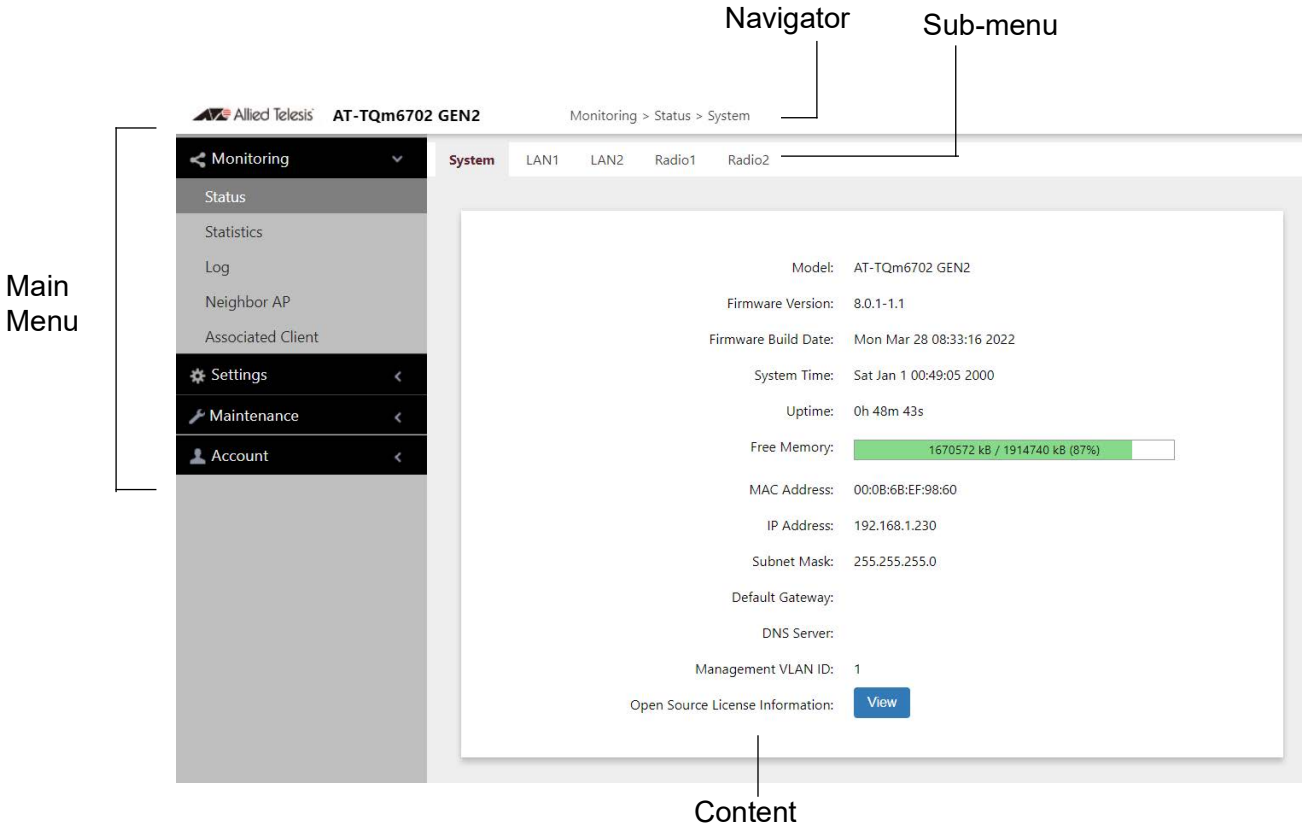

Figure 2. Sample Management Window

Main Menu

The main menu is displayed on the left side of the windows and consists of the following selections:

- Monitoring
- Settings
- Maintenance
- Account

Clicking a main menu option expands it to display the sub-items. The Monitoring option is expanded by default at the start of management sessions.

If the main menu is not displayed, the window might be too small to display the menu and content together. To display the main menu, you can either enlarge the window or click the main menu button, shown in Figure 3. Clicking the main menu button displays the menu over the content window. The menu is hidden again after you make a menu selection.

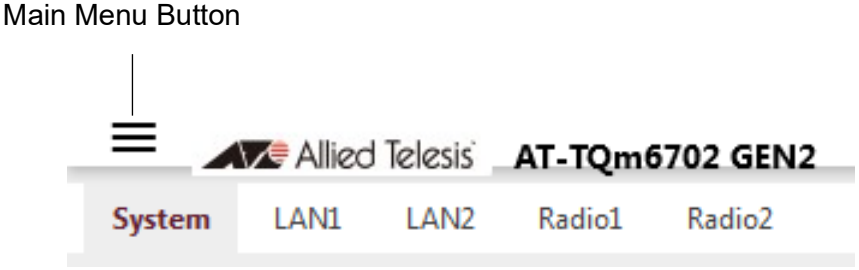

Figure 3. Main Menu Button

Navigation The Navigator shows the menu path of the current window.

Sub-menu Sub-menus are located across the tops of many management windows.

Content This is the main body of the windows. It displays parameters for you to configure or status or statistics information.

After you made changes on each page, you must save and apply the changes. The pages where you can change settings have the **Save & Apply** button. The VAP/Security pages have additional button: the **Stash** button. The Stash button allows you to save changes on a page temporarily, move to other pages within the VAP/Security section.

Saving and Applying Your Changes

After changing settings, click the **Save & Apply** button on the page. It saves the changes into the configuration file and activates the changes immediately. If you move to another page without clicking the **Save & Apply** button, you lose the changes you made in the previous page. A process to save changes into the configuration file and activate the changes might take some time to complete.

The VAP/Security pages have additional button: the **Stash** button. The **Stash** button allows you to save changes on a page temporarily. You can move to another page within the VAP/Security section without using the **Save & Apply** button. You click the **Save & Apply** button when you finish making changes on multiple pages. You can save time using the **Stash** button without using the **Save & Apply** button on every page.

Save & Apply Button

When you are finished changing settings in a management window, click the **Save & Apply** button to save and activate your changes. The button is located at the bottom of the windows as shown in Figure 4.

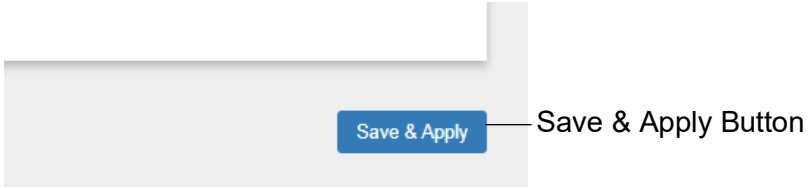

Figure 4. Save & Apply Button

When you click the button, the access point immediately saves changes in its configuration file and activates the changes.

Stash Button

If you change settings on the VAP/Security pages, click the **Stash** button after finishing the page and before moving to another page within the VAP/Security section. The **Stash** button allows you to save changes on a page temporarily. When finishing changing settings on the VAP/Security pages, click the **Save & Apply** button, which saves changes in the VAP/Security pages and activates the changes. See Figure 5.

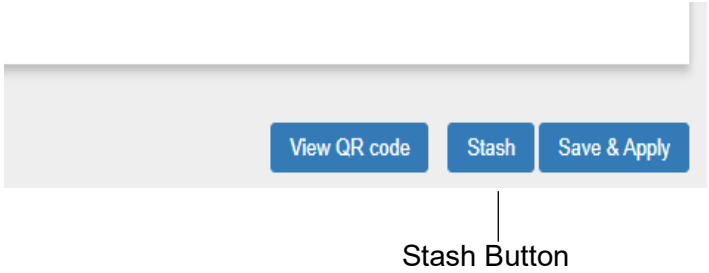

Figure 5. Stash Button

Ending Management Sessions

You should always log off when you are finished managing the unit. To log off, select **Account** > **Logout**. Click **OK** at the confirmation prompt. For added security, close your web browser.

What to Configure First

Here are suggestions on what to configure during the first management session:

1. Set the country code. Refer to “Setting the Country Code Setting” on page 91.

   Note
   The country codes for units sold in North America, Japan, and Taiwan are preset and cannot be changed.

   Note
   Changing the country setting disables the radios. The procedure is disruptive to network operations if the unit is actively forwarding client traffic.

2. Change the manager’s login name and password. Refer to “Changing the Manager’s Login Name and Password” on page 213.
3. If you prefer to use HTTPS management sessions, perform “Changing the Manager’s Login Name and Password” on page 213.
4. Set the language of the management interface to English or Japanese. The default is English. Refer to “Setting the Language of the Web Browser Interface” on page 215.

Chapter 2

Monitoring

This chapter has the following procedures:

Displaying Basic System Information

To display basic information about the access point, such as its firmware version number and MAC address, perform the following procedure:

1. Select **Monitoring** > **Status** from the main menu.
2. Select **System** from the sub-menu. This is the default window. Refer to Figure 6.

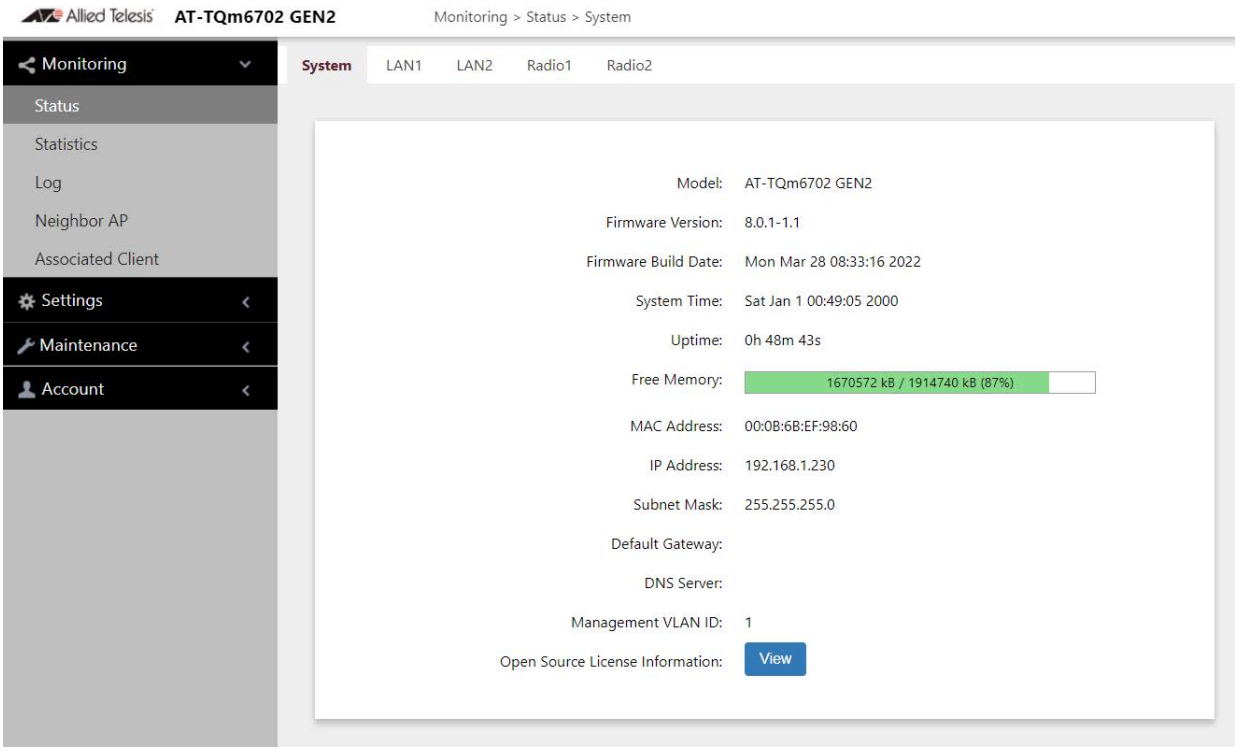

Figure 6. System Window

The fields are defined in Table 2.

Table 2. System Window

Item Name	Description
Model	Displays the product's model name.
Firmware Version	Displays the version number of the management software on the access point.
Firmware Build Date	Displays the date and time when the firmware was built.

Table 2. System Window (Continued)

Item Name	Description
System Time	Displays the date and time. To set the date and time, refer to “Manually Setting the Date and Time” on page 49 or “Setting the Date and Time with the Network Time Protocol (NTP)” on page 46.
Uptime	Displays the number of hours, minutes, and seconds that have elapsed since the unit was last reset or powered on.
Free Memory	Displays the amount of free memory in the access point, as follows: - The first value is the total amount of unused memory, in KB. - The second value is the total amount of memory, in KB. - The last number in parentheses is the percentage of total memory that is free.
MAC Address	Displays the MAC address of the access point and Radio1. Radio 2 has a different MAC address. To view the MAC address of Radio 2, select **Monitoring** > **Status** > **Radio2**. You cannot change the MAC addresses.
IP Address	Displays the IP address of the access point. To set this value, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 40 or “Assigning a Static IPv4 Address to the Access Point” on page 43.
Subnet Mask	Displays the subnet mask. To set this value, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 40 or “Assigning a Static IPv4 Address to the Access Point” on page 43.
Default Gateway	Displays the default gateway address. The default gateway is an IP address of an interface on a router or other Layer 3 routing device. It specifies the first hop to reaching the subnets or networks where your management devices, such as management workstations and syslog servers, reside. The access point can have only one default gateway. To set this value, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 40 or “Assigning a Static IPv4 Address to the Access Point” on page 43.

Table 2. System Window (Continued)

Item Name	Description
DNS Server	Displays the current DNS server address. Refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 40 or “Assigning a Static IPv4 Address to the Access Point” on page 43.
Management VLAN ID	Displays the management VLAN ID. The VLAN ID is 1.
Open Source License Information	When you click the **View** button, displays open source license information.

Displaying VAP and LAN Port Statistics

To view VAP and LAN port status and statistics, select **Monitoring** > **Statistics** window. See Figure 7.

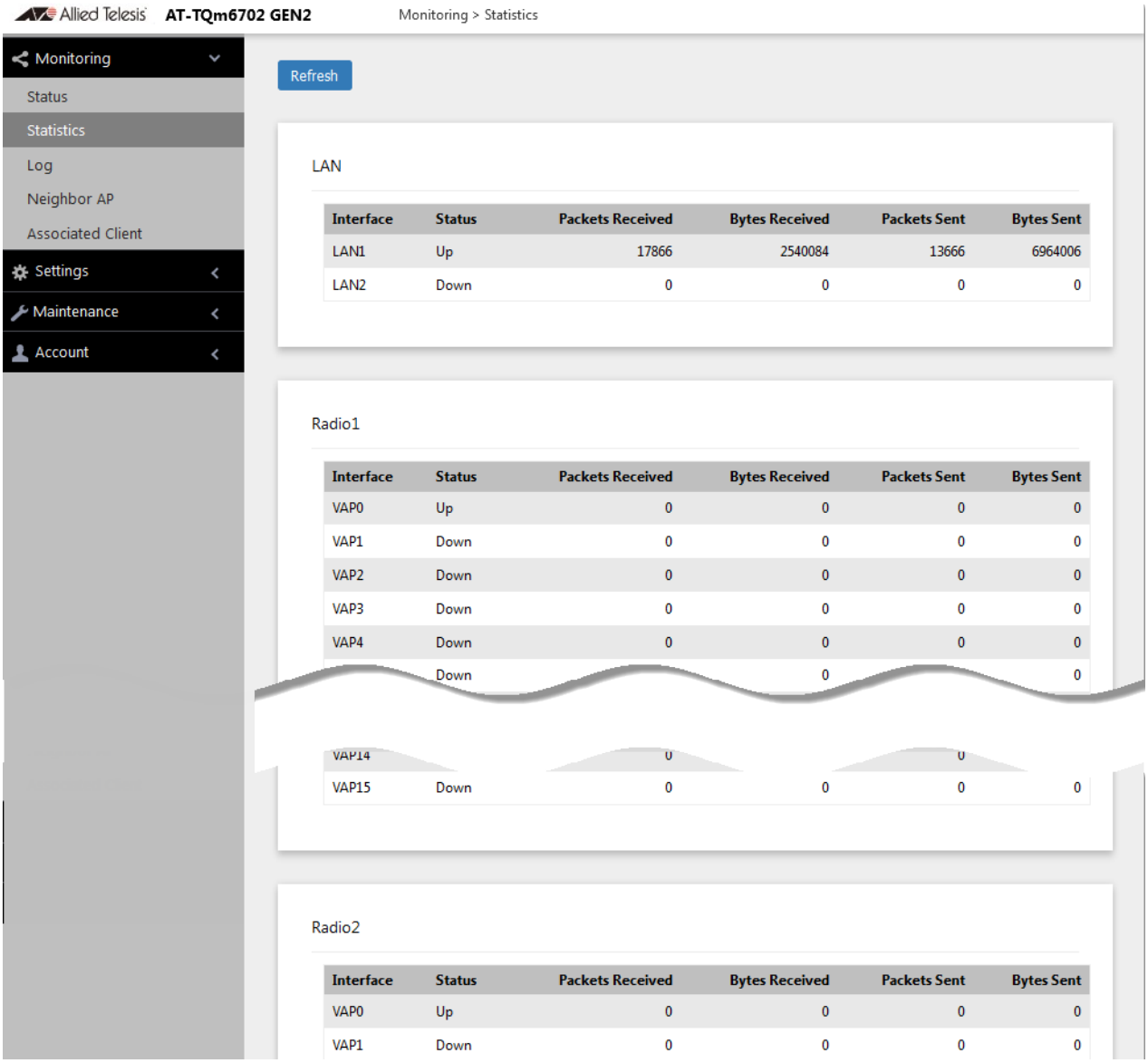

Figure 7. Statistics Window

The columns are defined in Table 3 on page 33.

Table 3. Statistics Window

Column	Description
Interface	Displays the LAN port and VAPs 0 to 15 on Radio1 and Radio2.
Status	Displays the status (up or down) of the interface.
Packets Received	Displays the total number of packets received on the interface.
Bytes Received	Displays the total number of bytes received on the interface.
Packets Sent	Displays the total number of packets transmitted on the interface.
Bytes Sent	Displays the total number of bytes transmitted on the interface.

Displaying the System Log

You can monitor the operations of the access point by viewing the messages in its system log. The events and the vital information about system activity help you identify and solve system problems.

The messages are divided into the eight severity levels listed in Table 4:

Table 4. Message Severity Levels

Severity Level	Description
0 - Emergency	System is unusable.
1 - Alert	State that must be dealt with immediately.
2 - Critical	Serious condition.
3 - Error	Error occurred
4 - Warning	Warning conditions exist.
5 - Notice	Normal but needs attention.
6 - Informational	Information message.
7 - Debug	Debug level message.

The system log default setting shows Informational messages.

You can restrict the log to display only certain messages by adjusting the Severity parameter in the syslog client. Refer to “Sending Log Messages to a Syslog Server” on page 58.

Note
All messages are deleted from the log when the access point is reset or powered off. To permanently save the messages, refer to “Sending Log Messages to a Syslog Server” on page 58.

To view the system log, select **Monitoring** > **Log**, Figure 8 on page 35 is an example.

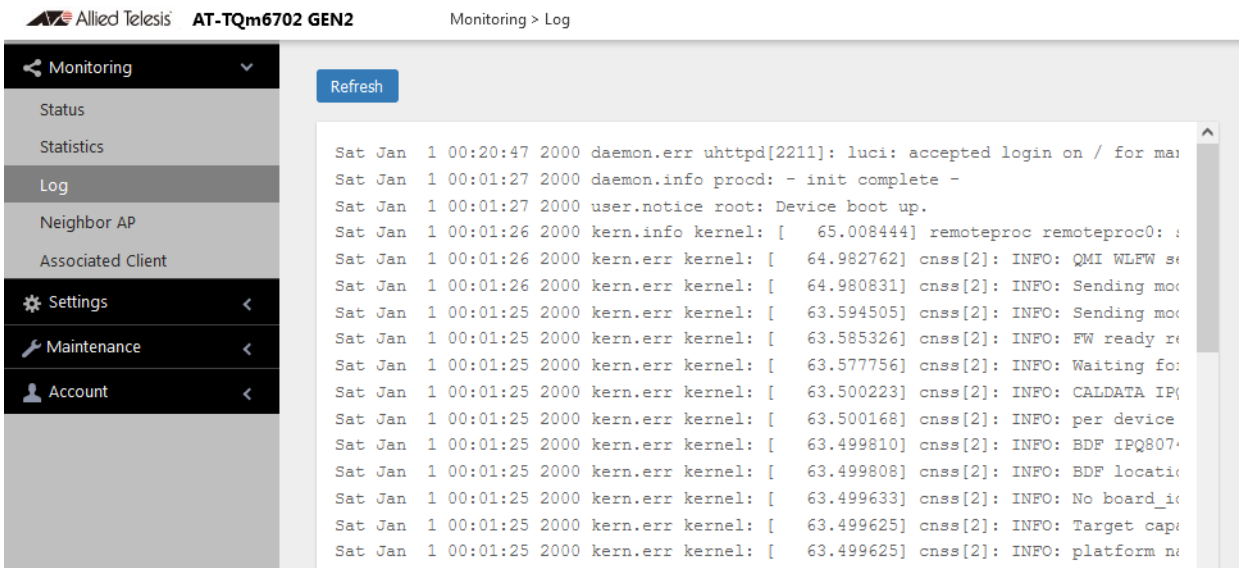

Figure 8. Log Window for Event Messages

Displaying Neighbor AP

To view information about all access points on the channels that the access point detects, select **Monitoring** > **Neighbor AP** from the main menu. Refer to Figure 9.

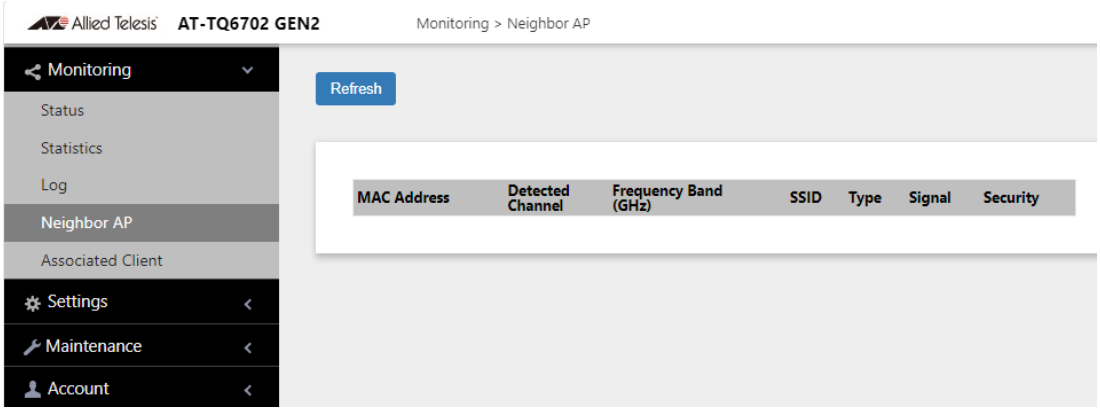

Figure 9. Neighbor AP Window

The columns are defined in Table 5.

Table 5. Neighbor AP Window

Column	Description
MAC Address	Displays the MAC address of the detected access point.
Detected Channel	Displays the channel of the detected access point.
Frequency Band (GHz)	Displays the frequency band the detected access point is operating within.
SSID	Displays the network name (SSID) of the detected access point
Type	Displays the mode of the detected access point: AP or Adhoc.
Signal	Displays the intensity of the received signal in a four-level bar graph icon. Pointing to the icon displays dB (dBm).
Security	Displays the security status of the detected access point.

Displaying Associated Clients

To view the active wireless clients on the VAPs of the access point, select **Monitoring** > **Associated Clients** from the main menu. Refer to Figure 10.

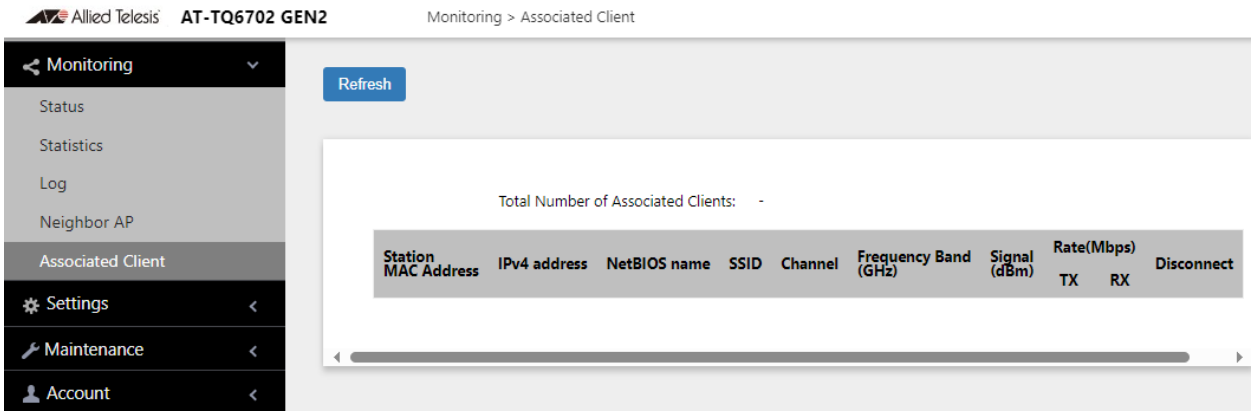

Figure 10. Associated Client Window

The columns are defined in Table 6.

Table 6. Associated Client Window

Column	Description
MAC Address	Displays the MAC addresses of associated clients.
IPv4 address	Displays the IPv4 address of associated clients. It is displayed when IPv4 is used.
NetBIOS name	Displays the NetBIOS name of associated clients. It displays "n/a" when NetBIOS name is not acquired or during the acquisition.
SSID	Displays the network name (SSIDs) to which the client is connected.
Channel	Displays the radio channel the client is using.
Frequency Band (GHz)	Displays the frequency band the associated client is operating within.
Signal (dBm)	Displays the strength of the signal from the client.
Rate (Mbps)	Displays the transmission (Tx) and reception (Rx) rates in Mbps.

Table 6. Associated Client Window (Continued)

Column	Description
Disconnect	Displays the Disconnect button. Clicking the button disconnects the client.

Chapter 3

System Settings

This chapter contains the following procedures:

Assigning a Dynamic IP Address from a DHCP Server

This section explains how to activate the DHCP client so that the access point receives its IP address from a DHCP server on your network. The unit uses the address to communicate with devices on your network, such as management workstations, syslog servers, and RADIUS servers. The access point can have only one IP address.

If your network does not have a DHCP server or you prefer to manually assign it an IP address, refer to “Assigning a Static IPv4 Address to the Access Point” on page 43.

Note
Changing the IP address of the access point might interrupt your management session. To resume managing the device, start another session using the access point’s new IP address.

Note
The default setting for the DHCP client is enabled. You only need to perform this procedure if you disabled the client and assigned the device a static IP address, but now want to reactivate the client.

To configure the access point to receive its IP address from a DHCP server, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Network** from the sub-menu.
3. Select **DHCP** from the Connection Type pull-down menu. The options in the window change. See Figure 11.

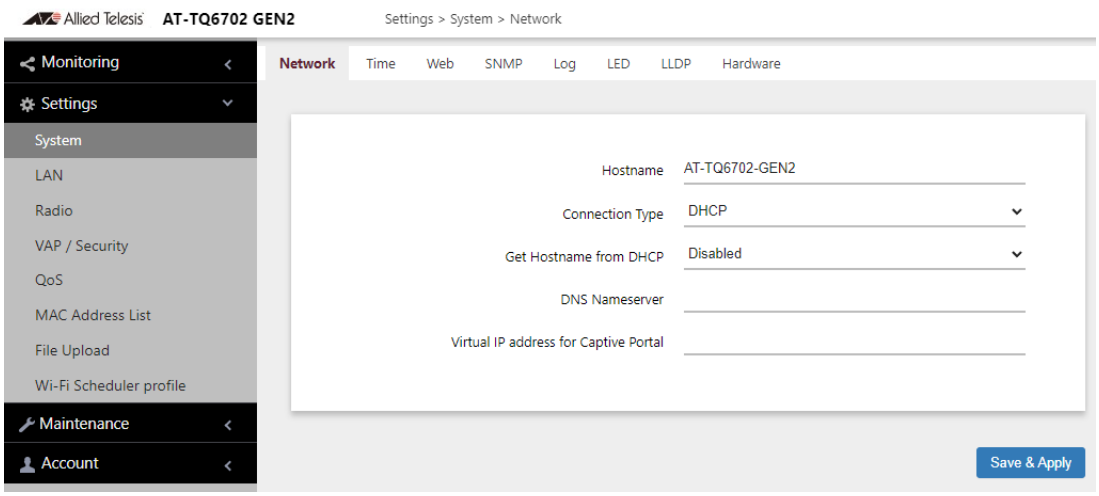

Figure 11. Network DHCP Window

4. Configure the fields by referring to Table 7.

Table 7. Network DHCP Window

Parameter	Description
Hostname	Enter a hostname for the access point. Here are the guidelines: - The hostname can be from 1 to 63 alphanumeric characters. - The hostname cannot contain spaces or any special characters, except hyphens. - The first or last character cannot be a hyphen. - The access point can have only one hostname. - The default is one of the following, depending upon the model of your access point: • AT-TQ6702 GEN2 • AT-TQm6702 GEN2 • AT-TQ6602 GEN2 • AT-TQm6602 GEN2 - If you want the DHCP server to supply the hostname, enable the Get Hostname from DHCP Server option in this window.

Table 7. Network DHCP Window (Continued)

Parameter	Description
Connection Type	Select **DHCP**. This is the default. The Static IP selection is explained in “Assigning a Static IPv4 Address to the Access Point” on page 43.
Get Hostname from DHCP	Select one of the following options: - Enabled: When the DHCP server assigns an IP address to the access point, the server assigns a host name as well. - Disabled: The DHCP server does not change the hostname of the access point. This is the default setting.
DNS Nameserver	Enter the IP address of the DNS server. If this field is left blank, the access point tries to obtain the address from the DHCP server. The default is no name.
Virtual IP Address for Captive Portal	Assigns a virtual IP address for Captive Portal. Wireless clients use the virtual address instead of the device’s actual IP address to log on to captive portals. Using a virtual address increases the security of your wireless network. The device supports one virtual IP address. **Note** This field is not supported with Wireless Distribution System (WDS) bridges. This field is optional. The default value is NULL.

5. Click the **Save & Apply** button to save and update the configuration.

Note
If the access point stops responding to the web management windows, start a new management session using the new IP address that the access point received from the DHCP server.

Assigning a Static IPv4 Address to the Access Point

This section explains how to manually assign an IP address to the access point. The unit uses the address to communicate with devices on your network, such as management workstations, syslog servers, and RADIUS servers. The access point can have only one IP address.

If you prefer the access point obtain its IP configuration from a DHCP server on your network, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 40.

Note
Changing the IP address of the access point might interrupt your management session. To resume managing the device, start a new session using the access point’s new IP address.

To assign a static IP address to the device, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Network** from the sub-menu.
3. Select **Static IP** from the Connection Type pull-down menu. The options in the window change. Refer to Figure 12.

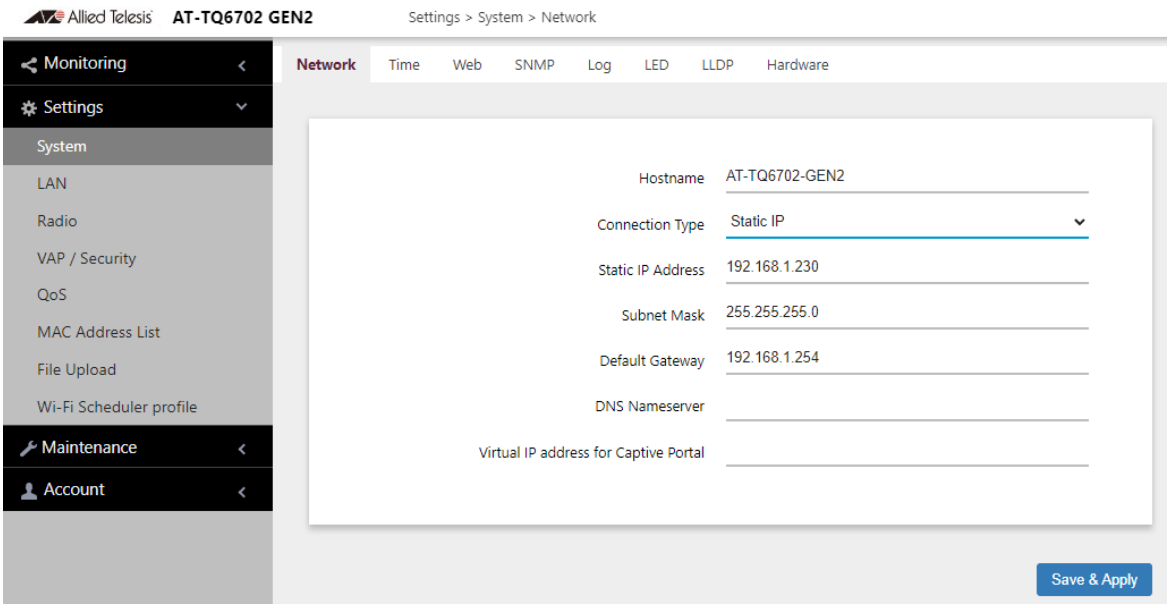

Figure 12. Network Static IP Address Window

4. Configure the field values by referring to Table 8.

Table 8. Network Static IP Selection Window

Item Name	Description
Host Name	Enter a host name for the access point. Here are the guidelines: - The host name can be from 1 to 63 alphanumeric characters. - The hostname cannot contain spaces or any special characters, except hyphens. - The first or last character cannot be a hyphen. - The access point can have only one hostname. - The default is one of the following, depending upon the model of your access point: • AT-TQ6702 GEN2 • AT-TQm6702 GEN2 • AT-TQ6602 GEN2 • AT-TQm6602 GEN2
Connection Type	Select **Static IP**.
Static IP Address	Enter the new IP address for the access point. The device can have only one IP address. The default is 192.168.1.230.
Subnet Mask	Enter the subnet mask for the IP address. The default is 255.255.255.0.
Default Gateway	Enter the default gateway address for the unit. The default value is 192.168.1.254.
DNS Nameserver	Specify the Domain Name Service (DNS) server address. This field is optional. The default is no name.

Table 8. Network Static IP Selection Window (Continued)

Item Name	Description
Virtual IP Address for Captive Portal	Assigns a virtual IP address to the wireless access point. Wireless clients use the virtual address instead of the device's actual IP address to log on to captive portals. Using a virtual address increases the security of your wireless network. The device supports one virtual IP address. **Note** This option is not supported with Wireless Distribution System (WDS) bridges. This field is optional. The default value is NULL.

5. Click the **Save & Apply** button to save and update the configuration.

Setting the Date and Time with the Network Time Protocol (NTP)

The access point has a Network Time Protocol (NTP) client for setting its date and time from an Simple Network Time Protocol (SNTP) server on your network or the Internet. The access point adds the date and time to log messages and SNMP traps.

Here are the guidelines to using the client:

- You need to know the domain name or IPv4 address of an SNTP server on your network or the Internet. You can specify only one server.
- The access point must have an IPv4 address and subnet mask.
- The access point must also have a default gateway address if the NTP server is on a different subnet or network. The default gateway must specify the first router hop to the subnet or network of the SNTP server.
- The client is compatible with SNTP servers. It is not compatible with NTP servers.

To configure the NTP client, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Time** from the sub-menu. Refer to Figure 15 on page 49.
3. From the Set System Time pull-down menu, select **Using Network Time Protocol (NTP)**. The window is updated with new options. Refer to Figure 13.

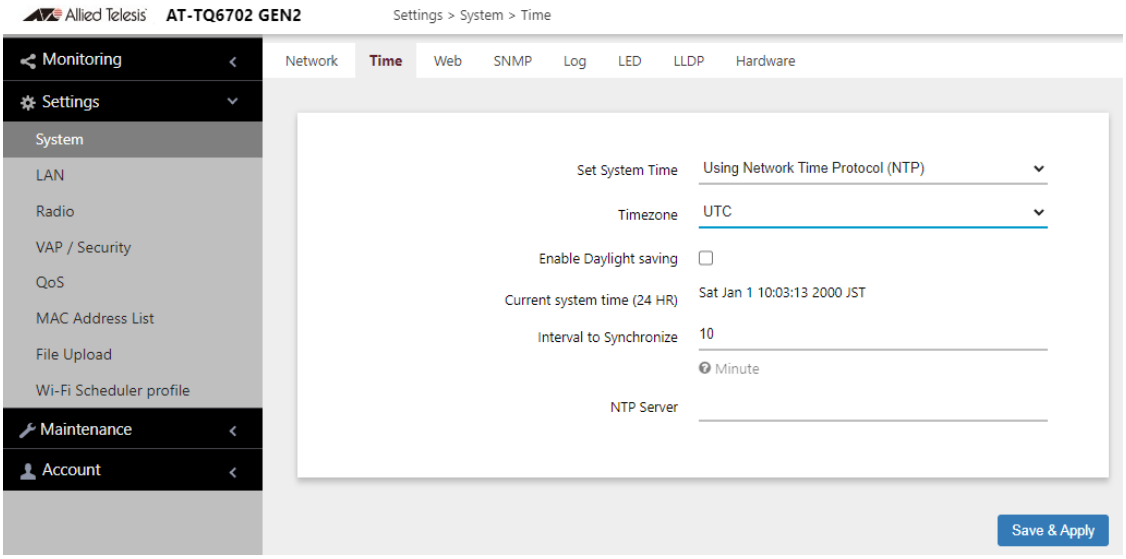

Figure 13. Time Window - NTP Option

4. Configure the fields by referring to Table 9.

Table 9. Time Window - NTP Option

Item Name	Description
Set System Time	Select **Network time protocol (NTP)** to synchronize the date and time of the product with the NTP server. The factory default is Manually.
Timezone	Use this pull-down menu to set the time zone of the location of the access point. If the SNTP server is providing Coordinated Universal Time (UTC), the access point uses the time zone parameter to determine its UTC offset, which is the number of hours its location is ahead or behind UTC. It adjusts the time accordingly.
Enable Daylight Saving	If the location of the access point observes daylight savings time, click the check box for this option. The window displays the fields in Figure 14 on page 48. If the area does not observe Daylight Savings time, leave the check box empty.
Start (Daylight Saving)	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End (Daylight Saving)	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset (Daylight Saving)	Use the pull-down menu to select the number of minutes to adjust the time at the start and end Daylight Saving Time. The default is 60 minutes.
Current System Time (24 HR)	Displays the date and time of the access point.
Interval to Synchronize	Enter the interval in minutes at which the access point synchronizes its time with the SNTP server. The range is 1 to 9999 minutes. The default is 10 minutes.

Table 9. Time Window - NTP Option (Continued)

Item Name	Description
NTP Server	Specify the SNTP server using one of the following methods: - IP address (example, 12.34.56.78) - Fully qualified domain name (FQDN) (example, ntp.mydomain.com) Here are the guidelines: - You can specify only one server. - The first character must be a letter or number. It cannot be a special character. - The last character cannot be a hyphen or period. - The factory default is no server. Observe these guidelines when using an FQDN to identify the server: - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters. - An FQDN can have up to 253 characters.

Figure 14 contains the settings for Daylight Savings Time.

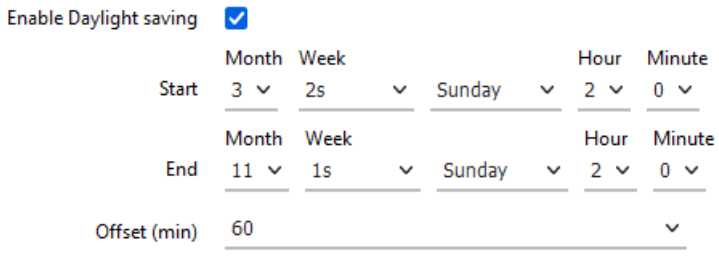

Figure 14. Daylight Savings Time Settings

5. Click the **Save & Apply** button to save and update the configuration.

Manually Setting the Date and Time

This section explains how to manually set the date and time on the access point.

