TQ7403

Hybrid Wi-Fi 6E (IEEE802.11ax) Wireless Access Point

Management Software User Guide

613-003266 Rev.E

Contents

List of Figures

List of Tables

Preface

This guide contains instructions on how to manage the TQ7403 Wireless Access Point with your web browser and the product's web browser management interface. The 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 Allied Telesis technical support, visit **www.alliedtelesis.com/support**.

Chapter 1

Getting Started

Here are the sections in this chapter:

Hardware Features

The components on the TQ7403 access point are illustrated in Figure 1.

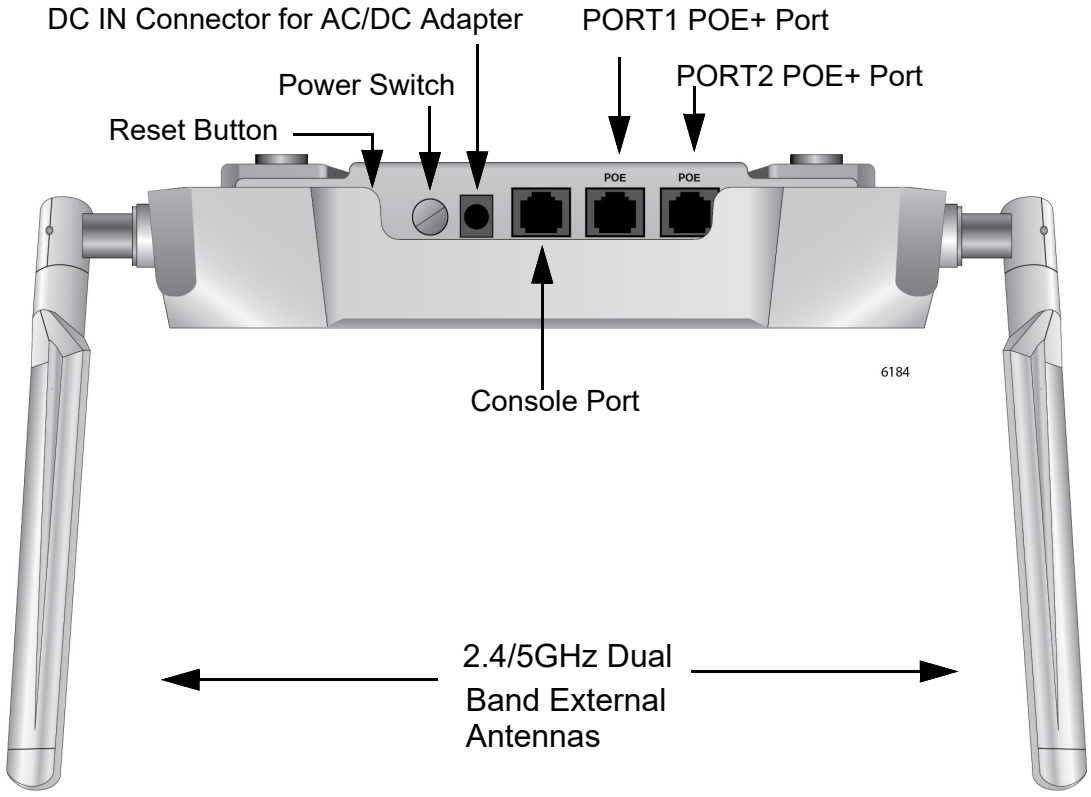

Figure 1. Components on the Back of the Access Point

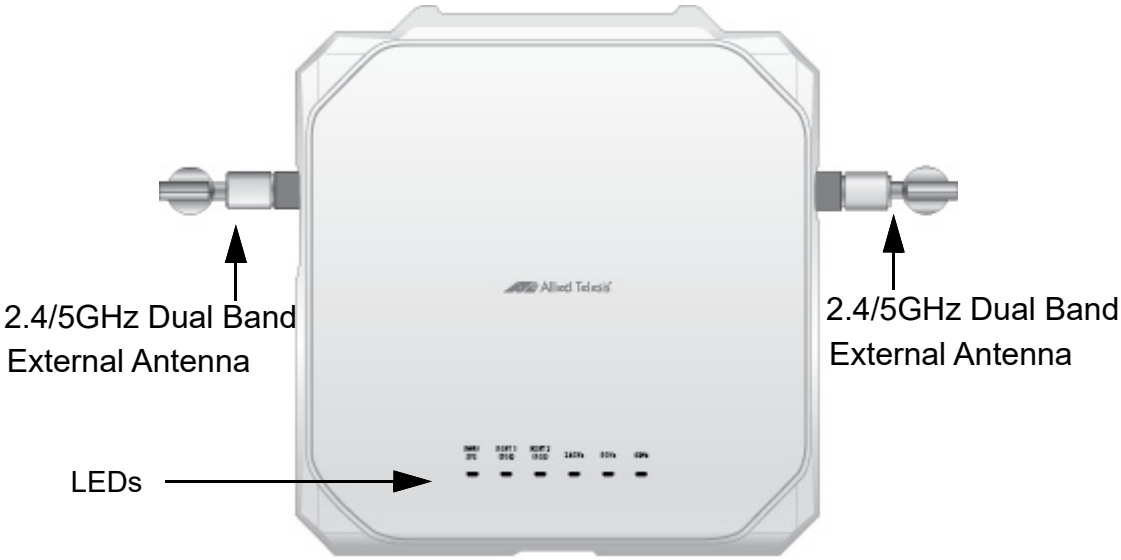

Figure 2. LEDs on the Top of the Access Point

The hardware components are listed in Table 1.

Table 1. Hardware Components on the TQ7403 Access Point

Component	Description
Two Embedded Antennas	Embedded 2.4G Bluetooth® Low Energy/ 6G dual band antennas
Two 2.4G/5GHz Antenna Connectors	N-type female connectors for the 2.4G/5GHz dual-band antennas **Note** The access point comes with two 2.4GHz/5GHz dual band external antennas.
PORT1 and PORT2 (PoE+ LAN Ports)	PORT1 and PORT2 are standard 100M/1000M/2.5G Ethernet ports. They are used to connect the access point to your local area network and to provide power to the device from a PoE+ source device.
Console Port	The serial port is for RS-232 communication.
DC IN Connector for AC/DC Adapter	Connects an AC/DC adapter to supply DC power to the access point.
Power Switch	Turns On or OFF the access point when power is supplied to the access point only from the AC adapter, not from PORT1 or PORT2 PoE+ port.
Reset Button	The reset button returns the access point to its default settings.
LEDs	The access point has the following LEDs: ❒ PORT1 and PORT2- Display status information about the Ethernet LAN ports. ❒ 2.5G, 5G, and 6G - Display status information about the radios. ❒ PWR/SYS - Displays status information about the system and PoE+.

Note
For a complete list of hardware and software features, see the product's data sheet and the TQ7403 Access Point Installation Guide at **www.alliedtelesis.com/support**.

Management Tools

You can manage the access point with the following management tools.

Web Browsers

The wireless access point comes with a graphical web browser interface that you can access with a web browser on your management workstation. You can manage one unit at a time with the interface. It supports both non-secure HTTP (by default) and secure HTTPS management sessions. The product has been tested with the following web browsers:

- Google Chrome™
- Microsoft Edge™

Vista Manager

You can also manage this product with these Vista Manager products and the Autonomous Wave Controller (AWC) plug-in:

- Vista Manager EX (version 3.12.0 or later)
  The access point firmware must be version 10.0.4-0.1 or later.
- Vista Manager Network Appliance
- Vista Manager mini

AWC simplifies managing multiple devices because it allows you to create groups of devices 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 the AWC plug-in. The features require the web browser interface:

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

SNMPv1, SNMPv2c, and SNMPv3

You can also 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 50. You cannot change the parameter settings on the access point with SNMP.

Starting the First Management Session

This section contains the procedures for starting the first management session with the access point.

After you install and power on the access point, it queries the subnet on Port1 for a DHCP server. If a DHCP server responds to its query, the unit uses the IP address assigned by the server. If the access point does not receive a response from a DHCP server, it uses its default IP address.

Note
The default IP address of the access point is **192.168.1.230**.

Here are the procedures:

- ❒ "With a DHCP Server" next
- ❒ "With the Default IP Address" on page 18

With a DHCP Server

This section contains the procedure for starting the first management session with the access point on a network that has a DHCP server. To start the management session, perform the following procedure:

1. Enter the MAC address of the access point in your DHCP server so that the server assigns an IP address to the access point when you power it on.
2. Connect PORT1 on the access point to a port on a PoE source device.

   Use a Standard TIA/EIA 568-compliant Category 5, 100 ohm, 4-pair unshielded cable that complies with IEEE 802.3ab 1000Base-T specifications. Category 5e is recommended. See the *TQ7403 Access Point Installation Guide* for instructions.
3. Wait several minutes for the access point to initialize its management software and obtain an IPv4 address from the DHCP server on your network.
4. Open a web browser on your management workstation.
5. Enter the access point's assigned IP address from the DHCP server in the URL field of your web browser and press Return.

   Your web browser displays the login window from the access point. See Figure 3 on page 18.

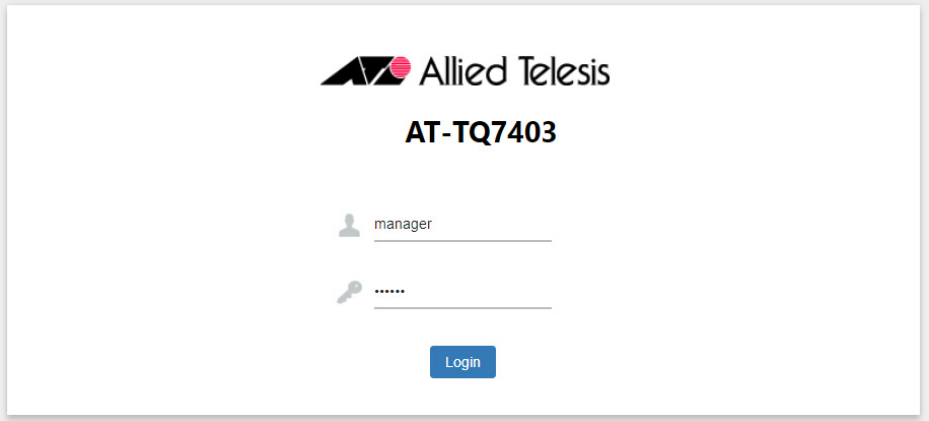

Figure 3. Log On Window

6. Enter the username and password.
   - ❒ Username: manager
   - ❒ Password: friend

   Note
   The user name and password are case-sensitive.

7. Click the **Login** button.

   The first window you see is the **System** tab in the **Monitoring** > **Status** window. See Figure 9 on page 27.

With the Default IP Address

If your network does not have a DHCP server, you can use its default IP address 192.168.1.230 to start the first management session. To start the management session, perform the following procedure:

1. Change the IP address of your workstation to 192.168.1.*n*/24 (255.255.0.0), where *n* is any number from 1 to 254, but not 230.
2. Connect PORT1 on the access point to a port on a PoE source device.

   Use a Standard TIA/EIA 568-compliant Category 5, 100 ohm, 4-pair unshielded cable, complying with IEEE 802.3ab 1000Base-T specifications. Category 5e is recommended.
3. Wait several minutes for the access point to start its management software.
4. Connect the Ethernet port on your workstation to an Ethernet port on the same switch to which the access point is connected.

If your network is divided into virtual LANs (VLANs), you must connect the access point and your computer to ports that are members of the same VLAN on the Ethernet switch. 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, you can connect the access point and your computer to any ports on the Ethernet switch.

5. Open your web browser on your management workstation.

6. Enter the access point's default IP address **192.168.1.230** in the URL field of your web browser and press Return.

   Your web browser displays the login window from the access point. Refer to Figure 3 on page 18.

7. Enter the username and password.

   - ❒ Username: manager
   - ❒ Password: friend

   Note
   The user name and password are case-sensitive.

8. Click the **Login** button.

   The first window you see is the **System** tab in the **Monitoring** > **Status** window. See Figure 9 on page 27.

Starting a Management Session

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

Note
If you have not assigned the access point an IP address, go to “Starting the First Management Session” on page 17 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.

   Your web browser displays the login window as shown in Figure 3 on page 18.

   Note
   If you are using 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 username and password.
   - ❒ Username: manager
   - ❒ Password: friend

   Note
   The user name and password are case-sensitive.

4. Click the **Login** button.

Management Windows

This section reviews the management windows and menus. The main parts of the management windows are identified in Figure 4.

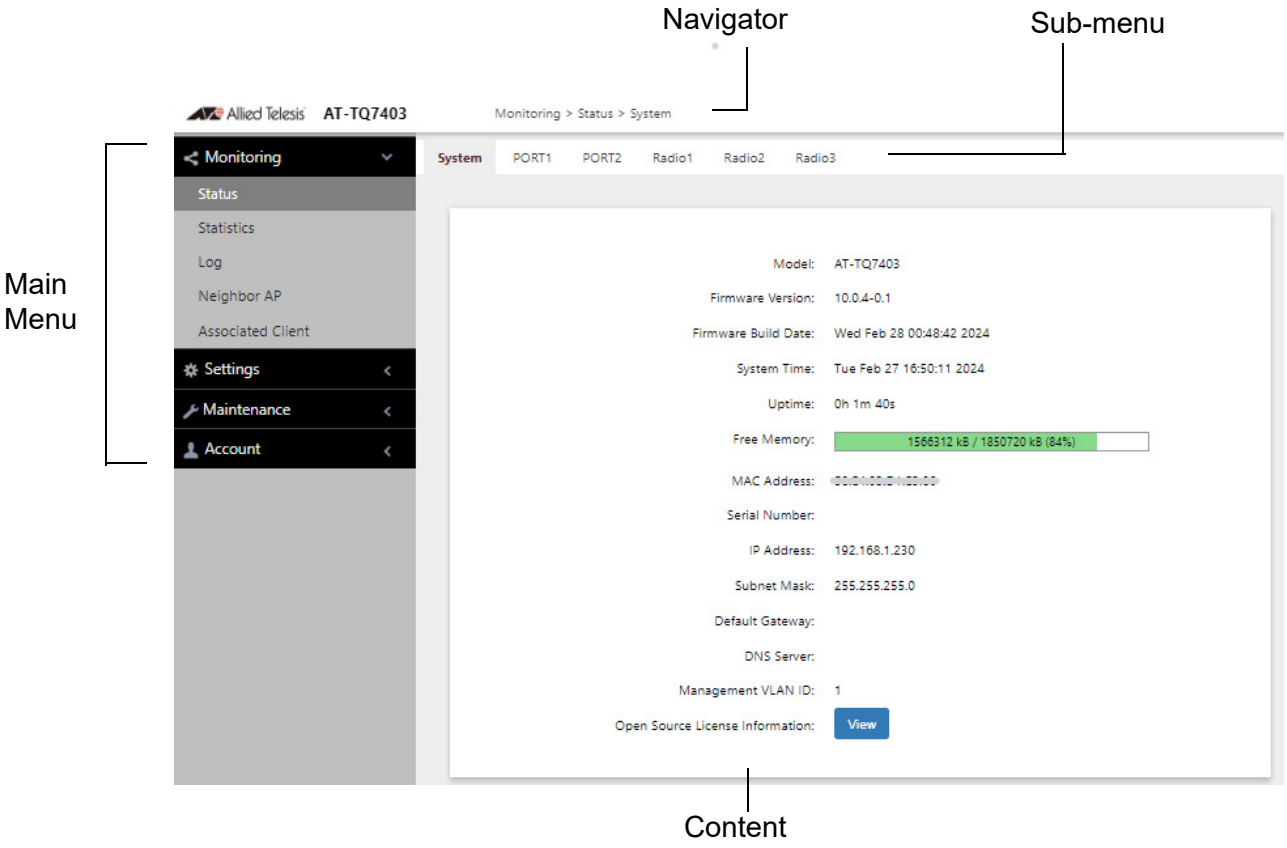

Figure 4. Sample Management Window

Main Menu

The main menu is displayed on the left side of the window, with the following selections:

- Monitoring
- Settings
- Maintenance
- Account

Clicking a main menu option displays its 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 5 on page 22.