Note
The access point does not have a real-time clock with backed up batteries. Consequently, the date and time, when set manually, are returned to their default values (Jan 1 00: 00: 00 2018) when the device is reset or powered off.

Note
Allied Telesis recommends using an SNTP server to set the date and time. For instructions, refer to “Setting the Date and Time with the Network Time Protocol (NTP)” on page 46.

To manually set the date and time, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Time** from the sub-menu. Refer to Figure 15.

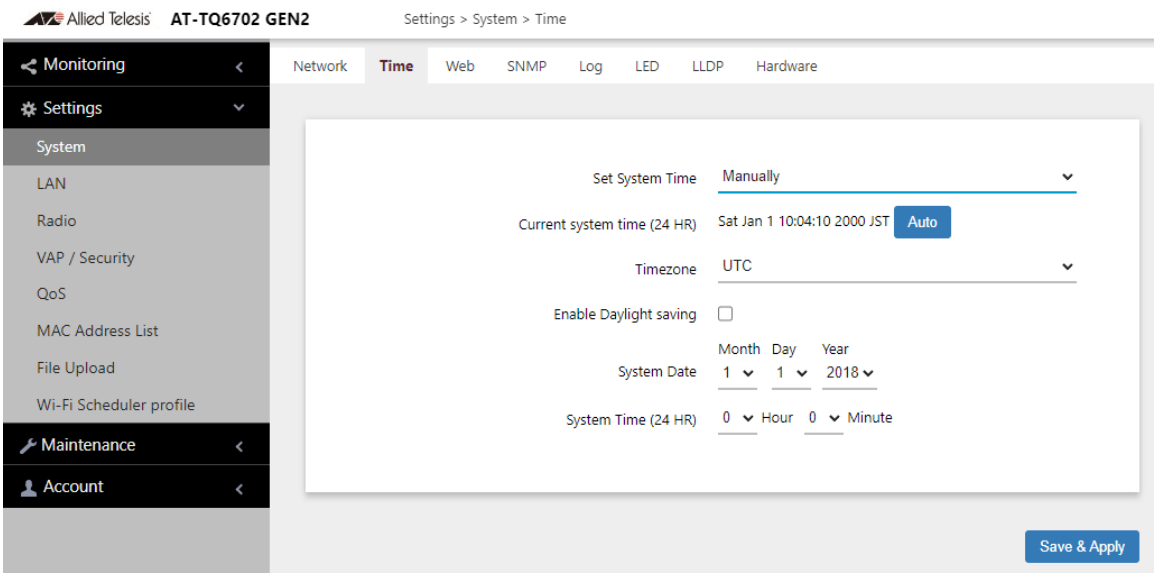

Figure 15. Time Window - Manually Optionn

3. Configure the parameters by referring to Table 10.

Table 10. Time Window - Manually Option

Field	Description
Set System Time	Select **Manually**. This is the default.
Current System Time (24 HR)	Displays the current date and time settings. Click the AUTO button to set the date and time on the access point according to your management workstation.
Timezone	Select the Time Zone of the access point from the pull-down menu.
Enable Daylight Savings	If the location of the access point observes daylight savings time, click the dialog box for the Adjust Time for Daylight Savings parameter. The window displays the fields in Figure 14 on page 48 If the area does not observe Daylight Savings time, leave the check box empty.
Start (Daylight Saving)	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End (Daylight Saving)	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset (Daylight Saving)	Use the pull-down menu to select the number of minutes to adjust the time at the start and end Daylight Saving Time. The default is 60 minutes.
System Date	Use the pull-down menus to set the current month, day, and year.
System Time	Use the pull-down menus to set the current hours and minutes. The hours are in 24 hours. For example, 14 represent 2:00 p.m.

4. Click the **Save & Apply** button to save and update the configuration.

Configuring the Web Browser Interface

This section has the following management functions:

- Specify the maximum number of administrators that can manage the access point at one time with the web browser interface.
- Specify the time interval after which the access point automatically ends inactive management sessions.
- Enable or disable HTTP or HTTPS web management.
- Generate a self-signed HTTPS certificate.

Note
Do not disable both HTTP and HTTPS. Otherwise, you will not be able to manage the access point with a web browser.

Note
HTTP management is non-secure, meaning the packets exchanged between the access point and your workstation are sent in clear text, leaving them vulnerable to snooping. For this reason, Allied Telesis recommends using HTTPS to manage the access point.

To configure the above functions, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Web** from the sub-menu. Refer to Figure 16.

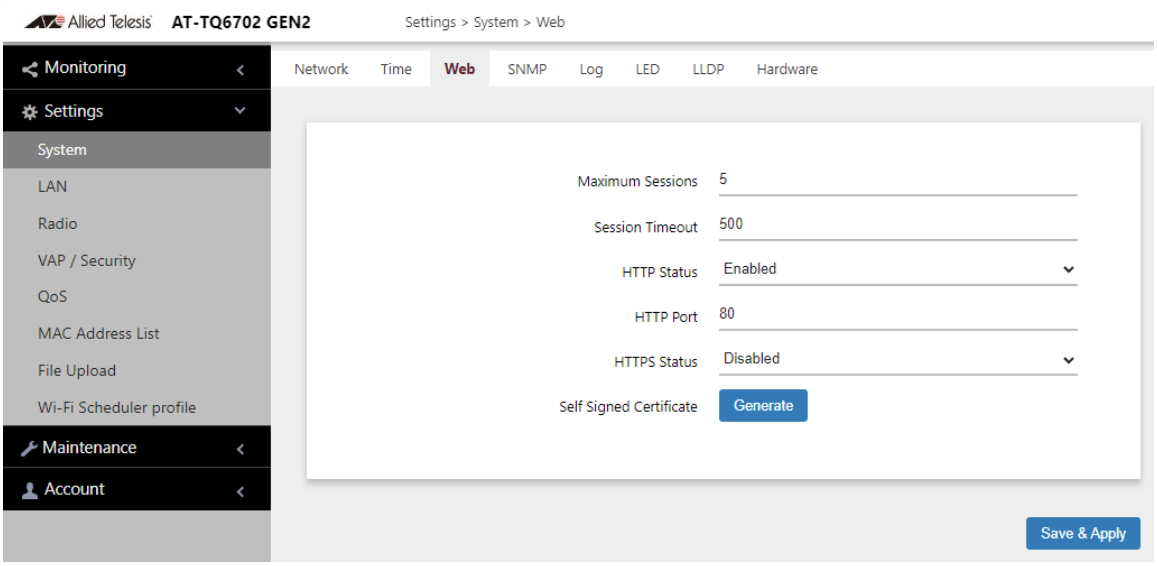

Figure 16. Web Window

3. Configure the fields by referring to Table 11.

Table 11. Web Window

Field	Description
Maximum Sessions	Specify the maximum number of active management sessions the access point will support at one time. Here are the guidelines: - The range is 1 to 10 sessions. - The number of sessions is the sum of HTTP and HTTPS connections. - The default is five sessions. - The access point blocks new management session after reaching the maximum number of sessions.
Session Timeout	Specify the time in minutes when the access point automatically ends inactive sessions. The range is 1 to 1440 minutes (1440 minutes = 1 day). The default is five minutes.
HTTP Status	Enable or disable HTTP management. The default is enabled.
HTTP Port	Specify the port number of the HTTP server. The range is 0 to 65535. The default is 80.
HTTPS Status	Enable or disable HTTPS management. The default is disabled. The HTTPS server uses port 443. It cannot be changed.
Self Signed Certificate	Generate a self-signed certificate for HTTPS management. The access point comes with a certificate, but you can generate a new one with this option. The new certificate automatically replaces the old certificate.

4. Click the **Save & Apply** button to save and update the configuration.

Note
If you disabled the HTTP or HTTPS mode you are currently using to manage the device, the access point ends your management session. To resume managing the device, start a new session using the other mode.

Configuring SNMPv1, SNMPv2, and SNMPv3

You can use SNMP to view the settings and client statistics on the access point, and receive traps. Here are the guidelines:

- You cannot use SNMP to change the settings on the access point.
- The access point has one read-only community string.
- The unit must have an IP address for SNMP management.

  For more information, see“Assigning a Dynamic IP Address from a DHCP Server” on page 40 or “Assigning a Static IPv4 Address to the Access Point” on page 43.

To enable or disable SNMP, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **SNMP** from the sub-menu. Refer to Figure 17.

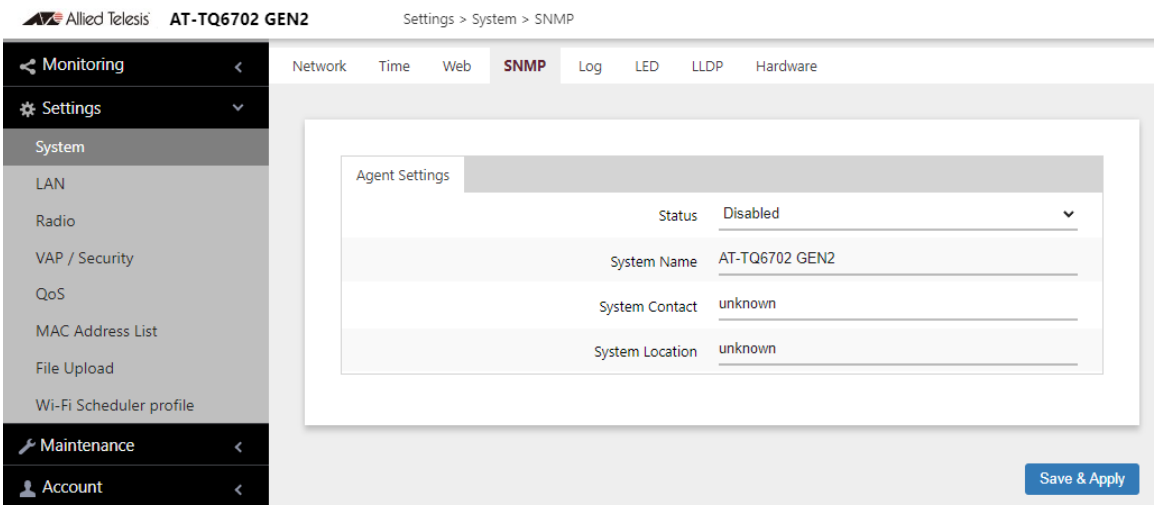

Figure 17. SNMP Window

3. Select Disabled or Enabled in the Status field. To configure SNMP, select Enabled.

   When Enabled is selected, the SNMPv1 and SNMPv2 or SNMPv3 configuration window appears. See Figure 18 on page 54.

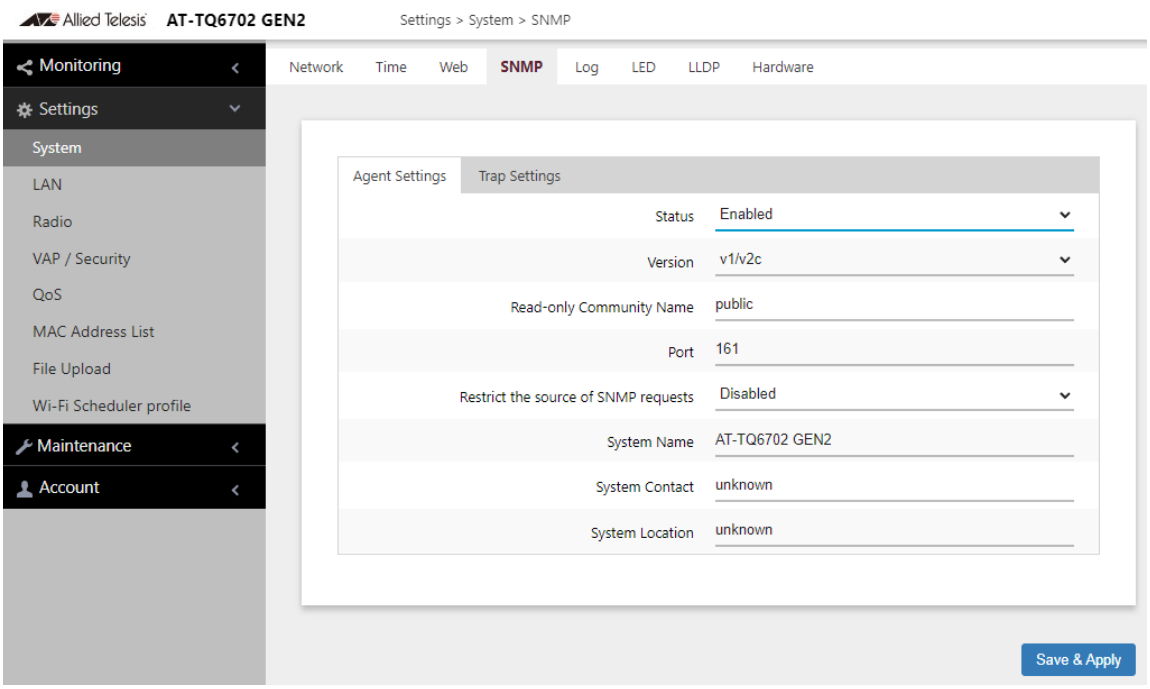

Figure 18. SNMP Window - SNMP Enabled

4. Configure the parameters by referring to Table 12.

Table 12. SNMP Window

Field	Description
Status	Use this option to activate or deactivate the SNMP agent on the access point. The options are explained here: - Enabled: Select this option to activate the SNMP agent and trap settings. This allows you to use SNMP to view the parameter settings on the access point. It also allows the access point to send traps. You have to enable SNMP to configure the settings in this window and the Trap Settings window. - Disabled: Select this option to disable SNMP and the trap settings. This is the default setting.
Version	Select the desired SNMP version: - v1/v2c: SNMPv1 and SNMPv2c - v3: SNMPv3

Table 12. SNMP Window (Continued)

Field	Description
Read-Only Community Name (SNMPv1 and SNMPv2c only)	Specifies the community name.
Port	Specify the port number for SNMP. The range is 1 to 65535. The default is 161.
Restrict the Source of SNMP Requests (SNMPv1 and SNMPv2c only)	Restricts the use of SNMP to specific subnets or individual workstations. The options are: - Enabled: Restrict the use of SNMP on the access point to only the management stations specified in the Only allow from the designated hosts or subnets field. - Disabled: Permit any workstation to use the community string to view the device. This is the default setting.
Username (SNMPv3 only)	Specify a user name for SNMP.
Password (SNMPv3 only)	Specify a password for SNMP.

Table 12. SNMP Window (Continued)

Field	Description
Only allow from the designated hosts or subnets (Only when the Restrict the source of SNMP requests is enabled)	Specify management workstations permitted to use SNMP to view the device. This parameter applies only to SNMPv1 and SNMPv2c. Here are guidelines: - You can specify only one value in the field. - You can specify a workstation by its IPv4 address (for example, 192.168.1.5). - You can specify a group of workstations that fall in the same subnet. (for example, 192.168.1.0/24). - You can specify a workstation by its Fully Qualified Domain Name (FQDN). - The default is blank. Observe these guidelines when using an FQDN to specify the workstation: - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters - An FQDN can have up to 253 characters.
System Name	Specify the SNMP system name of the access point. The default is the access point's model name.
System Contact	Specify the system administrator name. The system contact can be up to 64 alphanumeric characters. The default is Unknown.
System Location	Specify the location of the device. It can be up to 64 alphanumeric characters. The default is Unknown.

5. Click the **Save & Apply** button to save and update the configuration.

Displaying the System Log

See “Displaying the System Log” on page 34.

Sending Log Messages to a Syslog Server

To configure the access point to send the log messages to a syslog server on your network, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Log** from the sub-menu. Refer to Figure 19.

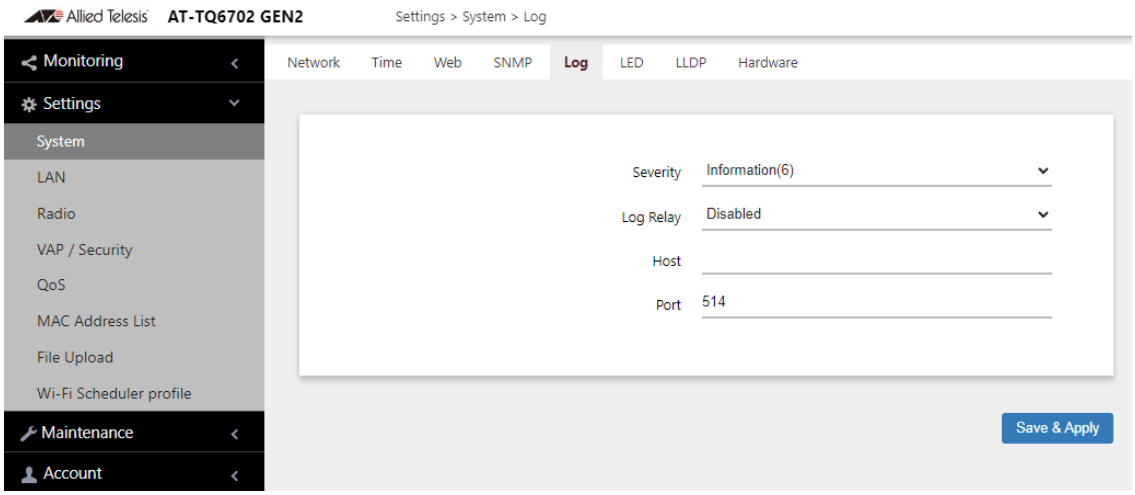

Figure 19. Log Window for Syslog Client

3. Configure the fields by referring to Table 13.

Table 13. Log Window for Syslog Client

Field	Description
Severity	Select the severity of messages the access point is to display in the log file and transmit to the syslog server. The severity levels are listed in Table 4 on page 34. Here are the guidelines: - You can specify only one severity level. - The severity level applies to both the messages displayed in the log file and transmitted to a syslog server. - The selected level includes that level and all numerically lower (higher severity) messages. For example, selecting level 3, error, designates system messages levels 0 to 3. - The default is level 7, debug. This is the highest value; it designates all messages.

Table 13. Log Window for Syslog Client (Continued)

Field	Description
Log Relay	Select one of the following: - Enabled: Activates the syslog client to transmit the event messages to your syslog server. - Disabled: Deactivates the syslog client to stop the access point from transmitting event messages. This is the default.
Host	Enter the IPv4 address (for example, 10.10.1.200) or host name (FQDN) of the syslog server. Here are the guidelines: - You can enter only one host. - Do not include a subnet mask with IP address. - The factory default is blank. Observe these guidelines when using an FQDN to identify the host: - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters. - An FQDN can have up to 253 characters.
Port	Enter the port number of the syslog server. The range is 1 to 65535. The default is 514.

4. Click the **Save & Apply** button to save and update the configuration.

Enabling or Disabling the LEDs

The access point has an Eco Mode. When activated, it turns off the LEDs on the top panel. You might activate the mode when you are not using the LEDS to monitor or troubleshoot the device. The default setting for the LEDs is on.

To turn the LEDs on or off, perform the following procedure:

1. Select **Settings** > **System** in the main menu.
2. Select **LED** in the sub-menu. Refer to Figure 20.

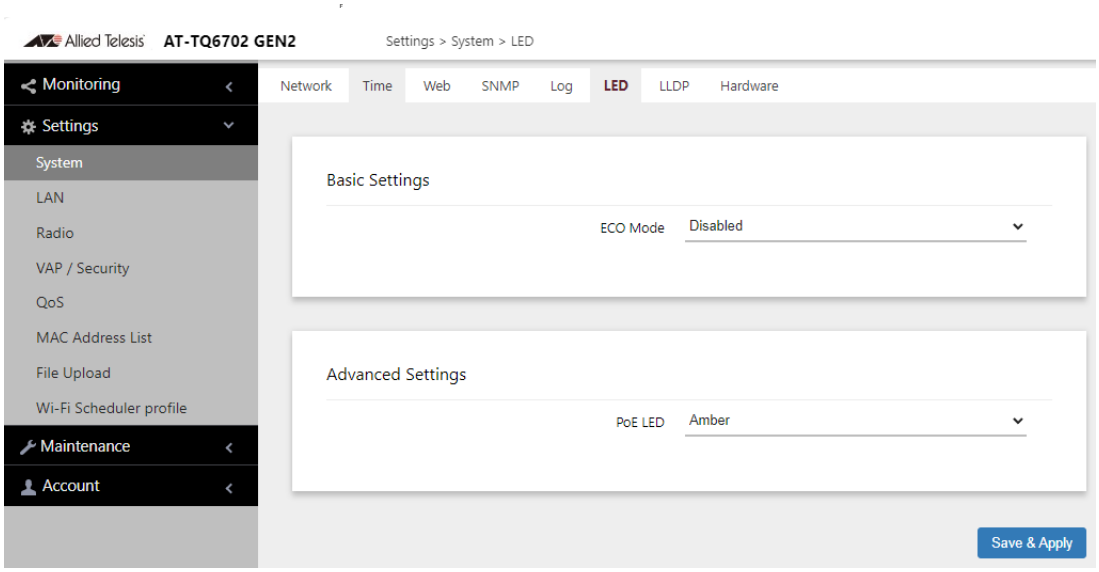

Figure 20. LED Window

3. In Basic Settings, from the **Eco Mode** drop-down menu, select one of the following:
   - ❒ Enabled: The Eco Mode is enabled. The LEDs are off.
   - ❒ Disabled: The Eco Mode is disabled. The LEDs are on. This is the default setting.
4. In Advanced Settings, from the PoE LED drop-down menu, select one of the following:
   - ❒ Amber. This is the default.
   - ❒ Green
5. Click the **Save & Apply** button to save and update the configuration.

Configuring PoE Negotiation with Link Layer Discovery Protocol (LLDP)

This feature is applicable when the access point is powered by Power over Ethernet (PoE) and the LAN1 port is connected to a network device that supports LLDP Media Endpoint Devices (LLDP-MED).

LLDP and LLDP-MED allow Ethernet network devices to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. The shared data allows network devices to discover other devices directly connected to them as well as advertise parts of their Layer 2 configuration to each other.

LLDP is a “one” hop” protocol; LLDP information can only be sent to and received by devices that are directly connected to each other, or connected via a hub or repeater. Devices that are directly connected to each other are called neighbors. Advertised information is not forwarded on to other devices on the network because LLDP is a on-way protocol. That is, the information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors.

LLDP transmits information in packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each containing a particular type of information about the device or port transmitting it.

The Extended Power Management TLV in LLDP-MED is for powered devices like the access point. They use it to send their power requirements to their PoE sources, which in turn, store the information or use it to adjust the power supplied to the access point.

Here are guidelines for PoE negotiation with LLDP:

- ❒ The access point must be powered with PoE.
- ❒ The LAN1 port must be connected to an LLDP-Med device.
- ❒ The LLDP-MED device must be configured for the Extended Power Management TLV.
- ❒ This feature is optional. The access point can be powered by PoE without enabling this feature.

To enable or disable the Reset button, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **LLDP** from the sub-menu. Refer to Figure 21 on page 62.

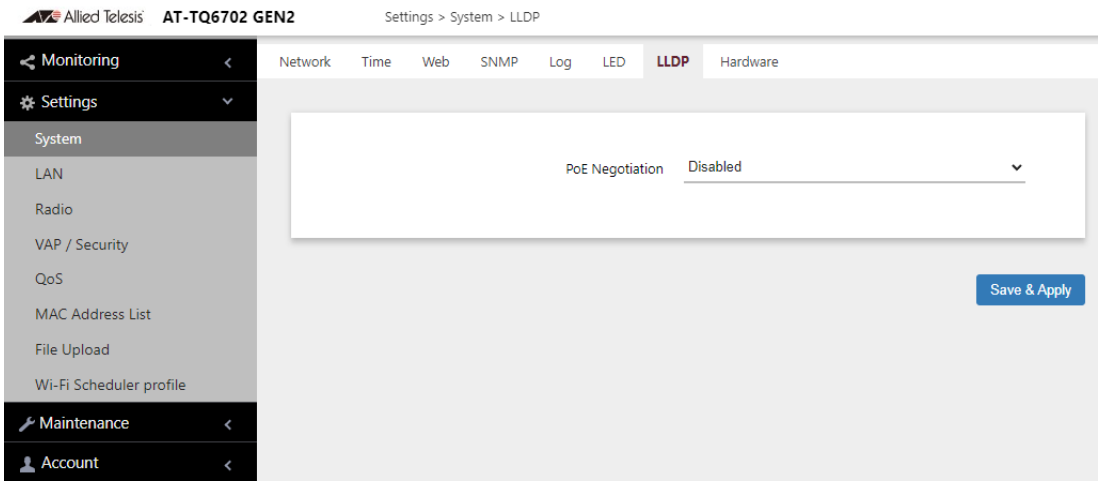

Figure 21. LLDP Window

3. Select one of the following from the PoE Negotiation:
   - ❒ Enabled: Enables PoE negotiation. The access point transmits the Extended Power Management TLV on the LAN1 port.
   - ❒ Disabled: Disables PoE negotiation. This is the default setting.
4. Click the **Save & Apply** button to save and update the configuration.

Enabling or Disabling the Reset Button

This section explains how to enable or disable the Reset button on the rear panel of the access point. You use the Reset button to restore the default settings to the device.

If the unit is installed in a non-secure area, you might disable the button to prevent unauthorized individuals from pressing it and disrupting the operations of your wireless network.

Note
If you disable the Reset button, be sure not to forget the manager account password. Otherwise, you will not be able to manage the unit with the web browser interface.

To enable or disable the Reset button, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Hardware** from the sub-menu. Refer to Figure 22.

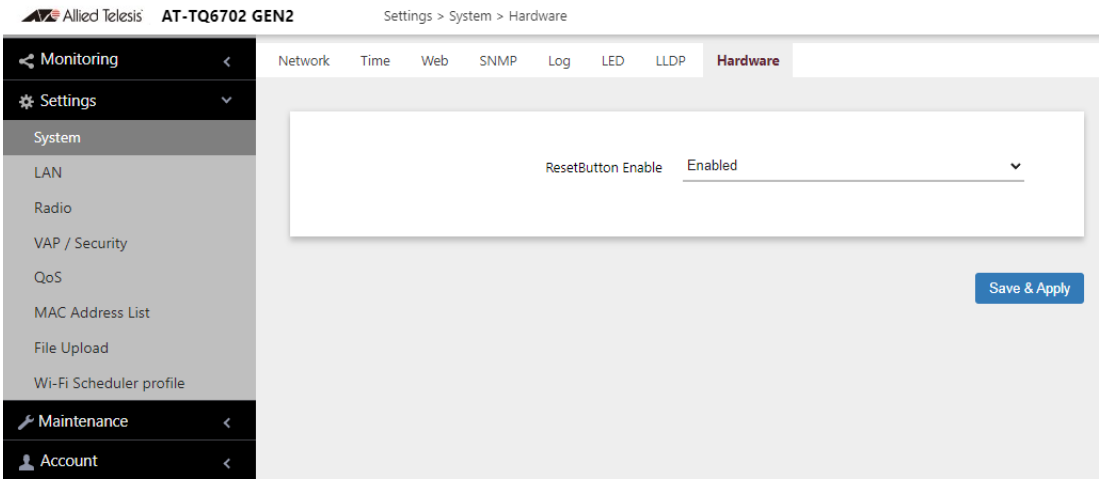

Figure 22. Hardware Window

3. From the **ResetButton Enable** pull-down menu, select one of the following:
   - ❒ Enabled: The Reset button is enabled. This is the default setting.
   - ❒ Disabled: The Reset button is disabled.
4. Click the **Save & Apply** button to save and update the configuration.

Chapter 4

LAN Port

This chapter describes the following procedures:

Enabling the Management VLAN Tag

You can enable or disable Management VLAN Tag on the LAN Settings window.

Guidelines for Management VLAN Tag

Here are the guidelines to enabling the management VLAN Tag:

- When the management VLAN is disabled, the default setting, the access point handles untagged packets as members of VLAN 1.
- When the management VLAN Tag is enabled, the access point accepts only tagged packets and discards all untagged packets.

Enabling or Disabling the Management VLAN Tag

To enable or disable the management VLAN Tag, perform the following procedure:

1. Select **Settings** > **LAN** from the main menu. Refer to Figure 23.

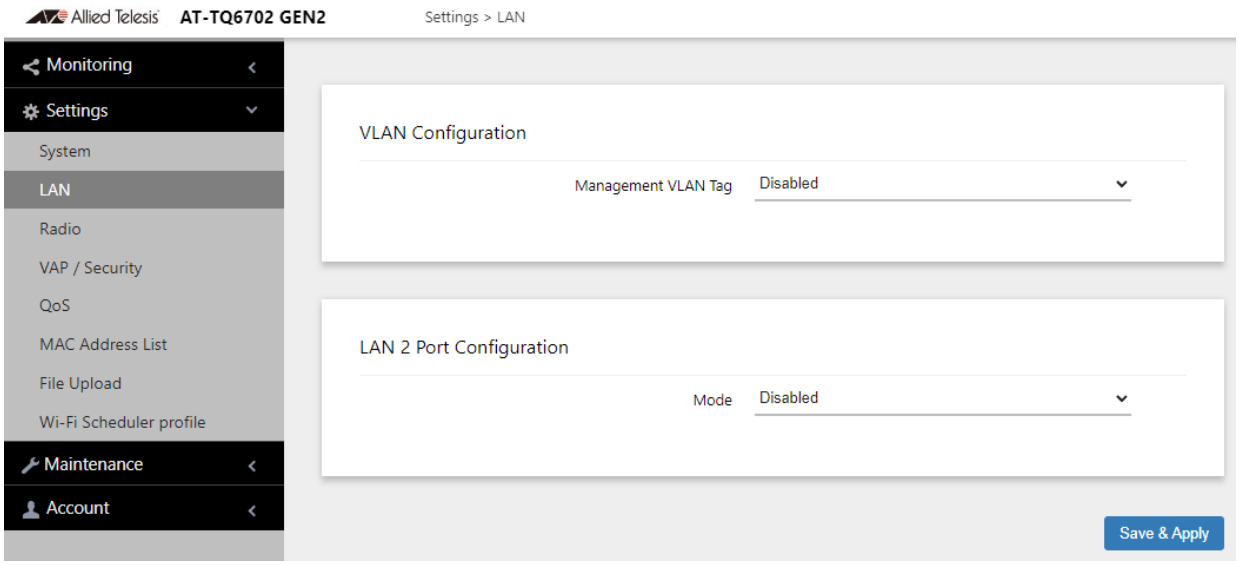

Figure 23. LAN Settings Window

2. Enable or disable Management VLAN Tag.
   - Enable: Activates the management VLAN Tag.
   - Disable: Deactivates the management VLAN Tag. This is the default setting.
3. Click the **Save & Apply** button to save and update the configuration.

Configuring the LAN2 Port

The access point has two Ethernet ports, labeled LAN1 and LAN2. You use the ports to connect the wireless access point to your wired network.

Here are their basic properties:

- The default setting for LAN1 port is enabled. You cannot disable it.
- LAN1 and LAN2 ports support PoE+.
- The default setting for LAN2 port is disabled.
- LAN1 and LAN2 ports can be combined into a Static Link Aggregation (LAG) to double the bandwidth between the access point and the wired network.
- LAN2 can be configured as a separate Ethernet port for another network device. This is referred to as the Cascade mode.

Static Link Aggregation (LAG)

You can double the bandwidth between the access point and your wired network by combining LAN1 and LAN2 ports into a static LAG. A static LAG functions as a single logical link between the access point and another network device, such as an Ethernet switch or router. A static LAG also provides link redundancy. If one link goes down, the access point maintains connectivity to the wired network over the remaining link. Refer to Figure 24.

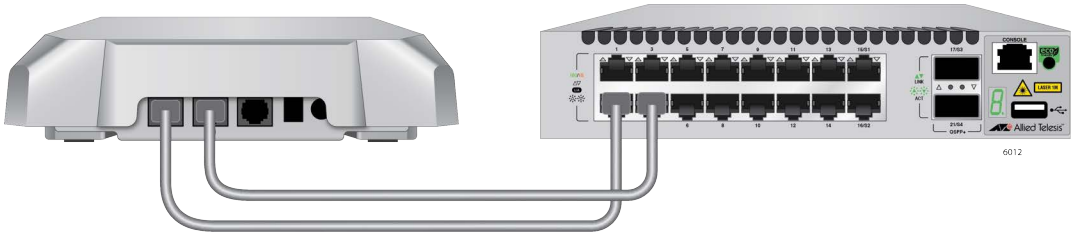

Figure 24. LAN1 and LAN2 Ports in a Static LAG

Here are guidelines to using LAN1 and LAN2 ports as a static LAG:

- You have to connect the ports to the same network device, such as an Ethernet switch or router, or virtual stacking devices. Do not connect the LAN ports to different network devices.
- The network device has to support static LAGs.
- You have to configure the two ports on the network device as a static LAG.

You activate the static LAG for LAN1 and LAN2 ports with the on-board web browser management interface, or with the AWC plug-in Vista Manager EX. You must use Vista Manager EX version 3.9.0 or later for the TQ6000 GEN2 access point.

Note
Do not enable and cable the LAN2 port until you have configured the other network device for the static LAG.

Cascade Mode

The LAN2 port has a Cascade mode. The mode allows you to use the port to connect another device to your network. The device can be an end node such as a printer or computer, as shown in Figure 25.

Figure 25. LAN2 Port in Cascade Mode with an End Node

It can also be a networking device such as a switch, router, or media converter. Refer to Figure 26.

Figure 26. LAN2 Port in Cascade Mode with a Networking Device

Here are the Cascade mode guidelines:

- The Cascade mode requires firmware version 8.0.1-1.1 or later.
- You set the Cascade mode with the on-board web browser management interface, or with the Vista Manager EX (version 3.9.0or later).
- Do not connect both LAN1 and LAN2 ports to the same network device when the LAN2 port is in the Cascade mode.

Configuring the LAN2 Port

To configure the LAN2 port, perform the following procedure:

1. Select **Settings** > **LAN** from the main menu. See Figure 27 on page 68.

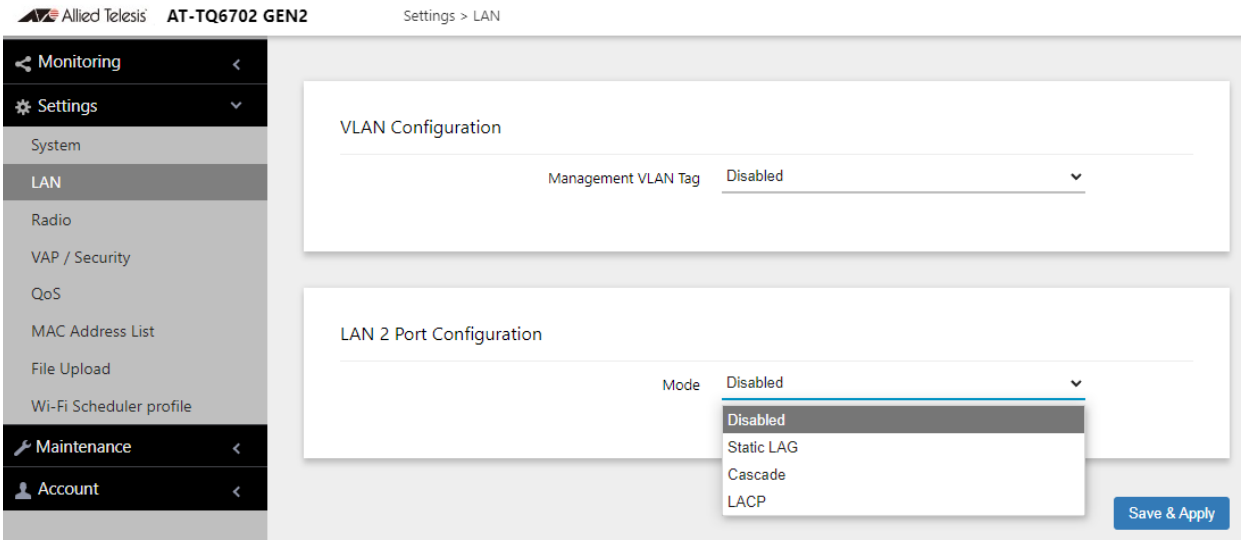

Figure 27. LAN Settings Window - LAN2 Port Configuration

The window has two sections. The LAN2 port is controlled with the LAN2 Port Configuration section. For information on the VLAN Configuration section, see “Enabling or Disabling the Management VLAN Tag” on page 65.

2. From the Mode pull-down menu in the LAN2 Port Configuration section configure the settings by referring to Table 14.

Table 14. LAN Settings Window - LAN2 Port Configuration Section

Item	Description
Mode	Select one of the following: - Disabled: Disable LAN2 port. - Static LAG: Combines LAN11 and LAN2 ports into a static LAG. - Cascade: Activates the Cascade mode on LAN2 port so that you can use the port to connect another device to your network. - LACP: Not supported.

3. Click the **Save & Apply** button to save and update your configuration.

If you enabled the Static LAG mode, the access point automatically combines LAN1 and LAN2 ports into a static LAG. Configure the ports on the other network device as a static LAG and connect LAN1 and LAN2 ports to it.

If you enabled the Cascade mode, connect the LAN2 port to a network device, such as a personal computer or an Ethernet switch. The access point begins forwarding and receiving traffic on the port.

Displaying the Status of LAN Port

To display the status of LAN port, perform the following procedure:

1. Select **Monitoring** > **Status** from the main menu.
2. Select **LAN**1 or **LAN2** from the sub-menu. See Figure 28.

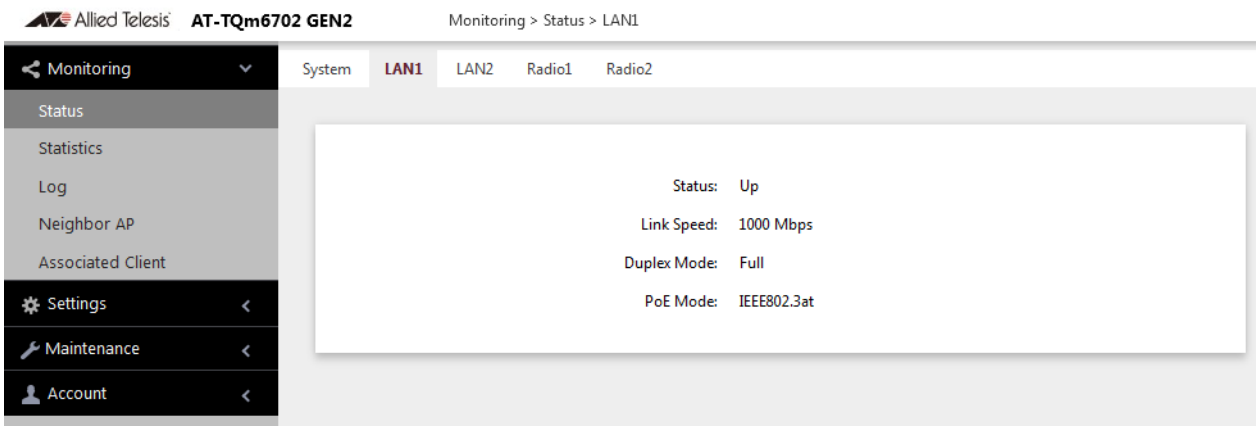

Figure 28. Status of LAN1 Port Window

The fields are defined in Table 15.

Table 15. Status of LAN1 or LAN2 Window

Item Name	Description
Mode (LAN2 Only)	Displays LAN2 Port Configuration. The options are: - Disabled - Static LAG - Cascade
Status	Displays the status of the LAN port. The possible states are listed here: - Up: The port has established a link with a network devices, such as an Ethernet switch or router. - Down: The port has not established a link with a network device.
Link Speed	Displays the speed of the link (100, 1000, 2500, or 5000 Mbps).