Figure 5. Main Menu Button

Clicking the main menu button displays the menu over the content window. The menu is hidden again after you make a menu selection.

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.

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 an 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 6.

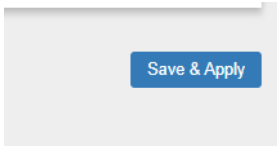

Figure 6. Save & Apply Button

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 making changes on a 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 made on the VAP/Security pages and activates the changes. See Figure 7.

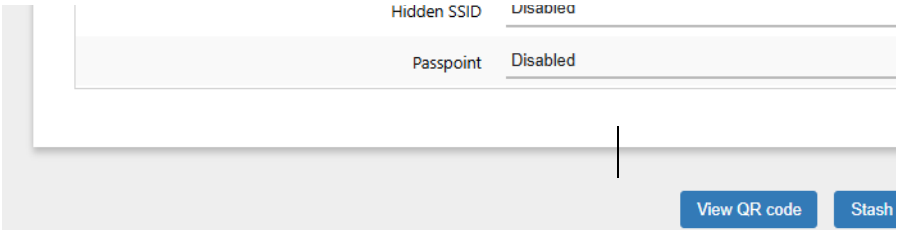

Figure 7. Stash Button

Ending Management Sessions

To log off, perform the following procedure:

1. Select **Account** > **Logout** from the main menu. See Figure 8.

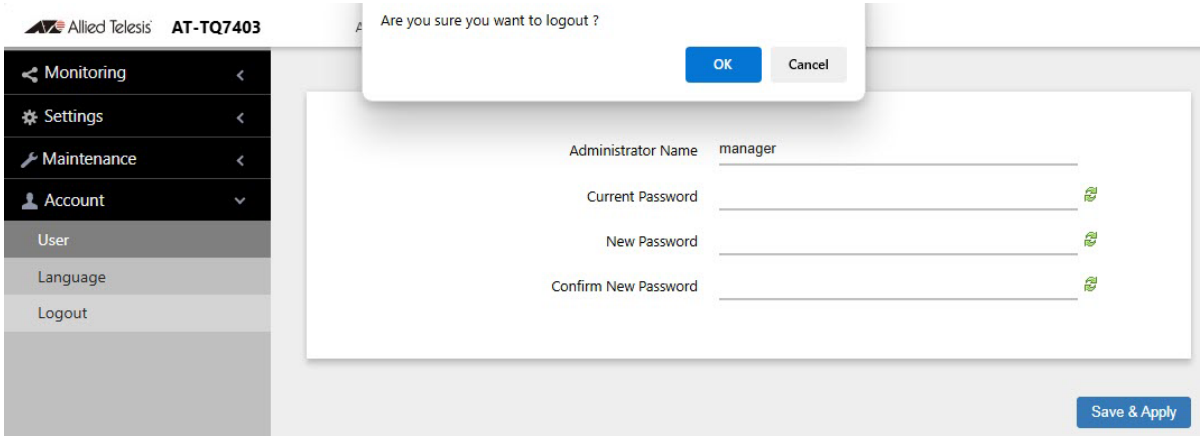

Figure 8. Logout Menu under Account

2. Click **OK** at the confirmation prompt.

   Your management session ended and the web browser shows the login window as shown in Figure 3 on page 18.

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. Set the language of the management interface. The options are English and Japanese. The default is English. See “Setting the Language of the Web Browser Interface” on page 232.

3. Change the manager’s login name and password. See “Changing the Manager’s Login Name and Password” on page 230.

4. If you prefer to use HTTPS management sessions, perform “Starting a Management Session” on page 20.

5. Configure and enable the radios. See “Configuring Basic Radio Settings” on page 71.

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 9.

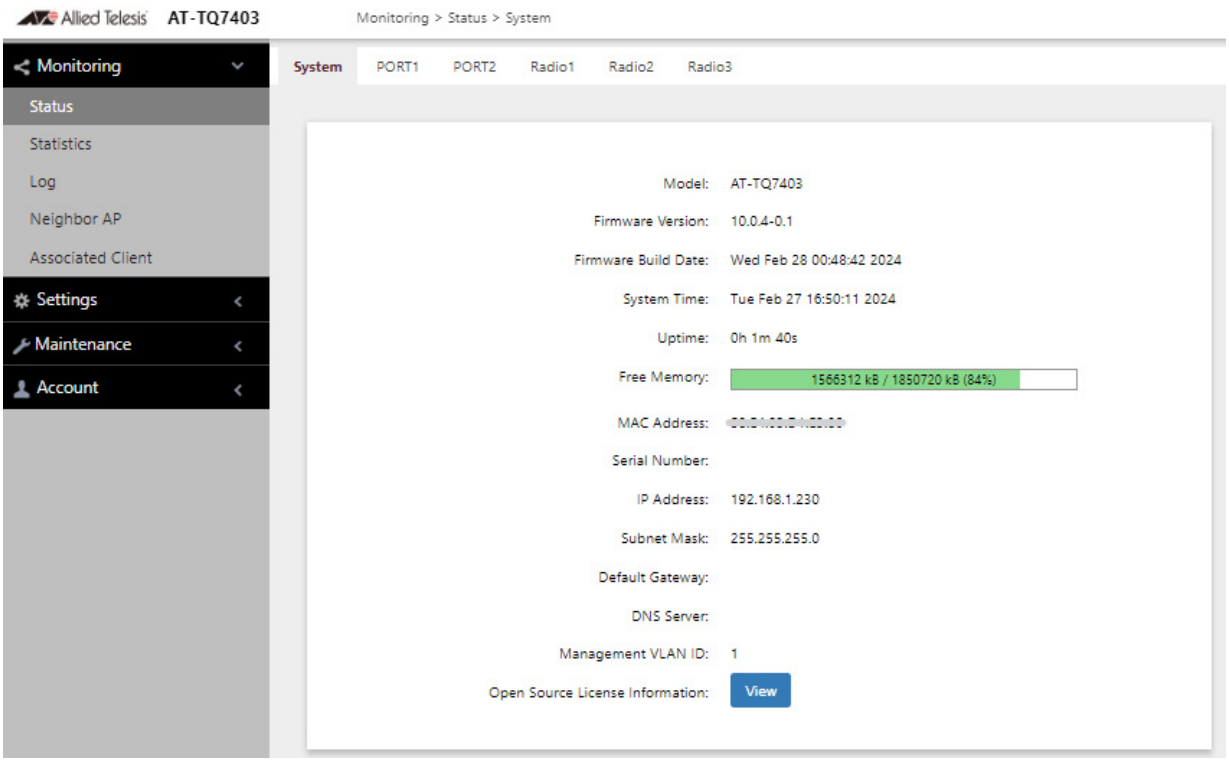

Figure 9. System Window

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.
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 46 or “Setting the Date and Time with the Network Time Protocol (NTP)” on page 43.
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 amount of unused memory, in KB. - The second value is the total amount of used and unused memory, in KB. - The third number in parentheses is the percentage of unused memory.
MAC Address	Displays the MAC address of the access point and Radio1. Radio2 and Radio3 have a different MAC address. The Radios must be enabled to display their MAC addresses. To view the MAC address of Radio2 or Radio3, select **Monitoring** > **Status** > **Radio2** or **Radio3**. You cannot change the MAC addresses.
Serial Number	Displays the serial number assigned to the access point.
IP Address	Displays the IP address of the access point. The wireless access point uses its IP address for management functions, such as management sessions, downloading new firmware versions.To set this value, refer to “Assigning a Dynamic IPv4 Address from a DHCP Server” on page 38 or “Assigning a Static IPv4 Address to the Access Point” on page 41.
Subnet Mask	Displays the subnet mask. To set this value, refer to “Assigning a Dynamic IPv4 Address from a DHCP Server” on page 38 or “Assigning a Static IPv4 Address to the Access Point” on page 41.

Table 2. System Window (Continued)

Item Name	Description
Default Gateway	Displays the default gateway address, used for management functions. 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 IPv4 Address from a DHCP Server” on page 38 or “Assigning a Static IPv4 Address to the Access Point” on page 41.
DNS Server	Displays the current DNS server address. The DNS server address has to be provided by a DHCP server, along with the access point’s IP address. Refer to “Assigning a Dynamic IPv4 Address from a DHCP Server” on page 38 or “Assigning a Static IPv4 Address to the Access Point” on page 41.
Management VLAN ID	Displays the management VLAN ID. By default, the VLAN ID is set to 1.
Open Source License Information	Clicking the **View** button displays open source license information.

Displaying VAP and LAN Port Statistics

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. To configure VAPs, refer to Chapter 6, “Virtual Access Points” on page 92.

To view VAP and LAN port status and statistics, select **Monitoring** > **Statistics** window. See Figure 10.

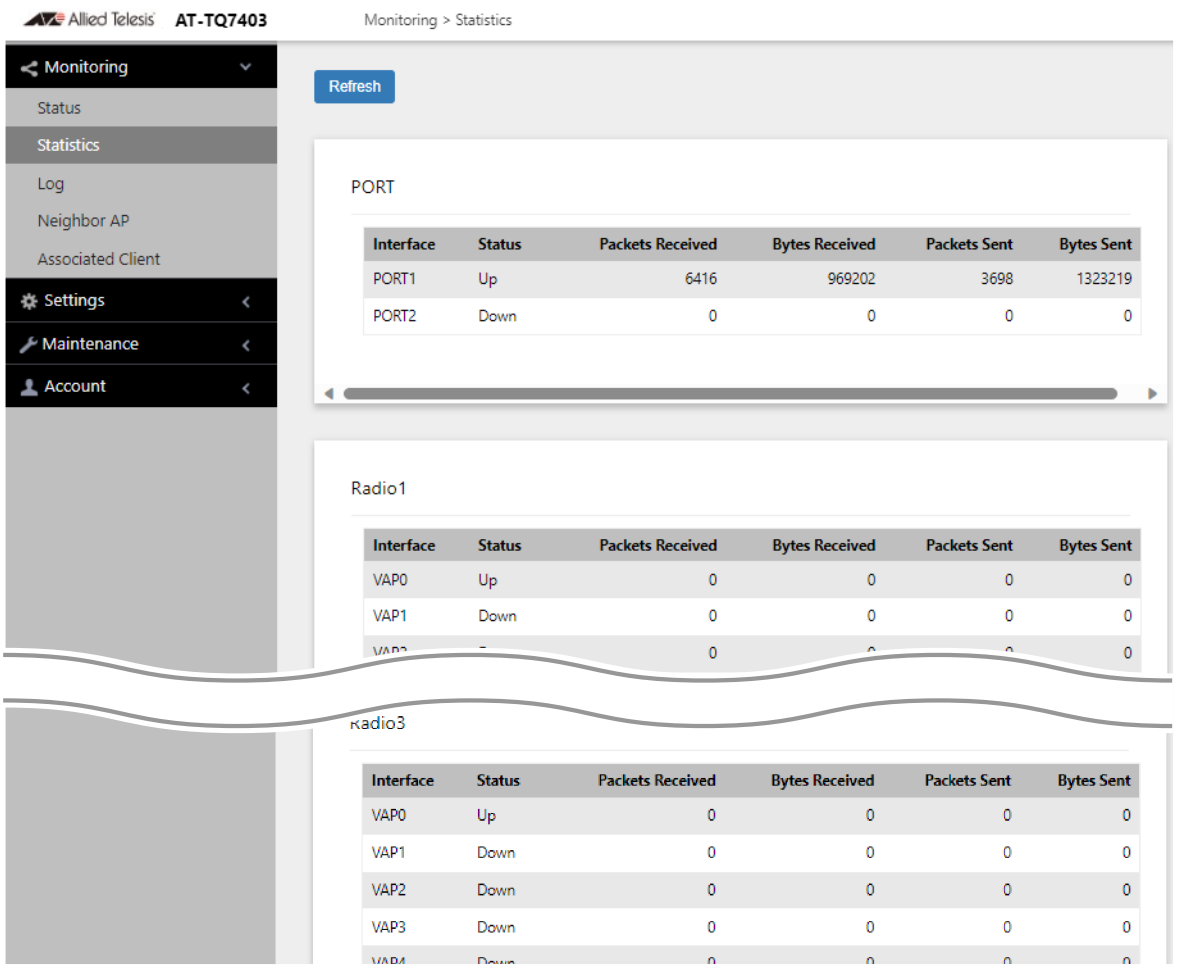

Figure 10. Statistics Window

The columns are defined in Table 3 on page 31.

Table 3. Statistics Window

Column	Description
Interface	Displays the LAN port and VAPs 0 to 15 on Radio1, Radio2, and Radio3.
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 have 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 configure 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 56.

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 56.

To view the system log, select **Monitoring** > **Log**, Figure 11 on page 33 is an example.

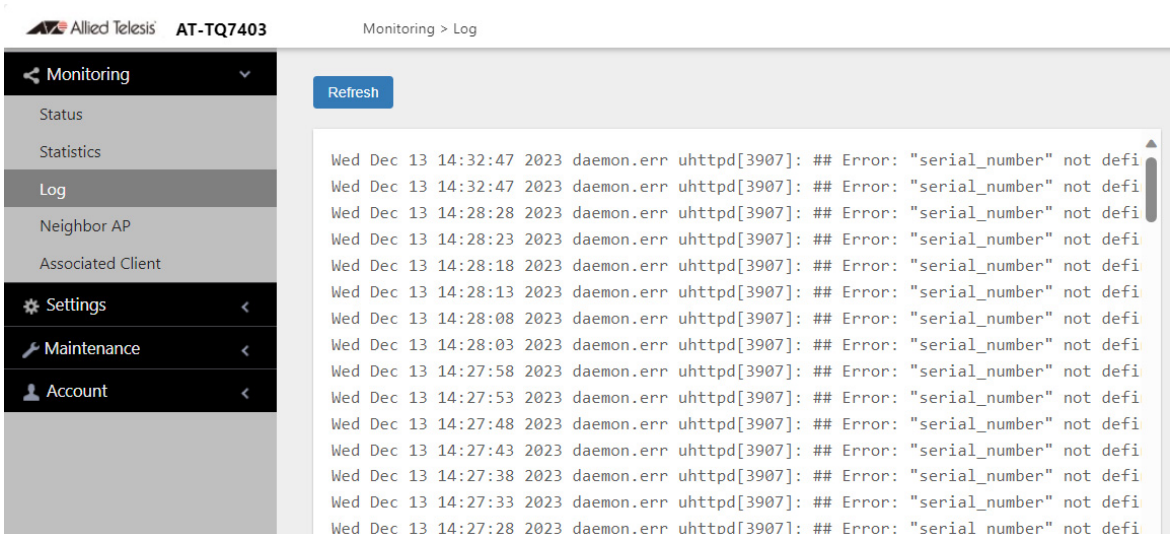

Figure 11. Log Window with Event Messages

Displaying Neighbor Access Points

To view information about the neighboring access points that this access point detects on its channels, select **Monitoring** > **Neighbor AP** from the main menu. Refer to Figure 12.

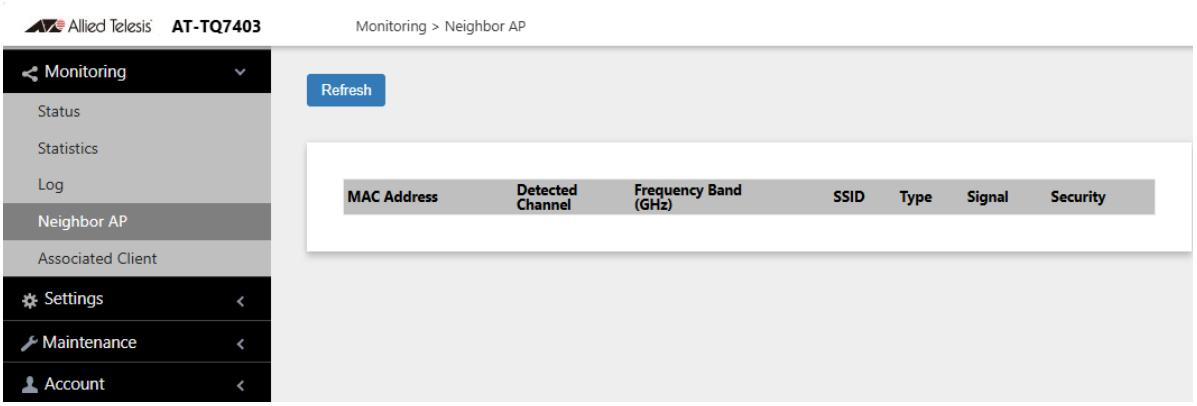

Figure 12. Neighbor AP Window

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 on which it detected the neighboring access point.
Frequency Band (GHz)	Displays the frequency band the detected access point is operating within.
SSID	Displays the network name (SSID) of the neighboring access point.
Type	Displays the mode of the neighboring access point: AP or Adhoc. An adhoc network refers to two or more devices that are communicating directly with each other without any intermediary devices, such as access points.
Signal	Displays the intensity of the received signal in a four-level bar graph icon. Pointing to the icon displays the dB (dBm) strength of the signal.
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 13.

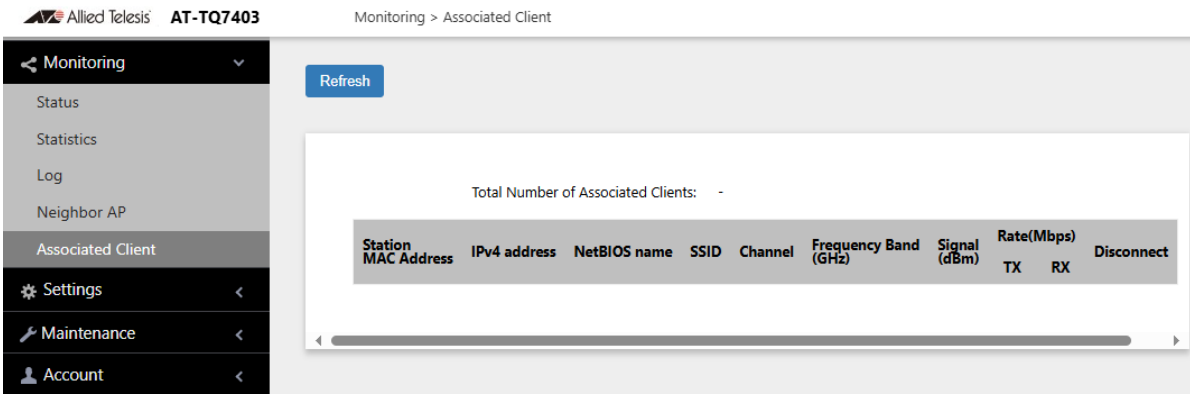

Figure 13. Associated Client Window

The columns are defined in Table 6.

Table 6. Associated Client Window

Column	Description
Station MAC Address	Displays the MAC addresses of the associated clients.
IPv4 address	Displays the IPv4 addresses, if used, of the associated clients.
NetBIOS name	Displays the NetBIOS name of associated clients. It displays "n/a" when a NetBIOS name is being acquired or not received.
SSID	Displays the network name (SSIDs) to which the client is connected on the access point.
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 IPv4 Address from a DHCP Server

This section explains how to activate the DHCP client so that the access point receives its IPv4 address from a DHCP server on your wired network through its LAN port. The unit uses the address to communicate with management devices on your wired 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 if you prefer to manually assign an IPv4 address to the access point, refer to “Assigning a Static IPv4 Address to the Access Point” on page 41.

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 14 on page 39.

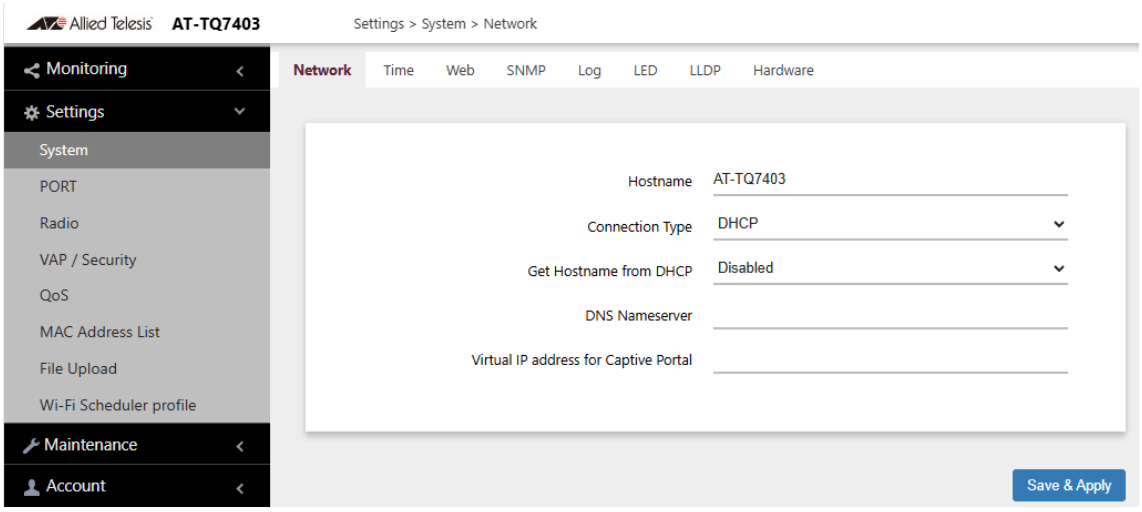

Figure 14. Network Window - DHCP

4. Configure the fields by referring to Table 7.

Table 7. Network Window - DHCP

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 AT-TQ7403. - If you want the DHCP server to supply the hostname, enable the Get Hostname from DHCP Server option in this window.
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 41.

Table 7. Network Window - DHCP (Continued)

Parameter	Description
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 IPv4 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 IPv4 address for use with Captive Portals. Wireless clients use this address instead of the device's actual IP address to connect to Captive Portals. This increases the security of your wireless network by hiding the IP address of the access point. The access point supports one virtual IPv4 address. For more information, refer to Chapter 8, "Captive Portals" on page 154. This field is optional. The default value is no address. **Note** This field is not supported with Wireless Distribution System (WDS) bridges.

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 a static IP address to the access point. The unit uses the address to communicate with management devices on your wired network through its LAN port, 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 wired network, refer to “Assigning a Dynamic IPv4 Address from a DHCP Server” on page 38.

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 15.

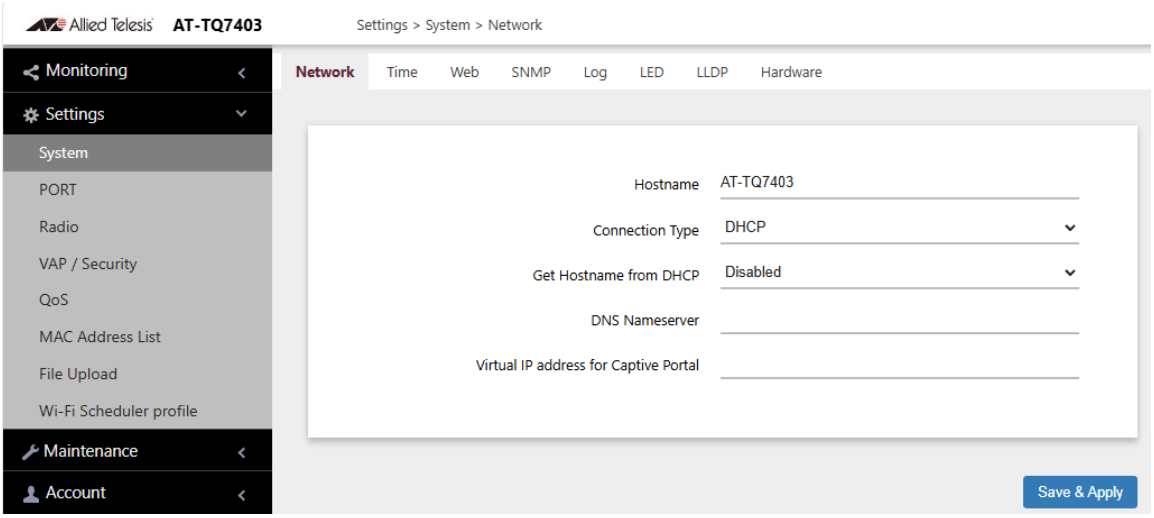

Figure 15. Network Window - Static IP Address

4. Refer to Table 8 to configure the window parameters.

Table 8. Network Window - Static IP Address

Item Name	Description
Hostname	Enter a static 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 AT-TQ7403.
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.
Virtual IP Address for Captive Portal	Assigns a virtual IPv4 address to the Captive Portals. Wireless clients used this address instead of the device's actual IP address to connect to captive portals. This increases the security of your wireless network by hiding the IP address of the access point. The access point supports one virtual IPv4 address. This field is optional. The default value is no address. For more information, refer to Chapter 8, "Captive Portals" on page 154.

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. See Figure 18 on page 46.
3. From the Set System Time pull-down menu, select **Using Network Time Protocol (NTP)**. The window is updated with new options. See Figure 16.

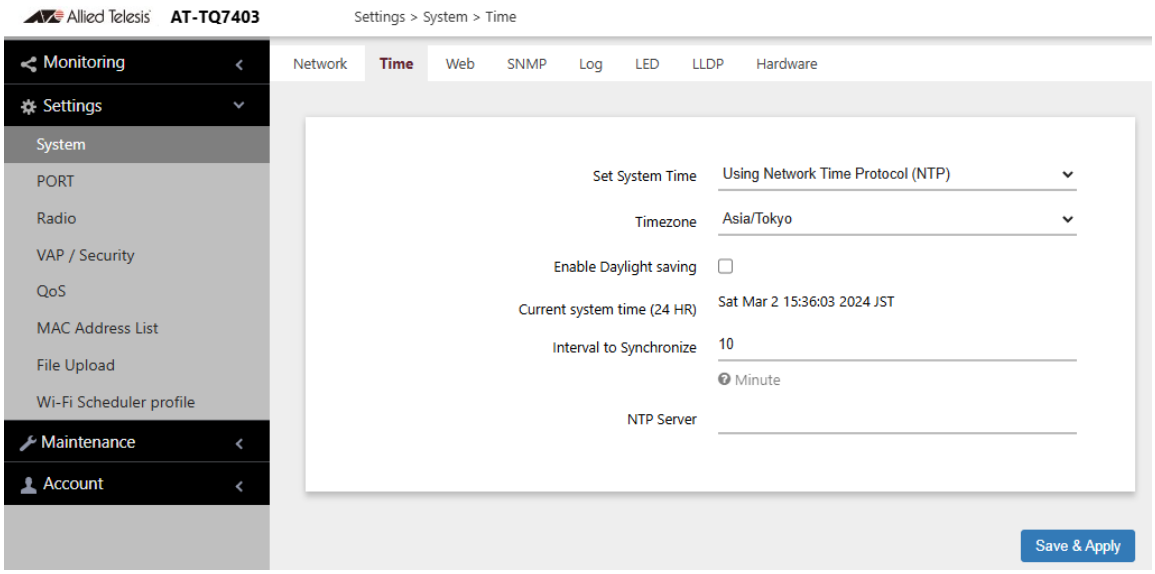

Figure 16. Time Window - NTP Option

4. Configure the fields by referring to Table 9.

Table 9. Time Window - NTP Option

Item Name	Description
Set System Time	Select **Using Network Time Protocol (NTP)** to synchronize the date and time of the product with an 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 17 on page 45. 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 17 contains the settings for Daylight Savings Time.

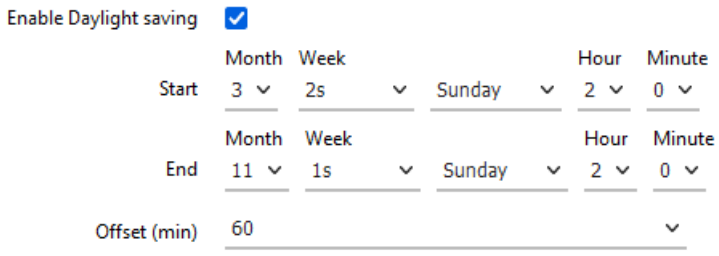

Figure 17. Daylight Savings Time Settings

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) whenever 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 43.

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 18.

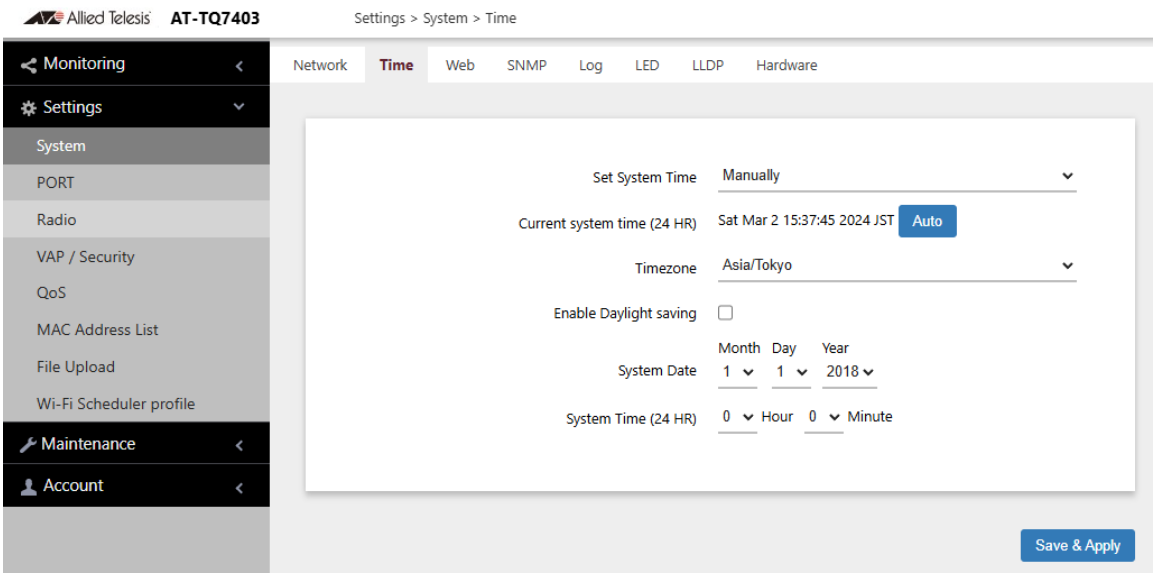

Figure 18. Time Window - Manually Option

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. Clicking the AUTO button sets 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 17 on page 45 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 19.

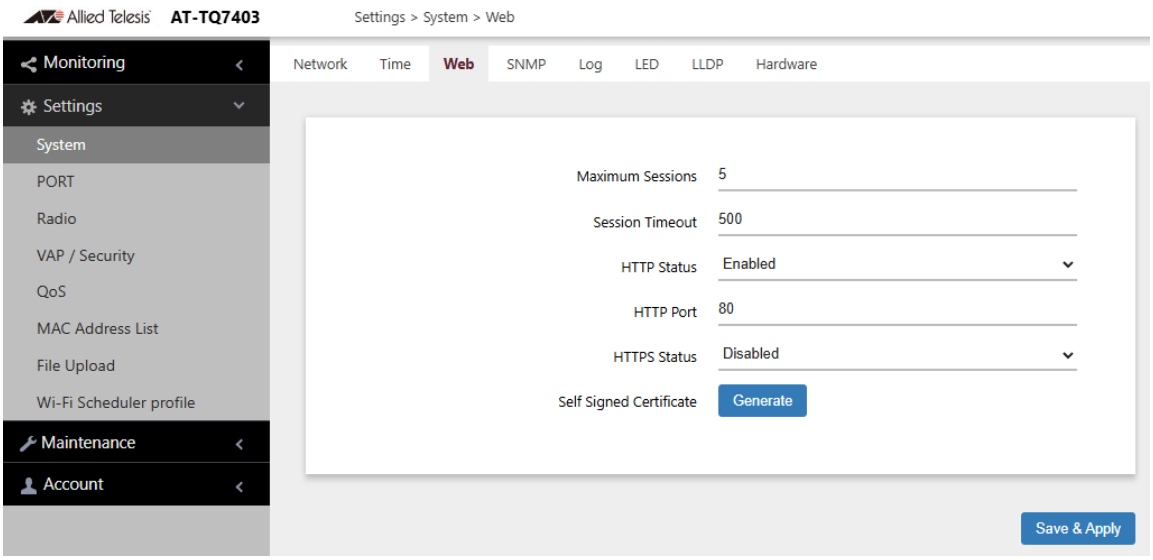

Figure 19. Web Window

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 configure the access point.
- The access point has one read-only community string.
- The unit must have an IPv4 address for SNMP management. For more information, see“Assigning a Dynamic IPv4 Address from a DHCP Server” on page 38 or “Assigning a Static IPv4 Address to the Access Point” on page 41.