Table 15. Status of LAN1 or LAN2 Window (Continued)

Item Name	Description
Duplex Mode	Displays the duplex mode of the port, as follows: - Full: Full-duplex. - Half: Half-duplex.
PoE Mode	Displays the PoE mode.

Chapter 5

2.4GHz and 5GHz Radios

This chapter has the following procedures:

Configuring the Radios

The radio settings are divided into two groups:

- ❒ “Configuring Basic Radio Settings” next
- ❒ “Configuring Advanced Radio Settings” on page 76
- ❒ “Configuring Wi-Fi Scheduler” on page 81

Configuring Basic Radio Settings

To configure the basic settings for Radio1 or Radio2, perform the following procedure:

1. Select **Settings** > **Radio**.
2. Select **Radio1** or **Radio2** from the sub-menu. You can configure only one radio at a time.
3. Click the **Basic Settings** tab shown in Figure 29. This is the default tab.

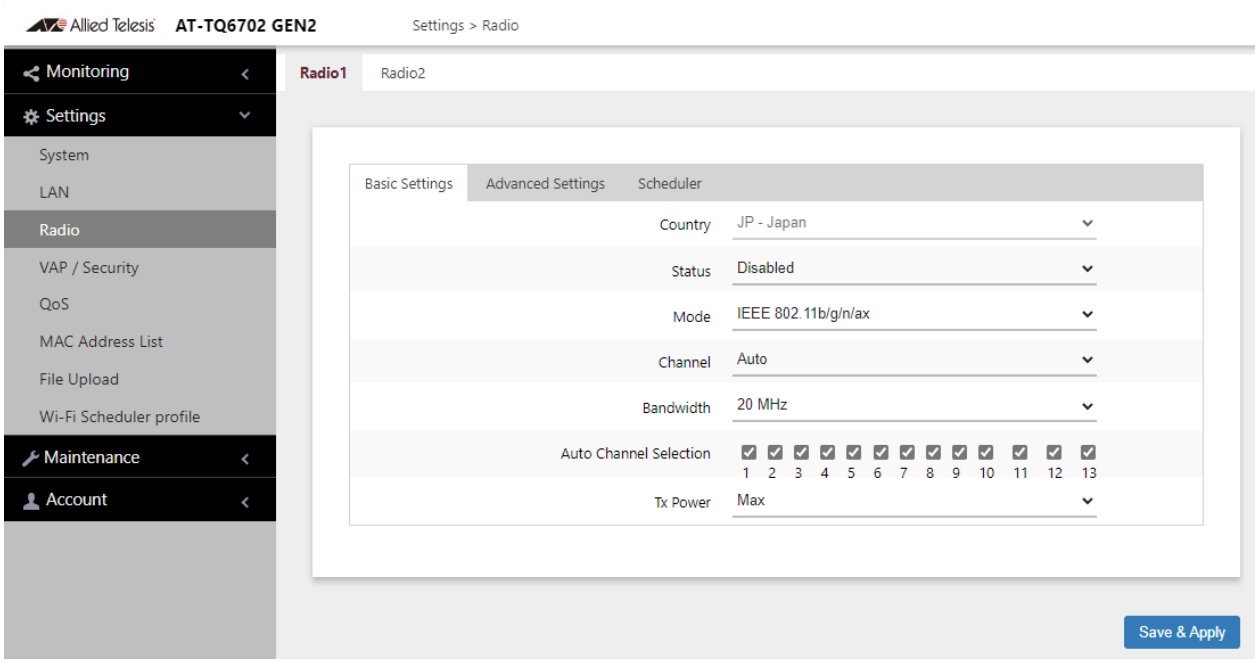

Figure 29. Basic Radio Settings Window

4. Configure the settings by referring to Table 16 on page 74.

Table 16. Basic Radio Settings Window

Field	Description
Country	Select the country code that applies to your country or region. The country code ensures that the device operates in compliance with the codes and regulations of your region or country. Here are the guidelines: - You can select only one country. - The Country Code parameter is shown in the Basic Settings windows of both radios but it can only be set from Radio1. - The same country code applies to both radios. - Changing the country code disables the radios. - You have to reconfigure the radio settings if you change the country code. - You cannot change the country code on units sold in North America, Japan, or Taiwan.
Status	Activate or deactivate the radio. The selections in the pull-down menu are described here: - Enabled: Activates the radio. - Disabled: Deactivates the radio. This is the default setting.
Mode (Radio1)	Select the communications protocol for Radio1 from the pull-down menu. The selections are listed here: - IEEE 802.11b/g: The access point accepts 802.11b and 802.11g clients. - IEEE 802.11b/g/n: The access point accepts 802.11b, 802.11g and 802.11n clients. - IEEE 802.11b/g/n/ax: The access point accepts 802.11b, 802.11g, 802.11n,and 802.11ax clients. This is the default for Radio1.

Table 16. Basic Radio Settings Window (Continued)

Field	Description
Mode (Radio2)	Select the communications protocol for Radio2 from the pull-down menu. The selections are listed here: - IEEE 802.11a: The access point accepts 802.11a clients. - IEEE 802.11a/n: The access point accepts 802.11a and 802.11n clients. - IEEE 802.11a/n/ac: The access point accepts 802.11a, 802.11n and 802.11ac clients. - IEEE 802.11a/n/ac/ax: The access point accepts 802.11a, 802.11n, 802.1ac,and 802.11ax clients. This is the default for Radio2. Wi-Fi multimedia (WMM) has to be enabled (default) to use IEEE 802.11n, IEEE 802.11ac, or IEEE 802.11ax. Refer to “Configuring QoS Basic Settings” on page 190.
Channel	Select the channel for the radio from the pull-down menu. Here are the guidelines: - You can select only one channel. - The channels vary by radio, bandwidth, and country. - To view the current active channel, refer to “Displaying Radio Status” on page 87.
Bandwidth (Radio1)	Select the bandwidth for Radio1 from the pull-down menu. The selections for IEEE 802.11n are listed here: - 20 MHz. This is the default setting. - 40 MHz For IEEE 802.11n modes, channel width can be 40 MHz-wide or the legacy 20 MHz-wide. The 40 MHz-wide channel allows for higher data rates, but reduces the number of available channels for other wireless devices. The only bandwidth for IEEE 802.11b/g is 20 MHz.

Table 16. Basic Radio Settings Window (Continued)

Field	Description
Bandwidth (Radio2)	Select the bandwidth for Radio2 from the pull-down menu. The available bandwidths for IEEE 802.11n/ac/ax are listed here: - 20 MHz. This is the default setting. - 40 MHz - 80 MHz - 80+80 MHz The only bandwidth for IEEE 802.11a is 20 MHz.
Auto Channel Selection (Radio 1)	Select the channels that the radio can choose from when the Channel parameter is set to Auto. Here are the guidelines: - A channel is enabled when its check box has a check and disabled when the check box is empty. - The available channels very by radio, mode, bandwidth, and country. - By default, all available channels are enabled. - This parameter is disabled when the channel is selected manually.
Tx Power	Select the strength of the radio transmitter. The selections are Max (maximum), High, Middle, Low, Min (minimum). The default is Max.

5. Click the **Save & Apply** button to save and update the configuration.

Configuring Advanced Radio Settings

To configure the advanced parameters for Radio1 or Radio2, perform the following procedure:

1. Select **Settings** > **Radio** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. You can configure only one radio at a time.
3. Click the **Advanced Settings** tab. See Figure 30 on page 77.

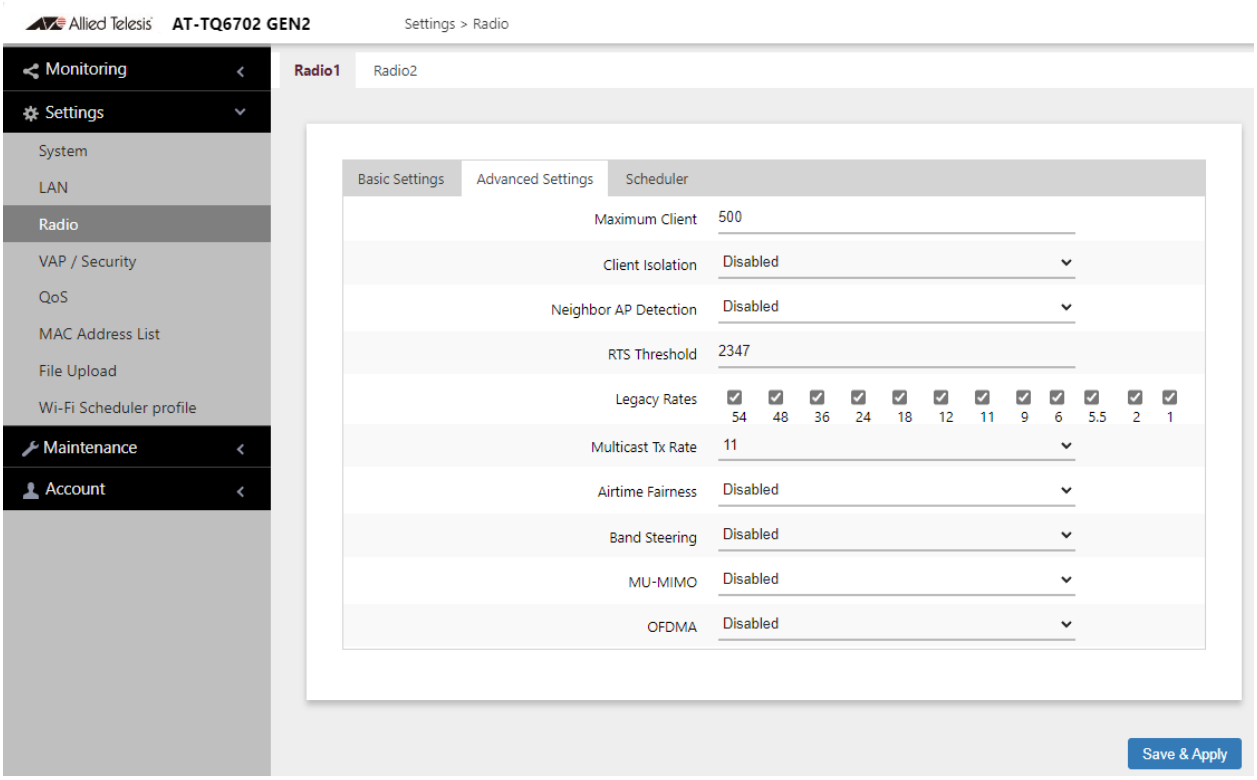

Figure 30. Advanced Radio Settings Window

4. Configure the parameters by referring to Table 17.

Table 17. Advanced Radio Settings Window

Field	Description
Maximum Clients	Use this option to specify the maximum number of wireless clients that a radio will support at one time. You might use the option to control the distribution of clients over the radios. A radio rejects all clients when the parameter is set to 0. The maximum numbers of wireless clients that a radio supports at one time are: - 2.4GHz Radio1 - 320 clients (default setting) - 5GHz Radio2 - 320 clients (default setting)

Table 17. Advanced Radio Settings Window (Continued)

Field	Description
Client Isolation	Enable or disable Client Isolation. The options are: - Disabled: Disable Client Isolation. The access point allows wireless clients to communicate with other clients in the same VAP or different VAPs, and with the wired LAN. This is the default setting. - Within VAP: enables Client Isolation. Devices connected to the same VAP are prevented from communicating with each other, thus effectively isolating them. This feature is often utilized in public or guest Wi-Fi networks to safeguard the privacy and security of individual users. - Within AP: enables Client Isolation. The access point will not allow wireless clients to communicate with other clients on the same or other VAPs.
Neighbor AP Detection	Enable or disable Neighbor AP Detection, which controls whether the access point listens for neighboring access points. Here are the options: - Enabled: The access point listens for neighboring access points and displays them in the Neighbor AP window. See “Displaying Neighbor AP” on page 36 - Disabled: The access point does not listen for neighboring access points. This is the default setting.
RTS Threshold	Not supported.
Legacy Rates	Select the supported and advertised data transmission rates for IEEE 802.11b/g of the radio. Here are the guidelines: - The data rates vary by country. - The default is all data rates are enabled. - Radios are generally more efficient when they advertise subsets of their supported data rates.

Table 17. Advanced Radio Settings Window (Continued)

Field	Description
Multicast Tx Rate	Select the maximum amount of multicast packets the radio can transmit per second. The default values are listed here: - 2.4GHz Radio1: 11Mbps - 5GHz Radio2: 6Mbps
Airtime Fairness	Airtime Fairness equalizes airtime among VAPs. When a wireless client is communicating with multiple VAPs, the airtime is equally divided among the corresponding VAPs. The airtime of a VAP with which the wireless client is not communicating is allocated to VAPs that the wireless client is corresponding. Here are the options: - Enabled: Activates Airtime Fairness. - Disabled: Turn Airtime Fairness off. This is the default setting. The maximum number of wireless clients that Airtime Fairness can control at a time is 50.
Band Steering	Use this option to enable or disable band steering on the radios. Band steering reduces radio congestion by forcing wireless clients that support both 2.4GHz and 5GHz radios to associate with VAPs on a different radio during periods of traffic congestion. Band steering forces clients to associate with VAPs on a 5GHz radio when there is traffic congestion on the 2.4GHz radio. Conversely, clients are forced to associate with VAPs on the 2.4GHz radio when the 5GHz radios are congested. Here are the guidelines: - Enabling band steering on one radio activates it on the other radio. Conversely, disabling the feature on one radio disables it on the other radio. - Ideally, the VAP settings on both radios should be identical. This includes SSID names, VLAN IDs, and security settings. - The default setting is disabled.

Table 17. Advanced Radio Settings Window (Continued)

Field	Description
MU-MIMO	Multi-user, Multiple Input, Multiple Output (MU-MIMO) helps increase the number of simultaneous users a single access point can support. The options are: - Disabled: MU-MIMO is disabled. This is the default setting. - Enabled: the access point can support up to 4 wireless clients simultaneously.
OFDMA	Orthogonal Frequency Division Multiple Access (OFDMA) allows the access point to serve multiple wireless clients at the same time by dividing packets into separate bands. The options are: - Disabled: OFDMA is disabled. This is the default setting. - Enabled: The access point can serve multiple wireless clients at the same time.

Table 17. Advanced Radio Settings Window (Continued)

Field	Description
Off-channel CAC (Radio 2 only) (Wi-Fi regulation: CE countries only)	Off-channel CAC is a mandate for a 5GHz radio to detect radar systems, stop transmitting, and switch to another channel to avoid interfering with the radar systems. This feature provides seamless change of channels and connectivity to wireless clients. The options are: - Disabled: Off-channel CAC is disabled. This is the default setting. - Enabled: Off-channel CAC is enabled. When detecting radar systems, the 5GHz radio switches to another channel and keeps connectivity of wireless clients. The access point keeps connectivity; however, a wireless client continues to be connected or disconnected and reconnected depending upon the behavior of wireless clients. Here are guidelines to enable Off-channel CAC: - For TQ6702 GEN2 and TQm6702 GEN2, Off-channel CAC can be enabled only when the bandwidth is set to 80+80MHz. - For TQ6602 GEN2 and TQm6602 GEN2, Off-channel CAC can be enabled only when the bandwidth is set to 20, 40, or 80MHz. - The feature is available for Wi-Fi regulation: CE countries only. For more information, see Chapter 6, “Dynamic Frequency Selection (Off-Channel CAC)” on page 97.

5. Click the **Save & Apply** button to save and update the configuration.

Configuring Wi-Fi Scheduler

Wi-Fi Scheduler can be configured manually (per radio) or by assigning a Wi-Fi Scheduler Profile to a Radio.

To configure Wi-Fi Scheduler for Radio 1 or Radio2, perform the following:

1. Select **Settings** > **Radio** from the main menu.

2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select the **Scheduler** tab.
4. Select Enabled in the Wi-Fi Scheduler field.

Note
Radio and VAP schedulers run independently of each other and the configuration priority is in the following order: Radio Scheduler > VAP Scheduler > manual configuration. For example, if a VAP is enabled for a specific time period, and the Radio with that VAP is disabled for that same time period, then the VAP will be disabled.

Manually configuring a Schedule

1. Select **Manual Configuration** as the Schedule configuration method. See Figure 31.

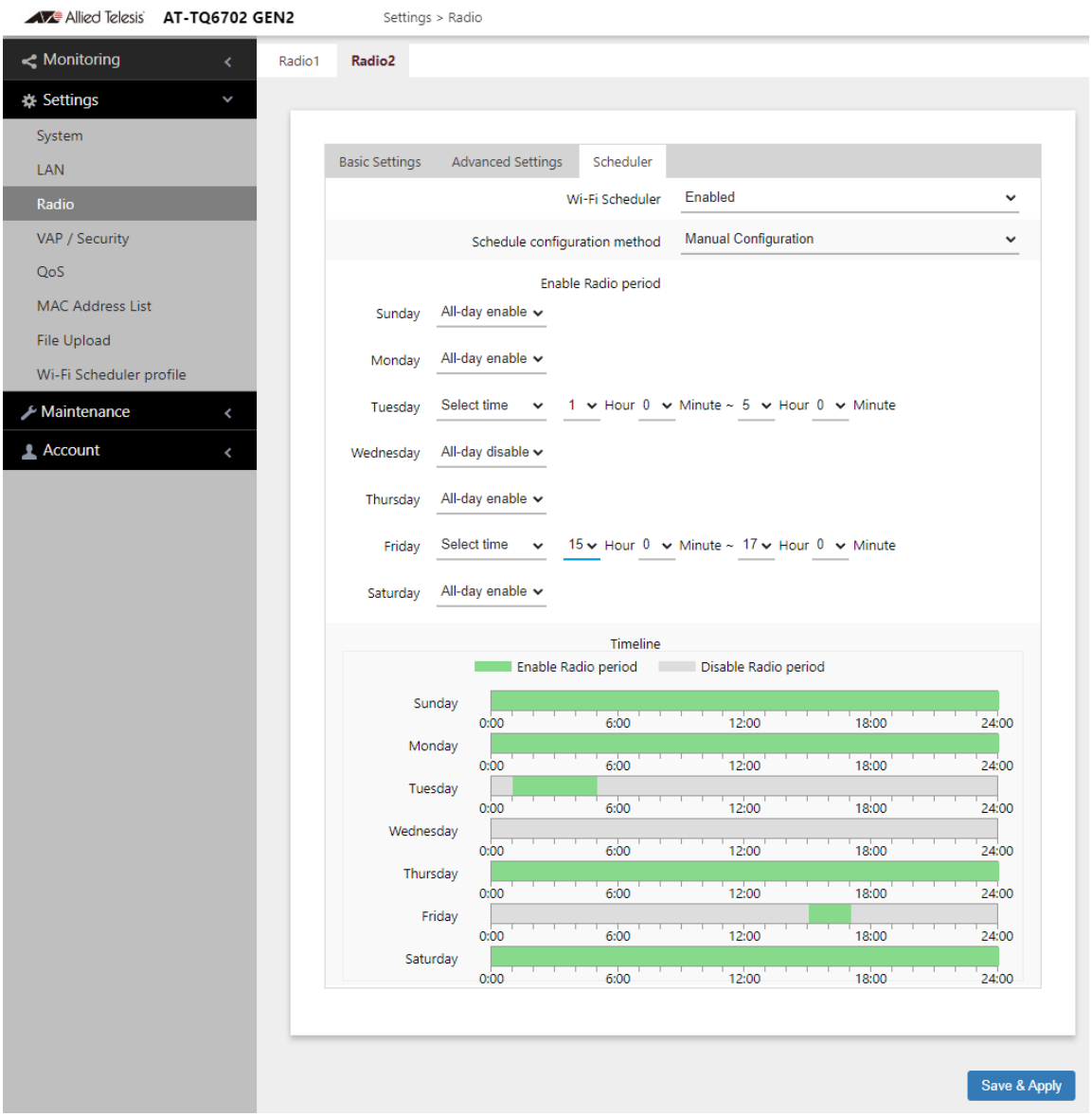

Figure 31. Radio Wi-Fi Scheduler - Manual configuration

2. Configure the parameters by referring to Table 18.

Table 18. Radio Wi-Fi Scheduler - Manual configuration

Field	Description
Wi-Fi Scheduler	Enable or Disable Wi-Fi Scheduler. Disabled is the default setting.

Field	Description
Schedule configuration method	Choose the Profile Configuration method (once Wi-Fi Scheduler has been enabled): - Manual Configuration: Allows the time and day to be set for that specific radio. - Profile Configuration: Assign a profile to that Radio.
Enable Radio period	For each day, the following can be selected: - All-day enable: Wi-Fi is enabled for the 24 hour period. - All-day disable: Wi-Fi is disabled for the 24 hour period. - Select time: Manually set the time that the Radio will be enabled.
Timeline	Graphical display of the timeline configured.

Assigning a Wi-Fi Scheduler Profile

1. Select **Profile Configuration** as the Schedule configuration method. See Figure 32.

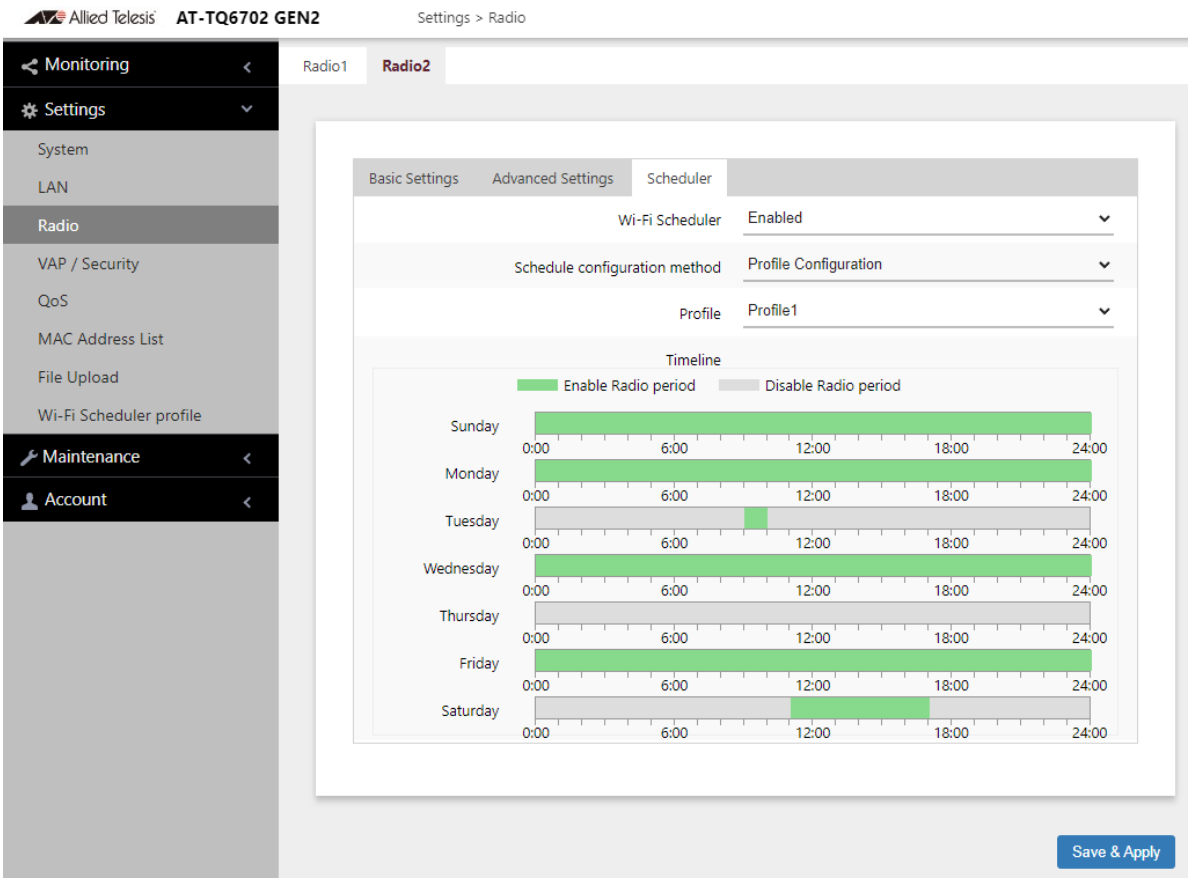

Figure 32. Assigning a Wi-Fi Scheduler Profile to a Radio

2. Configure the parameters by referring to Table 19.

Table 19. Radio Wi-Fi - Assigning a Scheduler Profile

Field	Description
Wi-Fi Scheduler	Enable or Disable Wi-Fi Scheduler. Disabled is the default setting.
Schedule configuration method	Choose the Profile Configuration method (once Wi-Fi Scheduler has been enabled): - Manual Configuration: Allows the time and day to be set for that specific radio. - Profile Configuration: choose from Profile 1 to Profile 10. These profiles are configured in “Configuring a Wi-Fi Scheduler Profile” on page 201.

Table 19. Radio Wi-Fi - Assigning a Scheduler (Continued)Profile

Field	Description
Profile	Choose from Profile 1 to Profile 10. These profiles are configured in Wi-Fi Scheduler profile. See “Configuring a Wi-Fi Scheduler Profile” on page 201
Timeline	Graphical display of the timeline configured.

3. Click the **Save & Apply** button to save and update the configuration.

Displaying Radio Status

To display operational information about a radio, perform the following procedure:

1. Select **Monitoring** > **Status** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. You can view only one radio at a time. The example in Figure 33 is for Radio1.

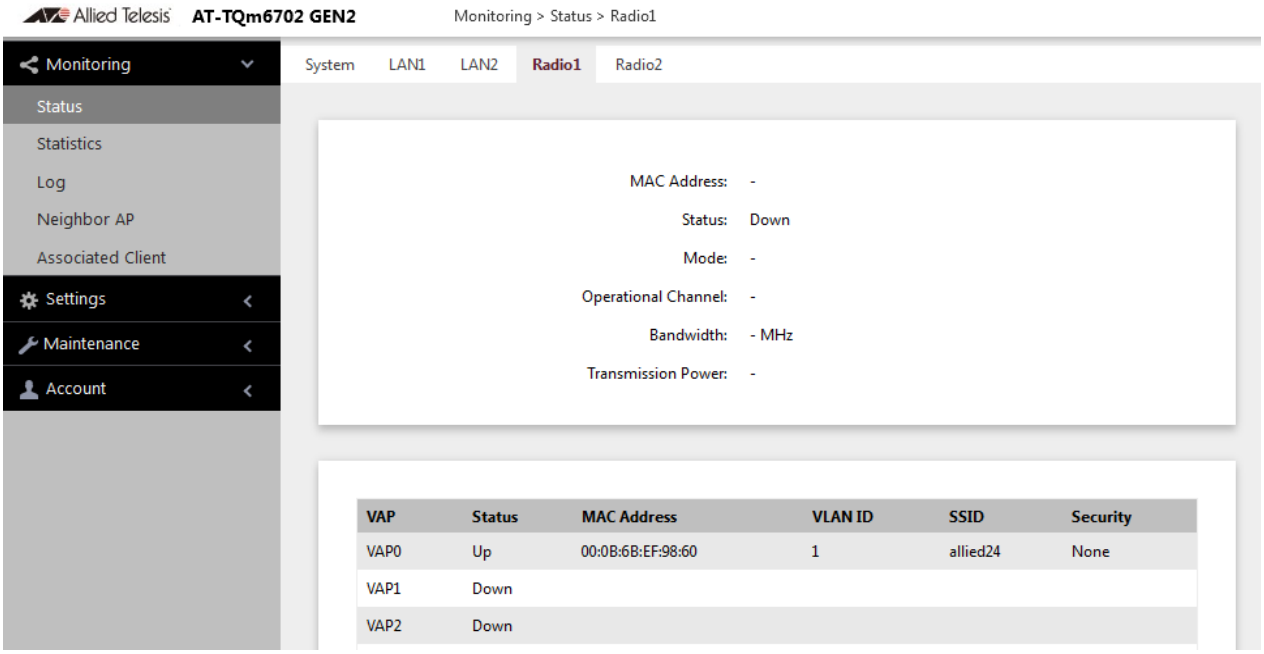

Figure 33. Radio1 Status Window

Figure 34 is an example for Radio2.

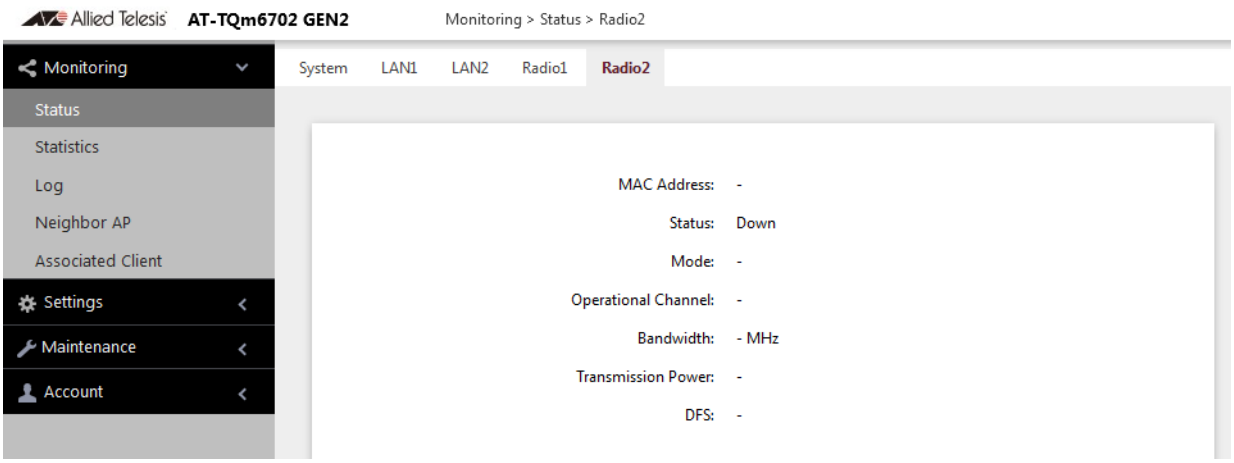

Figure 34. Radio2 Status Window

Note
The radio status window for Radio2 includes a DFS (Dynamic Frequency Selection) field. For information, see “Dynamic Frequency Selection” on page 90.

The fields are defined in Table 20.

Table 20. Radio Status Window

Field	Description
MAC Address	Displays the MAC address of the wireless interface.
Status	Displays the status (up, down) of the wireless interface.
Mode	Displays the current wireless communication mode. Radio1 has these modes: - IEEE 802.11b/g - IEEE 802.11b/g/n - IEEE 802.11b/g/n/ax Radio2 has these modes: - IEEE 802.11a - IEEE 802.11a/n - IEEE 802.11a/n/ac - IEEE 802.11a/n/ac/ax
Operational Channel	Displays the active channel. The channel may have been selected manually.
Bandwidth	Displays the current bandwidth.
Transmission Power	Displays the transmission power, in dBm.

Table 20. Radio Status Window (Continued)

Field	Description
DFS (Radio2 only)	Displays the status of DFS (Dynamic Frequency Selection). For background information, refer to “Dynamic Frequency Selection” on page 90. The possible states are listed here: - IDLE: DFS is inactive because the radio is using a W52 or W58 channel. Those channels are not used by DFS. - CAC: Channel Availability Check: The radio has selected a W53 or W56 channel and is performing the DFS radar detection period for one minute before beginning to transmit or receive wireless traffic. If no radar is detected, the radio moves to the ISM status. - ISM: In-Service Monitoring: The radio is using a DFS target channel. If radar is detected, it changes the channel. The DFS status changes to IDLE if the new channel is W52 or W58, or to CAC if the new channel is W53 or W56. - OOC: Out Of Channels: The radio has stopped transmitting and receiving client packets because radar signals are detected on all channel candidates. After 30 minutes, it transitions to CAC.

Dynamic Frequency Selection

Dynamic frequency selection (DFS) is an industry standard that defines how wireless access points are to respond to the presence of radar signals on 5GHz channels. The standard states that a wireless access point that detects radar signals on its current 5GHz channel has to stop transmitting and select another channel to avoid interfering with the signals.

The wireless access points support DFS on 5GHz channels that countries or regions have designated as DFS channels. If an access point detects a radar signal on its current 5GHz channel and if the channel is designated as a DFS channel, it immediately marks the channel as unusable for a minimum of thirty minutes and randomly selects another channel with which to communicate with its clients.

Here are the guidelines for DFS on the wireless access points:

- ❒ DFS channels vary by country or region.
- ❒ DFS cannot be disabled on the wireless access points.
- ❒ DFS does not apply to channels on the 2.4GHz radio.

Note
To determine whether Radio2 is using a DFS channel, refer to “Displaying Radio Status” on page 87.

Setting the Country Code Setting

Note
You cannot change the country code on units sold in North America, Japan, Canada, or Taiwan.

You should set the country code setting of the access point as soon as you install the unit so that it operates in compliance with the codes and regulations of your region or country.

Note
Changing the country setting disables the radios. The procedure is disruptive to the operations of your network if the unit is actively forwarding network traffic.

To set the country code setting, perform the following procedure:

1. Select **Settings** > **Radio**.
2. Select **Radio1** from the sub-menu. The country code must be set from Radio1.
3. Click the **Basic Settings** tab. This is the default tab. Refer to Figure 29 on page 73.
4. Select the **Country Code** pull-down menu and choose your country or region. Here are the guidelines:
   - ❒ You can select only one country.
   - ❒ The Country Code parameter is shown in the Basic Settings windows of both radios, but can only be set from Radio1.
   - ❒ The same country code applies to Radio2.
   - ❒ Changing the country code disables the radios.
   - ❒ You have to reconfigure the radio settings after changing this parameter.
5. Click the **Save & Apply** button to save and update the configuration.

Chapter 6

Wireless Distribution System Bridges

This chapter contains the procedures for managing Wireless Distribution Bridges. The chapter contains the following sections:

Introduction to Wireless Distribution Bridges

A wireless distribution system (WDS) bridge is a wireless connection between access points that allows units to forward traffic directly to each other over a wireless connection, as if they were connected with a physical Ethernet wire. The feature is typically used to extend networks into areas where Ethernet cable installation might be impractical or expensive.

A WDS bridge consists of one parent and up to three children. The parent is connected to the wired network through its LAN ports. The children function as wireless clients of the parent, communicating with the wired network over the WDS bridge to the parent. An example of a parent with three children is shown in Figure 35.

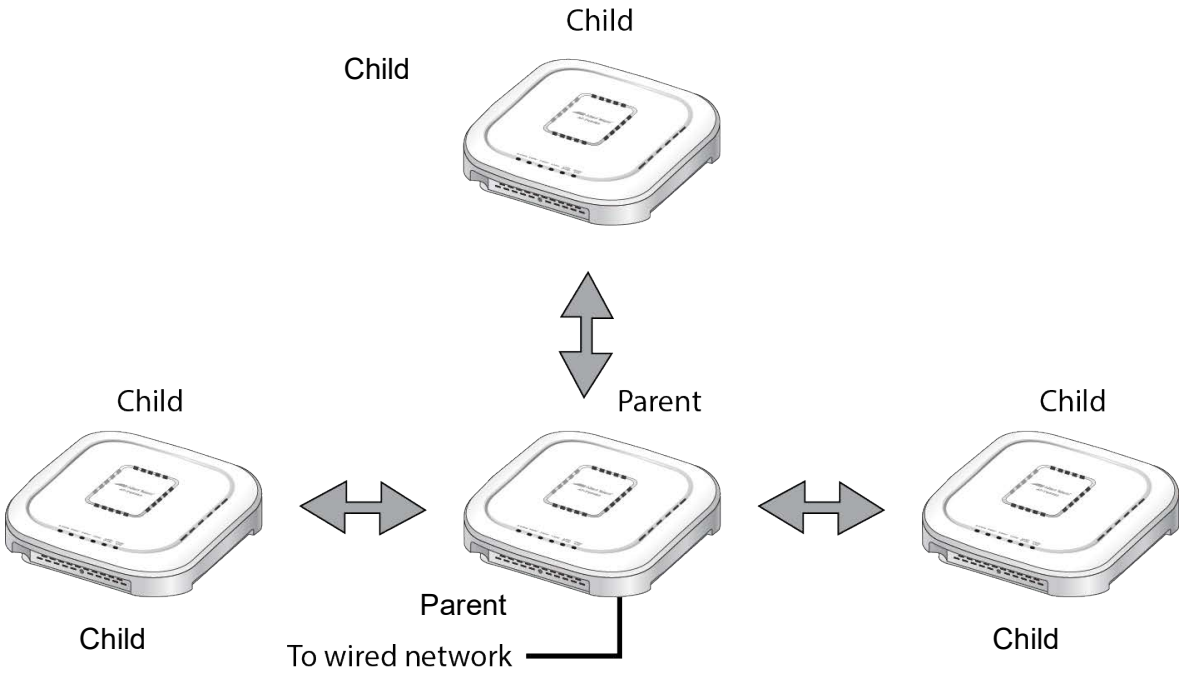

Figure 35. WDS Bridge

When a child receives traffic from a wireless client that is intended for the wired network, it transmits the traffic over the WDS bridge to the parent, which forwards the packets on its LAN ports. Conversely, when a parent receives traffic on the wired network intended for a wireless client associated on a child, it transmits the packets to the child over the bridge.

A WDS bridge consists of a radio and a radio channel. You can use Radio1 or Radio2 and any channel. An important rule to follow is that the parent and children of a bridge must all use the same radio and channel. The selected radio should only be used for the WDS bridge. Wireless clients should use other radios to access the network.

Additionally, because the access points have to use the same channel, you have to select the channel manually, instead of using the default auto channel setting. In the example in Figure 36, the parent and children are using Radio2 and channel 40 for the WDS bridge. Wireless clients can access the network using either Radio1 or Radio2.

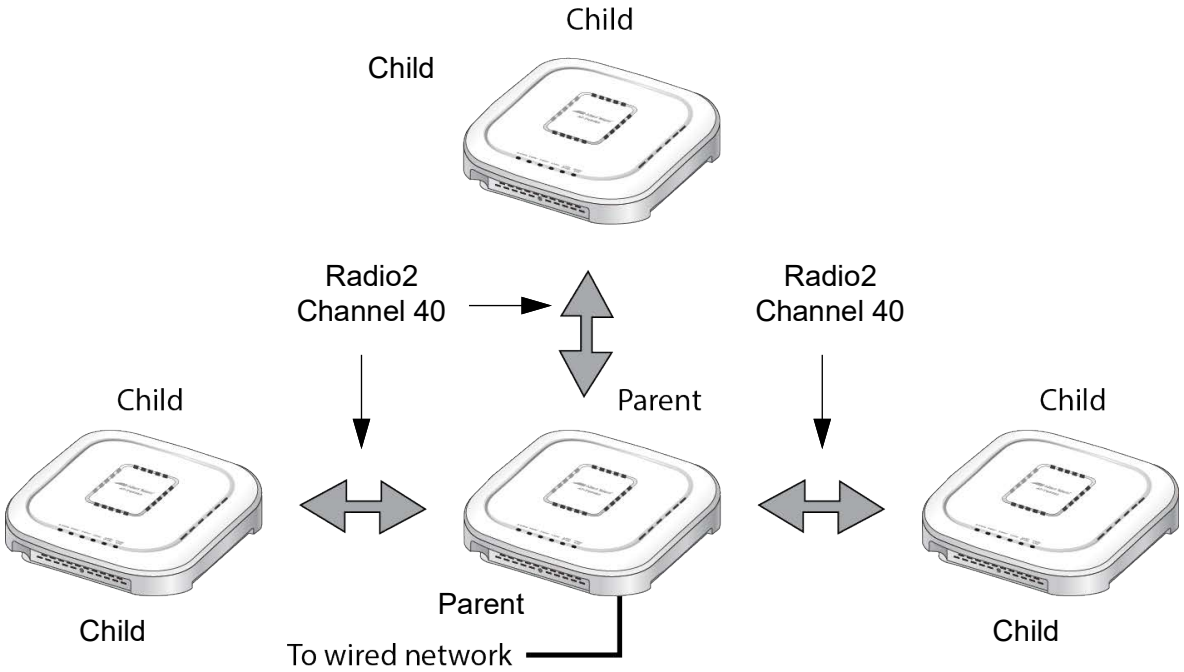

Figure 36. Example of Radio and Channel Assignments in a WDS Bridge

An access point can be both parent and child at the same time in different WDS bridges. That is, it can be a parent in one WDS bridge and a child in another. Figure 37 on page 95 is an example. Access Point A is functioning as the parent to children 1 and 2 in one WDS bridge, and as child 5 to Access Point B in another bridge. In contrast, Access Point B is functioning solely as a parent, in this case to children 3, 4, and 5, which is Access Point A.