To enable or disable SNMP, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **SNMP** from the sub-menu.
3. If SNMP is already enabled, select the **Agent Settings** tab. Refer to Figure 20.

Note
The Trap Settings tab is hidden when SNMP is disabled.

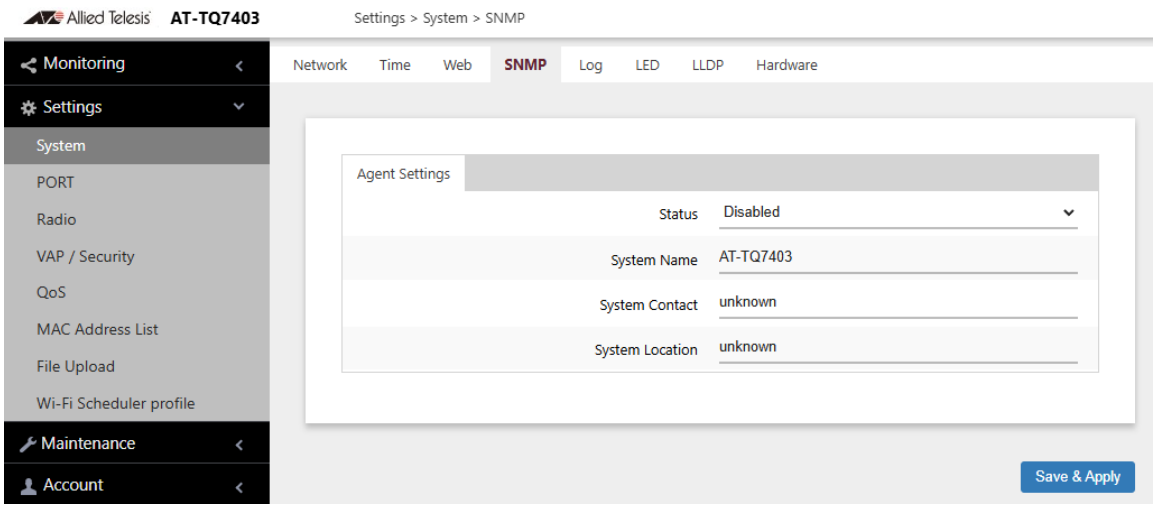

Figure 20. SNMP Window - SNMP Disabled

4. 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 21 on page 51.

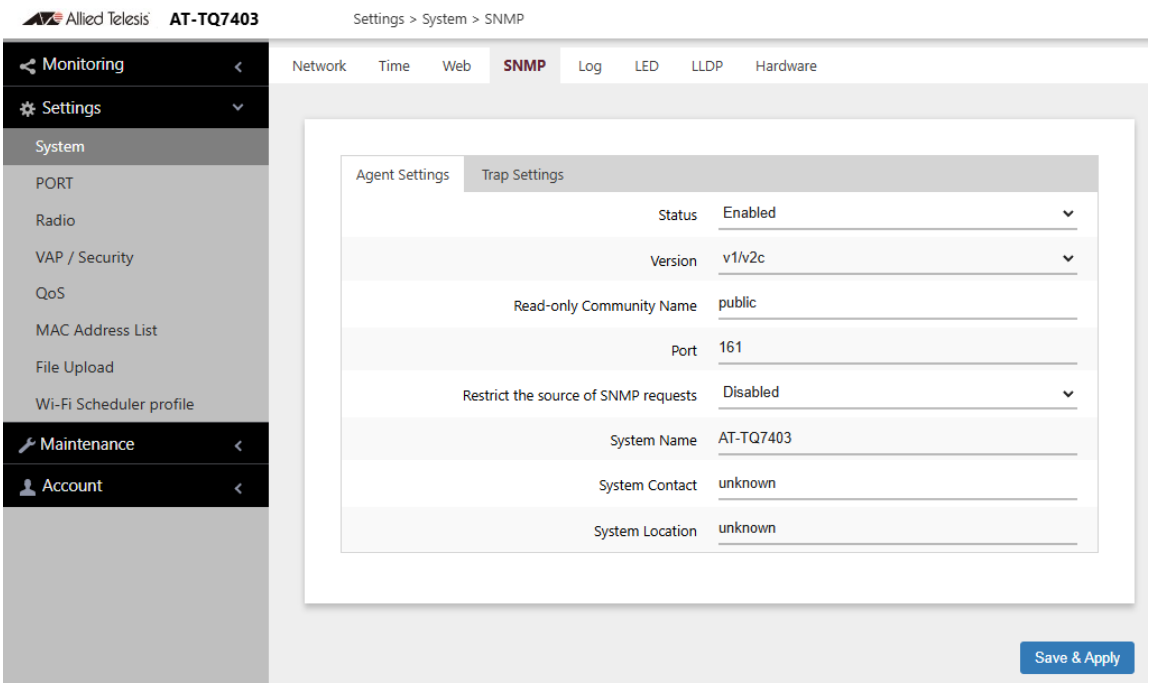

Figure 21. SNMP Window - SNMP Enabled

5. 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)	Enter a new community name. The default is public.
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 specified management stations. Selecting this option displays the new field “Only allow from the designated hosts or subnets.” - 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 SNMPv3. There is no default user name.
Password (SNMPv3 only)	Specify a password for SNMPv3. There is no default password
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 workstation by its Fully Qualified Domain Name (FQDN). - You can specify a subnet (for example, 192.168.1.0/24). - The default is blank.

Table 12. SNMP Window (Continued)

Field	Description
Only allow from the designated hosts or subnets (continued)	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 AT-TQ7403.
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.

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

Configuring Traps

To configure the switch to transmit SNMP traps on its LAN port, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **SNMP** from the sub-menu.
3. Enable and configure SNMP by referring to “Configuring SNMPv1, SNMPv2, and SNMPv3” on page 50.

Note
The Trap Settings tab is hidden when SNMP is disabled.

4. Select the **Agent Settings** tab. Refer to Figure 22 on page 54.

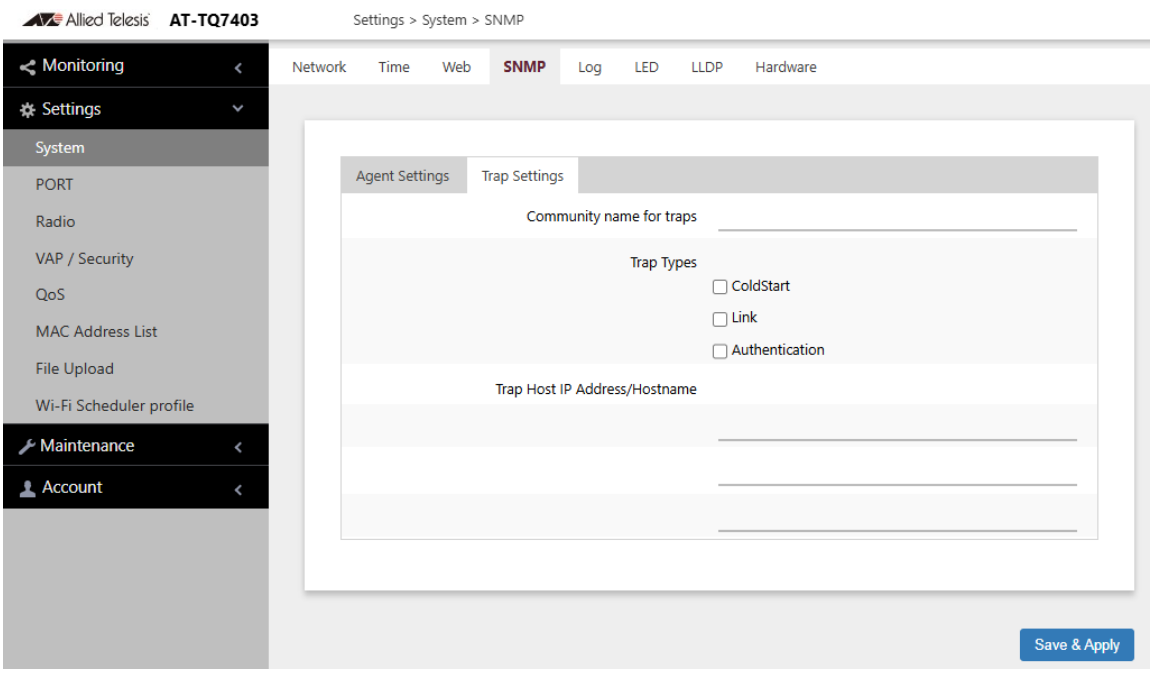

Figure 22. SNMP Window - Trap Settings

5. Configure the fields by referring to Table 13.

Table 13. SNMP Window - Trap Settings

Field	Description
Community name for traps	Enter a community name for the traps. The switch has the default SNMP v1/v2c read-only community string “public”. Here are the guidelines for specifying a new SNMP v1/v2c community string: - The switch supports only one community string. - The string can be up to thirteen characters. - Letters and numbers are supported. - Spaces and special characters are not recommended. If you select SNMP v3, this field displays the switch’s unique EngineID instead of the community name. This value is not configurable.

Table 13. SNMP Window - Trap Settings (Continued)

Field	Description
Trap Types	Specify the events that are to trigger traps: - Coldstart - The access point transmits a trap whenever it is powered on. - Link - The access point transmits a trap whenever the status of its LAN port changes from offline to online. - Authentication - The access point transmits a trap whenever a network manager logs on.
Trap Host IP Address/Hostname	Enter the IPv4 addresses or hostnames of up to three network devices to receive the traps.

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

Sending Log Messages to a Syslog Server

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

1. Select **Settings** > **System** from the main menu.
2. Select **Log** from the sub-menu. Refer to Figure 23.

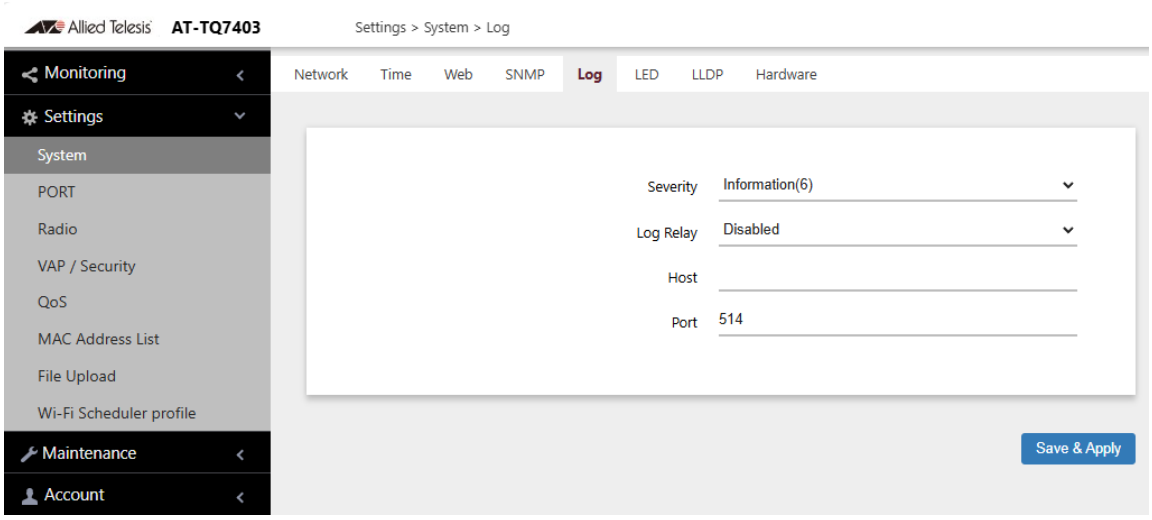

Figure 23. Log Window for Syslog Client

3. Configure the fields by referring to Table 14.

Table 14. Log Window for Syslog Client

Field	Description
Severity	Select the severity of messages the access point is to display in its log file and transmit to the syslog server. The severity levels are listed in Table 4 on page 32. 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, includes system messages levels 0 to 3. - The default is level 6, Information. It is the second highest value.

Table 14. 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. Stops 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 on your wired network. Here are the guidelines: - You can enter only one host. - Do not include a subnet mask with the IP address. - The factory default is none. 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. You can enter only one port.

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 front 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 24.

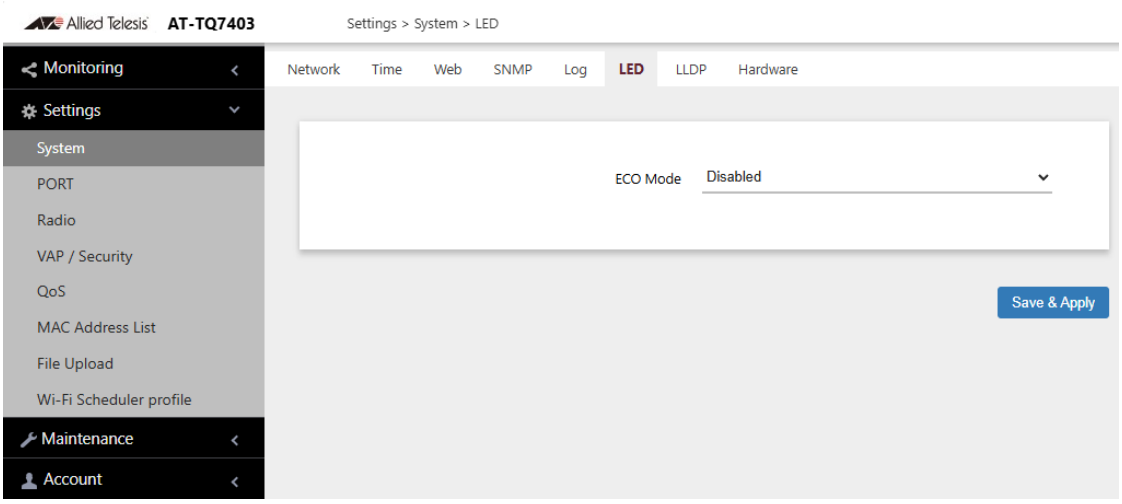

Figure 24. LED Window

3. From the **Eco Mode** pull-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. Click the **Save & Apply** button to save and update the configuration.

Configuring PoE Negotiation with Link Layer Discovery Protocol (LLDP)

This feature requires 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 one-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 LAN 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 PoE Negotiation, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **LLDP** from the sub-menu. Refer to Figure 25 on page 60.

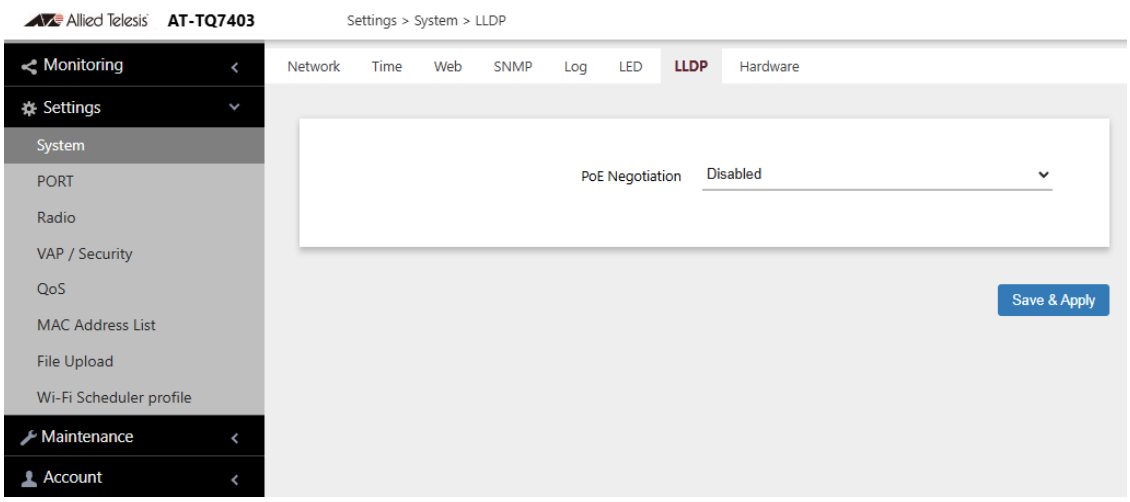

Figure 25. LLDP Window

3. Select one of the following from the PoE Negotiation menu:
   - ❒ Enabled: Enables PoE negotiation. The access point transmits the Extended Power Management TLV on its LAN 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 front 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. See Figure 26.

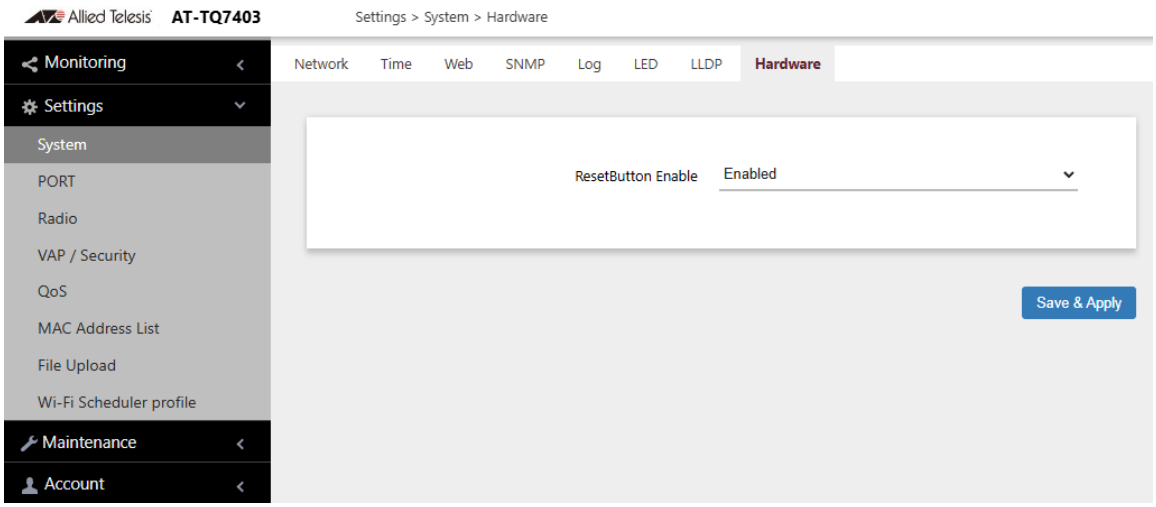

Figure 26. Hardware Window

3. From the **Reset Button 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.

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

Chapter 4

LAN Ports

This chapter describes the following procedures:

Enabling the Management VLAN Tag

You can enable or disable the Management VLAN Tag on the LAN Settings window. Here are the guidelines:

- 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.

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

1. Select **Settings** > **PORT** from the main menu. See Figure 27.

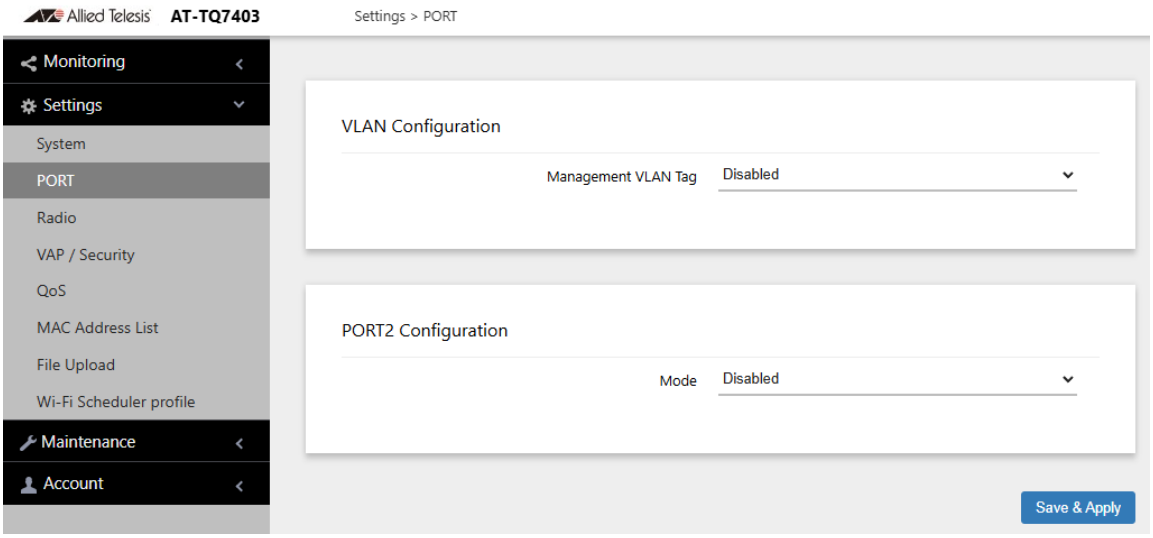

Figure 27. PORT Settings Window

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 PORT2

The access point has two Ethernet ports, labeled PORT1 and PORT2. You use these ports to connect the access point to your wired network.

Here are the basic properties:

- The default setting for PORT1 is enabled. You cannot disable it.
- PORT1 and PORT2 support PoE+.
- The default setting for PORT2 is disabled.
- PORT1 and PORT2 can be combined into a Static Link Aggregation (LAG) to double the bandwidth between the access point and the wired network.
- PORT2 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 PORT1 and PORT2 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. See Figure 28.

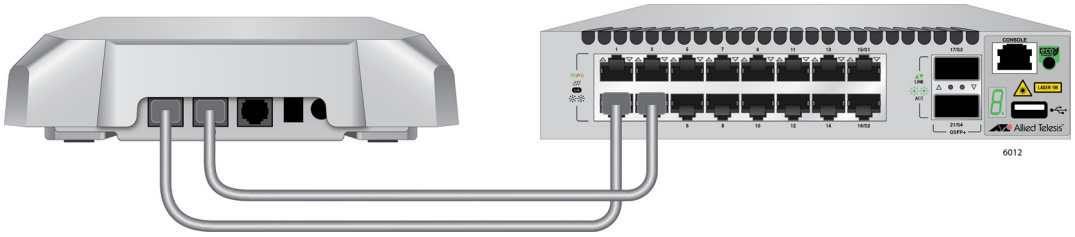

Figure 28. PORT1 and PORT2 in a Static LAG

Here are guidelines to using PORT1 and PORT2 as a static LAG:

- You must connect the ports to the same network device, such as an Ethernet switch or router, or virtual stacking devices. Do not connect the these ports to different network devices.
- The network device must support Static LAG.
- You must configure the two ports on the network device as Static LAG.

You activate the static LAG for PORT2 with the on-board web browser management interface, or with the AWC plug-in Vista Manager EX.

Note
Do not enable and cable PORT2 until you have configured the other network device for the static LAG.

Link Aggregation Control Protocol (LACP)

With LACP, you can form a LAG between the access point and your wired network through PORT1 and PORT2 automatically without configuring switch ports. You activate LACP on PORT2 and an LACP-supported switch configures the ports that are connected to PORT1 and PORT2 automatically. A LAG formed by LACP also provides link redundancy. If one link goes down, the access point maintains connectivity to the wired network over the remaining link.

Here are guidelines to using PORT1 and PORT2 using LACP:

- You must connect the ports to the same network device, such as an Ethernet switch or router, or virtual stacking devices. Do not connect the these ports to different network devices.
- The network device must support LACP.

Cascade Mode

PORT2 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 29.

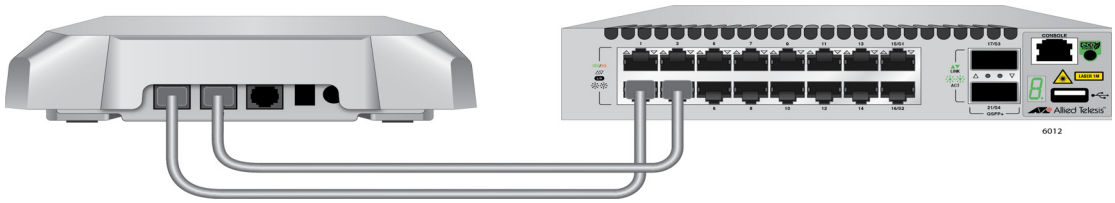

Figure 29. PORT2 in Cascade Mode with an End Node

It can also be a networking device such as a switch, router, or media converter. See Figure 30.

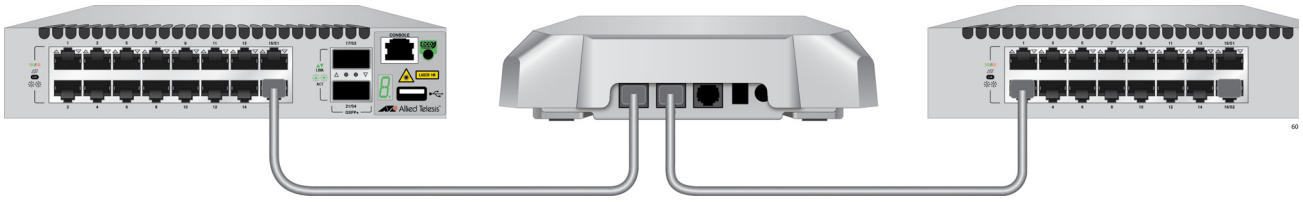

Figure 30. PORT2 in Cascade Mode with a Networking Device

Note
Do not connect both PORT1 and PORT2 to the same network device when PORT2 is in the Cascade mode.

Configuring PORT2

To configure PORT2, perform the following procedure:

1. Select **Settings** > **PORT** from the main menu. See Figure 31.

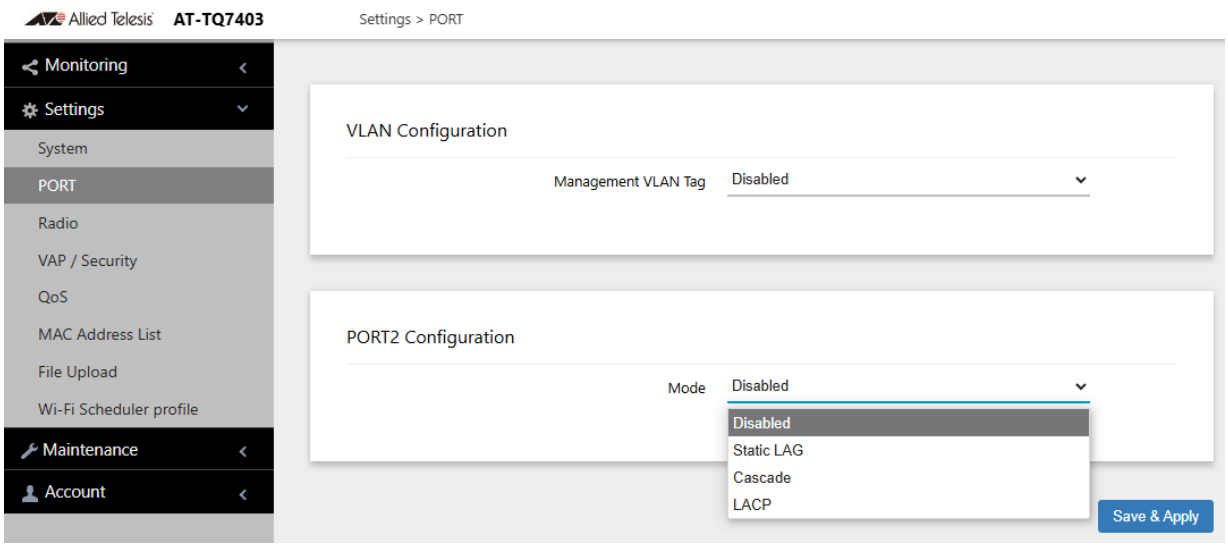

Figure 31. PORT Settings Window - PORT2 Configuration

The window has two sections. PORT2 is controlled with the PORT2 Configuration section. For information on the VLAN Configuration section, see “Enabling the Management VLAN Tag” on page 63.

2. From the Mode pull-down menu in the PORT2 Configuration section configure the settings by referring to Table 15.

Table 15. PORT Settings Window - PORT2 Configuration

Item	Description
Mode	Select one of the following: - Disabled: Disable PORT2. - Static LAG: Combines PORT1 and PORT2 into a static LAG. - Cascade: Activates the Cascade mode on PORT2 so that you can use the port to connect another device to your network. - LACP: Forms a LAG automatically without configuring the switch ports that PORT1 and PORT2 are connected.

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

If you enabled the Static LAG mode, the access point automatically combines PORT1 and PORT2 into a static LAG. Configure the ports on the other network device as a static LAG and connect PORT1 and PORT2 to it.

If you activate LACP, the ports on the other network device are configured automatically.

If you enabled the Cascade mode, connect PORT2 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 PORT1 and PORT2

To display the status of PORT1, perform the following procedure:

1. Select **Monitoring** > **Status** from the main menu.
2. Select **PORT1** or **PORT2** from the sub-menu. See Figure 32 for PORT1 and Figure 33 for PORT2.

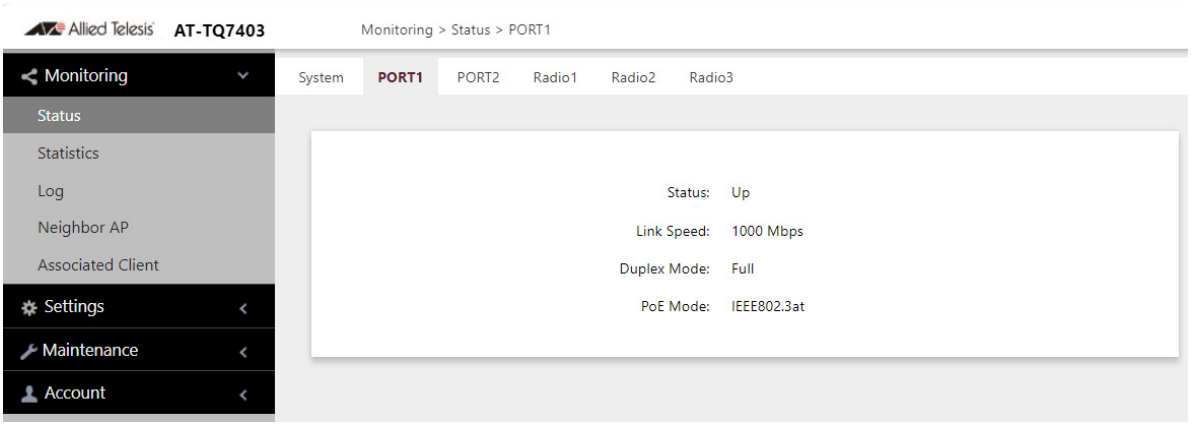

Figure 32. Status of PORT1 Window

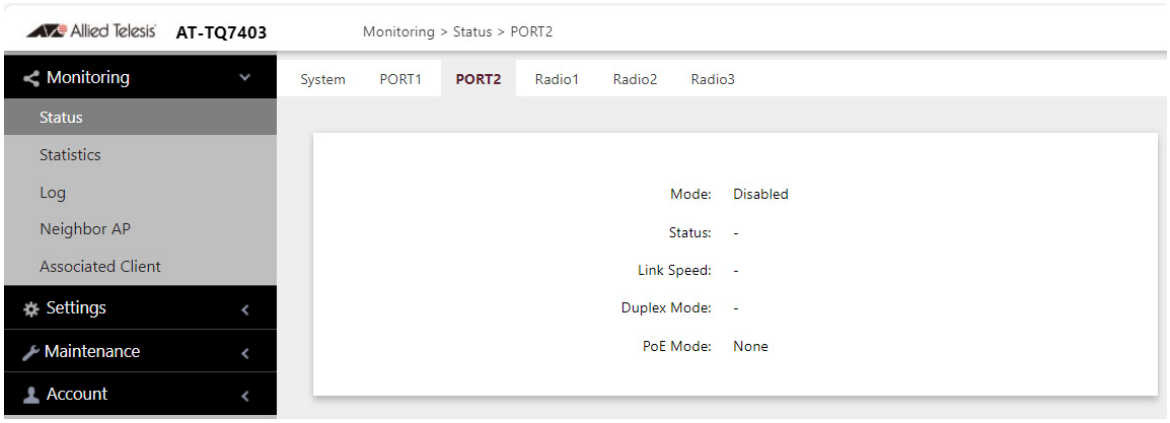

Figure 33. Status of PORT2 Window

The fields are defined in Table 16.