Each WDS bridge has to use a different radio and channel. This is illustrated in the example where Access Point A, as parent, and children 1 and 2 are using Radio 1 and channel 10 for their WDS bridge. In contrast, Access Point B and its children are using Radio2 and channel 40.

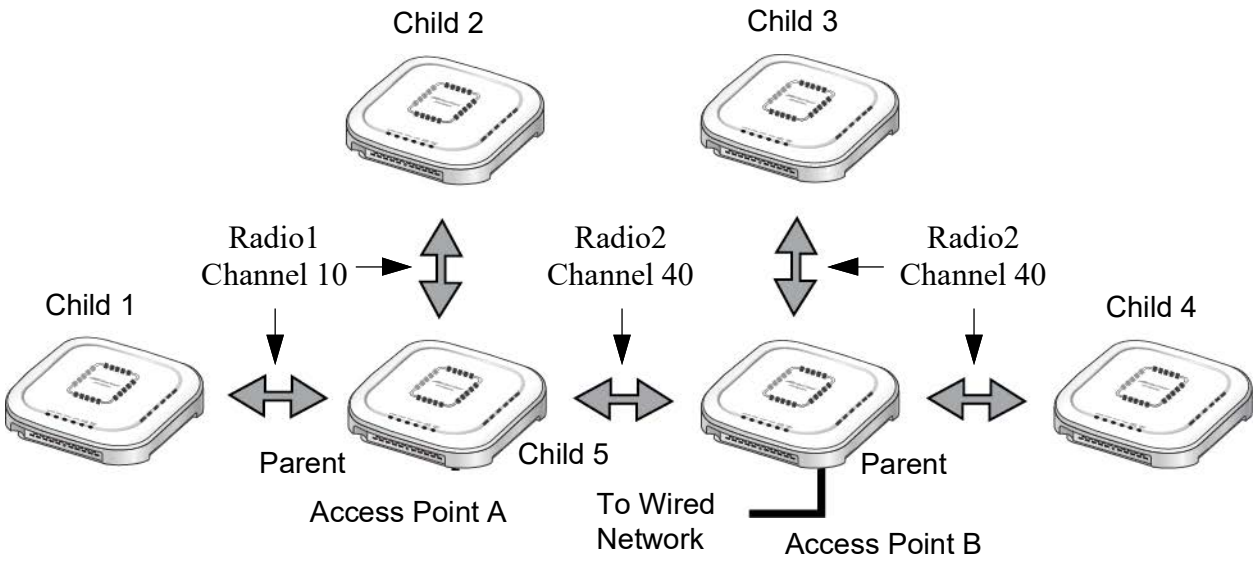

Figure 37. Example of an Access Point as Both Parent and Child

Note
Only one parent should be connected to the wired network. Connecting the LAN ports on both parents to the wired network might form a loop in your network topology, which might cause broadcast storms.

WDS Bridge Elements

This section describes the various elements of a WDS bridge.

Radio

You can use Radio1 or Radio2 for a WDS bridge. Here are the guidelines:

- The access points must all use the same radio for a bridge.
- The selected radio should only be used for a WDS bridge. It should not be used by wireless clients.
- A bridge uses VAP0 on the selected radio.
- VAP1 to VAP15 on the selected radio are automatically disabled and cannot be used.

VAP0

The WDS bridge uses VAP0 on the selected radio as the wireless link. The VAP assignment cannot be changed. VAP1 to VAP15 are automatically disabled. Wireless clients should not be allowed to use VAP0 of the designated radio when the devices are arranged in a WDS bridge because the bridge might experience a reduction in performance. Instead, wireless clients should use the other radios and VAPs to access the network.

The VLAN ID, SSID, security and channel settings for VAP0 must be the same on all the access points in the WDS bridge.

Radio Channel

When access points are operating in close proximity to each other such that there is an overlap in coverage, the usual practice is to set the radios to different channels to minimize radio interference and improve performance.

The radios in the access points of a WDS bridge, however, have to use the same channel. This means that you have to disable automatic channel selection, which is the default settings on the units, and manually select the channel. The common channel between the access points can be any available channel.

Parents and Children

When configuring an access point for a WDS bridge, you designate it as either parent or child. The parent is usually the unit with its LAN port connected to the wired network. Children are units that access the wired network through the parent. A WDS bridge can have only one parent and no more than three children. An example of a bridge of four units is shown in Figure 35 on page 93.

Security

Here are the available security settings for the VAP0 of a WDS bridge:

- No security
- WPA Personal

Note
You cannot use WPA Enterprise on VAP0 of a WDS bridge.

Dynamic Frequency Selection (Off-Channel CAC)

Dynamic frequency selection (DFS) is an industry standard that defines how wireless access points are to respond to the presence of radar signals on 5GHz channels. The standard states that a wireless access point that detects radar signals on its current 5GHz channel has to stop transmitting and select another channel to avoid interfering with the signals.

The wireless access points support DFS on 5GHz channels that countries or regions have designated as DFS channels. If an access point detects a radar signal on its current 5GHz channel and if the channel is designated as a DFS channel, it immediately marks the channel as unusable for a minimum of thirty minutes and randomly selects another channel with which to communicate with its clients.

If a wireless access point is using a DFS 5GHz channel for a WDS bridge and it detects radar signals, it randomly selects another channel so as not to interfere with the signals. This action, however, renders the bridge non-functional.

You can prevent this from occurring by selecting a non-DFS 5GHz channel as the communication link between the wireless access points of a WDS bridge. Here are three examples of non-DFS channels:

- 36 - 5180 MHz
- 40 - 5200 MHz
- 44 - 5220 MHz

Here are the guidelines for DFS on the wireless access points:

- DFS channels vary by country or region.
- DFS cannot be disabled on the wireless access points.
- DFS does not apply to channels on the 2.4GHz radio.

Guidelines

Here are the guidelines for WDS bridges:

- A WDS bridge can have from two to four wireless access points.
- One access point is the parent and the others are children.
- The LAN ports on the parent are connected to the wired network.
- If two WDS bridges are connected together, as shown in Figure 37 on page 95, you should connect the LAN ports on only one parent to the wired network. Connecting the LAN ports on both access points might form a loop in the network topology.
- The LAN ports on children should not be connected to the wired network.
- You can use Radio1 or Radio2 for the WDS bridge.
- You can use no security or WPA Personal for VAP0 on the selected radio of the bridge. Allied Telesis recommends using WPA Personal security.
- A WDS bridge has to be consisted of AT-TQ6702 GEN2, AT-TQm6702 GEN2, AT-TQ6602 GEN2, or AT-TQm6602 GEN2 access points.
- The radios of the WDS bridge have to be set to the same mode and channel.
- You must set the channel manually. Do not use the Auto setting.
- If you use Radio1or Radio2 for the bridge, Allied Telesis recommends selecting a channel that is not part of dynamic frequency selection. This is to minimize the chance that the access points have to change channels and break the WDS bridge due to radar signals.
- A WDS bridge uses VAP0 on the selected radio as the communications link. The VAP should not be used by wireless clients. All other VAPs on the radio are disabled.
- An access point can be a parent in one bridge and a child in another.
- The WDS bridge feature on these access points is not compatible with the same feature on other products from Allied Telesis or other companies.

Preparing Access Points for a WDS Bridge

This procedure contains the general steps to preparing access points for a WDS bridge. The procedure assumes the following:

- ❒ You have selected the access points for the bridge.
- ❒ You have decided which access point will be the parent and which will be the children.
- ❒ You have chosen the radio that the access points will use for the bridges. It can be Radio1 or Radio2.
- ❒ You have chosen the radio mode and channel that all the access points will use for the bridges.
- ❒ You have chosen the security level for VAP0 of the selected radio for the bridges. The security level can be none or WPA Personal. Allied Telesis recommends using WPA Personal security.

The settings must be the same on all the access points of a WDS bridge. To prepare an access point for a WDS bridge, perform the following procedure:

1. Start a management session.
2. On the selected radio for the bridge, set the mode and channel. Refer to “Configuring Basic Radio Settings” on page 73. Here are the guidelines:
   - ❒ You can use any available radio mode for the bridge, but the radios in the different access points must use the same mode.
   - ❒ You can use any available channel, but the devices must use the same channel. Do not use the Auto setting.
3. Configure the security setting for VAP0 on the radio. The security setting can be none or WPA Personal. For instructions, refer to “Configuring VAP Security” on page 109.
4. Select **Settings** > **VAP / Security**.
5. Choose the radio for the WDS bridge by selecting **Radio1** or **Radio2** from the sub-menu.
6. Select **VAP0** from the sub-menu. This is the default VAP.
7. Select the **Virtual Access Point** tab. This is the default tab.
8. From the Mode pull-down menu, select either **WDS Parent** or **WDS Child**. This can only be set on VAP0.

9. Click the **Save & Apply** button to save and update the configuration, or click the **View QR code** button to view the QR code.

   Note
   The access point disables VAPs 1 to 15 on the same radio.

10. Repeat this procedure on all access points to be in the WDS bridge.

    When an access point is designated as a child, it automatically begins searching for a parent on the designated radio and channel. If it finds one, it forwards traffic from its wireless clients over the bridge to the parent, as needed, and transmits traffic from the parent to its clients. To view the children of a parent, display the Associated Clients window, as explained in “Displaying Associated Clients” on page 37.

Chapter 7

Virtual Access Points

This chapter contains the procedures for managing virtual access points (VAPs). The chapter contains the following sections:

VAP Introduction

Virtual access points (VAPs) are independent broadcast domains that function as the wireless equivalent of Ethernet VLANs. They are seen by clients as independent access points, with their own VIDs, SSIDs, and security methods.

VAP parameters are divided into these two groups:

- “Configuring Basic VAP Parameters” on page 103
- “Configuring VAP Security” on page 109

VAP Guidelines

Here are guidelines to configuring VAP:

- Each radio can have up to eight VAPs. Allied Telesis recommends no more than five VAPs per radio for best performance.
- The VAPs are numbered from 0 to 15.
- You can enable or disable the VAPs individually, except for VAP0, which can only be disabled by disabling its radio.
- You can enable 16 VAPs per radio.
- The VAPs of a radio can have different security methods.
- VAPs can have the same or different VLAN IDs.
- The available VAP securities are Static WEP, WPA Personal, and WPA Enterprise and OSEN.
- Static WEP can be selected only when the Radio mode is set to IEEE 802.11b/g or IEEE 802.11a.

Configuring Basic VAP Parameters

To configure basic VAP settings, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Virtual Access Point** tab. This is the default tab. The example in Figure 38 shows the settings for VAP0 on Radio1.

> **Note**
> Passpoint must be enabled in the Virtual Access Point tab for the 802.11u Settings, Passpoint Settings and OSU Settings tabs to become visible.

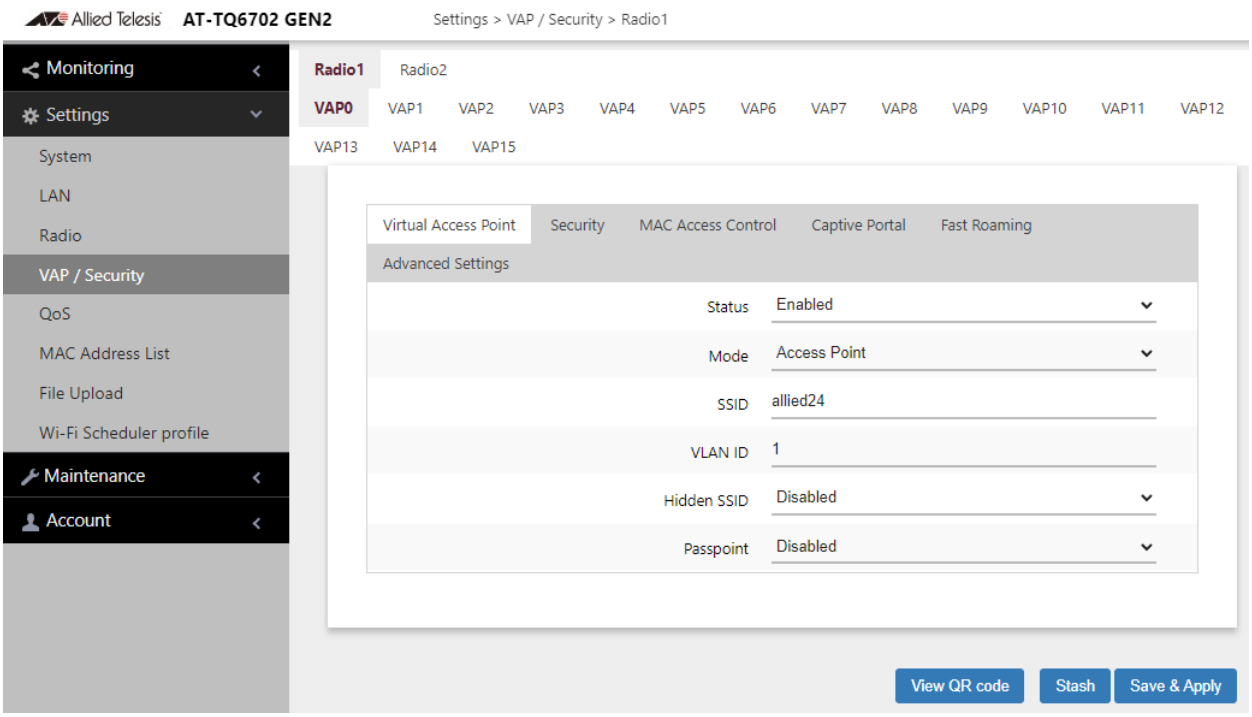

Figure 38. Virtual Access Point

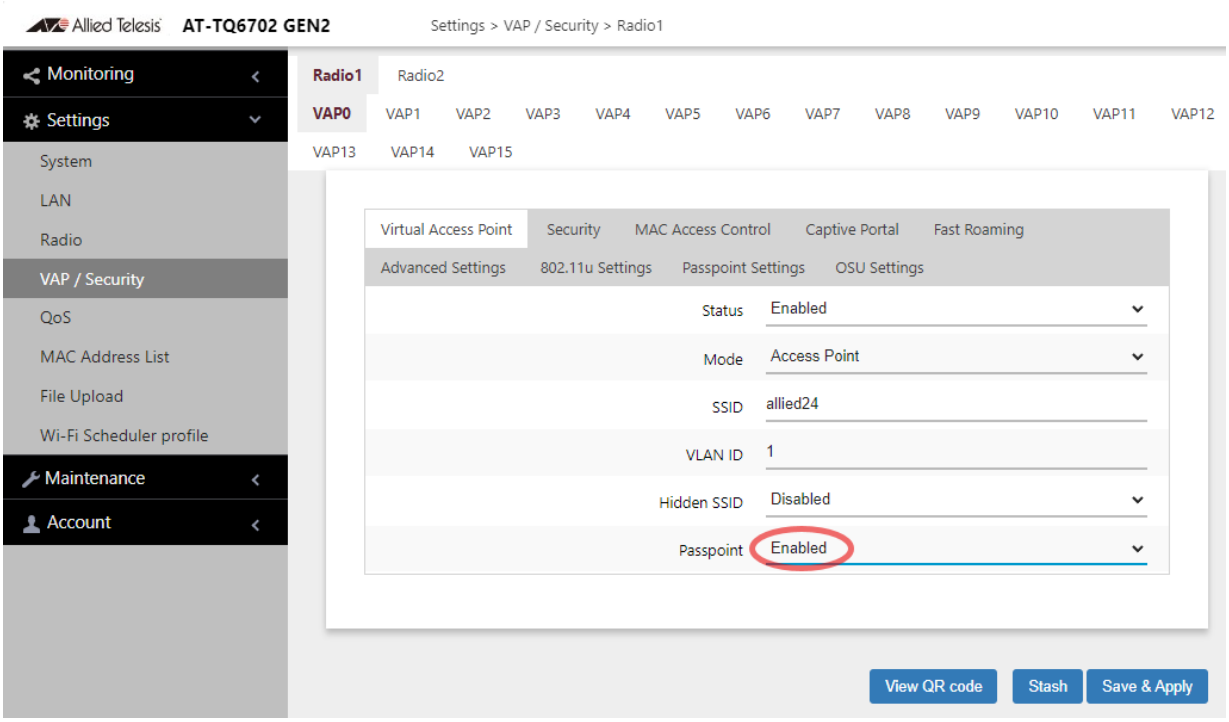

Figure 39. Virtual Access Point - Passpoint enabled

5. Configure the parameters by referring to Table 21.

Table 21. Virtual Access Point Tab

Field	Description
Status	Enable or disable the VAP. Here are the guidelines. - A disabled VAP does not forward any ingress or egress traffic. - The default setting for VAP0 is enabled. - The default setting for VAP1 to VAP15 is disabled. - You cannot disable VAP0. To stop VAP0 from forwarding traffic from wireless clients, you have to disable its radio.

Table 21. Virtual Access Point Tab (Continued)

Field	Description
Mode	Select a mode setting from the pull-down menu. This parameter applies only to VAP0. The menu choices are listed here: - Access Point: Select this mode to have a VAP function as a normal VAP, without WDS bridging. This is the default setting. **Note** The mode option for VAP1 to VAP15 is only Access Point. - WDS Parent - WDS Child For more information, see Chapter 6, “Wireless Distribution System Bridges” on page 92.
SSID	Enter a name for the VAP. Here are the guidelines: - A VAP must have a name. - A name can be from 1 to 32 alphanumeric characters. - Spaces are allowed except the first and last characters of an SSID. - You can assign the same name to more than one VAP. - The default names for VAP0 on Radio1 and Radio2 are allied24 and allied5, respectively. - The default names for VAP1 to VAP15 are Virtual Access Points 1 to 15.

Table 21. Virtual Access Point Tab (Continued)

Field	Description
VLAN ID	Enter a VID for the VAP. Here are the guidelines: - The range is 1 to 4094. - The default is VID 1. - A VAP can have only one VID. - You can assign the same VID to more than one VAP. - This VID is ignored for wireless clients that receive their VIDs from a RADIUS server for WPA Enterprise security. VIDs from a RADIUS server override the number in this field.
Hidden SSID	Select whether the access point should advertise the VAP SSID to clients. Here are the options: - Disabled: The access point transmits the SSID to advertise the VAP to clients. This is the default setting. - Enabled: The access point does not advertise the VAP. Clients who want to connect to an unauthorized VAP have to know its name.
Passpoint	Not supported.

6. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

7. Or click **View QR code** to generate a QR code.

Generating a Quick Response (QR) Code for a VAP

You can generate a QR code for an individual VAP on the access point. Wireless clients can scan the QR code to join the VAP on the access point without having to manually enter the information.

Here are guidelines:

- Codes are generated by clicking the View QR code button in any pages in a VAP.
- QR codes are not supported on VAPs that use RADIUS servers to authenticate wireless clients.
- When a Radio is disabled, a QR code for a VAP in the Radio wioo not generated.

To generate a QR code for a VAP, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP. See Figure 38 on page 104 as an example.

   The default is VAP0. You can configure only one VAP at a time.
4. Configure the VAP.
5. Click **View QR code**.

   The QR code appears as shown in Figure 40 on page 108.

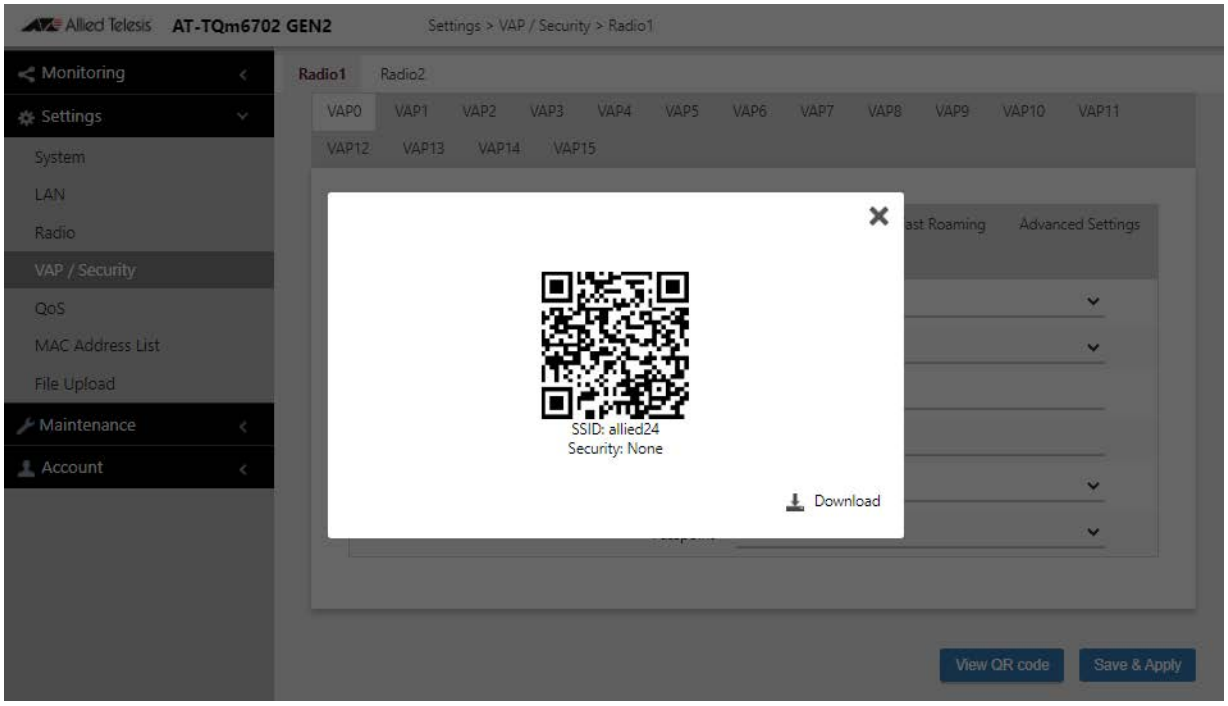

Figure 40. QR Code

6. Download the QR code.

   The QR code is ready to be used.

Configuring VAP Security

The procedures for configuring VAP security is provided in the following sections:

No Security

VAPs not requiring any security can be set to the None security level. Wireless clients do not use encryption or authentication to access VAPs with no security. This is the default setting.

To configure a VAP for no security, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Security** tab.
5. Select **None** from the Mode pull-down menu. This is the default setting. See Figure 41 on page 110.

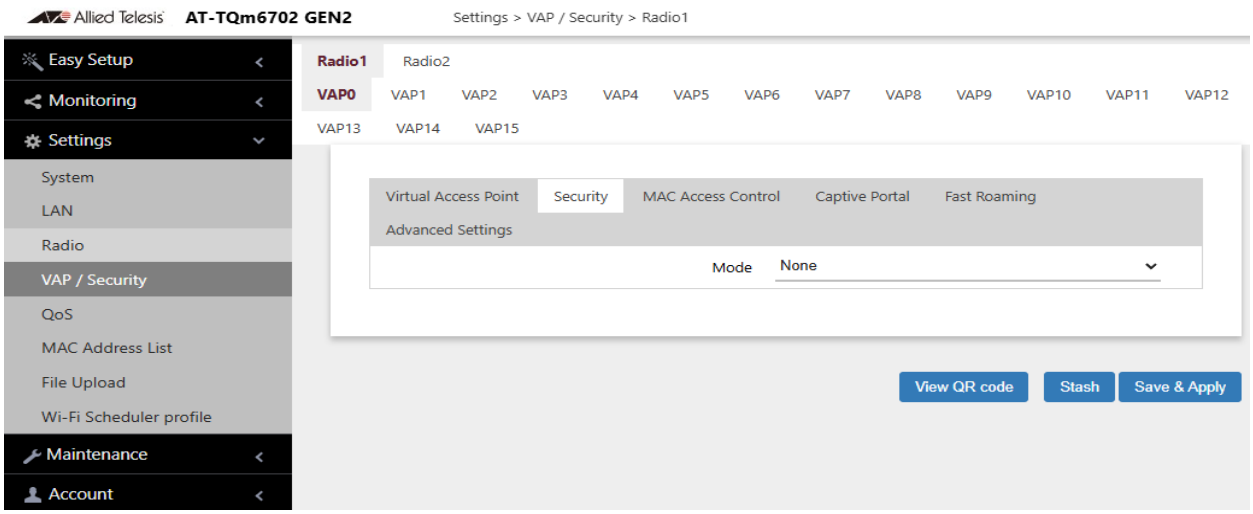

Figure 41. None Selected in the VAP Security Tab

6. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

Static WEP

To configure a VAP for Static WEP security, perform the following procedure:

> **Note**
> Static WEP is only supported when the radio mode is set to IEEE802.11b/g or IEEE802.11/a. See “Configuring Basic Radio Settings” on page 73.

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Security** tab.
5. Select **Static WEP** from the Mode pull-down menu. See Figure 42 on page 111.

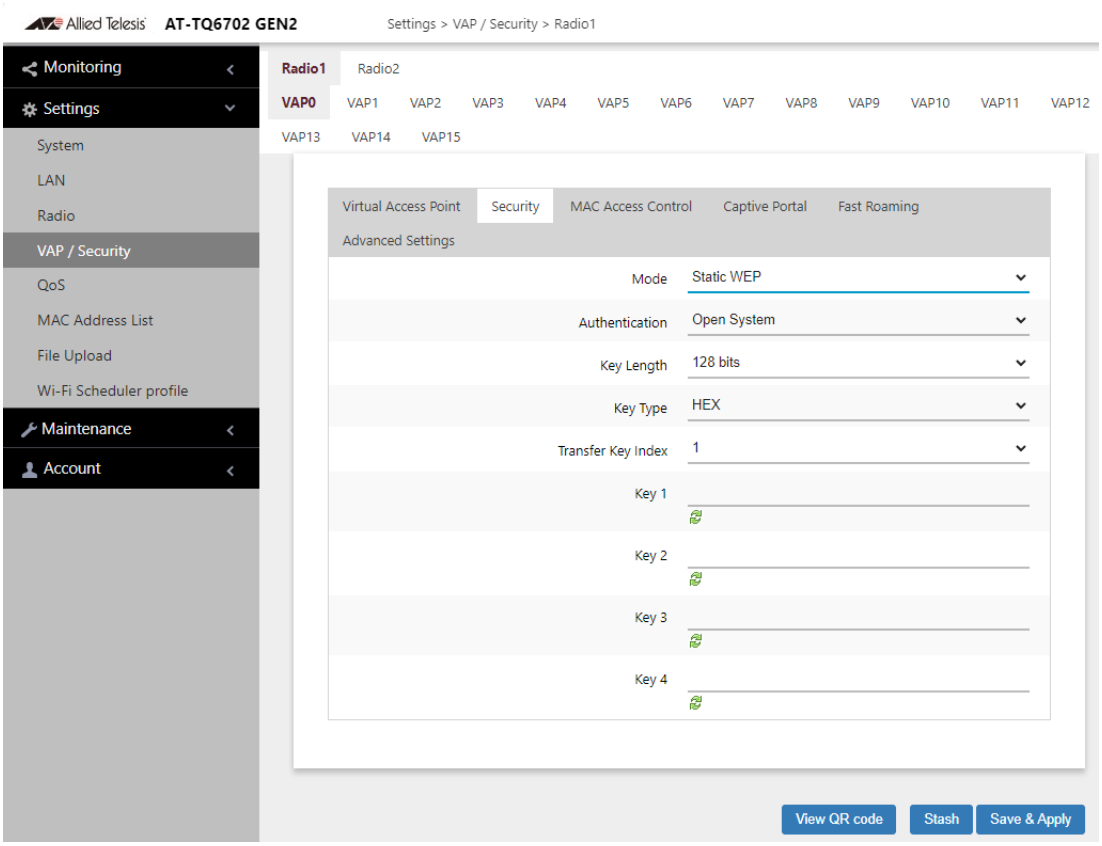

Figure 42. Static WEP in the VAP Security Tab

6. Configure the parameters by referring to Table 22.

Table 22. Static WEP Security Tab

Field	Description
Mode	Select **Static WEP**.
Authentication	Specify whether the access point authenticates VAP clients. Here are the options. - Open System: The access point does not authenticate VAP clients. All clients, even those without correct WEP keys, can connect to the VAP. This is the default setting. Clients in an open system VAP still must have the correct WEP key to encrypt and decrypt the traffic they exchange with the access point. - Shared Key: Clients must have the correct WEP key to connect with the VAP. Clients without the correct WEP key cannot associate with it.

Table 22. Static WEP Security Tab (Continued)

Field	Description
Key Length	Select a key length. The options are: - 128 bits. This is the default setting. - 64 bits
Key Type	Seelect a key type: The options are: - Hex: Enter keys in hexadecimal numbers. This is the default setting. - ASCII: Enter keys in ASCII
Transfer Key Index	Select the key the access point should use to encrypt network traffic. You can select only one key.
Key 1 to 4	Enter up to four WEP keys in the fields numbered 1 to 4. Here are the guidelines: - When the key length is set to 128 bits: 26 hexadecimal numbers in Hex 13 alphanumeric characters in ASCII. - When the key length is set to 64 bits: 10 hexadecimal numbers in Hex 5 alphanumeric characters in ASCII. - Keys are case-sensitive. - The order of the keys has be the same on the access point and clients. The small double-arrow symbols by the fields toggle the keys between alphanumeric characters and asterisks.

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
8. Or click **View QR code** to generate a QR code.

WPA Personal (Pre-Shared Key)

To configure a VAP for WPA Personal security, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

Note
You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Security** tab.
5. Select **WPA Personal** from the Mode pull-down menu. See Figure 43.

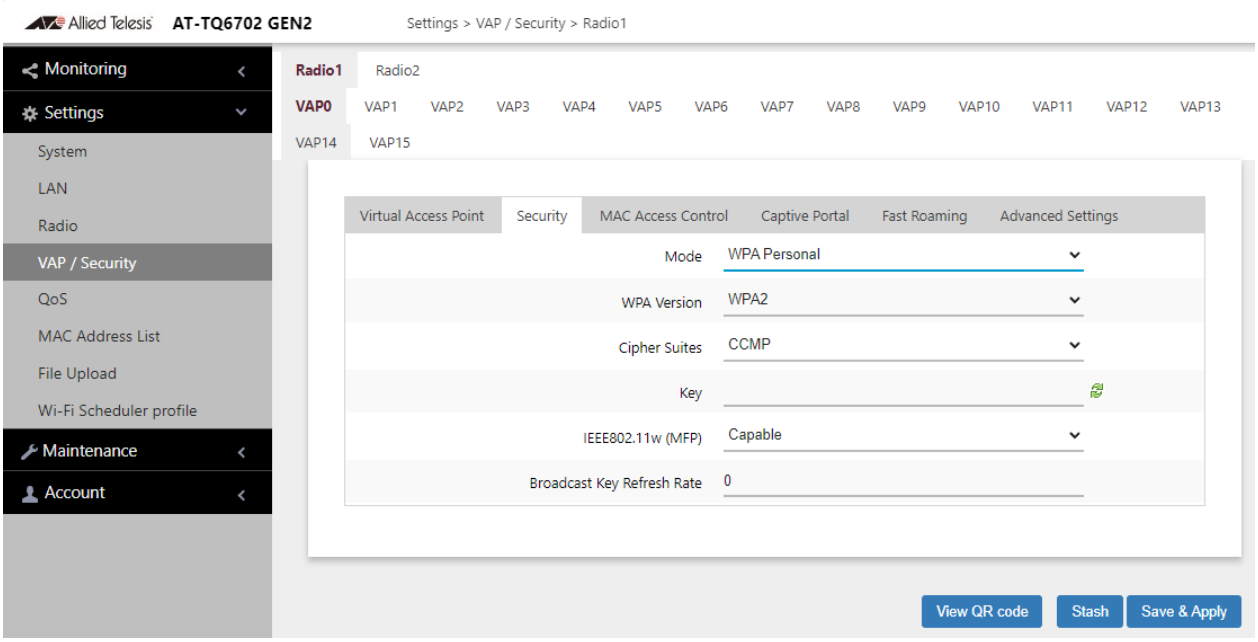

Figure 43. WPA Personal Security Tab

6. Configure the parameters by referring to Table 23.

Table 23. WPA Personal Security Tab

Field	Description
Mode	Select **WPA Personal**.

Table 23. WPA Personal Security Tab (Continued)

Field	Description
WPA Version	Select the WPA version. The options are listed here: - WPA and WPA2: Select this option if the VAP has both WPA and WPA2 clients. - WPA2: Select this option if clients support WPA2 only. This is the default setting. - WPA2 and WPA3: Select this option if the VAP has both WPA2 and WPA3 clients. - WPA3: Select this option if clients support WPA3 only. This is the default setting.
Cipher Suites	The settings are listed here: - CCMP When the WPA version is WPA2, WPA2 and WPA3, or WPA3, CCMP is the only option. - TKIP and CCMP When the WPA version is WPA and WPA2, TKIP and CCMP is the only option. For the TKIP and CCMP setting, clients who are using WPA must have one of the following: - A valid TKIP key. - A valid CCMP (AES) key.
Key	Enter a shared secret key. Here are the guidelines: - The key can be from 8 to 63 alphanumeric characters. - It can include special characters. - It is case sensitive. - The default is no key. The small double-arrow symbol next to the field toggles the key between alphanumeric characters and asterisks.

Table 23. WPA Personal Security Tab (Continued)

Field	Description
IEEE802.11w (MFP)	Control IEEE 802.11w management frame protection. The options are available only when the WPA version is WPA2. - Disabled: Disable Management frame protection. This is the default. - Capable: Enable Management frame protection.
Broadcast Key Refresh Rate	Specify the refresh interval rate for the broadcast (group) key. The range is 0 to 86400 seconds. The key is not refreshed when this parameter is set to 0 seconds, which is the default.

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
8. Or click **View QR code** to generate a QR code.

WPA Enterprise

To configure a VAP for WPA Enterprise security, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

Note
You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Security** tab.
5. Select **WPA Enterprise** from the Mode pull-down menu. See Figure 44.

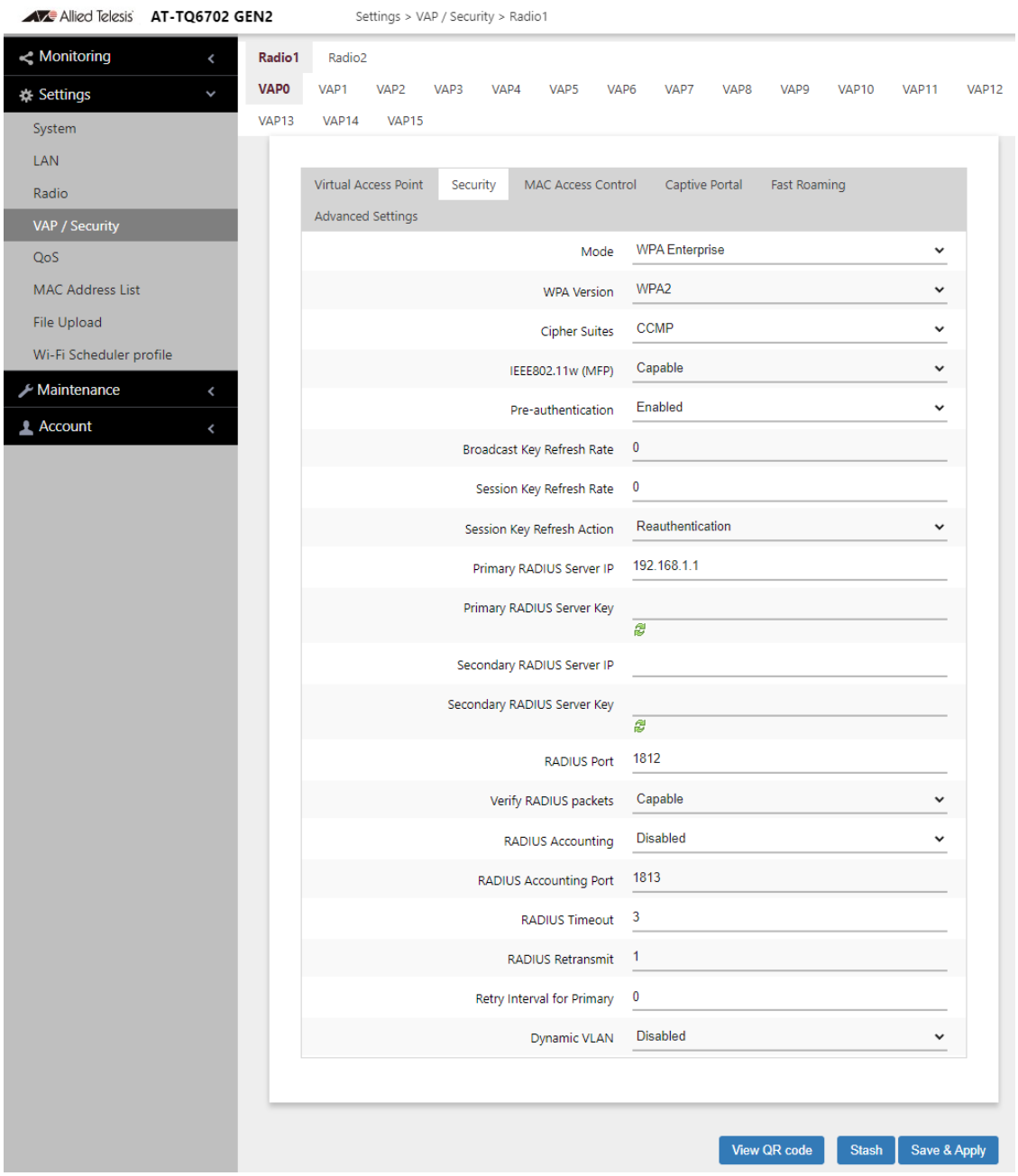

Figure 44. WPA Enterprise Security

6. Configure the parameters by referring to Table 24.

Table 24. WPA Enterprise Security

Field	Description
Mode	Select **WPA Enterprise**.

Table 24. WPA Enterprise Security (Continued)

Field	Description
WPA Version	Select the WPA version for the VPA. The options are listed: - WPA and WPA2 - Select this option if the VAP has both WPA and WPA2 clients. - WPA2: Select this option if all the clients support WPA2 only. This is the default setting. - WPA2 and WPA3 - Not supported. - WPA3: Select this option if clients support WPA3 only.
Cipher Suites	The settings are listed here: - CCMP. This is the default. When the WPA version is WPA2, or WPA2 and WPA3, CCMP is the only option. - TKIP and CCMP When the WPA version is WPA and WPA2, TKIP and CCMP is the only option. - GCMP When the WPA version is WPA3, the options are GCMP and CCMP. GCMP is the default. For the TKIP and CCMP setting, clients configured to use WPA with RADIUS must have one of the following: - A valid TKIP RADIUS IP address and RADIUS key. - A valid CCMP IP address and RADIUS key.
IEEE802.11w (MFP)	Control IEEE 802.11w management frame protection. The options are available only when the WPA version is WPA2. - Disabled: Management frame protection is disabled. This is the default setting. - Capable: Management frame protection is enabled.