Table 16. Status of PORT1 or PORT2 Window

Item Name	Description
Mode (PORT2 only)	Displays PORT2 Configuration. The options are: - Disabled - Static LAG - Cascade - LACP
Status	Displays the status of the port. The possible states are listed here: - Up: The port has established a link with a network device, 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, or 2500Mbps).
Duplex Mode	Displays the duplex mode of the port, as follows: - Full: Full-duplex. - Half: Half-duplex.
PoE Mode	Displays the corresponding PoE standard.

Chapter 5

2.4GHz Radio1, 5GHz Radio2, and 6GHz Radio3

This chapter has the following procedures:

Configuring Basic Radio Settings

To configure the basic settings of Radio1 and Radio2, perform the following procedure:

1. Select **Settings** > **Radio**.
2. Select **Radio1**, **Radio2**, or **Radio3** from the sub-menu. You can configure only one radio at a time.
3. Click the **Basic Settings** tab. Figure 34 shows the tab for Radio1. This is the default tab.

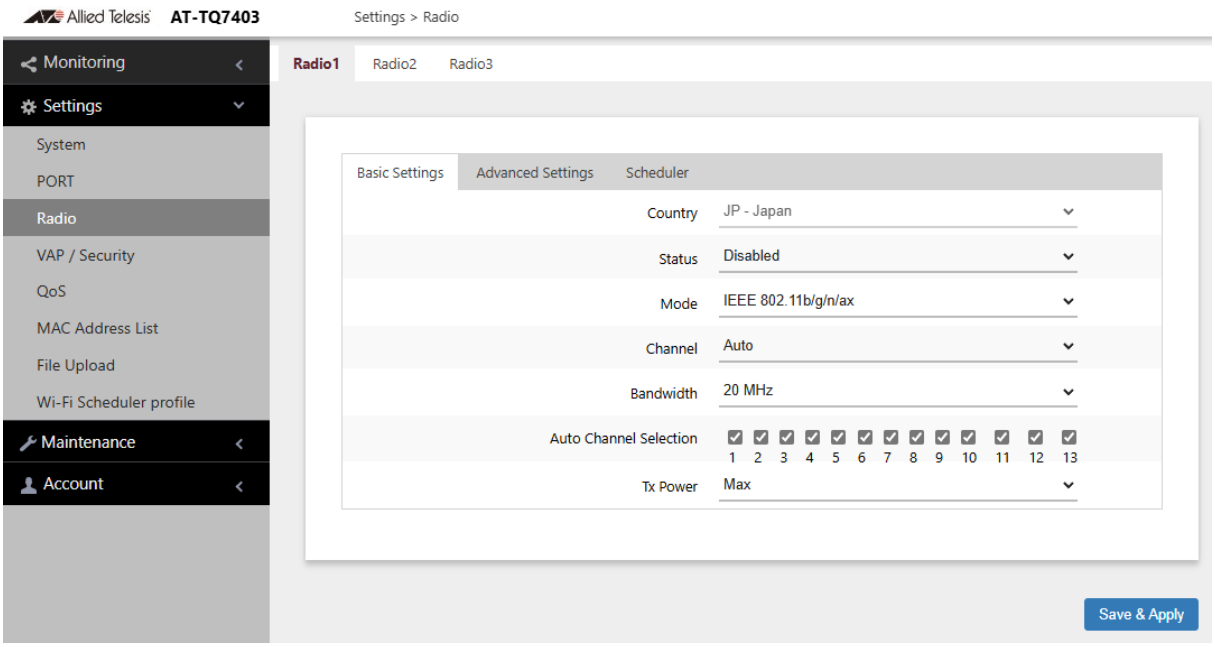

Figure 34. Basic Radio Settings Window - Radio1

Figure 35 shows the Basic Settings tab for Radio.2

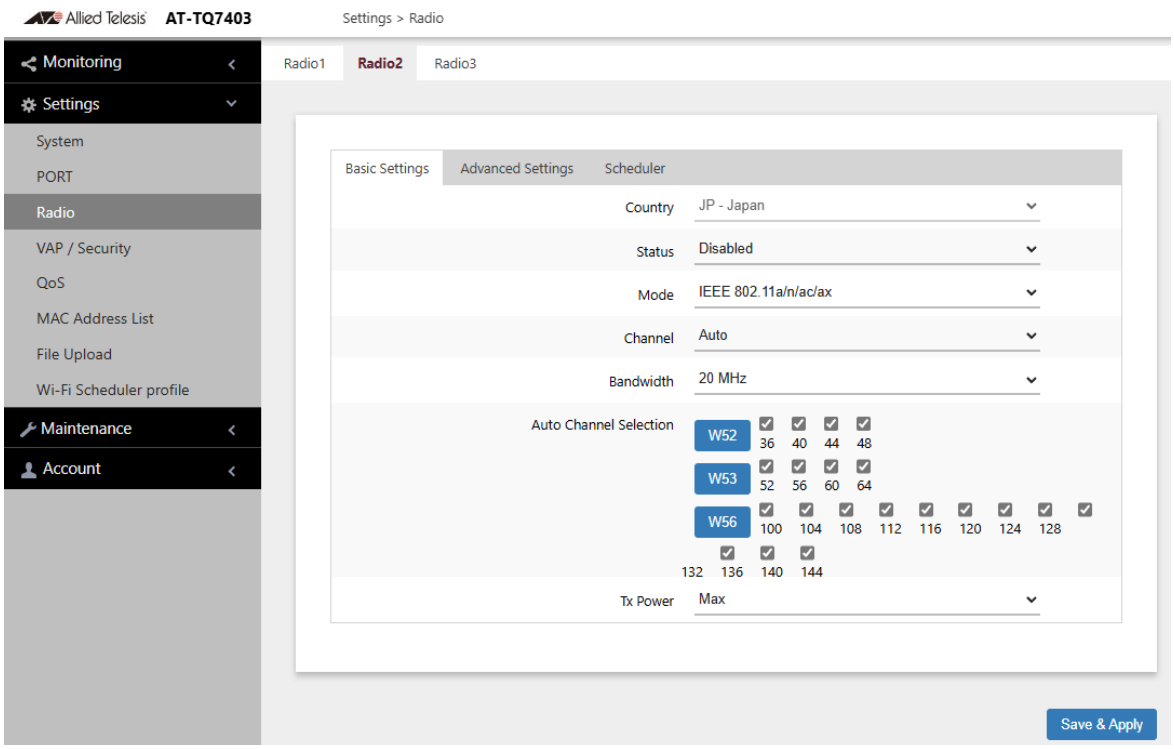

Figure 35. Basic Radio Settings Window - Radio2

Figure 36 shows the Basic Settings tab for Radio.3

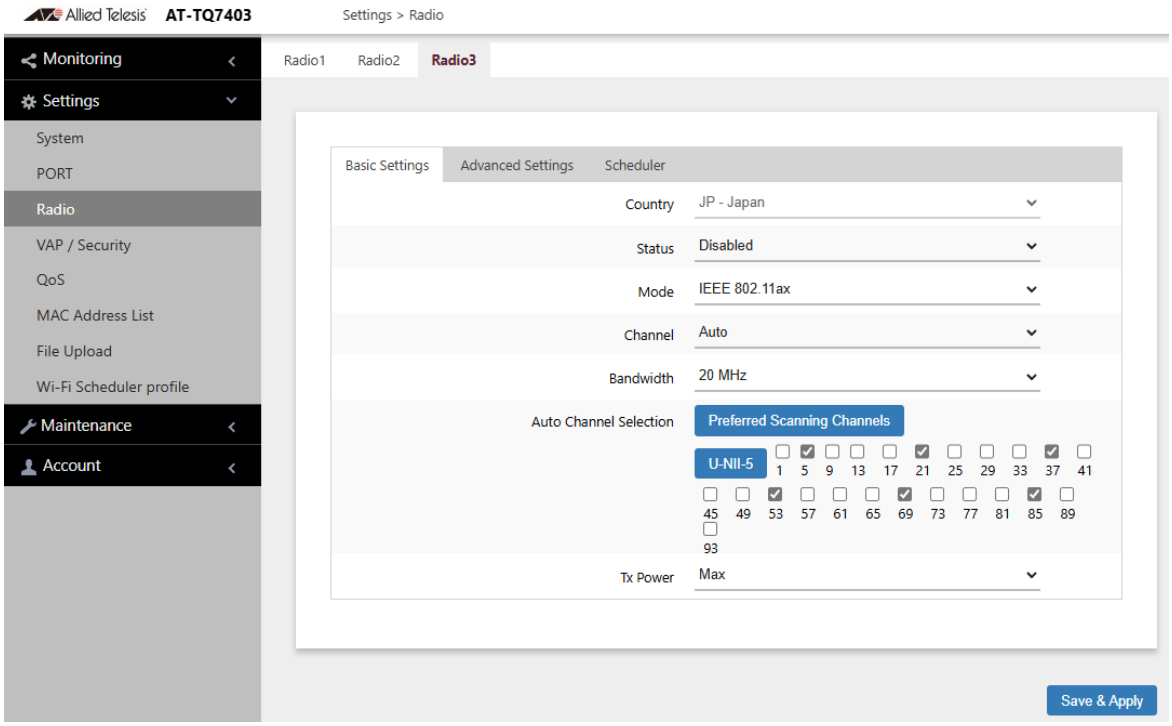

Figure 36. Basic Radio Settings Window - Radio3

4. Configure the settings by referring to Table 17.

Table 17. Basic Radio Settings Window

Field	Description
Country	Select the country that applies to your country or region. This setting 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 same country setting applies to both radios. - The country parameter is shown in the Basic Settings windows of both radios but it can only be set from Radio1. - Changing the country disables the radios. - You have to reconfigure the radio settings if you change the country. - You cannot change the country on units sold in North America, Japan, or Taiwan. The country is preset in products sold in those countries.
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. This is the default for Radio 1. - 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.

Table 17. 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 802.1ac 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 179.
Mode (Radio3)	The mode for Radio3 is only IEEE 802.11ax. You cannot change it.
Channel	Select the channel for the radio from the pull-down menu. Here are the guidelines: - Select Auto, the default setting, to have the access point select the channel automatically. - 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 802.11b/g/n/ax are listed here: - 20 MHz. This is the default setting. - 40 MHz 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 17. Basic Radio Settings Window (Continued)

Field	Description
Bandwidth (Radio2)	Select the bandwidth for Radio2 from the pull-down menu. The available bandwidths for IEEE 802.11a/n/ac/ax are listed here: - 20 MHz. This is the default setting. - 40 MHz - 80 MHz The only bandwidth for IEEE 802.11a alone is 20 MHz.
Bandwidth (Radio3)	Select the bandwidth for Radio3 from the pull-down menu. The available bandwidths for IEEE 802.11a/n/ac/ax are listed here: - 20 MHz. This is the default setting. - 40 MHz - 80 MHz - 160 MHz
Auto Channel Selection	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 vary 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, Radio2, and Radio3, perform the following procedure:

1. Select **Settings** > **Radio** from the main menu.
2. Select **Radio1**, **Radio2**, or **Radio3** from the sub-menu. You can configure only one radio at a time.
3. Click the **Advanced Settings** tab. Figure 37 displays the tab for Radio1.

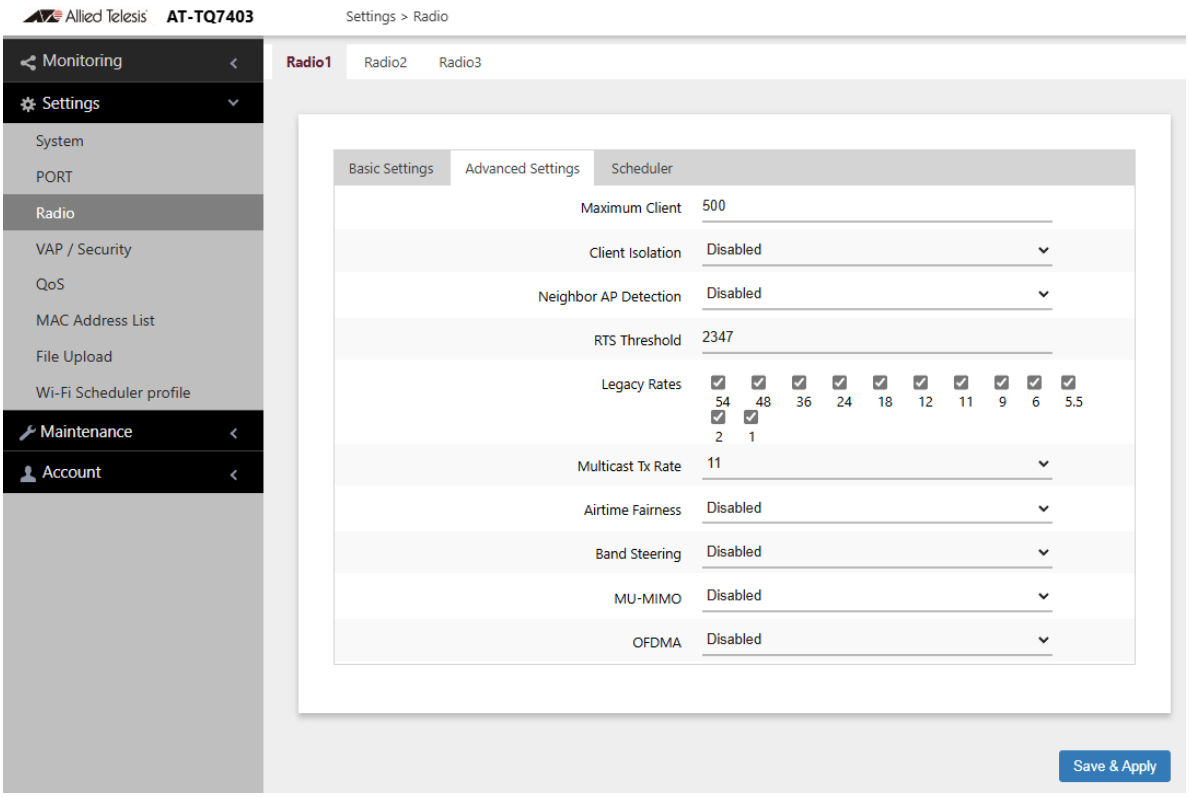

Figure 37. Advanced Settings Window for Radio1

Figure 38 displays the tab for Radio2.

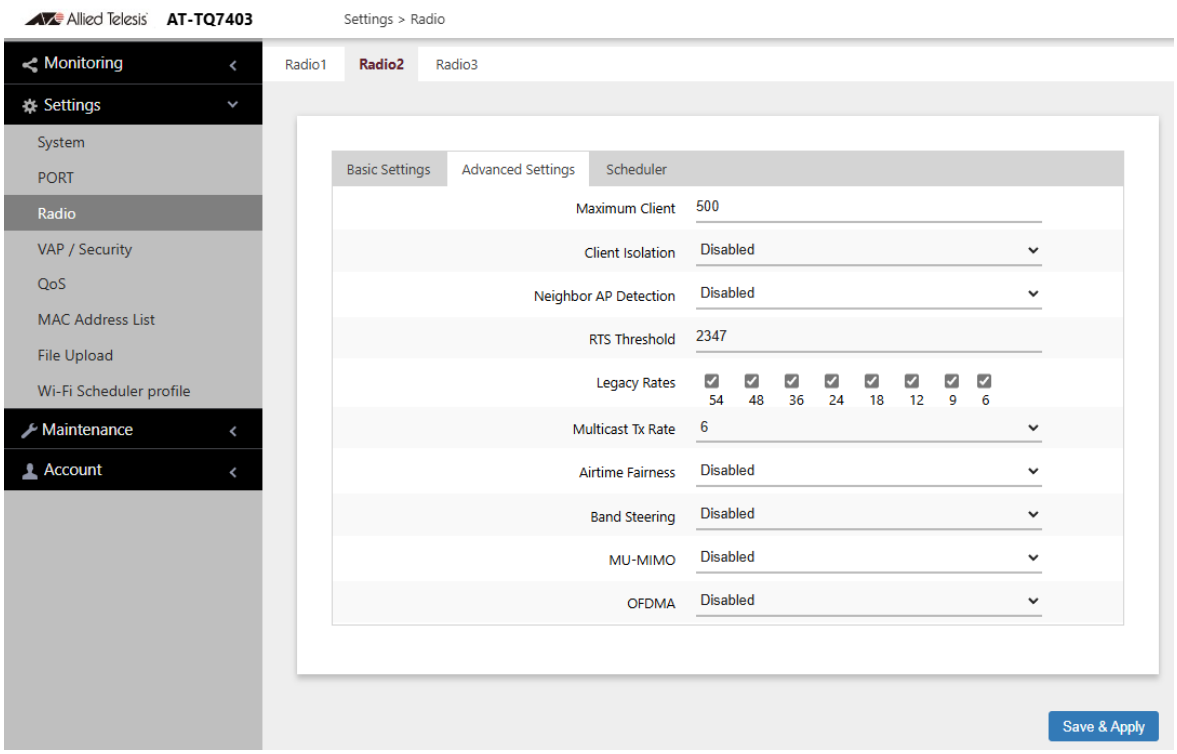

Figure 38. Advanced Settings Window for Radio2

Figure 39 displays the tab for Radio3.

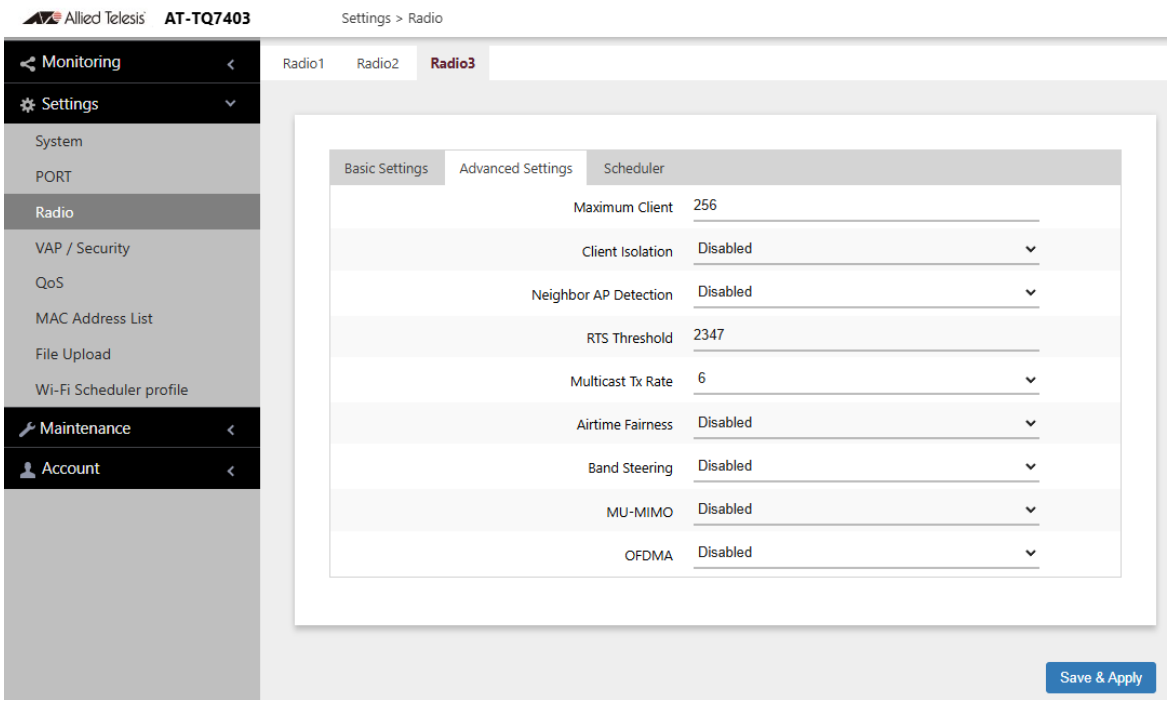

Figure 39. Advanced Settings Window for Radio3

4. Configure the parameters by referring to Table 18.

Table 18. 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 the radios support at one time are: - 2.4GHz Radio1 - 500 clients (default setting) - 5GHz Radio2 - 500 clients (default setting) - 6GHz Radio3 - 256clients (default setting)
Client Isolation	Enable or disable Client Isolation. The options are: - Disabled: Disables 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.

Table 18. Advanced Radio Settings Window (Continued)

Field	Description
Neighbor AP Detection	Enable or disable Neighbor AP Detection, which controls whether the access point listens for neighboring access points on the radios. Here are the options: - Enabled: The access point listens for neighboring access points on the radio and displays them in the Neighbor AP window. See “Displaying Neighbor Access Points” on page 34 - Disabled: The access point does not listen for neighboring access points. This is the default setting.
RTS Threshold	Specify the size in octets of MPDUs that initiate a Request to Send (RTS) and Clear to Send (CTS) handshake. The range is 0 to 2347 octets. The default is 2347 octets. You can use this parameter to control the use of RTS/ CTS handshakes when the access point transmits MPDUs. The access point uses the handshake before transmitting MPDUs that exceed the defined threshold. If you specify a low value, RTS packets are sent more frequently, which may consume more bandwidth and reduce the throughput. But more RTS packets may help a network recover from interference or collisions, which might occur on a busy network.
Legacy Rates (only Radio1 and Radio2)	Select the supported and advertised data transmission rates. 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.
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 - 6GHz Radio3: 6Mbps

Table 18. Advanced Radio Settings Window (Continued)

Field	Description
Airtime Fairness	Airtime fairness is intended for networks that are supporting both up-to-date as well as older, slower devices. The feature prevents the slower devices from reducing the overall performance of the wireless network. When a radio has more than 50 clients, the remaining bandwidth not allocated by Airtime Fairness is shared among the clients above the limit. Here are the options: - Evenly: Activates Airtime Fairness. - Manual: Activates Airtime Fairness with specified percentages. When you select Manual and click the Save & Apply button, the Pre-allocated Airtime Percentage fields become available on all the Advanced VAP Settings pages on the radio. To enter the Pre-allocated Airtime Percentage, go to Settings > VAP/Security > Advanced Settings as shown in Figure 51 on page 120. The Airtime Percentage of each VAP must be 0 to 100 and the total Airtime Percentage of the VAPs must not exceed 100. See Table 29 on page 121 for more information. - Disabled: Turn off Airtime Fairness. This is the default setting.
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 all three radios to associate with VAPs on a different radio during periods of traffic congestion. When traffic congestion is loaded on one radio, Band steering forces clients to associate with VAPs on other radios. Here are the guidelines: - Enabling band steering on one radio activates it on the other radios. Conversely, disabling the feature on one radio disables it on the other radios. - Ideally, the VAP settings, such as SSID names, VLAN IDs, and security settings, should be the same on the three radios. - The default setting is disabled.

Table 18. 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. This option is supported only when the radio modes in the Basic Settings tabs are set to IEEE 802.11b/g/n/ax for Radio1, IEEE 802.11a//n/ac/ax for Radio2. MU-MIMO is supported on Radio3.
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. This option is supported only when the radio modes in the Basic Settings tabs are set to IEEE 802.11b/g/n/ax for Radio1 and IEEE 802.11a//n/ac/ax for Radio2. OFDMA is supported on Radio3.

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, Radio 2 or Radio 3, perform the following:

1. Select **Settings** > **Radio** from the main menu.
2. Select **Radio1**, **Radio2**, or **Radio3** from the sub-menu. The default is Radio 1. 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 40.

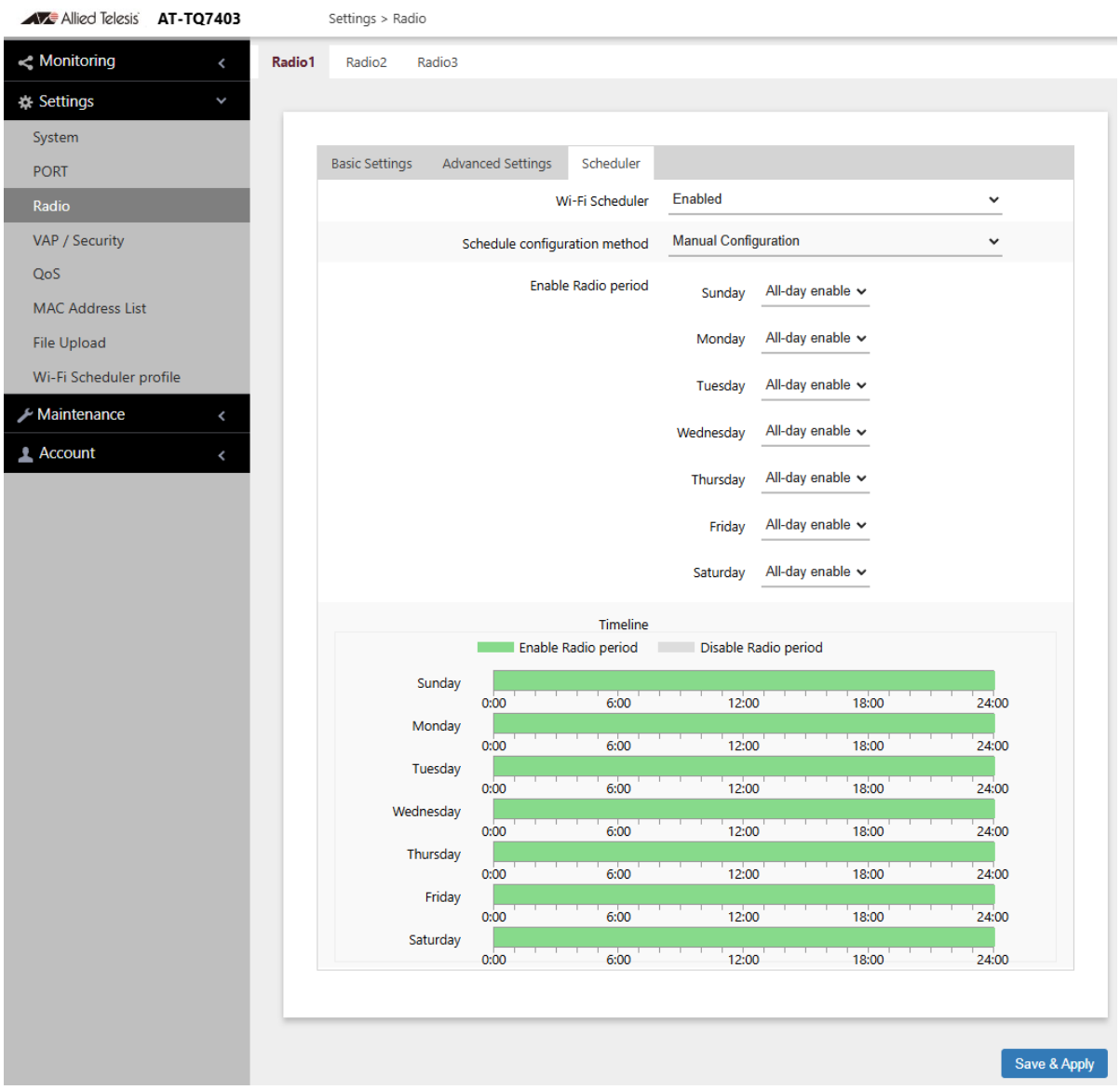

Figure 40. Radio Wi-Fi Scheduler - Manual configuration

2. Configure the parameters by referring to Table 19.

Table 19. 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 41.

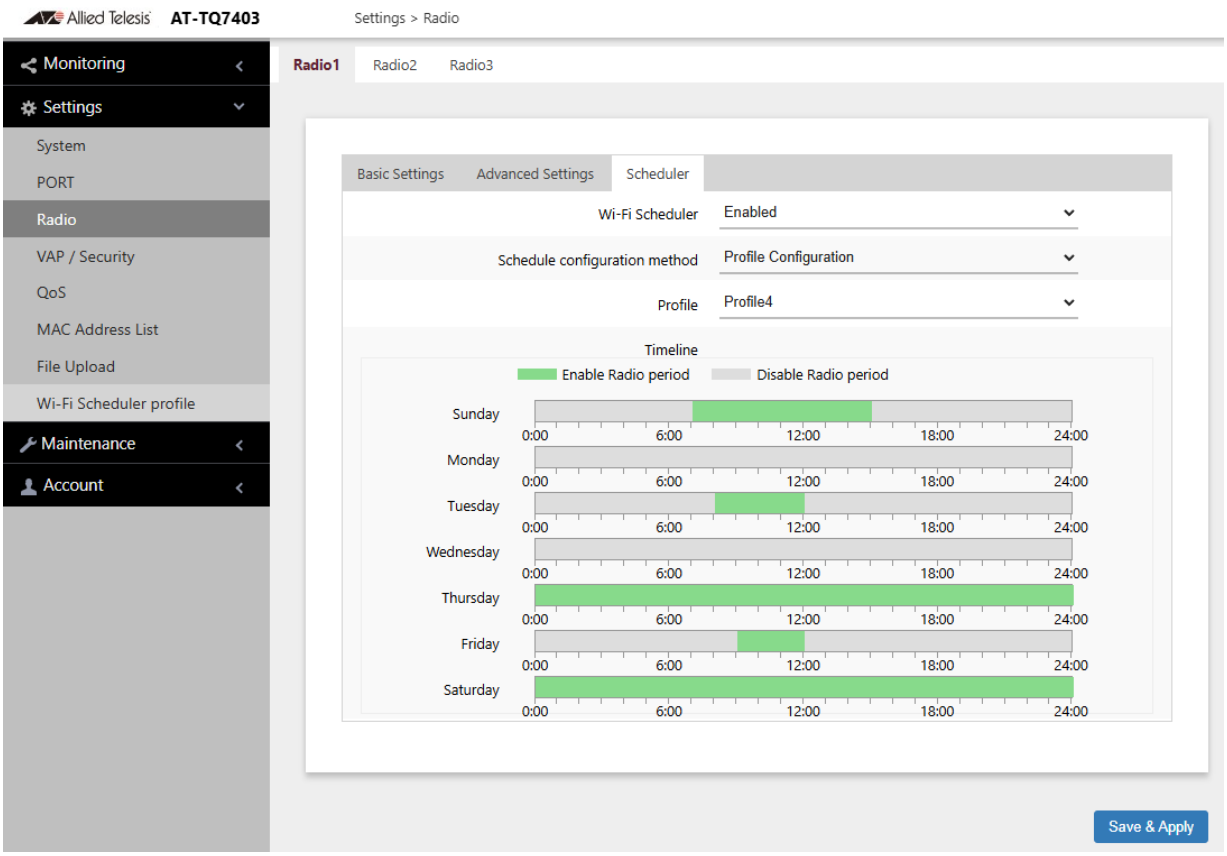

Figure 41. Assigning a Wi-Fi Scheduler Profile to a Radio

2. Configure the parameters by referring to Table 20.

Table 20. 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 218.