Table 24. WPA Enterprise Security (Continued)

Field	Description
Pre-authentication	Pre-authentication can speed up authentication process for roaming clients . The access point forwards pre-authentication information from wireless clients to the next access points as they associate with different access points. The options are: - Enabled: Enables pre-authentication. This is the default. - Disabled: Disables pre-authentication.
Broadcast Key Refresh Rate	Enter the interval for updating the key of the broadcast packet to be sent to the wireless clients connected to the VAP. The range is 0 to 86400 seconds. The key is not updated when this parameter is set to 0 (zero). The default is 0.
Session Key Refresh Rate	Enter the interval for refreshing unicast session key to be sent to the wireless clients connected to the VAP. Session keys are unique to each client. The range is 0 to 86400 seconds. The key is not updated when this parameter is set to 0 (zero). The default is 0.
Session Key Refresh Action	Select an action that the access point takes when a session is expired. The options are: - Reauthentication: Wireless clients are re-authenticated. This is the default setting. - Disconnection: Wireless clients are disconnected
Primary RADIUS Server IP	Enter the IPv4 address of the primary RADIUS server. The default is 192.168.1.1.
Primary RADIUS Server Key	Enter the shared secret key for the primary RADIUS server. Here are the guidelines: - The key can be up to 128 alphanumeric characters. - It is case-sensitive. - It must be same on the access point and server. - The default is no key.

Table 24. WPA Enterprise Security (Continued)

Field	Description
Secondary RADIUS Server IP	Enter the IPv4 address of a secondary RADIUS server. This field is optional. The access point sends authentication requests to this address if the primary RADIUS server does not respond to requests.
Secondary RADIUS Server Key	Enter the shared secret key for the secondary RADIUS server.
RADIUS Port	Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must be using the same port number. The range is 0 to 65535. The default is 1812.
Verify RADIUS packets	This feature adds and verifies Message-Authenticator attribute for RADIUS requests and responses. The Message-Authenticator attribute is used to validate a RADIUS request. Required - The Message-Authenticator attribute is always added to RADIUS requests sent from the AP. - The Message-Authenticator attribute of RADIUS response packets received from the RADIUS server is always verified. Capable - The Message-Authenticator attribute will be verified if it is an EAP (Extensible Authentication Protocol) packet. Others will pass through without verification. The default is Capable.
RADIUS Accounting	Control RADIUS accounting, When accounting is enabled, the access point sends client information, such as usage time, to the RADIUS server. The options are listed here: - Enabled: Activate RADIUS accounting. - Disabled: Deactivate RADIUS accounting. This is the default setting.

Table 24. WPA Enterprise Security (Continued)

Field	Description
RADUIS Accounting Port	Enter the RADIUS accounting port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must use the same accounting port number. The range is 0 to 65535. The default is 1813.
RADIUS Timeout	Sets the maximum time the AP will wait for a response from the RADIUS server. The range is 1-29 seconds. The default is 3 seconds. Note, when registering: - only Primary RADIUS server IP, the values must be set such that "RADIUS Timeout" x "RADIUS Retransmit + 1" is less than or equal to 29. - both Primary RADIUS and Secondary RADIUS, and the keys are the same, the values must be set such that "RADIUS Timeout" x "RADIUS Retransmit + 1" x 2 is less than or equal to 29. - both Primary RADIUS and Secondary RADIUS, with different keys, set the values such that "RADIUS Timeout" x "RADIUS Retransmit + 1" is less than or equal to 29.
RADIUS Retransmit	Sets the maximum number of times the AP will resend an authentication request to the RADIUS server. The range is 0-8. The default is 1.
Retry Interval for Primary	Sets the time interval after which the AP will try to connect to the primary RADIUS server again, when a back-up server is handling authentication. The range is 0 - 600 seconds. The default is 0 seconds. Note: when the value is 0, no retry will occur.

Table 24. WPA Enterprise Security (Continued)

Field	Description
Dynamic VLAN	Control whether the VAP only accepts clients that are assigned VIDs by RADIUS servers. The options are listed here: - Enabled: The VAP forwards packets only from clients that are assigned VIDs from RADIUS servers. - Disabled: The VAP forwards packets without regard to how clients are assigned VIDs. This is the default setting.

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

8. Or click **View QR code** to generate a QR code.

OSEN

Online sign-up (OSU) Server-only Authenticated L2 Encryption Network (OSEN) is used with Hotspot 2.0 (Passpoint). It provides security to wireless clients during their initial registrations by authenticating service provider networks. OSEN protects both authentication and non-related communications.

To configure a VAP for OSEN security, perform the following procedure:

Note
OSEN is not available on VAP0 when it is the parent or child of a WDS bridge.

1. Select **Settings** > **VAP / Security** from the main menu.

2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.

3. Select a VAP to configure from the next sub-menu. The default is VAP0.

Note
You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Security** tab.

5. Select **OSEN** from the Mode pull-down menu. See Figure 45.

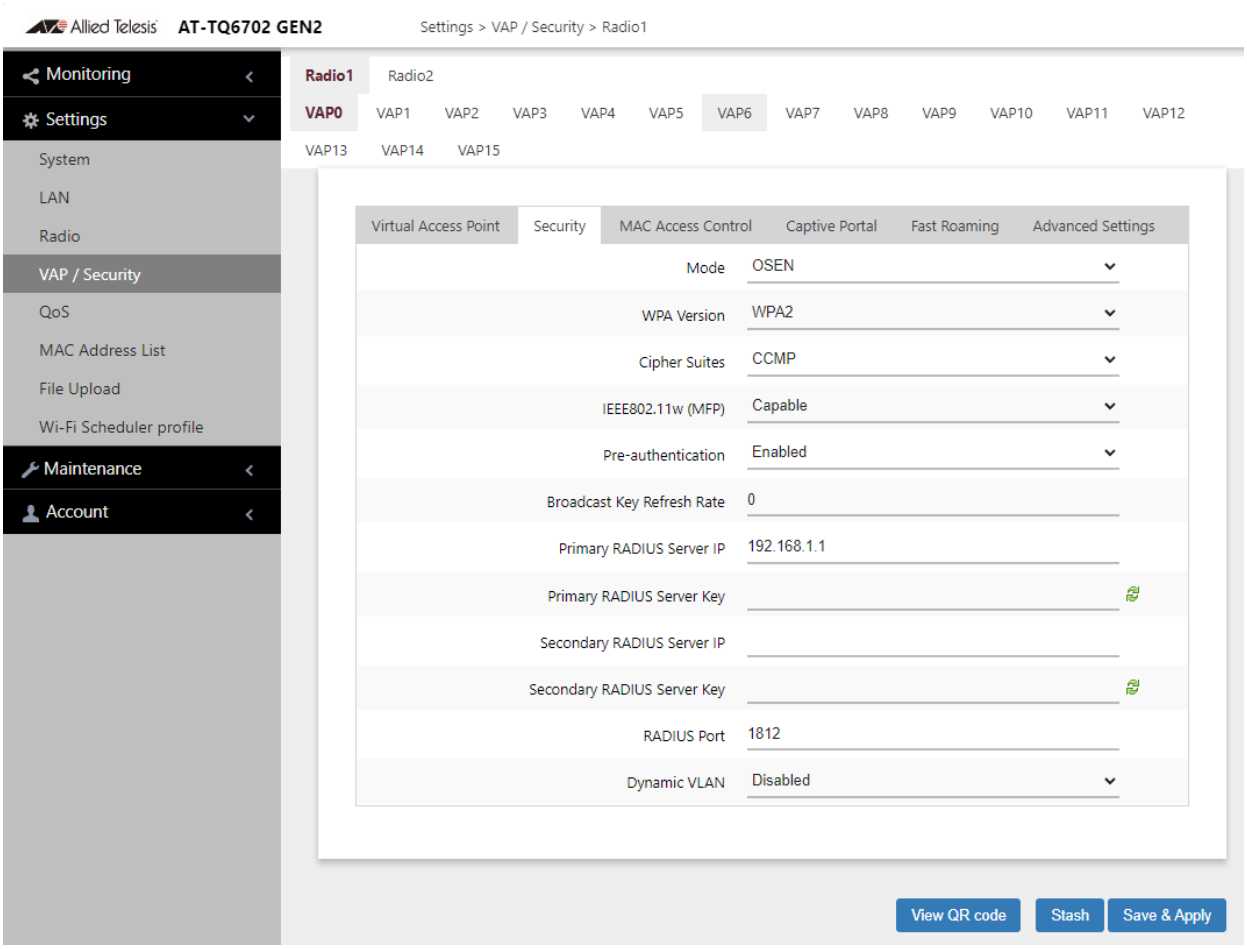

Figure 45. Security - OSEN

6. Configure the parameters by referring to Table 25 on page 123.

Table 25. OSEN Security Tab

Field	Description
Mode	Select **OSEN**.
WPA Version	See Table 24 on page 116.
Cipher Suites	
IEEE802.11w (MFP)	
Pre-authentication	
Broadcast Key Refresh Rate	
Primary RADIUS Server IP	
Primary RADIUS Server key	
Secondary RADIUS Server IP	
Secondary RADIUS Server key	
RADIUS Port	
Dynamic VLAN	

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

8. Or click **View QR code** to generate a QR code.

Configuring MAC Access Control

The access point has the MAC Access Control feature to add security to VAPs by authenticating the MAC addresses of wireless clients. The access point forwards traffic from only approved addresses.

You have the following options for MAC Access Control:

- “Disabling MAC Access Control” on page 124
- “Authenticating Using Both MAC Address List and RADIUS” on page 125
- “Authenticating Using RADIUS” on page 131
- “Authenticating Using MAC Address List” on page 133
- “Application Proxy” on page 134

Disabling MAC Access Control

To disable MAC Access Control of the on-board MAC address list and external RADIUS server, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **MAC Access Control** tab. See Figure 46.

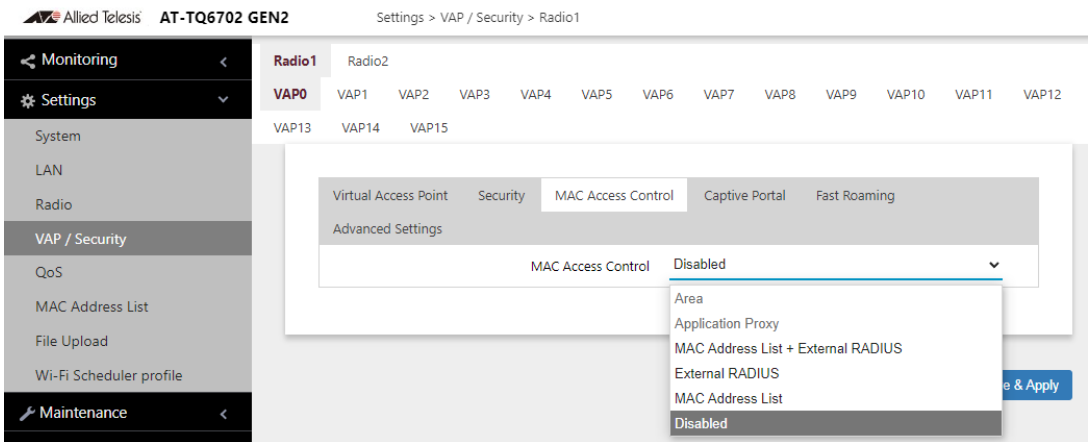

Figure 46. MAC Access Control Tab

5. Select **Disabled** from the MAC Access Control pull-down menu. See Figure 46 on page 124. This is the default setting.

6. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

Authenticating Using Both MAC Address List and RADIUS

This section contains the procedure for authenticating wireless clients on VAPs using both the access point's on-board MAC address list and an external RADIUS server. This is set with the MAC Address List + External RADIUS option in the MAC Address Control tab. Wireless access points are authenticated depending on the Allow or Deny setting of the on-board MAC address filter, as follows:

- When the on-board MAC address filter is set to Allow, the wireless access point authenticates wireless clients in this manner:
  - It accepts clients whose MAC addresses are in the on-board MAC address filter.
  - For MAC addresses not in the filter, it forwards them to the RADIUS server. It accepts clients whose addresses are on the server and denies clients whose addresses are not on the server.

In summary, when the on-board filter is set to Allow, the wireless access point accepts clients whose MAC address are either in the on-board filter or on the RADIUS server.

- When the on-board MAC address filter is set to Deny, the wireless access point authenticates wireless clients in this manner:
  - It rejects clients whose MAC addresses are in the on-board MAC address filter.
  - For clients whose addresses are not in the filter, it forwards their addresses to the RADIUS server. It accepts clients whose addresses are on the server and denies clients whose addresses are not on the server.

In summary, when the on-board filter is set to Deny, the wireless access point accepts clients whose MAC address are not in the on-board filter, but are on the RADIUS server.

To configure MAC Access Control with both on-board MAC address list and external RADIUS server, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.

2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.

3. Select a VAP to configure from the next sub-menu. The default is VAP0.

Note
You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **MAC Access Control** tab. See Figure 47.
5. Select the **MAC Address List + External RADIUS** option from the MAC Access Control pull-down menu. See Figure 47.

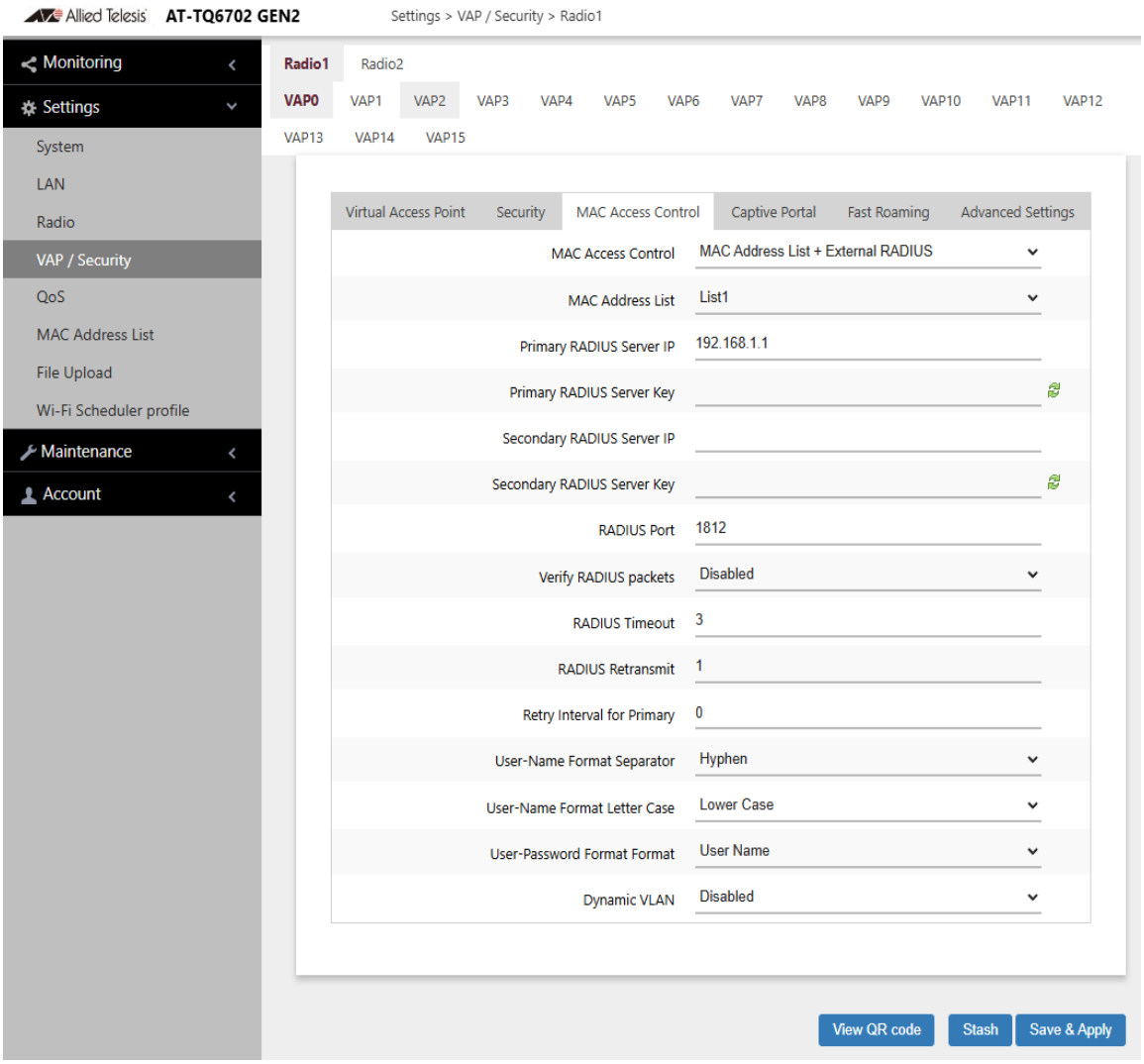

Figure 47. MAC Access Control - MAC Address List + External RADIUS

6. Configure the parameters by referring to Table 26.

Table 26. MAC Address List + External RADIUS Window

Field	Description
MAC Address List	Select a MAC address list from the pull-down.
Primary RADIUS Server IP	Enter the IPv4 address of the primary RADIUS server. The default is 192.168.1.1.
Primary RADIUS Server Key	Enter the shared secret key for the primary RADIUS server. Here are the guidelines: - The key can be up to 128 alphanumeric characters. - It is case-sensitive. - It must be same on the access point and server. - The default is no key.
Secondary RADIUS Server IP	Enter the IPv4 address of a secondary RADIUS server. This field is optional. The access point sends authentication requests to this address if the primary RADIUS server does not respond to requests.
Secondary RADIUS Server Key	Enter the shared secret key for the secondary RADIUS server.
RADIUS Port	Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must be using the same port number. The range is 0 to 65535. The default is 1812.

Table 26. MAC Address List + External RADIUS Window (Continued)

Field	Description
Verify RADIUS packets	This feature adds and verifies the Message-Authenticator attribute for RADIUS requests and responses. The Message-Authenticator attribute is used to validate a RADIUS request. Required - The Message-Authenticator attribute is always added to RADIUS requests sent from the AP. - The Message-Authenticator attribute of RADIUS response packets received from the RADIUS server is always verified. - If the Message-Authenticator attribute is not present or the attribute contains an invalid value, the RADIUS packet is dropped and the authentication is considered to have failed. Disabled - The Message-Authenticator attribute is not added to RADIUS requests sent from the AP. - The Message-Authenticator attribute of RADIUS response packets received from the RADIUS server is not verified. The default is Disabled.

Table 26. MAC Address List + External RADIUS Window (Continued)

Field	Description
RADIUS Timeout	Sets the maximum time the AP will wait for a response from the RADIUS server. The range is 1-29 seconds. The default is 3 seconds. Note, when registering: - only Primary RADIUS server IP, the values must be set such that "RADIUS Timeout" x "RADIUS Retransmit + 1" is less than or equal to 29. - both Primary RADIUS and Secondary RADIUS, and the keys are the same, the values must be set such that "RADIUS Timeout" x "RADIUS Retransmit + 1" x 2 is less than or equal to 29. - both Primary RADIUS and Secondary RADIUS, with different keys, set the values such that "RADIUS Timeout" x "RADIUS Retransmit + 1" is less than or equal to 29.
RADIUS Retransmit	Sets the maximum number of times the AP will resend an authentication request to the RADIUS server. The range is 0-8. The default is 1.
Retry Interval for Primary	Sets the time interval after which the AP will try to connect to the primary RADIUS server again, when a back-up server is handling authentication. The range is 0 - 600 seconds. The default is 0 seconds. Note: when the value is 0, no retry will occur.

Table 26. MAC Address List + External RADIUS Window (Continued)

Field	Description
User-Name Format Separator	Select the character that the access point should use to separate the octets in the MAC addresses it sends to the servers. (The MAC addresses function as the user-name attributes for the wireless clients.) The choices are listed here: - Hyphen (nn-nn-nn-nn-nn-nn) - Colon (nn:nn:nn:nn:nn:nn) - None (nnnnnnnnnnnn)
User-Name Format Letter Case	Specify whether the access point should send the MAC addresses using uppercase or lowercase characters. The options are listed here: - Upper Case: The wireless access point sends the MAC addresses in uppercase characters. - Lower Case: The wireless access point sends the MAC addresses in lowercase characters.
User-Password Format Format	Specify the password for the MAC addresses. The choices are listed here: - User Name: The MAC addresses are used as the password. If you select this option, wireless access points send the MAC addresses as both the user-name and user-password attributes of the clients to the servers. This is the default. - Fixed: A fixed value is used as the password for all MAC addresses. Selecting this option displays the User-Password Format Password field.
User-Password Format Password	Enter the fixed password for the MAC addresses. This field only applies to the Fixed setting in the User-Password Format Format option. The Password is case-sensitive.

Table 26. MAC Address List + External RADIUS Window (Continued)

Field	Description
Dynamic VLAN	Controls whether the VAP only accepts clients that are assigned VIDs by RADIUS servers. The options are listed here: Enabled: The VAP forwards packets only from clients that are assigned VIDs from RADIUS servers. Disabled: The VAP forwards packets without regards to how clients are assigned VIDs. This is the default setting.

Note
You must prepare a MAC address list. See “Configuring 802.11u Settings” on page 167.

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
8. Or click **View QR code** to generate a QR code.

Authenticating Using RADIUS

This section contains the procedure for authenticating wireless clients on VAPS with an external RADIUS server. The clients are authenticated by their MAC addresses, which the access point sends to the server on the wired network when clients connect to it. To use this form of authentication, you need to know the MAC addresses of the clients and enter them as their user names on the RADUIS server. You can specify up to two servers.

To configure MAC Access Control with external RADIUS server, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

Note
You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **MAC Access Control** tab. See Figure 48.
5. Select **External RADIUS** from the MAC Access Control pull-down menu. See Figure 48.

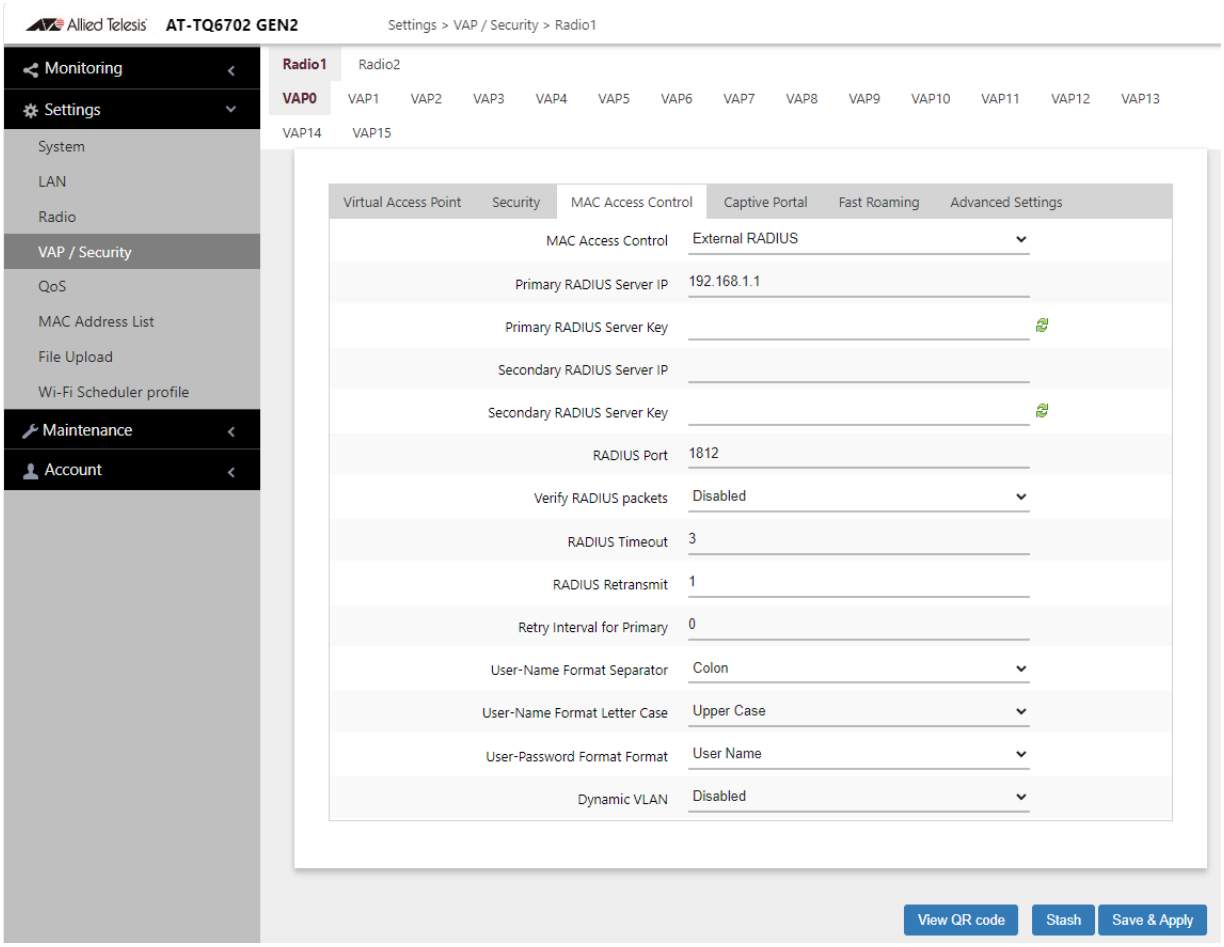

Figure 48. MAC Access Control - External RADIUS Window

6. Configure the parameters by referring to Table 26 on page 127.
7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
8. Or click **View QR code** to generate a QR code.

Authenticating Using MAC Address List

This section contains the procedure for authenticating wireless clients on VAPs with the access point's on-board MAC address list. The list consists of the MAC addresses of wireless clients that the access point is to accept or reject on the VAPs. To configure the MAC address list, see ""“Configuring 802.11u Settings” on page 167.

To configure MAC Access Control with external RADIUS server, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **MAC Access Control** tab. See Figure 49.
5. Select **MAC Address List** from the MAC Access Control pull-down menu. See Figure 49.

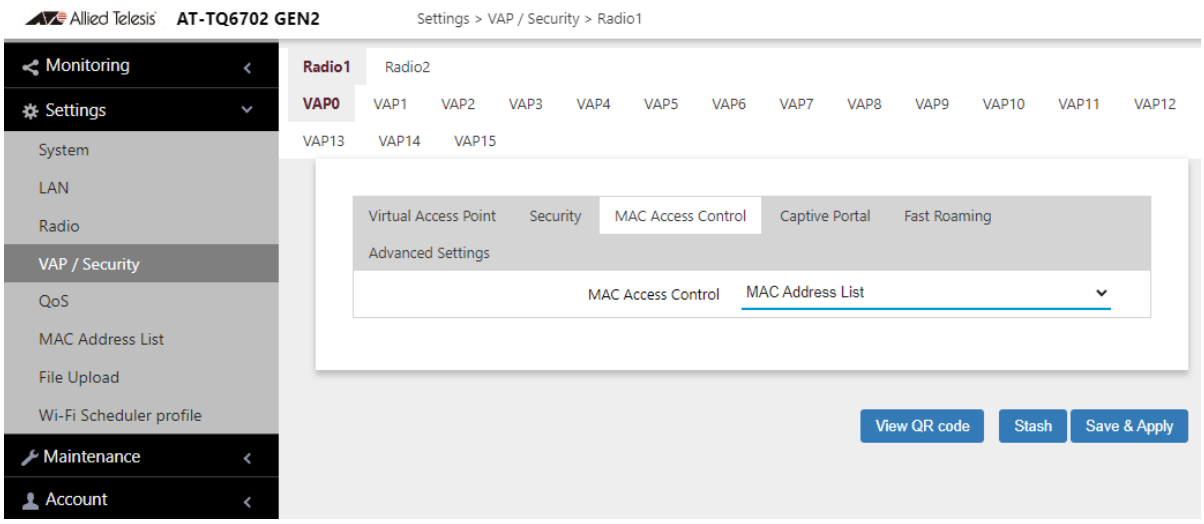

Figure 49. MAC Access Control - MAC Address List Window

> **Note**
> You must prepare a MAC address list. See “Configuring MAC Address Control Settings” on page 185.

6. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

7. Or click **View QR code** to generate a QR code.

Application Proxy

Application Proxy authenticates wireless clients using the AMF Application Proxy in the AMF Security controller. The application proxy allows you to add security policies that define where and when clients can access your wireless network. It also allows you to designate their network assignments by assigning them VLAN IDs.

This feature requires AMF Security mini or the AMF Security Controller (AMF-SEC) v2.2.2 or later. The TQ6000 GEN2 access points require Vista Manager EX v3.9.0 or later. Refer to the AMF Security mini User Guide or AMF Security Controller User Guide for further information.

Configuring Captive Portal

Captive Portal is a a web page that wireless clients view before their access is granted. Captive Portal pages usually identify the owners of the wireless networks or require wireless clients to agree to the terms of use. Captive Portal pages can require wireless clients to login, require information such as their email addresses, prior to allowing access to the networks.

Captive Portal Options

You can use Captive Portal to interact with wireless clients before allowing them to access your network resources. You can configure Captive Portal in the following ways:

- “No Captive Portal” on page 136

  No authentication, allowing any wireless client to access to your networks

- “No Authentication and Web Page Stored in the Access Point” on page 137

  A web page including your message and the Agree Button is displayed with no authentication. Your message in HTML is stored in the access point.

- “Delegating a Proxy Sever to Interact with Wireless Clients” on page 140

  Interacting with wireless clients is conducted by the proxy server that you specify. Place the HTML files or applications that you prepare on the proxy server.

- “RADIUS Server for Authentication and External URL for Web Hosting” on page 141

  Authentication is conducted by RADIUS servers. Wireless clients are redirect to an external URL for Web pages.

- “RADIUS Server for Authentication and Proxy Server for Web Hosting” on page 145

  Authentication is conducted by RADIUS servers. A Proxy server hosts web pages.

- “RADIUS Server for Authentication and No Proxy Server” on page 148

  Authentication is conducted by RADIUS servers. No web page is displayed to wireless clients.

No Captive Portal

To disable Captive Portal, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.

   You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Captive Portal** tab. See Figure 50.

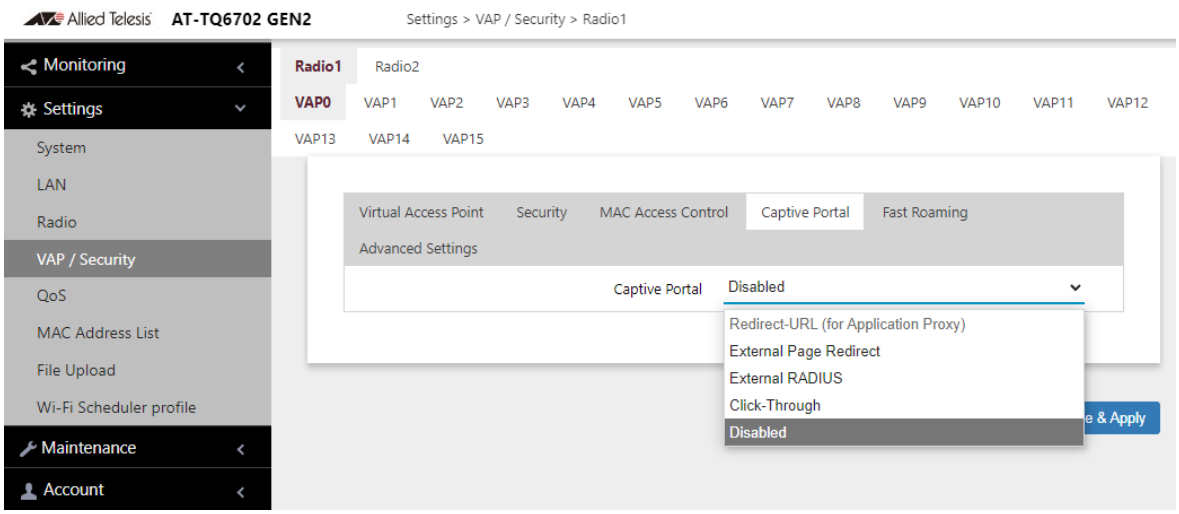

Figure 50. Capital Portal Window

5. Select Disabled from the Captive Portal pull-down menu.

   Disabled is the default setting.
6. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
7. Or click **View QR code** to generate a QR code.

No Authentication and Web Page Stored in the Access Point

When you want to display one web page with a Agree button to wireless client without authenticating wireless clients, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.

   You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

   Note
   You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.
4. Select the **Captive Portal** tab.
5. Select **Click-Through** from the Captive Portal pull-down menu. See Figure 52 on page 141.
6. Select **Disabled** from the Authentication Page Proxy pull-down menu.

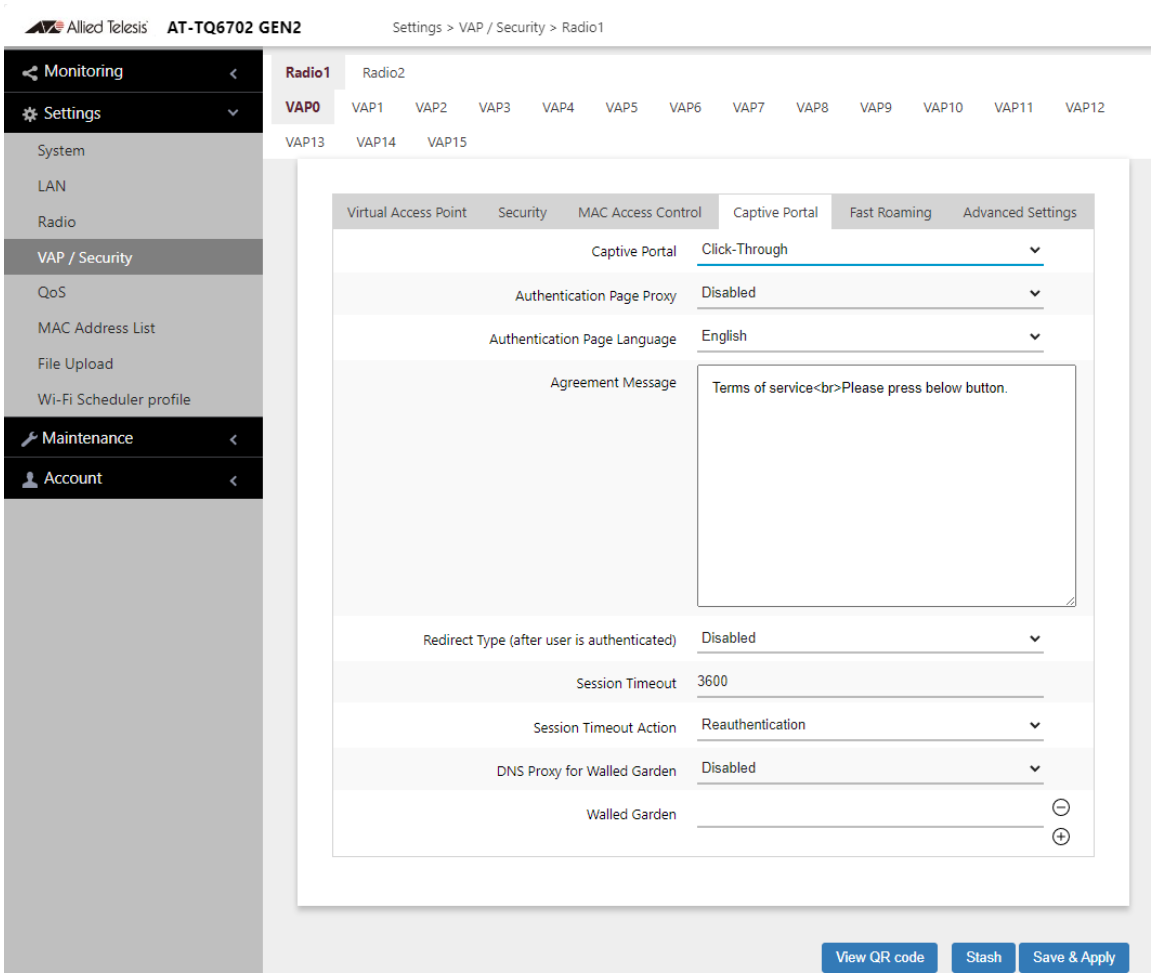

Figure 51. Capital Portal Window - Click-Through

7. Configure the parameters described in Table 27.

Table 27. Captive Portal - Click-Through

Field	Description
Authentication Page Proxy	Enable or disable Authentication Page Proxy on the Captive Portal: - Enabled: The access point uses other web server's authentication page via proxy with Captive Portal. See "Delegating a Proxy Sever to Interact with Wireless Clients" on page 140. - Disabled: The access point uses its own local authentication page with Captive Portal. This is the default setting. Select this option when you want to store a web page in the access point. Enter HTML codes in the Agreement Message field.

Table 27. Captive Portal - Click-Through (Continued)

Field	Description
Authentication Page Language	Select the language: English or Japanese. The default is English. This feature is available when “Click-Through” or “External RADIUS” is selected in Captive Portal and Authentication Page Proxy is disabled.
Agreement Message	Enter Conditions of Use or other information to display the introductory web page. The text can include HTML formatting and display codes. This field is available only when Authentication Page Proxy is disabled.
Base URL	Enter the URL for a page posted by the Authentication Page Proxy server. See “Creating Pages in HTML for a Proxy Server” on page 150 . This field is available only when Authentication Page Proxy is enabled.
Redirect Type (after user is authenticated)	Select the action to occur after the clients click the Agree button. The options are listed here: - Fixed URL: Directs clients to a specified web page. Selecting this option displays the Fixed URL field. - Session Keep: Directs clients to the web page they requested prior to the click-through window. - Disabled: Disables redirect. The welcome.html file that you prepared is displayed. When the Captive Portal field is Click-Through and the Authentication Proxy Page is Disabled, the welcome page on the access point is displayed. This is the default setting.
Session Timeout	Specify the time interval in seconds. The access point takes a specified action, either re-authenticating or disconnecting a wireless client after the specified time passes. The default value is 3600 seconds (60 minutes).
Session Timeout Action	Specify an action that the access point takes after the session timeout is reached. The options are: - Reauthentication: Re-authenticates the wireless client. This is the default setting. - Disconnection: Disconnects the wireless client.

Table 27. Captive Portal - Click-Through (Continued)

Field	Description
DNS Proxy for Walled Garden	Enables or disables DNS Proxy for Walled Garden. Disabled is the default.
Walled Garden	To add the first HTTP web site, enter it in the empty field. You can identify a site by its fully qualified domain name (FQDN), IPv4 address, or IPv4 address and mask (e.g 32.134.45.0/24). When using FQDN, do not include “HTTP://”. To add more URL addresses, click the “plus” button icon to the right of the last URL field. Use the “minus” button to remove URLs. You can enter up to fifty sites.

8. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

9. Or click **View QR code** to generate a QR code.

Delegating a Proxy Sever to Interact with Wireless Clients

When you want to display one web page with a Agree button to wireless client without authenticating wireless clients, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.

2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.

   You can configure only one radio at a time.

3. Select a VAP to configure from the next sub-menu. The default is VAP0.

   Note
   You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Captive Portal** tab.

5. Select **Click-Through** from the Captive Portal pull-down menu.

6. Select **Enabled** from the Authentication Page Proxy pull-down menu. See Figure 52.

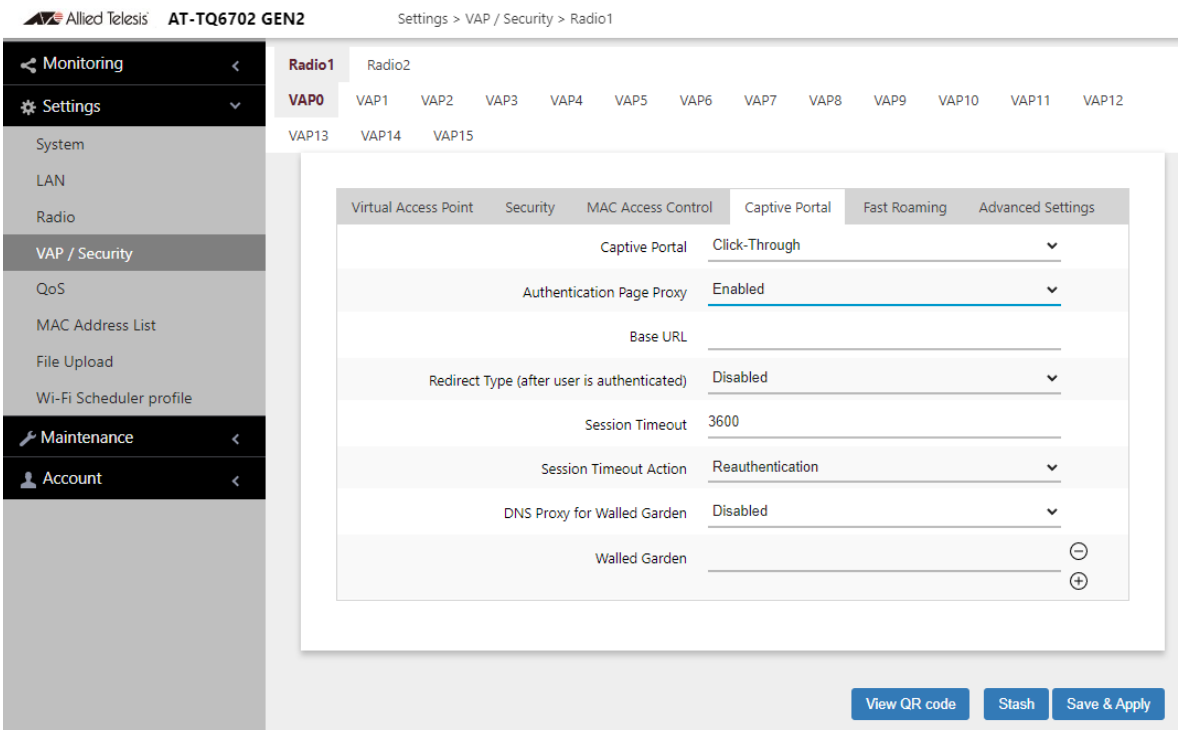

Figure 52. Capital Portal - Click-Through and Authentication Page Proxy

7. Specify the URL of your Page Proxy Server in the Base URL field.
8. Configure the rest of parameters by referring Table 27 on page 138.
9. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
10. Or click **View QR code** to generate a QR code.
11. Go to “Creating Pages in HTML for a Proxy Server” on page 150.

RADIUS Server for Authentication and External URL for Web Hosting

To redirect wireless clients to an external URL for a logon window and authenticate them with an external RADIUS server, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.

   You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

Note
You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Captive Portal** tab.

5. Select **External Page Redirect** from the Captive Portal pull-down menu. See Figure 53.

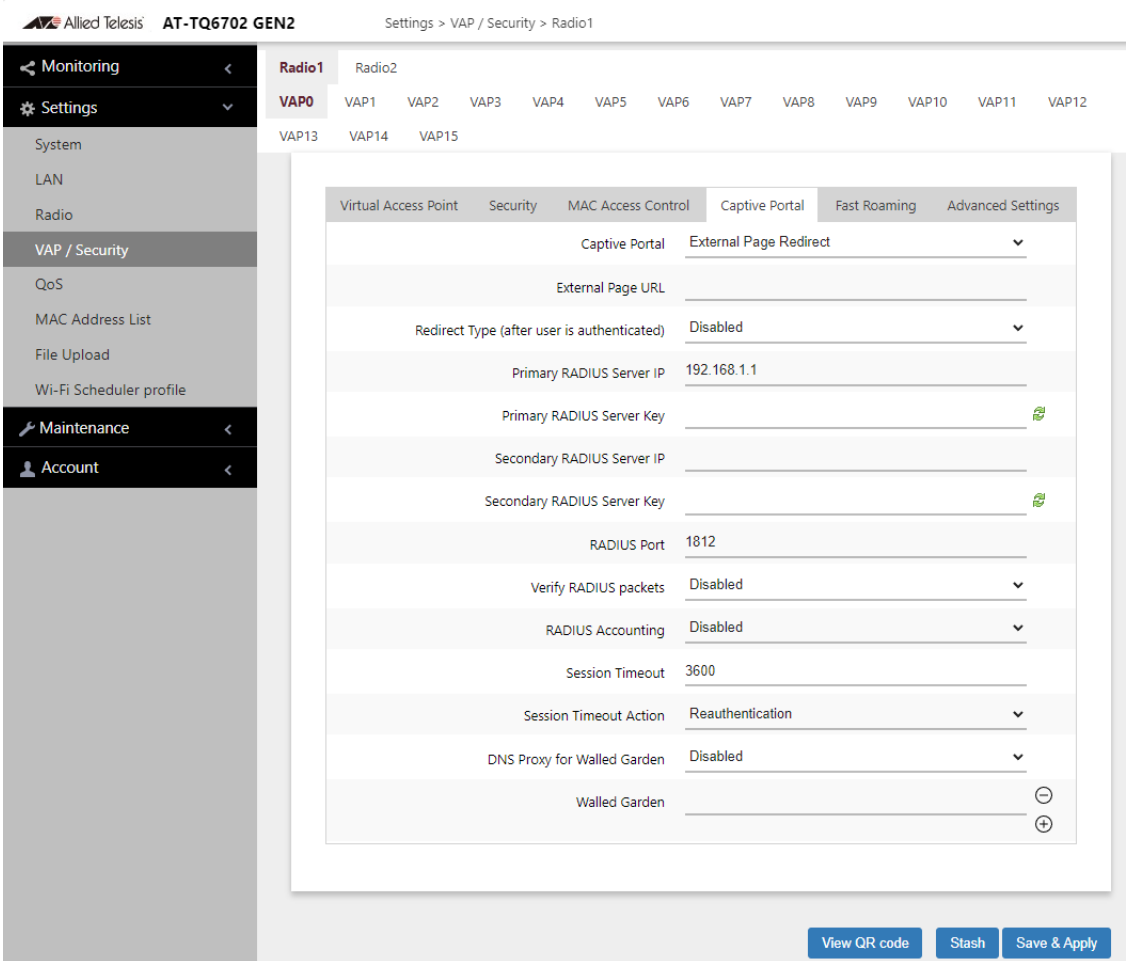

Figure 53. Capital Portal - External Page Redirect Window

6. Configure the parameters described in Table 28 on page 143.

Table 28. Captive Portal - External Page Redirect

Field	Description
External Page URL	Enter a URL that is directed to wireless clients when they access to the access point.
Redirect Type (after user is authenticated)	Select the action to occur after the clients click the Agree button. The options are listed here: - Fixed URL: Directs clients to a specified web page. Selecting this option displays the Fixed URL field. - Session Keep: Directs clients to the web page they requested prior to the click-through window. - Disabled: Disables redirect. The welcome.html file that you prepared is displayed. When the Captive Portal field is Click-Through and the Authentication Proxy Page is Disabled, the welcome page on the access point is displayed. This is the default setting.
Primary RADIUS Server IP	Enter the IPv4 address of the primary RADIUS server. The default is 192.168.1.1.
Primary RADIUS Server Key	Enter the shared secret key for the primary RADIUS server. Here are the guidelines: - The key can be up to 128 alphanumeric characters. - It is case-sensitive. - It must be same on the access point and server. - The default is no key.
Secondary RADIUS Server IP	Enter the IPv4 address of a secondary RADIUS server. This field is optional. The access point sends authentication requests to this address if the primary RADIUS server does not respond to requests.
Secondary RADIUS Server Key	Enter the shared secret key for the secondary RADIUS server.

Table 28. Captive Portal - External Page Redirect (Continued)

Field	Description
RADIUS Port	Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must be using the same port number. The range is 0 to 65535. The default is 1812.
Verify RADIUS packets	This feature adds and verifies the Message-Authenticator attribute for RADIUS requests and responses. The Message-Authenticator attribute is used to validate a RADIUS request. Required - The Message-Authenticator attribute is always added to RADIUS requests sent from the AP. - The Message-Authenticator attribute of RADIUS response packets received from the RADIUS server is always verified. - If the Message-Authenticator attribute is not present or the attribute contains an invalid value, the RADIUS packet is dropped and the authentication is considered to have failed. Disabled - The Message-Authenticator attribute is not added to RADIUS requests sent from the AP. - The Message-Authenticator attribute of RADIUS response packets received from the RADIUS server is not verified. The default is Disabled.
RADIUS Accounting	Control RADIUS accounting, When accounting is enabled, the access point sends client information, such as usage time, to the RADIUS server. The options are listed here: - Enabled: Activate RADIUS accounting. - Disabled: Deactivate RADIUS accounting. This is the default setting.

Table 28. Captive Portal - External Page Redirect (Continued)

Field	Description
RADIUS Accounting Port	Enter the RADIUS accounting port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must use the same accounting port number. The range is 0 to 65535. The default is 1813. This field is visible when RADIUS Accounting is enabled.
Session Timeout	See Table 27 on page 138.
Session Timeout Action	
DNS Proxy for Walled Garden	See Table 27 on page 138.
Walled Garden	See Table 27 on page 138. **Note** URLs where wireless clients are redirected must be entered.

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
8. Or click **View QR code** to generate a QR code.

RADIUS Server for Authentication and Proxy Server for Web Hosting

To delegate RADIUS servers to authenticate wireless clients and a Proxy server to host web pages, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.

   You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

   Note
   You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.
4. Select the **Captive Portal** tab.

5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 54 on page 146.

6. Select **Enabled** from the Authentication Page Proxy pull-down menu.

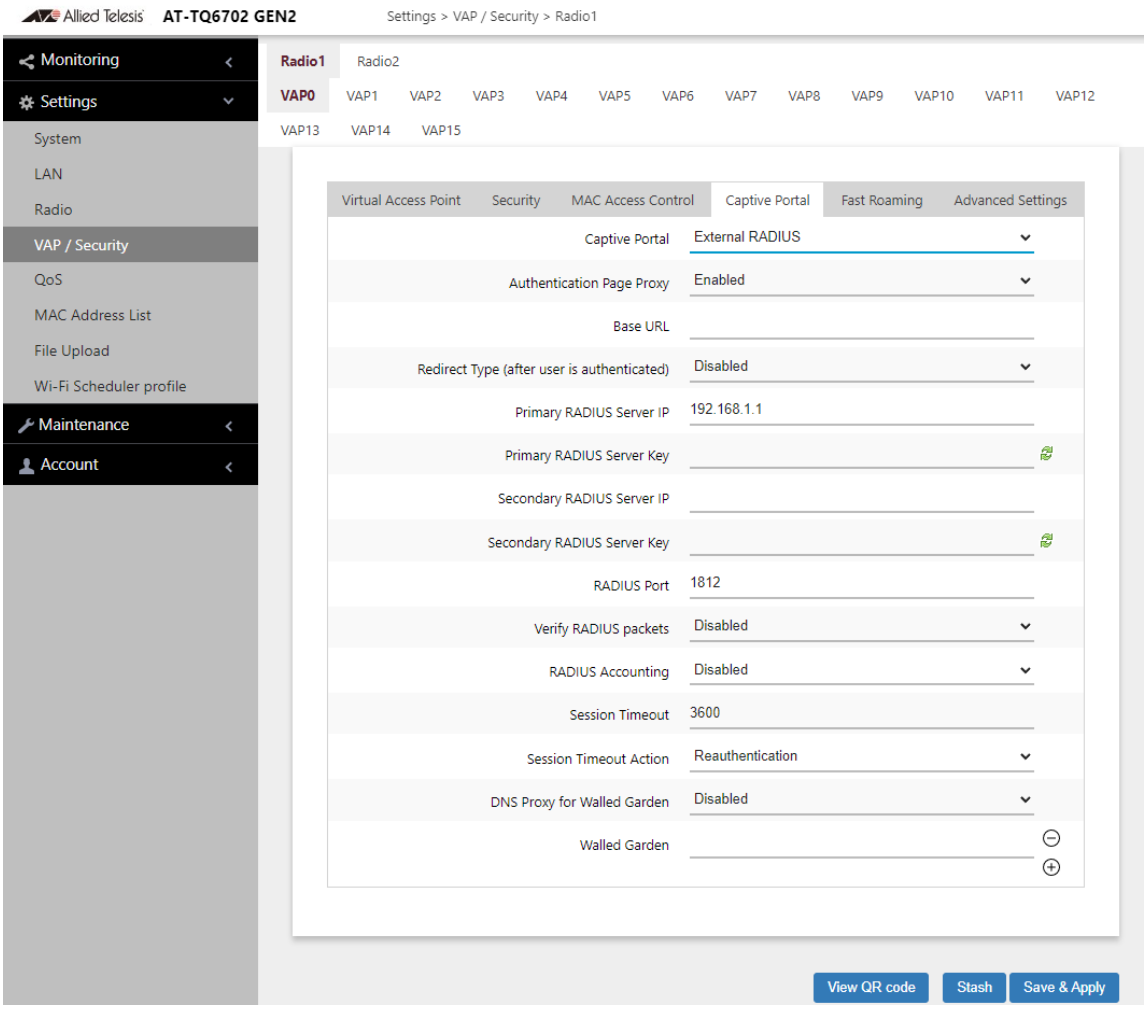

Figure 54. Capital Portal - RADIUS and Authentication Page Proxy

7. Configure the parameters described in Table 29.

Table 29. Captive Portal - External RADIUS and Proxy

Field	Description
Authentication page Proxy	See Table 27 on page 138.
Base URL	

Table 29. Captive Portal - External RADIUS and Proxy (Continued)

Field	Description
Redirect Type (after user is authenticated)	See Table 28 on page 143.
Primary RADIUS Server IP	
Primary RADIUS Server Key	
Secondary RADIUS Server IP	
Secondary RADIUS Server Key	
RADIUS Port	
Verify RADIUS packets	
RADIUS Accounting	
RADIUS Accounting port	
Session Timeout	See Table 27 on page 138.
Session Timeout Action	
DNS Proxy for Walled Garden	
Walled Garden	

8. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
9. Or click **View QR code** to generate a QR code.
10. Go to “Creating Login Pages in HTML When External RADIUS is Selected” on page 151.

RADIUS Server for Authentication and No Proxy Server

To delegate RADIUS servers to authenticate wireless clients and no Proxy server to host web pages, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.

   You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

   Note
   You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **SAVE & APPLY** button.
4. Select the **Captive Portal** tab.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 54.
6. Select **Disabled** from the Authentication Page Proxy pull-down menu.

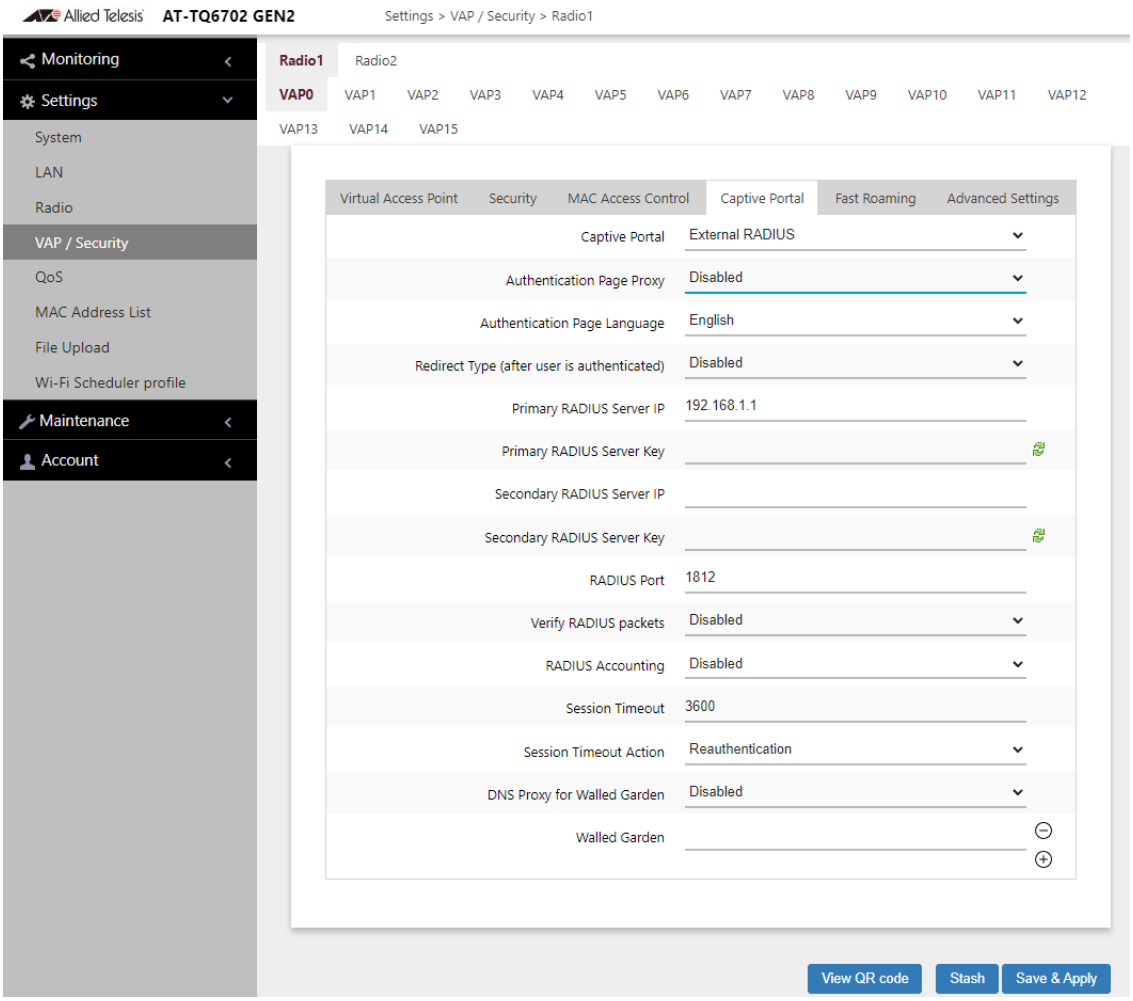

Figure 55. Capital Portal - RADIUS and Authentication Page Proxy

7. Configure the parameters described in Table 30.

Table 30. Captive Portal - External RADIUS and Proxy

Field	Description
Authentication page Proxy	See Table 27 on page 138.
Authentication Page Language	

Table 30. Captive Portal - External RADIUS and Proxy (Continued)

Field	Description
Redirect Type (after user is authenticated)	See Table 28 on page 143.
Primary RADIUS Server IP	
Primary RADIUS Server Key	
Secondary RADIUS Server IP	
Secondary RADIUS Server Key	
RADIUS Port	
Verify RADIUS packets	
RADIUS Accounting	
Radius Accounting Port	
Session Timeout	See Table 27 on page 138.
Session Timeout Action	
DNS Proxy for Walled Garden	
Walled Garden	

8. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
9. Or click **View QR code** to generate a QR code.

Creating Pages in HTML for a Proxy Server

When you are configuring Captive Portal to be hosted by a proxy server, create the following HTML files and place them on the proxy server:

- [*Base URL*]/click_through_login.html
- [*Base URL*]/click_through_login_fail.html
- [*Base URL*]/welcome.html (Optional)

Requirements for the click_through_login.html and click_through_login_fail.html

Here is a list of requirements:

- You must include a <form> element with the method attribute specified to “post” and no action attribute.
- In the <form> element, you must include a <button> tag or an <input> tag with the type attribute specified to “submit” for a wireless client to submit the data to the proxy server.
- No requirement for a welcome.html

HTML Code and Display Examples of Login Page

The following is an example of HTML code:

```
<html>
<head>
<title>Terms of Service</title>
</head>
<form method=”post”>
By using our service, you acknowledge that there
are risks <br>inherent in accessing information
through the internet.<br><br>
<input type=”submit” value=Agree></input>
</form>
</html>
```

Figure 56 shows its web page displayed in a web browser.

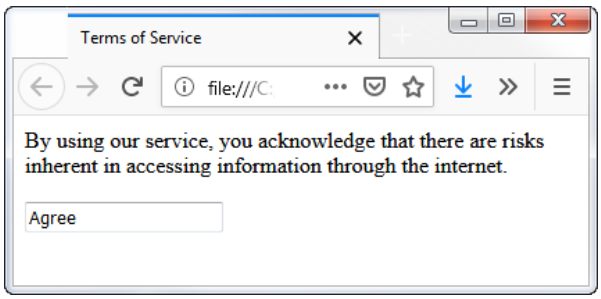

Figure 56. Captive Portal - Terms of Service Page Sample

Creating Login Pages in HTML When External RADIUS is Selected

When you are configuring Captive Portal to be authenticated by a RADIUS server and hosted by a proxy server, create the following HTML files on the proxy server:

- [*Base URL*]/radius_login.html
- [*Base URL*]/radius_login_fail.html
- [*Base URL*]/welcome.html (Optional)

Requirements for the radius_login.html and radius_login_fail.html

Here is a list of requirements:

- You must include a <form> element with the method attribute specified to “post” and no action attribute.
- In the <form> element, you must include an <input> tag with the name attribute specified to “userid” for a wireless client to enter a user ID. The <form> element ends at the </form> end tag.
- In the <form> element, you must include anther <input> tag with the name attribute specified to “password” for a wireless client to enter a password.
- In the <form> element, you must include a <button> tag or an <input> tag with the type attribute specified to “submit” for a wireless client to submit the data to the RADIUS server.
- There is no requirements for a welcome.html

HTML Code and Display Examples of Login Page

The following is an example of HTML code:

```
<html>
<head>
<title>Web Authentication Page</title>
</head>
<form method=”post”>
Username: <input type=”text” name=”userid”><br>
Password: <input type=”password”
name=”password”><br>
<input type=”submit” value=”Connect”></input>
</form>
</html>
```

Figure 57 shows its web page displayed in a web browser.

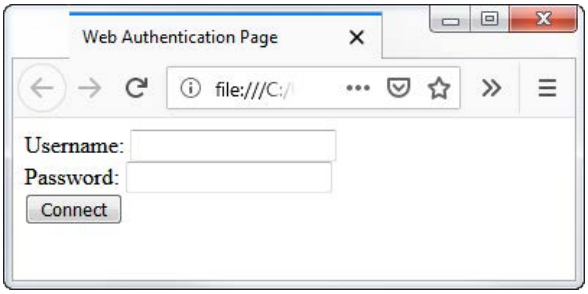

Figure 57. Captive Portal - Login Page Sample

Port Numbers

The following port numbers are used with the IP address of the access point:

- 8080 for HTTP

  `http://[access point's IP address]:8080/auth?redirect=[wireless client's originally requested URL]`

- 8443 for HTTPS

  `http://[access point's IPv4 address]:8443/auth?redirect=[wireless client's originally requested URL]`

Viewing Fast Roaming

The access point supports IEEE802.11k/v/r for high-speed roaming wireless clients.

Guidelines for Fast Roaming

Here are the guidelines:

- You cannot configure Fast Roaming on the access point. Configuring the settings requires Vista Manager EX and AWC.
- When the Security is set to WPA Personal or WPA Enterprise, you can view the parameter values.
- The **View QR code** button is not supported on the Fast Roaming window.

Viewing the IEEE802.11r Parameter Values

To view the parameter values set to **Fast Roaming IEEE802.11r**, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.
3. Select a VAP.The default is VAP0.
4. Select the **Fast Roaming** tab. See Figure 58 on page 155.

Note
The Fast Roaming window shown in Figure 58 on page 155 is when the VAP Security is set to WPA Personal or WPA Enterprise.

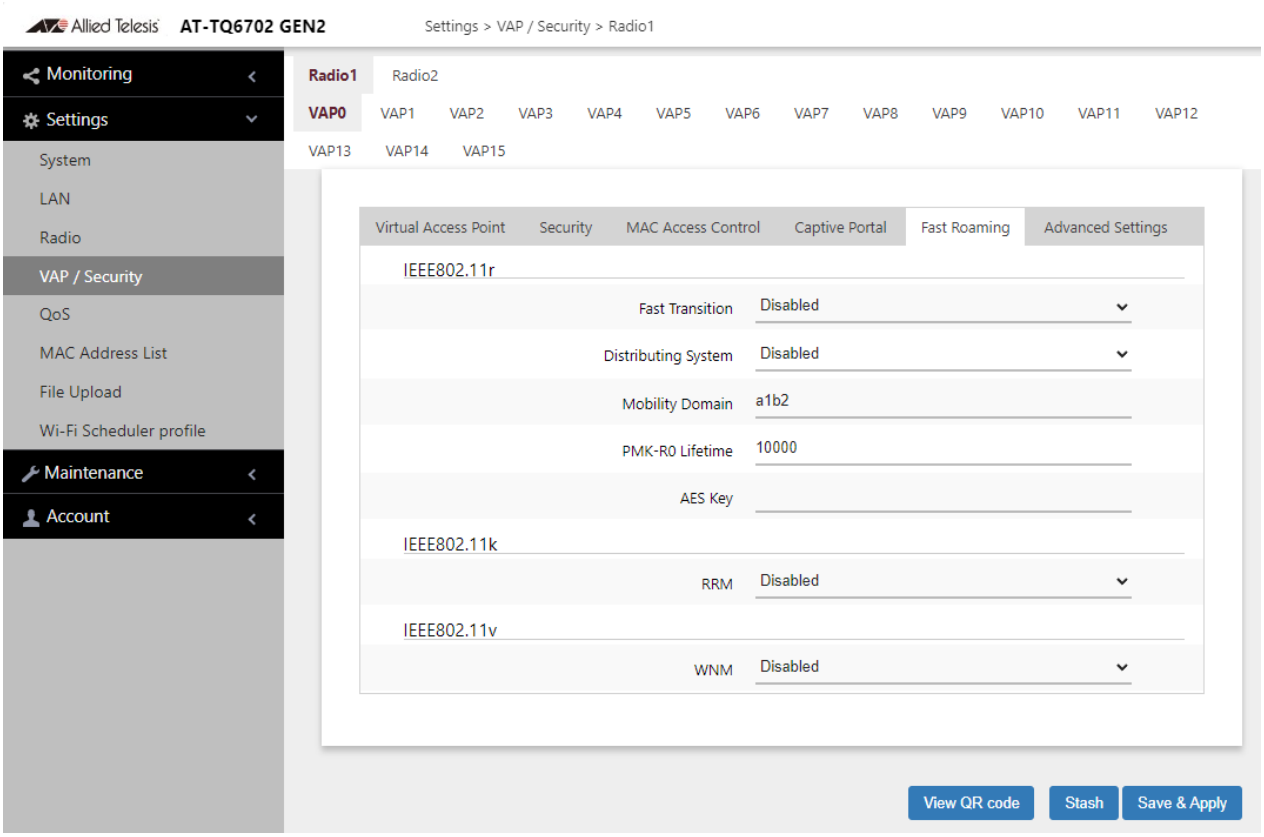

Figure 58. Fast Roaming Window

5. View the parameter values by referring to Table 31.

Note
When the Security is set to WPA Enterprise or WPA Personal, you can view the Fast Roaming settings, but cannot change them. Configuring the settings requires Vista Manager EX and AWC.

Table 31. Fast Roaming IEEE802.11r

Field	Description
Fast Transition	IEEE802.11r Fast Transition is enabled or disabled.
Distributing System	Enable or Disable Distributing System is enabled or disabled.

Table 31. Fast Roaming IEEE802.11r (Continued)

Field	Description
Mobility Domain	Shows the domain name of the access point that provides Fast Roaming. Here are the guidelines: - The name consists of 4 alphanumeric characters. - The key is not case-sensitive. - The default value is a1b2.
PMK-R0 Lifetime	Shows the RMK-R0 lifetime in minutes. The range is 1 to 65535. The default value is 1000.
AES Key	Shows the AES key. Here are the guidelines: - The key consists of 32 alphanumeric characters. - The key is not case-sensitive. - The default value is none.

Viewing IEEE802.11k RRM Status

To view whether **Fast Roaming IEEE802.11k** is enabled or disabled, perform the following procedure:

Note
You cannot enable or disable Fast Roaming on the access point. Enabling or disabling requires Vista Manager EX and AWC.

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.
3. Select a VAP from the next sub-menu. The default is VAP0.
4. Select the **Fast Roaming** tab. See Figure 58 on page 155.
5. View the status of IEEE802.11k.

   The options are:

   - ❒ Enabled: IEEE802.11k Radio Resource Measurement (RRM) is enabled.
   - ❒ Disabled: IEEE802.11k Radio Resource Measurement (RRM) is disabled.

Viewing IEEE802.11v WNM Status

To view whether **Fast Roaming IEEE802.11v** is enabled or disabled, perform the following procedure:

> **Note**
> You cannot enable or disable Fast Roaming on the access point. Enabling or disabling requires Vista Manager EX and AWC.

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1.
3. Select a VAP. The default is VAP0.
4. Select the **Fast Roaming** tab. See Figure 58 on page 155.
5. View the status of IEEE802.11v.

   The options are:

   - Enabled: IEEE802.11v Wireless Network Management (WNM) is enabled.
   - Disabled: IEEE802.11v Wireless Network Management (WNM) is disabled.

Configuring Advanced Settings

To configure advanced VAP settings, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. Select the **Advanced Settings** tab. See Figure 59.

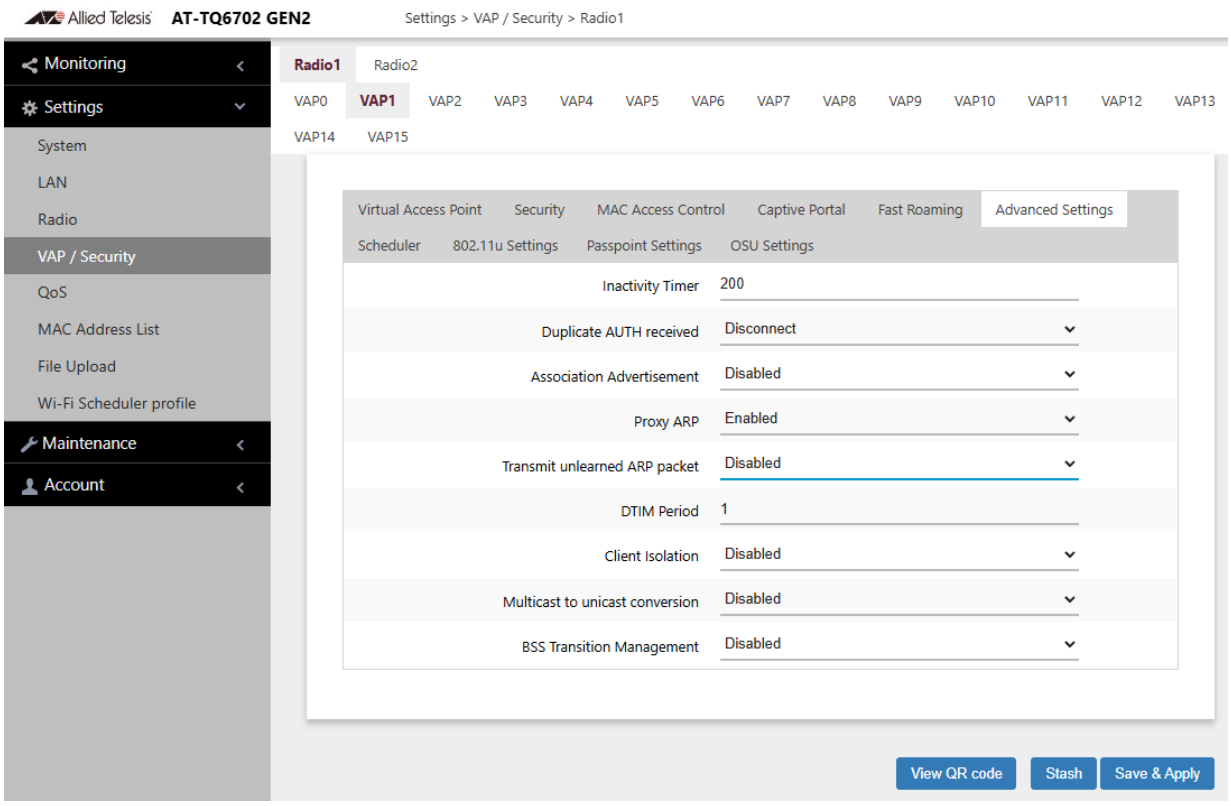

Figure 59. Advanced VAP Settings Window

5. Configure the parameters by referring to Table 32 on page 159.

Table 32. VAP Advanced

Field	Description
Inactivity Timer	Not supported. The value is always 300 seconds.
Duplicate AUTH Received	Controls how the access point responds when it receives authentication requests from wireless clients that has been already authenticated. **Note** To use this feature, the IEEE802.11w (MFP) field must be set to “Disabled.” See “WPA Personal (Pre-Shared Key)” on page 112. The options are listed here: - Disconnect: The access point responds to duplicate authentication requests by sending deauthentications and disconnecting the clients. This is the default setting. - Ignore: The access point responds to duplicate authentication requests by authenticating the clients again.
Association Advertisement	Controls whether the access point informs other access points of newly associated clients, over the wired network. When the access point associates new clients, it can inform the access points to which the clients were previously connected of the change. This enables access points to update their lists of associated clients more quickly. The options are listed here: - Disabled: The access point does not inform other access points of newly associated clients. This is the default setting. - Enabled: The access point does inform other access points of new clients. Other access points on the same subnet must have Association Advertisement enabled to function this feature.

Table 32. VAP Advanced (Continued)

Field	Description
Proxy ARP	Proxy ARP allows the access point to respond to Address Resolution Protocol (ARP) queries for the target IP address that is not on that network. The options are: - Enabled: Proxy ARP is enabled. - Disabled: Proxy ARP is disabled. This is the default setting. **Note** Proxy ARP is functional only when the access point is installed as standalone.
Transmit unlearned ARP packet	This feature allows ARP Request packets received by the AP with IP addresses, that Proxy ARP has not learned, to pass through. The options are: - Enabled: unlearned ARP packets will be transmitted . - Disabled: unlearned ARP packets will not be transmitted. **Note** This feature is available only when Proxy ARP is enabled.
DTIM Period	Controls the delivery traffic indication map (DTIM) period. This specifies the number of beacons an access point transmits before transmitting any buffered broadcast or multicast packets. This allows wireless clients that are in the Sleep Mode to wake up prior to receiving the packets. The range is 1 to 255 beacons. The default is 1 beacon. Specify the number of DTIM Period from 1 to 5. - When the number is higher, the energy saving is more efficacious though the response becomes slow. - When the number is lower, the energy saving is less efficacious though the response becomesquick.

Table 32. VAP Advanced (Continued)

Field	Description
Client Isolation	Enable or disable Client Isolation. The options are: - Disabled: Disable Client Isolation. The access point allows wireless clients to communicate with other clients in the same VAP or different VAPs, and with the wired LAN. This is the default setting. - Within VAP: enables Client Isolation. Devices connected to the same VAP are prevented from communicating with each other, thus effectively isolating them. This feature is often utilized in public or guest Wi-Fi networks to safeguard the privacy and security of individual users. - Within AP: enables Client Isolation. The access point will not allow wireless clients to communicate with other clients on the same or other VAPs.
Multicast to unicast conversion	Enable or disable the multicast-to-unicast conversion. The access point converts received multicast packets to unicast packets when forwarding packets to associated clients. - Enabled: The access point converts multicast packets to unicast packets and forwards them to associated clients. - Disabled: This feature is disabled. This is the default.
BSS Transition Management	Improves the wireless network performance by sharing information with associated wireless clients. Enabled: BSS Transition Management is enabled. Disabled: BSS Transition Management is disabled. This is the default.

6. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

7. Or click **View QR code** to generate a QR code.

Configuring Wi-Fi Scheduler

Wi-Fi Scheduler can be configured manually (per VAP) or by assigning a Wi-Fi Scheduler Profile to a VAP.

To configure Wi-Fi Scheduler, perform the following:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1**, **Radio2**, or **Radio3** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP from the next sub-menu: VAP1 to VAP15 . VAP0 can't have a Wi-Fi Scheduler configured as it can't be disabled.
4. Select the **Scheduler** tab.
5. Select Enabled in the Wi-Fi Scheduler field.

Note
Radio and VAP schedulers run independently of each other and the configuration priority is in the following order: Radio Scheduler > VAP Scheduler > manual configuration. For example, if a VAP is enabled for a specific time period, and the Radio with that VAP is disabled for that same time period, then the VAP will be disabled.

Manually configuring a Schedule

1. Select **Manual Configuration** as the Schedule configuration method. See Figure 60.

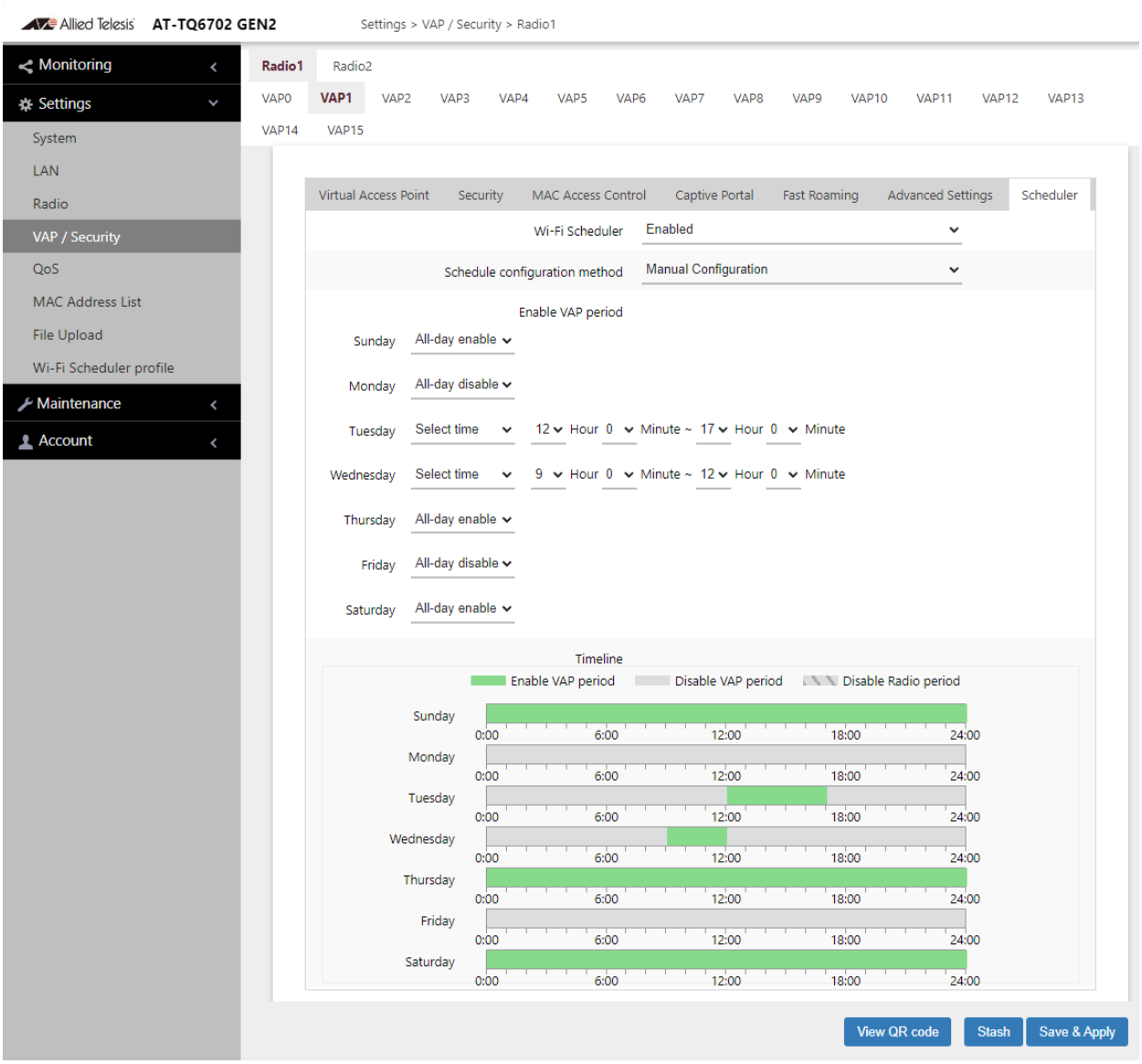

Figure 60. VAP Wi-Fi Scheduler - Manual configuration

2. Configure the parameters by referring to Table 33.

Table 33. VAP Wi-Fi Scheduler Settings - Manual

Field	Description
Wi-Fi Scheduler	Enable or Disable Wi-Fi Scheduler. Disabled is the default setting.
Schedule configuration method	Choose the Configuration method (once Wi-Fi Scheduler has been enabled): - Manual Configuration: Allows the time and day to be set for that specific radio. - Profile Configuration: Assign a profile to that VAP.
Enable VAP period	For each day, the following can be selected: - All-day enable: Wi-Fi is enabled for that 24 hour period - All-day disable: Wi-Fi is enabled for that 24 hour period - Select time: Manually set the time when the Radio/ VAP will be enabled.
Timeline	Graphical display of the timeline configured.

3. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
4. Or click **View QR code** to generate a QR code.

Assigning a Wi-Fi Scheduler Profile

1. In the **Scheduler** tab, select **Profile Configuration** as the Schedule

configuration method. See Figure 61

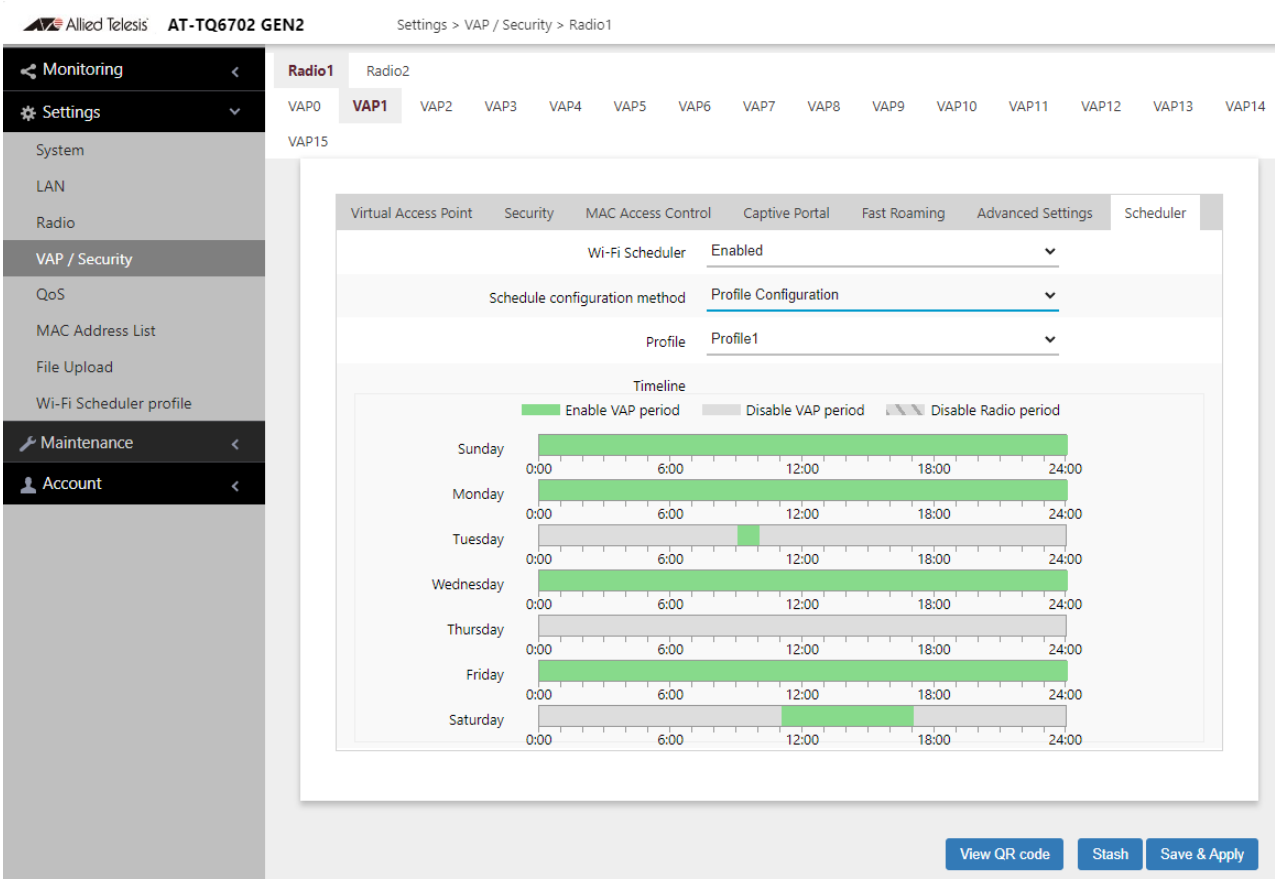

Figure 61. Assigning a Wi-Fi Scheduler Profile to a VAP

2. Configure the parameters by referring to Table 34.

Table 34. VAP Wi-Fi Scheduler Settings - Profile

Field	Description
Wi-Fi Scheduler	Enable or Disable Wi-Fi Scheduler. Disabled is the default setting.
Schedule configuration method	Choose the Configuration method (once Wi-Fi Scheduler has been enabled): - Manual Configuration: Allows the time and day to be set for that specific radio. - Profile Configuration: Assign a profile to that VAP.

Table 34. VAP Wi-Fi Scheduler Settings - Profile (Continued)

Field	Description
Profile	Choose from Profile 1 to Profile 10. These profiles are configured in Wi-Fi Scheduler profile. See “Configuring Wi-Fi Scheduler” on page 162.
Timeline	Graphical display of the timeline configured.

3. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

4. Or click **View QR code** to generate a QR code.

Configuring 802.11u Settings

802.11u is one of the features required by Hotspot2.0. If you want to use the Hotspot function, configure the IEEE 802.11u and Hotspot2.0 settings. 802.11u, an amendment to IEEE 802.11-2007, specifies interworking with the other external networks.

The 802.11u Settings window is only visible once Passpoint has been enabled in the Virtual Access Point tab.

To configure the 802.11u settings, perform the following procedure

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. In the **Virtual Access Point** tab, enable Passpoint. The **802.11u Settings** tab will now be visible. See Figure 39 on page 104.
5. Select the **802.11u Settings** tab. See Figure 62.

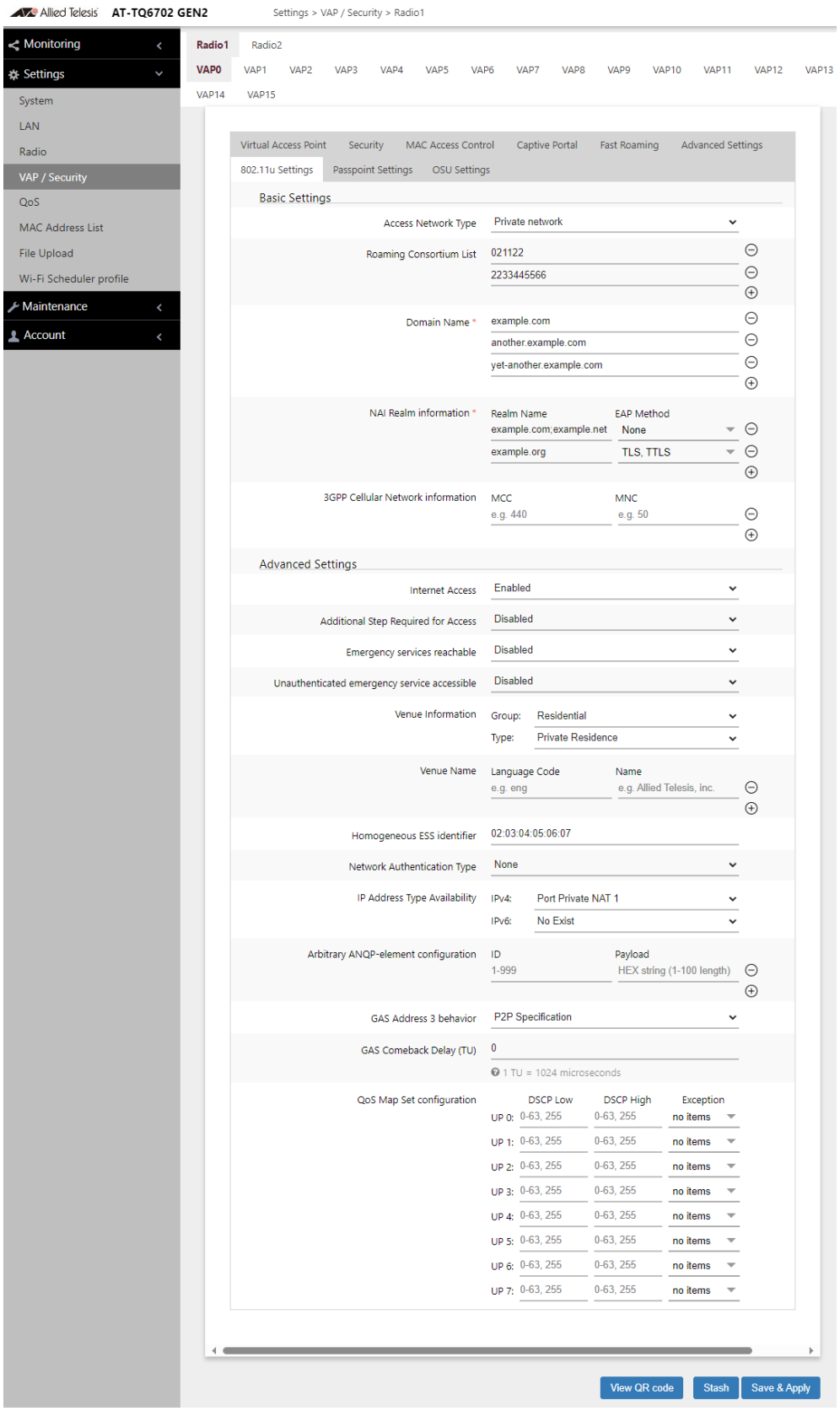
Allied Telesis AT-TQ6702 GEN2
Settings > VAP / Security > Radio1
Monitoring
Settings
System
LAN
Radio
VAP / Security
QoS
MAC Address List
File Upload
Wi-Fi Scheduler profile
Maintenance
Account
Radio1
Radio2
VAP0 VAP1 VAP2 VAP3 VAP4 VAP5 VAP6 VAP7 VAP8 VAP9 VAP10 VAP11 VAP12 VAP13 VAP14 VAP15
Virtual Access Point
Security
MAC Access Control
Captive Portal
Fast Roaming
Advanced Settings
802.11u Settings
Passpoint Settings
OSU Settings
Basic Settings
Access Network Type
Private network
Roaming Consortium List
021122
2233445566
Domain Name *
example.com
another.example.com
yet-another.example.com
NAI Realm information *
Realm Name
EAP Method
example.com;example.net
None
example.org
TLS, TTLS
3GPP Cellular Network information
MCC
MNC
e.g. 440
e.g. 50
Advanced Settings
Internet Access
Enabled
Additional Step Required for Access
Disabled
Emergency services reachable
Disabled
Unauthenticated emergency service accessible
Disabled
Venue Information
Group:
Residential
Type:
Private Residence
Venue Name
Language Code
Name
e.g. eng
e.g. Allied Telesis, inc.
Homogeneous ESS identifier
02:03:04:05:06:07
Network Authentication Type
None
IP Address Type Availability
IPv4:
Port Private NAT 1
IPv6:
No Exist
Arbitrary ANQP-element configuration
ID
Payload
1-999
HEX string (1-100 length)
GAS Address 3 behavior
P2P Specification
GAS Comeback Delay (TU)
0
1 TU = 1024 microseconds
QoS Map Set configuration
DSCP Low
DSCP High
Exception
UP 0: 0-63, 255 0-63, 255 no items
UP 1: 0-63, 255 0-63, 255 no items
UP 2: 0-63, 255 0-63, 255 no items
UP 3: 0-63, 255 0-63, 255 no items
UP 4: 0-63, 255 0-63, 255 no items
UP 5: 0-63, 255 0-63, 255 no items
UP 6: 0-63, 255 0-63, 255 no items
UP 7: 0-63, 255 0-63, 255 no items
View QR code
Stash
Save & Apply

Figure 62. 802.11u Settings Window

6. Configure the parameters by referring to Table 35 and Table 36 on page 171.

Note
Table 35 provides a brief description of the fields in Figure 62. For detailed information, see IEEE 802.11u STANDARD for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements, Part 11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 7: Interworking with External Networks.

Table 35. 802.11u Basic Settings

Field	Description
Access Network Type	Specifies the access network type. The default is Private network. - Private network – Network that unauthenticated users cannot enter. Example: Private networks, enterprise networks, etc. that use user accounts. - Private network with guest access – Guest accessible private network Example: Enterprise network with existing guest users. - Chargeable public network – By paying a fee Anyone anytime access is possible for network. Charge form etc. can be obtained by other methods. (IEEE 802.21, http/https redirect or DNS redirection). Example: Coffee shop monthly system network, Hotel room network. - Free public network – Anyone free access possible network. Example: Hotspot for airport, Network provided by the city. - Personal device network – Network for personal devices. Example: Network for photo printing connecting camera and printer. - Emergency services only network – Limited network provided by the emergency service (Police, Firefighting). Example: For emergency calls. For receiving emergency alerts. - Test or experimental – Test or experimental network. - Wildcard – Wildcard access network

Table 35. 802.11u Basic Settings (Continued)

Field	Description
Roaming Consortium List	Sets Roaming Consortium List with Organization Identifier (OI). Specify Hexadecimal (length 6-30). The default is 021122. Use the "plus" button to add more (up to 15 can be registered).
Domain Name	Specifies domain name used for certificate. Use the "plus" button to add multiple domains. Length 1-253. The defaults are: example.com Use the “minus” button to remove the defaults. The field is required.
NAI Realm information	Specifies the NAI (Network Access Identifier) Realm information. - Realm Name NAI Realm entered as a FQDN (fully qualified domain name) Defaults are: example.com; example.net; example.org. - EAP Method: Specify EAP Method type: • TLS • TTLS • SIM • AKA The defaults are None and TLS,TLLS. Use the “minus” button to remove the defaults. These fields are required.
3GPP Cellular Network information	Specifies 802.11u 3rd Generation Partnership Project (3GPP) Cellular Network Code. - MCC (Mobile Community Code): Specify Country Code (Three digits). Example, in Japan it is 440. - MNC (Mobile Network Code): Specify Career Mobile Network Code (Two or three digits). Use the "plus" button to create multiple entries. The default is blank.

Table 36. 802.11u Advanced Settings

Field	Description
Internet Access	Enables or disables Internet Access. Here are the settings: - Enabled: Activates Internet access. - Disabled: Deactivates Internet access. This is the default.
Additional Step Required for Access	Enables or disables Additional Step Required for Access. Here are the settings: - Enabled: Activates Additional Step Required for Access. - Disabled: Deactivates Additional Step Required for Access. This is the default.
Emergency services reachable	Enables or disables Emergency services reachable. Here are the settings: - Enabled: Activates Emergency services reachable. This is the default. - Disabled: Deactivates Emergency services reachable.
Unauthenticated emergency service accessible	Enables or disables Unauthenticated emergency service accessible. Here are the settings: - Enabled: Activates. - Disabled: Deactivates. This is the default.
Venue Information	Specifies the groups and type of the facility providing the service. - Group Specifies the category of the place where this product belongs. - Type Specifies category type specified by Venue Group. The defaults are: Group: Residential. Type: Private Residence.

Table 36. 802.11u Advanced Settings (Continued)

Field	Description
Venue Name	Specifies the language code and name of the facility providing the service. Use the "plus" button to add more entries. - Language Code Example: eng - Name Example: Allied Telesis corporation The default is blank.
Homogeneous ESS identifier	Specifies the Passpoint network on the other Wireless AP with the same SSID. The format specifies the MAC address in hexadecimal every octet (2 digits) separated by a colon. The default is 02:03:04:05:06:07.
Network Authentication Type	Specifies the Network Authentication Type: - None - Terms and Conditions - Online Enrollment - Redirect HTTP HTTPS - Redirect DNS When Terms and Conditions or Redirect HTTP HTTPS are selected, the Network Authentication Type - Redirect URL field appears. Example: http://example.com The default is None.

Table 36. 802.11u Advanced Settings (Continued)

Field	Description
IP Address Type Availability	Specifies the IPv4 and IPv6 address type. IPv4 - No Exist - Public - Port Restrict - Private NAT 1 - Private NAT 2 - Port Private NAT 1 - Port Private NAT 2 - Unknown The default is Port Private NAT 1. IPv6 - No Exist - Exist - Unknown The default is No Exist.
Arbitrary ANQP-element configuration	Access Network Query Protocol (ANQP). Specifies when there is an additional designation of Access Network Query Protocol (ANQP)-element. - ID: Specify the ID (1-999) The default is blank. - Payload: Specify ANQP payload with 100 characters or less. The default is blank.

Table 36. 802.11u Advanced Settings (Continued)

Field	Description
GAS Address 3 behavior	The Generic Advertisement Service (GAS) address setting. - P2P specification: When BSSID included in GAS Initial request packet is Wildcard BSSID(FF:FF:FF:FF:FF:FF) and Destination MAC address "Multi cast address and Client not Association" or "Broad cast address", respond using Wildcard BSSID(FF:FF:FF:FF:FF:FF). In other cases, respond using Wireless AP BSSID. - IEEE 802.11 standard: When Destination MAC address "Multi cast address and Client not Association" or "Broad cast address", respond using Wildcard BSSID(FF:FF:FF:FF:FF:FF). In other cases, respond using Wireless AP BSSID. - Force Non-Compliant Behavior: Under any conditions respond makes use of Wireless AP BSSID. The default is P2P Specification.
GAS Comeback Delay	Specifies GAS Comeback Time. The range is 0-65535TU(1TU=1024msec). The default is 0.

Table 36. 802.11u Advanced Settings (Continued)

Field	Description
QoS Map Set configuration	QoS Map Setting is specified by choosing the DSCP Low and High values, and selecting any exceptions. - DSCP Low - DSCP High Specify the DSCP values in the range of 0 to 63 or 255. When DSCP range is "255,255", User Priority is Not used . Example: When setting DSCP except two pieces and DSCP range corresponding to User priority (UP) 0-7 to the setting value in the following table, QOSMAP status. Specified value is "53,2,22,6,8,15,0,7,255,255,16,31,32,39, 255,255,40,47,255,255" Setting items | Set value | Explanation DSCP exception 1 | 53,2 | DSCP value 53 only Exceptionally use User priority 2. DSCP exception 2 | 22,6 | DSCP value 22 only Exceptionally use User priority 6. UP0 DSCP range | 8,15 | DSCP value 8-15 use User priority 0. UP1 DSCP range | 0,7 | DSCP value 0-7 use User priority 1. UP2 DSCP range | 255,255 | User priority 2 not used. UP3 DSCP range | 16,31 | DSCP value 16-31 use User priority 3. UP4 DSCP range | 32,39 | DSCP value 32-39 use User priority 4. UP5 DSCP range | 255,255 | User priority 5 not used. UP6 DSCP range | 40,47|: DSCP value 40-47 use User priority 6. UP7 DSCP range | 255,255 | User priority 7 not used. The default is blank

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
8. Or click **View QR code** to generate a QR code.

Configuring Passpoint Settings

Passpoint adds support for WiFi Certified Passpoint on captive portals. The feature allows mobile devices that support the IEEE 802.11u standard to automatically connect to subscribed Hotspot 2.0 services through the wireless access points. Passpoint is available on all radios, VAPs, and captive portals.

The Passpoint Settings window is only visible once Passpoint has been enabled in the Virtual Access Point tab.

To configure the Passpoint settings, perform the following procedure:

1. Select **Settings** > **VAP / Security** from t he main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. In the **Virtual Access Point** tab, enable Passpoint. The **Passpoint Settings** tab will now be visible. See Figure 39 on page 104.
5. Select the **Passpoint Settings** tab. See Figure 63 on page 177.

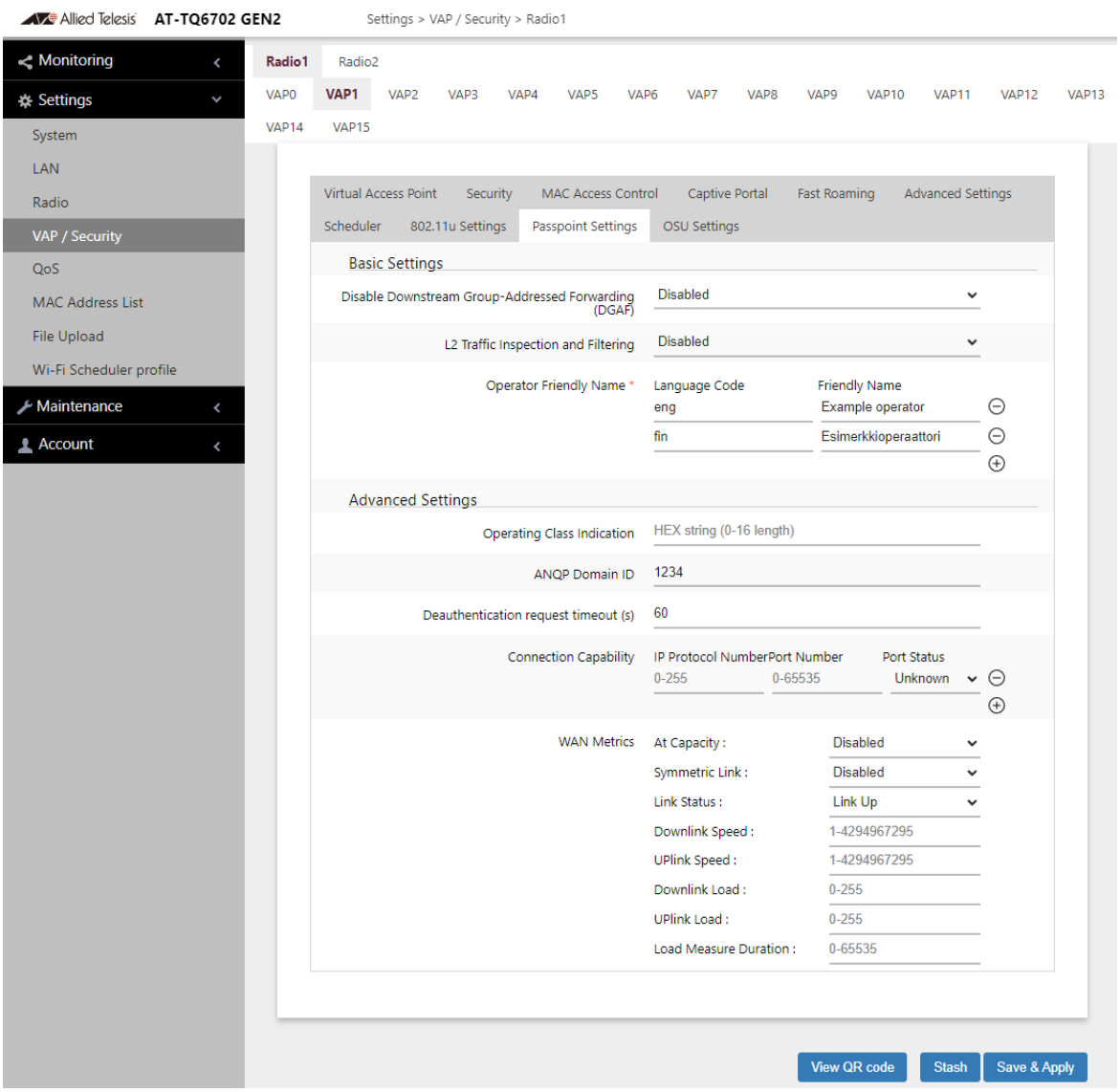

Figure 63. Passpoint Settings Window

6. Configure the parameters by referring to Table 37 and Table 38.

Table 37. Passpoint Basic Settings

Field	Description
Disable Downstream Group-Addressed Forwarding (DGAF)	Enables or disables sending of multicast and broadcast frames. - Enabled: Does not send Multicast and Broadcast - Disabled: Sends Multicast and Broadcast. This is the default.
L2 Traffic Inspection and Filtering	Enables or disables traffic between VAPs L2 traffic (ARP, ICMP, TDLS). - Enabled: Discards L2 traffic (ARP, ICMP, TDLS) between VAPs. - Disabled: Does not discard L2 traffic (ARP, ICMP, TDLS) between VAPs. This is the default.
Operator Friendly Name	Specifies the Language Code and the name of the operator providing the service in the following format: - Language Code: Example: “fin” or “eng”. Based on ISO 639-3 (International standard for language codes). The defaults are “fin” and “eng”. - Friendly Name: The defaults are “Example operator” and "Esimerkkioperaattori". These fields are required.

Table 38. Passpoint Advanced Settings

Field	Description
Operating Class Indication	Specifies the Operating Class Identification Number of the output wireless information. The default is blank. **Note** If using W52 or W53 on Radio 2, enter "7376". Radio | Operating Class(DEC) | Identification number (HEX) | Overview Radio1 (2.4GHz) | 81 | 51 | 2.4GHz : 1,2,3,4,5,6,7,8,9,10,11,12,13 Radio2 (5GHz Low Band) | 115(W52) , 118(W53) | 73(W52) , 76(W53) | 5GHz: 36,40,44,48,52,56,60,64 Radio3 (5GHz High Band) | 121 | 79 | 5GHz: 100,104,108,112,116,120,124,128,132,136,140
ANQP Domain ID	Specifies the Access Network Query Protocol (ANQP) Domain ID. The default is 1234
Deauthentication request timeout	Specifies the time (in seconds) during which the notification page containing the content of the connection refusal can be downloaded. The default is 60.
Connection Capability	Specifies the communication port protocol and status in the following format: - IP Protocol Number: Specify the protocol number in the range of 0 to 255. - Port Number: Specify the port number in the range of 0 to 65535. - Port Status: Select the port status: Closed Open Unknown The default is Unknown.

Table 38. Passpoint Advanced Settings (Continued)

Field	Description
WAN Metrics	Specify the link status on the WAN side. - At Capacity: Enabled or disabled. If enabled, when the network is running at full capacity no more clients will be able to associate until this feature s disabled. The default is disabled. - Symmetric Link: Specifies whether the uplink and downlink link speed are the same. The default is Disabled. - Link Status: specifies the link status. The default is Link Up. (what is Link Test) - Downlink/Uplink Speed: WAN side line speed enter kbps unit. 1Gbps → 1000000 (kbps) - Downlink/Uplink Load: WAN line Load factor enter. When unknown, specify 0. A formula: Rotational load factor (%) / 100×255 - Example: 75% → 75/100×255 = 191 - Load Measure Duration: specifies the time interval (in tenths of a second) over which the AP averages its load measurement. Example for a 1 minute duration enter 600.

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

8. Or click **View QR code** to generate a QR code.

Configuring OSU Settings

Online Sign Up (OSU) adds support for WiFi Certified Passpoint on captive portals. The feature allows mobile devices that support the IEEE 802.11u standard to automatically connect to subscribed Hotspot 2.0 services through the wireless access points. Passpoint is available on all radios, VAPs, and captive portals.

The OSU Settings window is only visible once Passpoint has been enabled in the Virtual Access Point tab.

To configure the OSU settings, perform the following procedure:

1. Select **Settings** > **VAP / Security** from t he main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

> **Note**
> You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **Save & Apply** button.

4. In the **Virtual Access Point** tab, enable Passpoint. The **802.11u, Settings**, **Passpoint Settings** and **OSU Settings** tabs will now be visible. See Figure 39 on page 104.
5. Select the **OSU Settings** tab. See Figure 64 on page 182.

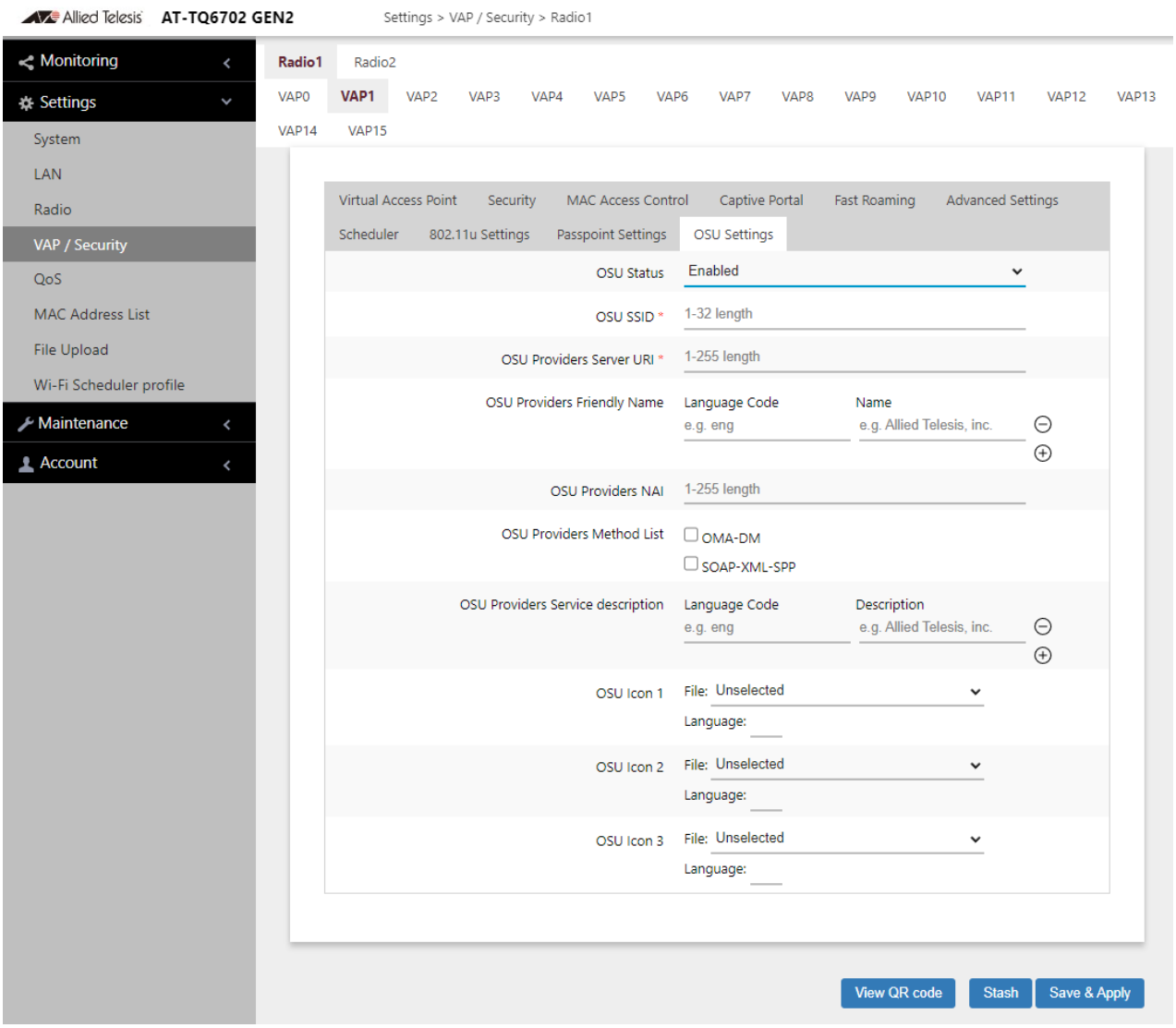

Figure 64. OSU Settings Window

6. Configure the parameters by referring to Table 39.

Table 39. OSU Settings

Field	Description
OSU Status	Enables or disables the Online Sign-Up (OSU) function. - Enabled: enables the OSU function. - Disabled: disables the OSU function. This is the default.

Table 39. OSU Settings (Continued)

Field	Description
OSU SSID	Specifies the OSU SSID. This is a required field when OSU is enabled. The default is blank.
OSU Providers Server URI	Specifies the Uniform Resource Identifier (URI) of the provider's OSU server. Example: osu-server.corp.example.com This is a required field when OSU is enabled. The default is blank.

Table 40. Passpoint Advanced Settings

Field	Description
OSU Providers Friendly Name	Specifies the language code and name of the OSU provider. Use the "plus" button to add more entries. - Language Code (ISO 639 language code) Example: eng - Name Example: Allied Telesis corporation The default is blank.
OSU Providers NAI	Specifies the Network Access Identifier (NAI) of the provider's OSU server. Example: joe@example.com The default is blank.
OSU Providers Method List	Specifies the OSU provider's provisioning list. - OMA-DM: Provisioning with Open Mobile Alliance - SOAP-XML-SPP: Simple Object Access Protocol provisioning using a subscription provisioning protocol based on XML.

Field	Description
OSU Providers Service description	Enter the OSU provider's service name.The name has two elements: - Language code: Specifies the language code. - Service name: Specifies the OSU provider's service name. The default is blank.
OSU Icon 1, 2, 3	Specify the OSU provider's icon. Icon files are uploaded to the access point with the File Upload option in the Settings menu. For instructions, refer to "Uploading a File" on page 198.

7. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

8. Or click **View QR code** to generate a QR code.

Configuring MAC Address Control Settings

This section explains how to add security to VAPs by having the access point authenticate the MAC addresses of wireless clients. It forwards wireless traffic from only approved addresses. The device can authenticate MAC addresses with its on-board MAC address filter, an external RADIUS server, or both. There are also options to authenticate clients by their physical locations with AMF.

Here are the guidelines to the MAC Address Control and MAC Address List:

- The access point has only one MAC Address Control.
- You can activate or deactivate MAC Address Control on individual VAPs.
- You can create multiple MAC address lists, up to a maximum of 48.
- You can apply multiple MAC address lists to each VAP, up to a maximum of 3,072.
- You cannot enter broadcast or multicast addresses.
- To activate MAC Address Control on VAPs, See “Configuring MAC Access Control” on page 124.

To add entries to the MAC address list, perform the following procedure:

1. Select **Settings** > **MAC Address List**. Refer to Figure 65.

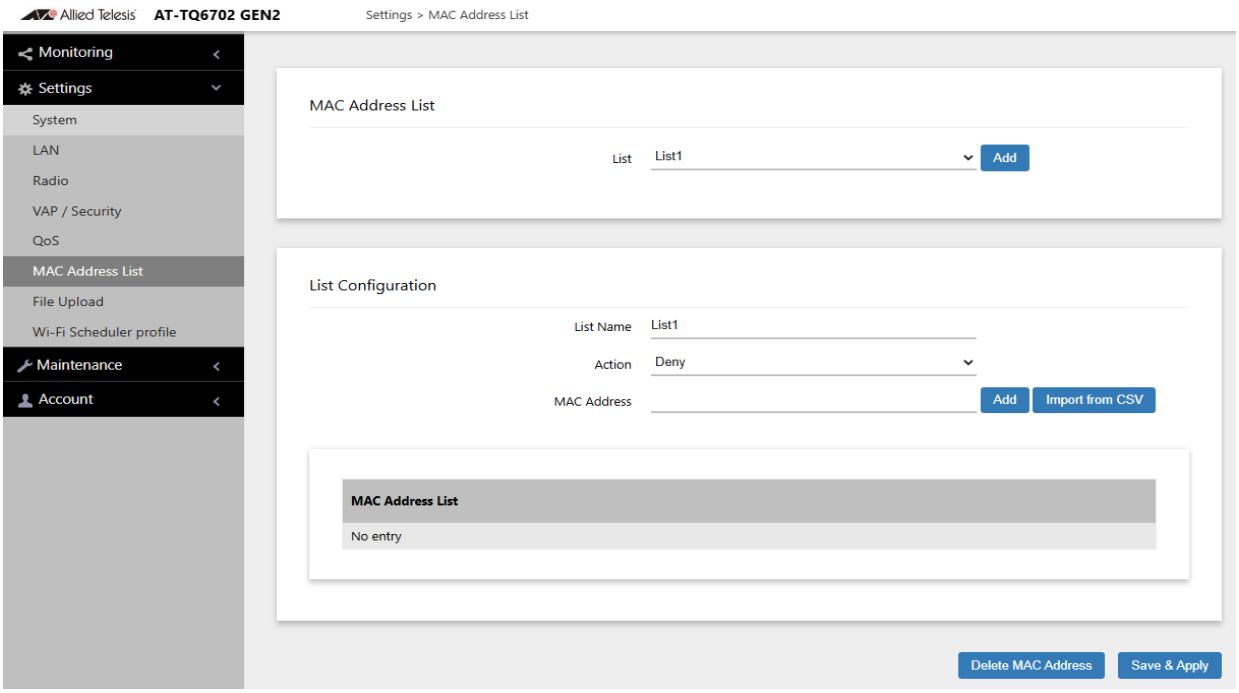

Figure 65. MAC Address List Window

2. In MAC Address List, from the **List** pull-down menu, select a list and click the **Add** button. You can apply multiple MAC address lists to a VAP.

3. To delete a MAC address list, select the list and click the **Delete List** button.

4. In List Configuration, from the **List Name** pull-down menu, choose a list.

5. From the **Action** pull-down menu, select one of the following:

   - Deny: Select this option to have the access point reject association requests from wireless clients whose MAC addresses you enter in the filter, and to accept association requests from all other clients. This is the default setting.
   - Allow: Select this option to have the access point accept association requests from the wireless clients whose MAC addresses you enter in the filter, and to reject association requests from all other clients.

6. To enter the MAC address of a wireless client the access point is to deny or accept, you have two methods to enter MAC addresses:

   - Click the **MAC Address** field and enter one MAC address in this format xx:xx:xx:xx:xx:xx and click **Add** button.
   - Click the **Import from CSV** button to upload a csv file, which includes one or more MAC addresses in the format xx:xx:xx:xx:xx:xx that are separated with a comma.

7. Click the **Add** button.

8. To remove addresses, do one of the following:

   - To delete MAC addresses individually, click the check boxes of the addresses in the list and click the **Delete MAC Address** button.
   - To delete all the addresses, click the check box to the right of the MAC Address List title and click the **Delete List** button.

9. Click the **Save & Apply** button to save and update the configuration, or **Delete List** button to delete the MAC Address list.

10. Or click **View QR code** to generate a QR code.

Chapter 8

Quality of Service

This chapter describes the following procedures:

Introduction to Quality of Service

Each radio in the access point has four QoS egress queues and four ingress queues. There are parameters that control the manner in which the device stores and handles packets in the queues. You should not adjust these values unless you are familiar with QoS. The parameters are divided into the following two groups:

- Access Point (AP) Enhanced Distributed Channel Access (EDCA) Parameters table contains parameters that control the four queues that store egress traffic the access point transmits to the wireless clients.
- The Station Enhanced Distributed Channel Access (EDCA) Parameters table controls the four queues that store ingress traffic the access point receives from the clients.

To configure the QoS settings for the radios, perform the following procedure.

1. Select **Settings** > **QoS** from the main menu.
2. Select **Radio**1 or **Radio2** from the sub-menu. You can configure only one radio at a time. Refer to Figure 66 on page 189.
3. Configure the QoS parameters by referring to the following sections:
   - “Configuring QoS Basic Settings” on page 190
   - “Configuring AP EDCA Parameters” on page 191
   - “Configuring Station EDCA Parameters” on page 194
4. Click the **Save & Apply** button to save and update your configuration.

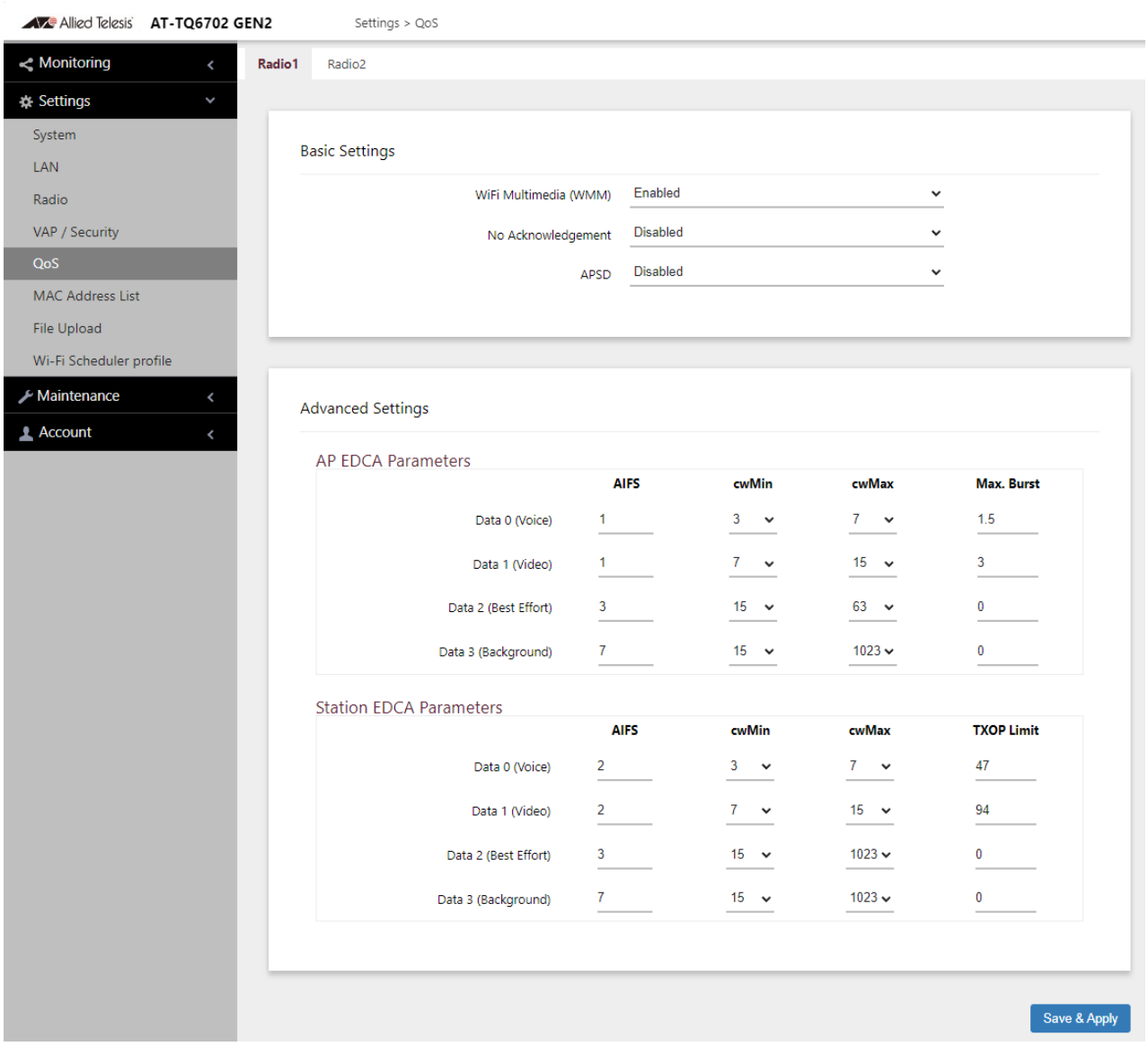

Figure 66. QoS Window

Configuring QoS Basic Settings

The fields for the Basic Settings section are defined in Table 41.

Table 41. QoS Window - Basic Settings

Parameter	Description
WiFi Multimedia (WMM)	Enable or disable QoS prioritizing and coordination. Here are the options: - Enabled: The access point uses the AP EDCA settings to control the flow of downstream traffic to the wireless clients and the station EDCA parameters to control the flow of upstream traffic from the clients. This is the default setting. - Disabled: QoS control of the upstream traffic from the clients is disabled. You can still configure some of the parameters that control the downstream traffic from the access point to the clients. WMM must be enabled on radios that use IEEE 802.11n or IEEE 802.11ac.
No Acknowledgment	Enable or disable No Acknowledgment. Acknowledgment is a verification signal data that wireless clients transmit to the access points. The Acknowledgment process takes bandwidth and airtime. Here are the options: - Enabled: The access point removes Acknowledgment to improve the amount of data transmission. - Disabled: No Acknowledgment is disabled. This is the default setting.
APSD	Enable or disable Automatic Power Save Delivery (APSD). APSD allows wireless clients to enter standby or sleep mode to in order to save battery while connected to the access point. Here are the options: - Enabled: Enable APSD. - Disabled: Disable APSD.

Configuring AP EDCA Parameters

Table 42 defines the AP EDCA parameters in the QoS window in Figure 66 on page 189.

Table 42. QoS Window - AP EDCA Parameters

Parameter	Description
Data Type (Queue)	Lists the four egress queues: - Data 0 (Voice): High priority queue, with low latency and guaranteed bandwidth. The queue is used to store time-sensitive data, such as VOIP and streaming media. - Data 1 (Video): High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as video traffic. - Data 2 (best effort): Medium priority queue, with minimum throughput and delay. The queue is used to store most traditional IP data. - Data 3 (Background): Lowest priority queue, with high throughput. This queue is used for bulk data that requires maximum throughput and is not time-sensitive, such as FTP packets.
AIFS (InterFrame Space)	Select the Arbitration Inter-Frame Spacing (AIFS) value to control the amount of time the access point waits after transmitting a frame and before transmitting the next frame. Queues with shorter wait times have higher priorities than queues with longer wait times. Here are the guidelines: - The wait time is measured in slots. - The range is 1 to 15 slots. - The defaults are 1 for Data 0 and Data 1, 3 for Data 2, and 7 for Data 3.

Table 42. QoS Window - AP EDCA Parameters (Continued)

Parameter	Description
cwMin (Minimum Contention Window)	Enter a value (in milliseconds) to be the lower limit of the range from which the access point determines the initial random back-off wait time.for resending packets during transmission conflicts. Here are the guidelines: - The access point generates the first random number between 0 and this number. - If the first random back-off wait time expires before the data frame is sent, a retry counter is increased and the random back-off value (window) is doubled. Doubling continues until the size of the random back-off value reaches the number defined in the maximum contention window. - Valid values for this parameter are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. - This parameter must be lower than the cwMax value. - The defaults are 3 for Data 0, 7 for Data 1, and 15 for Data 2 and Data 3.
cwMax (Maximum Contention Window)	Select the maximum contention window, which is the upper limit (in milliseconds) for doubling the random back-off value. The doubling continues until either the data frame is sent or the maximum contention size is reached. Once the maximum contention window is reached, retries continue until a maximum number of retries is reached. Here are the guidelines: - This parameter must be greater than or equal to the cwMin value. - Valid values are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. - The default values are 7 for Data 0, 15 for Data 1, 63 for Data 2, and 1023 for Data 3.

Table 42. QoS Window - AP EDCA Parameters (Continued)

Parameter	Description
Max. Burst	Specifies the maximum burst length (in seconds) for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Here are the guidelines: - This is an AP EDCA parameter only and as such applies only to egress traffic from the access point to the wireless clients. - The factory defaults are 1.5 for Data 0, 3.0 for Data 1, and 0 for Data 2 and Data 3. - The range is 0.0 to 8.1 seconds.

Configuring Station EDCA Parameters

Table 43 defines the Station EDCA parameters in the QoS window in Figure 66 on page 189.

Table 43. QoS Window - Station EDCA Parameters

Parameter	Description
Data Type (Queue)	Specifies the four ingress queues: - Data 0 (Voice) - High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as VOIP and streaming media. - Data 1 (Video): High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as video traffic. - Data 2 (best effort): Medium priority queue, with minimum throughput and delay. The queue is used to store most traditional IP data. - Data 3 (Background): Lowest priority queue, with high throughput. This queue is used for bulk data that requires maximum throughput and is not time-sensitive, such as FTP packets.
AIFS (InterFrame Space)	Select the Arbitration Inter-Frame Spacing (AIFS) value to control the wait time for data frames. The wait time is measured in slots and has the range 1 to 15 slots. The defaults are listed here:2 for Data 0 and Data 1, 3 for Data 2, and 7 for Data 3.

Table 43. QoS Window - Station EDCA Parameters (Continued)

Parameter	Description
cwMin (Minimum Contention Window)	Enter a value (in milliseconds) to be the lower limit of the range from which the station determines the initial random back-off wait time.for resending packets during transmission conflicts. Here are the guidelines: - The first random number the station generates will be between 0 and this number. - If the first random back-off wait time expires before the data frame is sent, a retry counter is increased and the random back-off value (window) is doubled. Doubling continues until the size of the random back-off value reaches the number defined in the maximum contention window. - This parameter must be less than or equal to the cwMax value. - Valid values for this parameter are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023 milliseconds. - The defaults are 3 for Data 0, 7 for Data 1, and 15 for Data 2 and Data 3.
cwMax (Maximum Contention Window)	Select the maximum contention window, which is the upper limit (in milliseconds) for doubling the random back-off value. The doubling continues until either the data frame is sent or the maximum contention size is reached. Once the maximum contention window is reached, retries continue until a maximum number of retries is reached. Here are the guidelines: - This parameter must be greater than or equal to the cwMin value. - Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023 milliseconds. - The default values are 7 for Data 0, 15 for Data 1, and 1023 for Data 2 and Data 3.

Table 43. QoS Window - Station EDCA Parameters (Continued)

Parameter	Description
TXOP Limit	Select the Transmission Opportunity (TXOP) limit. It defines the time intervals that a WME client has the right to initiate transmission to the access point. Here are the guidelines: - The time intervals are in 32 microseconds. - The range is 0 to 256 intervals. - The default intervals are 47 for Data 0, 94 for Data 1, and 0 for Data 2 and Data 3.

Chapter 9

File Upload

This chapter contains the following procedure:

Uploading a File

The File Upload window is used to upload Passpoint Online Sign-up (OSU) icon files to the wireless access point. The files contain the authentication server icons that are displayed on the mobile devices when wireless clients connect to a network. OSU vector icons are similar to iOS (iPhone OS) style icons. They are images with an .osu extension. Refer to Figure 63.

To upload a file, perform the following procedure:

1. Select **Settings** > **File Upload** from the main menu. See Figure 67.

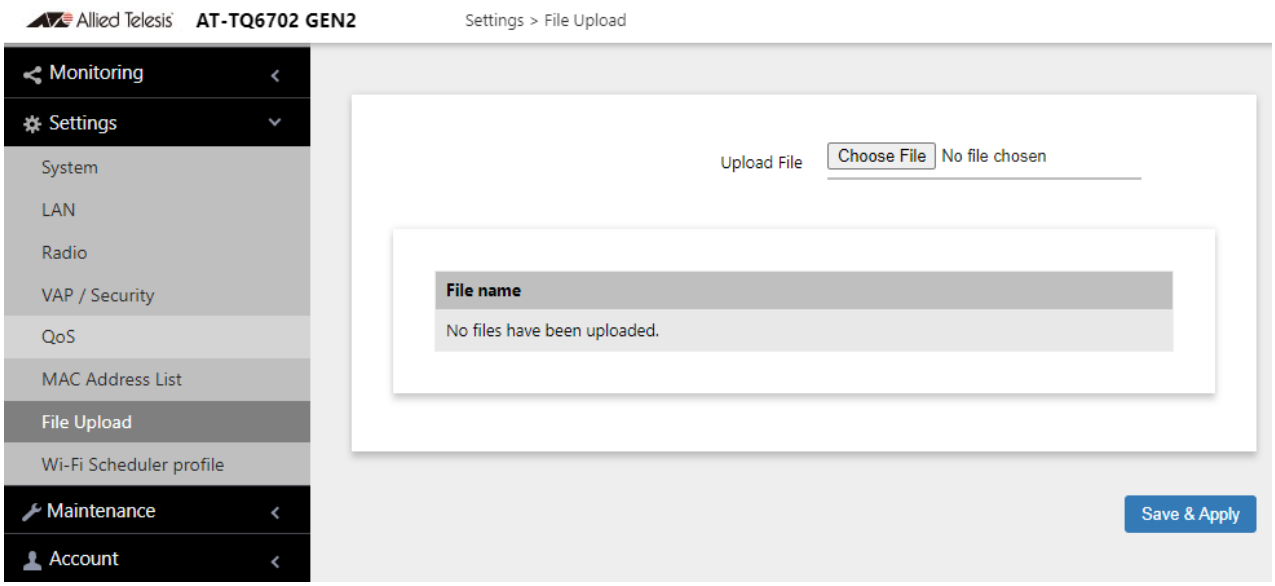

Figure 67. File Upload Window

2. Click the **Choose File** button to locate the OSU icon file on your workstation or network drive.

3. Click the **Save & Apply** button to upload the file to the wireless access point.

Chapter 10

Wi-Fi Scheduler

This chapter contains the following sections:

Introduction to Wi-Fi Scheduler

Wi-Fi Scheduler controls when Wi-Fi is enabled and disabled on radios and VAPs.

Wi-Fi Scheduler Profiles can be configured and then assigned to multiple Radios/VAPs.

Wi-Fi Scheduler can be configured on radios and VAPs, both manually and by assigning a Scheduler profile. See “Configuring Wi-Fi Scheduler” on page 162.

This chapter shows how to create a Wi-Fi Scheduler Profile.

Wi-Fi Scheduler Guidelines

Here are guidelines for configuring Wi-Fi Scheduler:

- Up to ten Scheduler Profiles can be configured.
- A scheduler Profile can be assigned to multiple Radios/VAPs.
- When Wi-Fi Scheduler is enabled, the schedule is shown graphically on the following pages:

  Settings > Radio > Scheduler

  Settings > VAP Security > Scheduler

  Settings > Wi-Fi Scheduler profile

- Radio and VAP schedulers run independently of each other and the configuration priority is in the following order:

  Radio Scheduler > VAP Scheduler > manual configuration.

  For example, if a VAP is enabled for a specific time period, and the Radio with that VAP is disabled for that same time period, then the VAP will be disabled.

Configuring a Wi-Fi Scheduler Profile

To configure a Wi-Fi Scheduler profile, perform the following procedure:

1. Select **Settings** > **Wi-Fi Scheduler profile** from the main menu. See Figure 68.

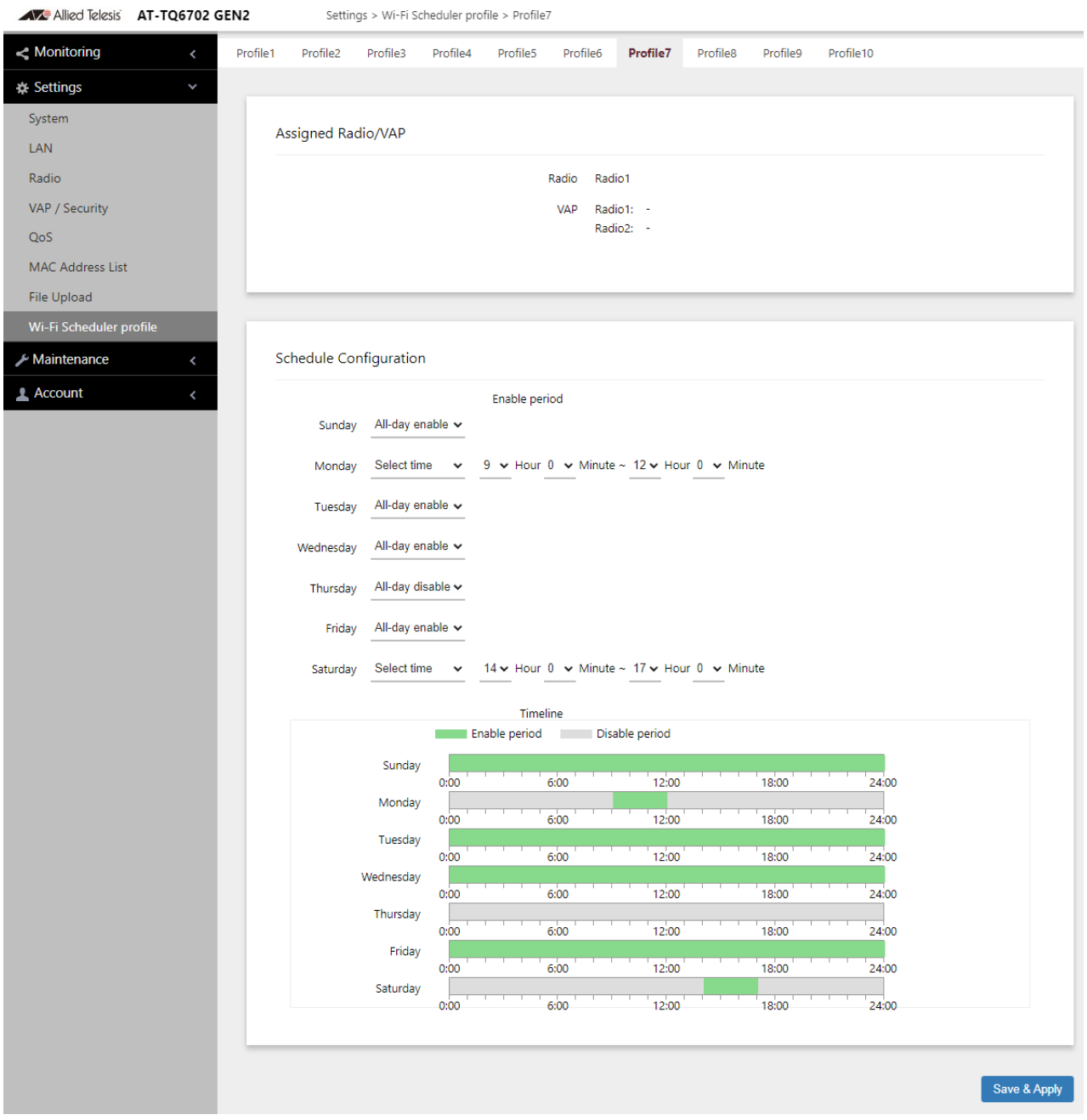

Figure 68. Wi-Fi Scheduler profile settings

2. Select a **Profile** (from 1 to 10).
3. Configure the parameters by referring to Table 44.

Table 44. Wi-Fi Scheduler profile settings

Field	Description
Assigned Radio/VAP	Lists all the Radios/VAPs assigned to this profile.
Schedule Configuration	For each day, the following can be selected: All-day enable: Wi-Fi is enabled for that 24 hour period. All-day disable: Wi-Fi is disabled for that 24 hour period. Select time: Manually set the time when the Radio/ VAP will be enabled.
Timeline	Graphical display of the timeline.

4. Click the **Save & Apply** button to save and update the configuration.

Chapter 11
Maintenance

This chapter has the following procedures:

Downloading the Configuration of the Access Point to Your Computer

This procedure explains how to download the configuration of the access point as a file to your computer. You might perform this procedure to maintain a history of the configurations of the unit so that you can easily restore a configuration, if needed. This procedure is also useful if there are several access points that are to have the same or nearly the same settings. You can configure one unit and then transfer its configuration to the other units. Please review the following information before performing this procedure:

- You cannot edit a configuration file with a text editor.
- This procedure does not interrupt the operations of the access point.

To download the configuration of the access point as a file to your workstation, perform the following procedure:

1. Select **Maintenance** > **Configuration** from the main menu. Refer to Figure 69.

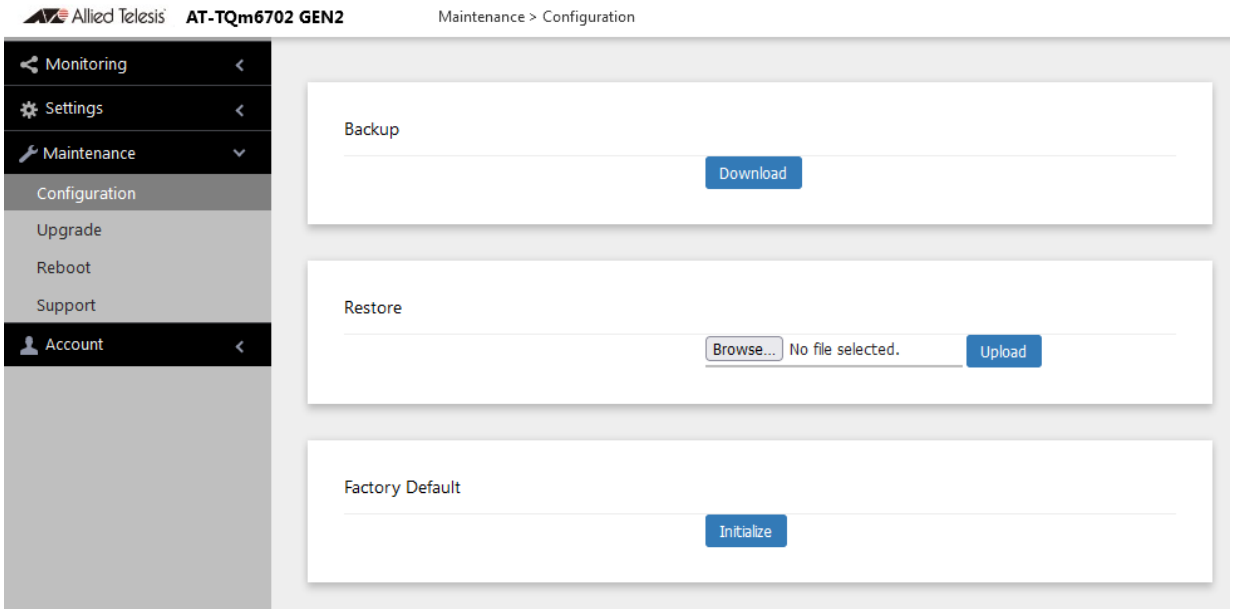

Figure 69. Configuration Window

2. Click the **Download** button in the Backup section of the window.

   Your web browser prompts you to save a config.txt file.

3. Save the file on your system.

   You can change the filename The filename suffix must be “txt”.

Restoring a Configuration to the Access Point

This procedure explains how to restore a configuration to the access point. You might perform this procedure to restore a previous configuration to the device, to configure a replacement unit, or to configure multiple access points with the same configuration. Here are the guidelines:

- ❒ You can only restore configuration files that are created with “Downloading the Configuration of the Access Point to Your Computer” on page 204.
- ❒ A configuration file must have the “txt” suffix.
- ❒ You can restore a configuration file to multiple access points to give them the same configuration. However, if a configuration file has a static IP address, you should change the IP address of a device immediately after you restore a configuration to prevent an IP address conflict from occurring among the devices.
- ❒ You cannot edit a configuration file with a text editor.

Note
The access point resets when you restore a configuration. It does not forward network traffic for one minute while it initializes its management software.

This procedure assumes that the configuration file is stored on your management workstation or a network server.

To restore a configuration to the access point, perform the following procedure:

1. Select **Maintenance** > **Configuration** from the main menu. Refer to Figure 69 on page 204.
2. Click the **Browse** button in the Restore section of the window and select the configuration file to restore to the access point from your management workstation or network server.
3. Click the **Open** button.
4. Click the **Upload** button.
5. Wait one minute for the access point to upload the file and reboot.
6. To resume managing the unit, establish a new management session.

Restoring the Default Settings to the Access Point

This procedure explains how to restore the default settings on the access point. Review the following information before performing the procedure:

- The manager name and password are reset to “manager” and “friend”, respectively.
- If the access point currently has a static IP address, the address is deleted and the DHCP client is activated. If the device does not receive a response from a DHCP server on the LAN port, it uses the default IP address 192.168.1.230.

Note
The default setting for the radios is off. Consequently, the access point stops forwarding network traffic when returned to its default settings.

To activate the default settings on the access point, perform the following procedure:

1. Select **Maintenance** > **Configuration** from the main menu. Refer to Figure 69 on page 204.
2. Click the **Initialize** button in the Factory Default section of the window.
3. At the confirmation prompt, click **OK** to restore the default settings or Cancel to cancel the procedure.
4. After clicking OK, wait one minute for the device to reset, and afterwards establish a new management session. For instructions, refer to “Starting the First Management Session” on page 18.

Uploading New Management Software to the Access Point

Allied Telesis might release new versions of the management software on the company's web site for customers who want to upgrade the firmware on their access points.

This procedure explains how to upload new firmware to the access point. Please review the following information before performing the procedure:

- The procedure assumes you have already obtained the new image file from the Allied Telesis web site and stored it on your computer or network server.
- The configuration settings of the access point are retained when a new firmware image is uploaded to the device.
- The access point does not compare the version numbers of the new and current firmware when it uploads the management software. You should compare the numbers yourself to avoid uploading an older version of the firmware to the access point.
- The upgrade process takes about 10 minutes.

Caution
Do not power off the device during the firmware upgrade. **E129**

Caution
The device does not forward network traffic while it uploads the management software and writes it to the flash memory. **E130**

To upload a new version of the management software to the access point, perform the following procedure:

1. Select **Maintenance** > **Upgrade** from the main menu. Refer to Figure 70 on page 208.

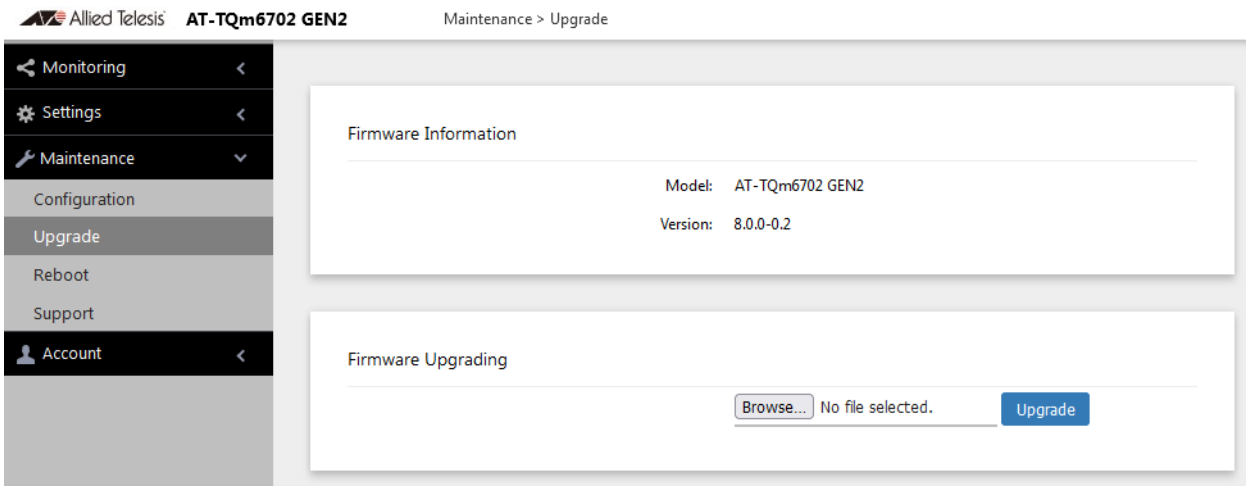

Figure 70. Upgrade Window

The version number of the current firmware is displayed in the Firmware Information section of the window.

2. Click the **Browse** button next to the New Firmware Image field and locate the new image file on your computer or network server.
3. Click the **Upgrade** button.

   The access point displays a confirmation prompt.
4. Click the **Proceed** button to start the upgrade procedure or **Cancel** to cancel the procedure.
5. Wait ten minutes for the access point to upload the firmware, write it into its flash memory, and reboot.

   Note
   Do not close the web browser window or change to a different window until the entire procedure is finished. Interrupting the transfer may corrupt the file on the access point.

6. To continue managing the device, start a new management session.

Rebooting the Access Point

This section explains how to reboot the access point. You might reboot the device if it is experiencing a problem.

Caution
The device does not forward network traffic while it reboots. Some network traffic may be lost. **E113**

To reboot the access point, perform the following procedure:

1. Select **Maintenance** > **Reboot** from the main menu. Refer to Figure 71.

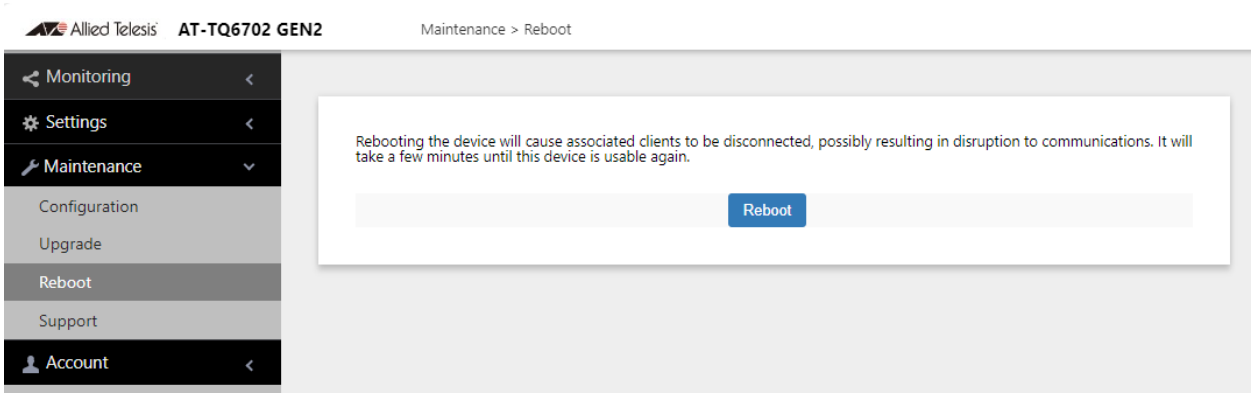

Figure 71. Reboot Window

2. Click the **Reboot** button.

   The access point displays a confirmation prompt.

3. Click **OK**.

   Your current management session is interrupted.

4. To resume managing the unit, wait one minute for it to complete initializing its management software and then start a new management session.

Collecting Technical Support Information to a File

If you contact Allied Telesis for technical assistance with the access point, you may be instructed to send Allied Telesis technical support information. Technical support information helps Allied Telesis technicians troubleshoot problems with the device.

> **Note**
> You should only perform this procedure when instructed to do so by an Allied Telesis technician.

To collect technical support information to a file and send it to Allied Telesis, perform the following procedure:

1. Select **Maintenance** > **Support** from the main menu. Refer to Figure 72.

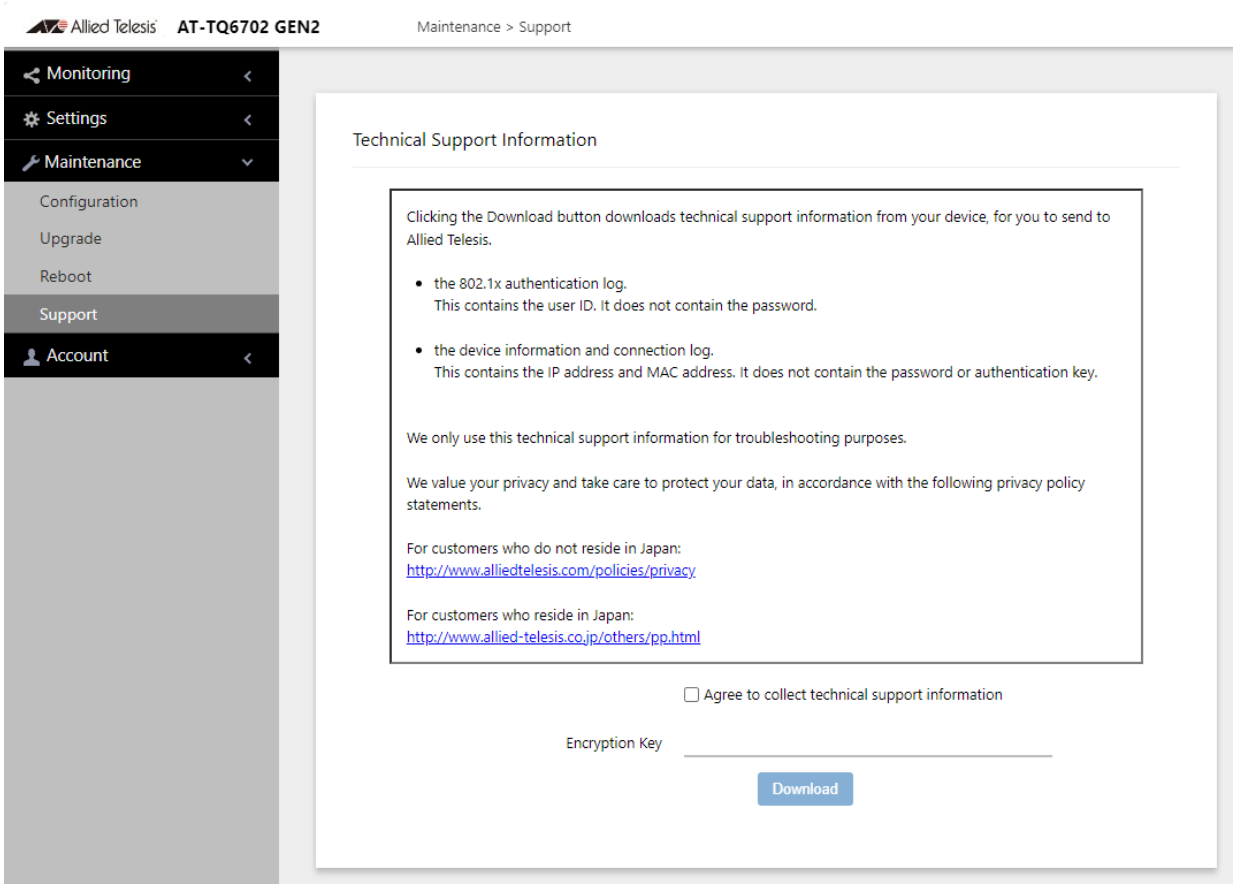

Figure 72. Support Window

2. Read the appropriate privacy policy statement by clicking on its link.

3. After reading the privacy policy statement, click the check box for **Agree to collect technical support information** to permission to collect the technical support information.

4. If you want to send the file encrypted, enter an encryption key in the Encryption Key field. This step is optional. Here are the guidelines:

   - The key can be up to 32 alphanumeric characters.
   - It is case sensitive.
   - Spaces are not allowed.
   - Be sure to send the key to the technicians at Allied Telesis.
   - The factory default is blank. The file is sent in clear text if you do not enter a key.

5. Click the **Download** button.

   Your web browser prompts you to save a zip file.

6. Save the zip file on your system.

7. Send the zip file to your Allied Telesis contact.

Chapter 12

Account Menu

This chapter contains the following procedures:

Changing the Manager's Login Name and Password

This procedure explains how to change the login name and password of the manager account on the access point. The default values are "manager" and "friend", respectively. The access point has only one manager account.

Changing the name and password does not affect your current management session.

Note
Allied Telesis strongly recommends changing the factory default password during the first management session to protect the device from unauthorized access.

To change the login name and password of the manager account, perform the following procedure:

1. Select **Account** > **User** from the main menu, Refer to Figure 73.

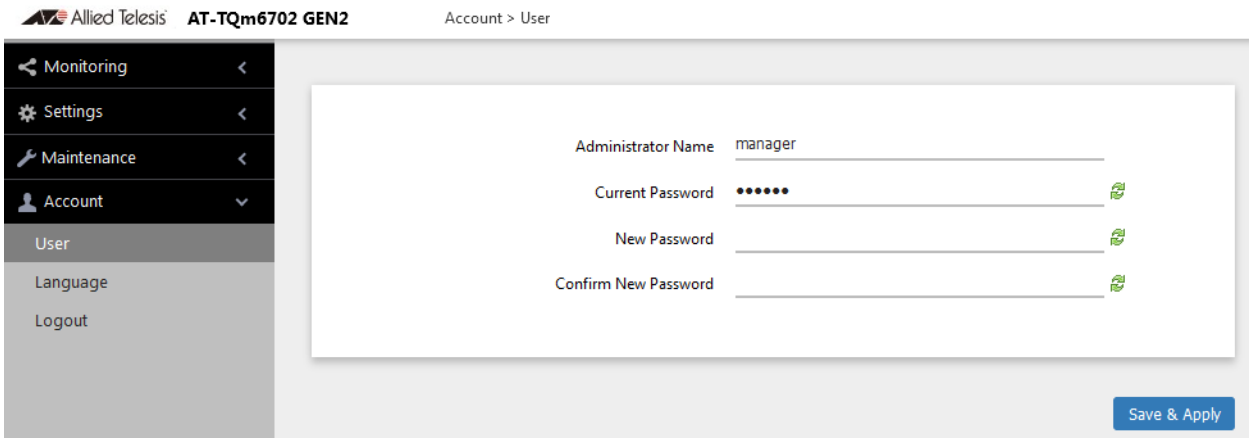

Figure 73. User Window

2. To change the manager name, select the **Administrator Name** field and enter a new name. Here are the guidelines:
   - The name can be up to 12 alphanumeric characters.
   - The first character must be a letter. It cannot be a number or special character.
   - The name is case-sensitive.
   - The default name: manager

3. To change the password, select the **Current Password** field and enter the account's current password.

   - ❒ The default password: friend

   To display the password as alphanumeric characters or asterisks, click the green, double arrow symbol.

4. Select the **New Password** field and enter a new password. The new password. Here are the guidelines:

   - ❒ The password can be up to 32 alphanumeric characters.
   - ❒ It can not contain spaces or any of these special characters: “, $, :, <, >, ’, &, *.
   - ❒ It is case-sensitive.

5. Select the **Confirm New Password** field and enter the new password again.

6. Click the **Save & Apply** button to save and update the configuration. You must use the new manager name and password in all future management sessions.

Setting the Language of the Web Browser Interface

The access point can display the web browser interface in either English or Japanese. The default is English. To set the language, perform the following procedure:

1. Select **Account** > **Language** from the main menu. Refer to Figure 74.

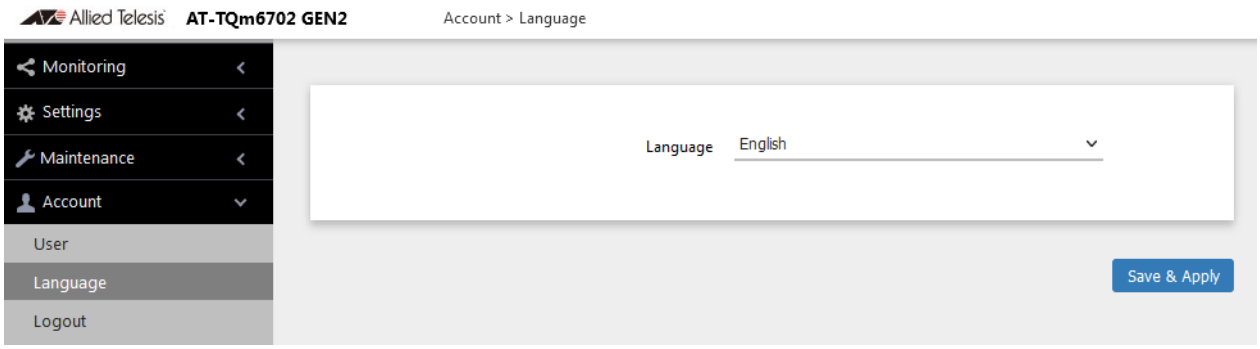

Figure 74. Language Window

2. From the **Language** pull-down menu, select one of the following:
   - ❒ English
   - ❒ Japanese
3. Click the **Save & Apply** button to save and update the configuration. The management interface changes to the designated language.