Table 20. 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 -218
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**, **Radio2**, or **Radio3** from the sub-menu. You can view only one radio at a time. The example in Figure 42 is for Radio2.

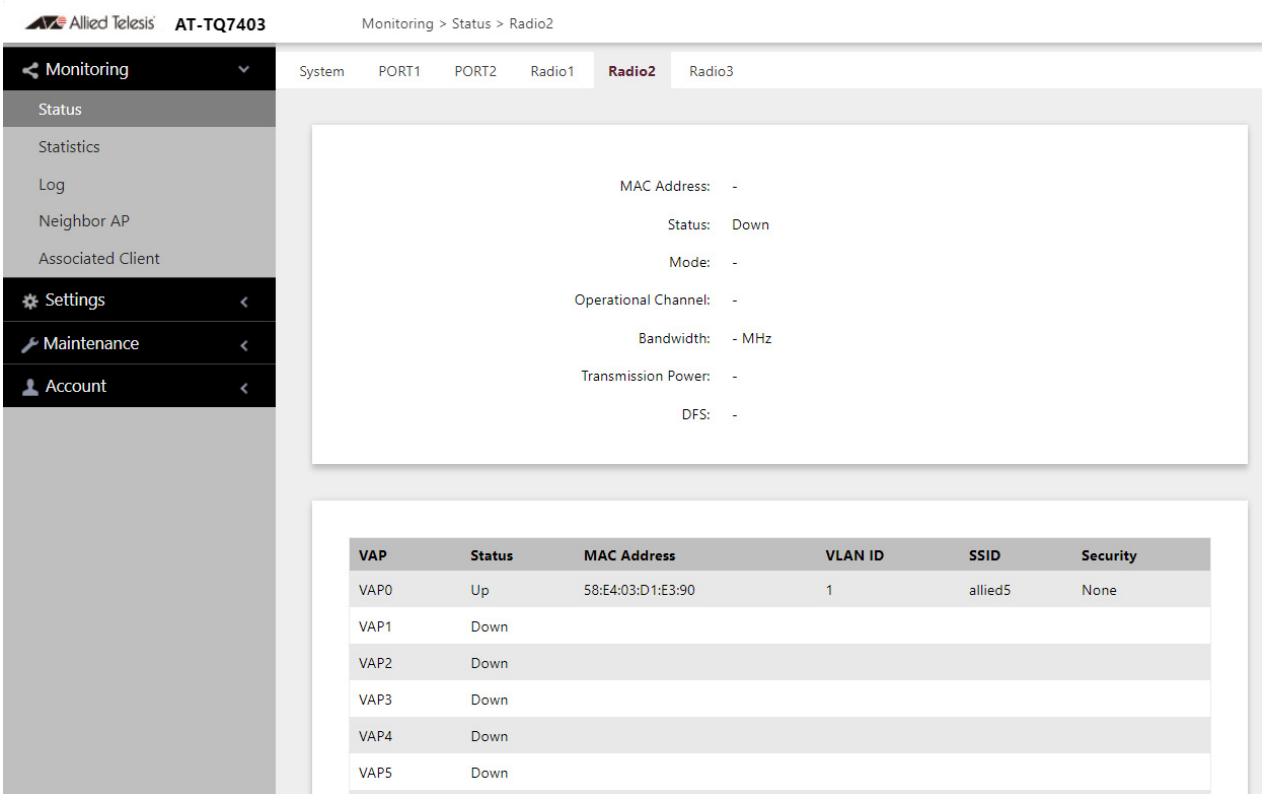

Figure 42. Radio2 Status Window

The fields are defined in Table 21.

Table 21. 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.

Table 21. Radio Status Window (Continued)

Field	Description
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 Radio3 has only one mode: - IEEE 802.11ax
Operational Channel	Displays the active channel. The channel may have been selected dynamically or manually.
Bandwidth	Displays the current bandwidth.
Transmission Power	Displays the transmission power, in dBm.

Table 21. 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 do not use 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 and region.
- ❒ DFS cannot be disabled on the wireless access points.
- ❒ DFS only applies to 5GHz Radio2.

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 34 on page 71.
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

Virtual Access Points

This chapter contains procedures for configuring the security on 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.

Here are guidelines to configuring VAPs:

- The radios have sixteen VAPs. Allied Telesis recommends enabling no more than five VAPs per radio for best performance.
- The VAP IDs are 0 to 15.
- You can enable or disable the VAPs individually, except for VAP0. To disable VAP0, you have disable its radio.
- VAPs can have the same or different VLAN IDs.
- You can assign different security methods to the VAPs of a radio.
- Static WEP security is supported on Radio 1 only when its Radio mode is set to IEEE 802.11b/g.
- Static WEP security is supported on Radio 2 only when its Radio mode is set to IEEE 802.11a.

Configuring Basic VAP Parameters

This section explains how to configure the following basic VAP functions:

- Enable or disable VAPs. Disabled VAPs are unavailable to wireless clients.
- Specify the role of VAP0 in Wireless Distribution System Bridges.
- Specify the VLAN IDs.
- Specify the SSIDs, which are the VAP names.
- Specify whether the SSIDs are to be hidden from clients.
- Specify whether VAPs are to be part of IEEE 802.11u and Passpoint to automate client associations.

To configure basic VAP functions, perform the following procedure:

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 the VAPs of 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 having to save each VAP configuration page individually. Clicking the **Save & Apply** button saves the changes you made to all VAPs of the selected radio.

4. Select the **Virtual Access Point** tab. This is the default tab. The example in Figure 43 on page 95 shows the settings for VAP0 on Radio1.

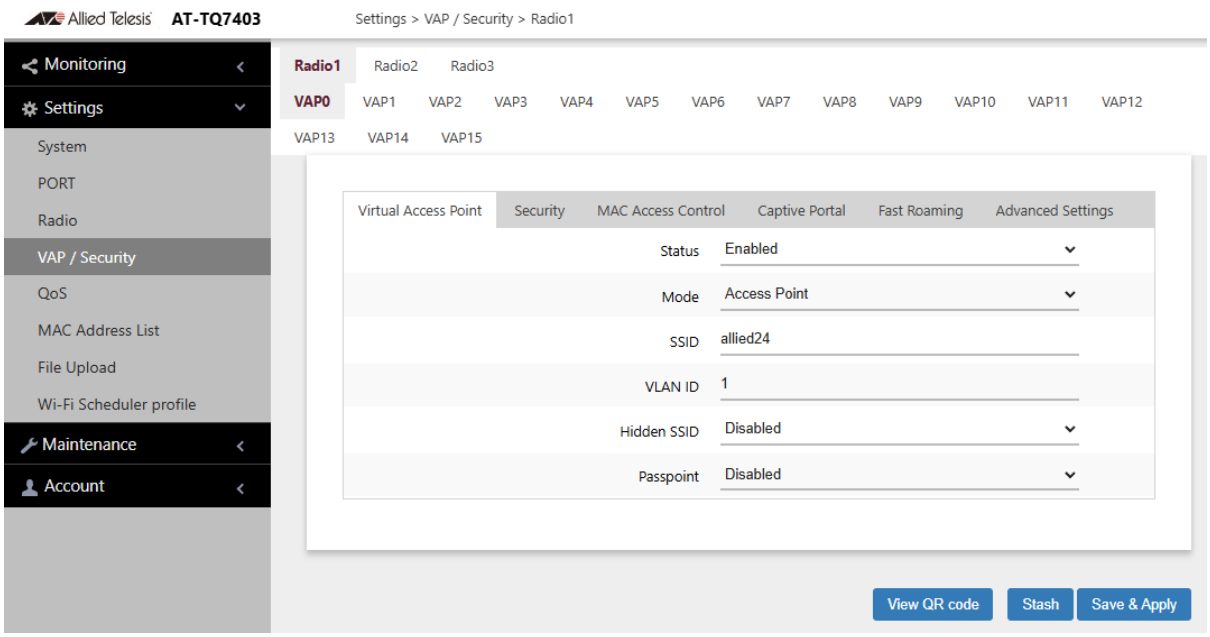

Figure 43. Virtual Access Point Tab

For information on the **View QR code** button at the bottom of the window, see “Generating Quick Response (QR) Codes for VAPs” on page 135.

5. Configure the parameters by referring to Table 22.

Table 22. 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 must disable its radio.

Table 22. 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 the 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: Select this option to assign VAP0 as a parent in a WDS bridge. - WDS Child: Select this option to assign VAP0 as a child in a WDS bridge. For information about WDS, see Chapter 10, “Wireless Distribution System Bridges” on page 186.
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 as the first or last character. - VAPs can have the same name. - The default names for VAP0 on Radio1, Radio2, and Radio3 are allied24, allied5, and allied6 respectively. - The default names for VAP1 to VAP15 are Virtual Access Point 1 to 15.

Table 22. 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 SSID. Clients who want to connect to an unauthorized VAP have to know its name.
Passpoint	This feature adds support for WiFi Certified Passpoint on captive portals. It allows mobile devices that support the IEEE 802.11u standard to automatically connect to subscribed Passpoint and Hotspot 2.0 services through the wireless access point. The feature is available on all radios, VAPs, and captive portals. Here are the options: - Disabled: Disables Passpoint on the VAP. This is the default setting. - Enabled: Enables Passpoint. Configure the settings in the 802.11 Settings and Passpoint Settings tabs before enabling the feature. See Chapter 11, “802.11u, Passpoint & OSU” on page 195.

6. Click the **Save & Apply** button to save your changes.

Assigning No Security to VAPs

The VAPs on Radio1 and Radio2 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.

> **Note**
> The VAPs on Radio3 do not have the None security option.

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.
4. Select the **Security** tab.
5. Select **None** from the Mode pull-down menu. This is the default setting. See Figure 44 as an example.

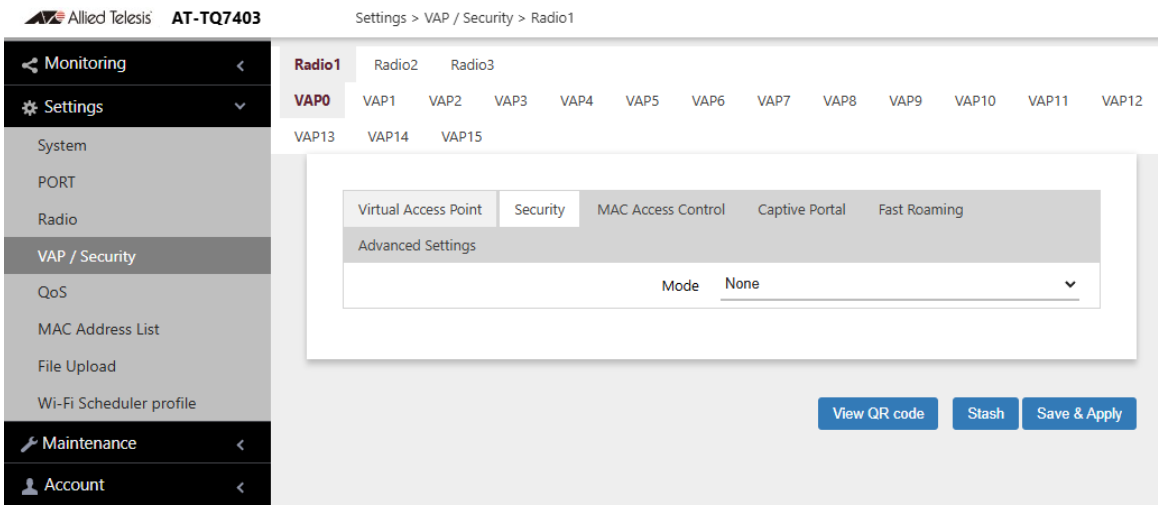

Figure 44. None Selection in the VAP Security Tab

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

Configuring Static WEP Security

The VAPs on Radio1 and Radio2 have the Static WEP option as security level.

Here are guidelines for Static WEP:

- Radio1 must be set to IEEE802.11b/g to support Static WEP. For instructions on setting radio modes, “Configuring Basic Radio Settings” on page 71.
- Radio2 must be set to IEEE802.11/a to support Static WEP.
- For instructions on setting the radio mode to IEEE802.11b/g or IEEE802.11/a, see “Configuring Basic Radio Settings” on page 71.
- Radio3 does not have the Static WEP option.

To configure a VAP for Static WEP security on Radio1 or Radio2, 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. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **Static WEP** from the Mode pull-down menu. See Figure 45 on page 100.

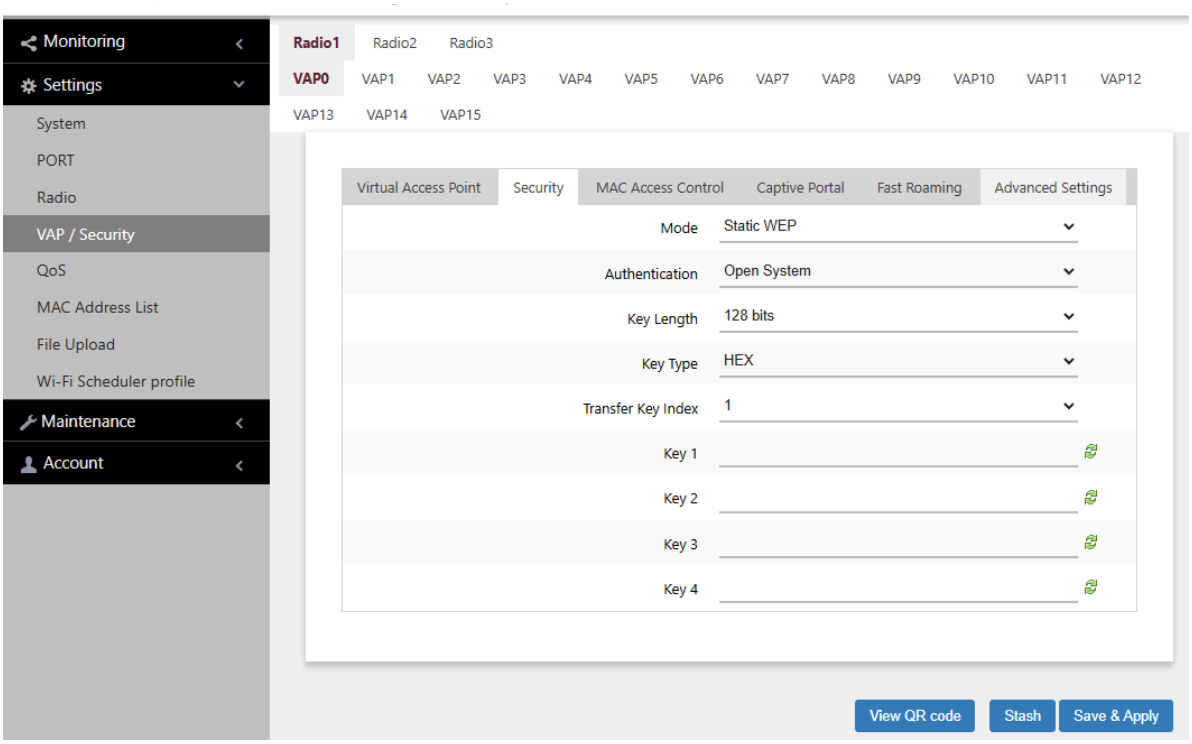

Figure 45. Static WEP in the VAP Security Tab

6. Configure the parameters by referring to Table 23.

Table 23. Static WEP Security Tab

Field	Description
Mode	Select **Static WEP**.
Authentication	Specify whether the access point is to authenticate 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 23. 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	Select 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. The default is key 1.
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 all the changes later.

Configuring Enhanced Open Security

To configure VAPs for Enhanced Open security, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **Enhanced Open** from the Mode pull-down menu. See Figure 46 as an example.

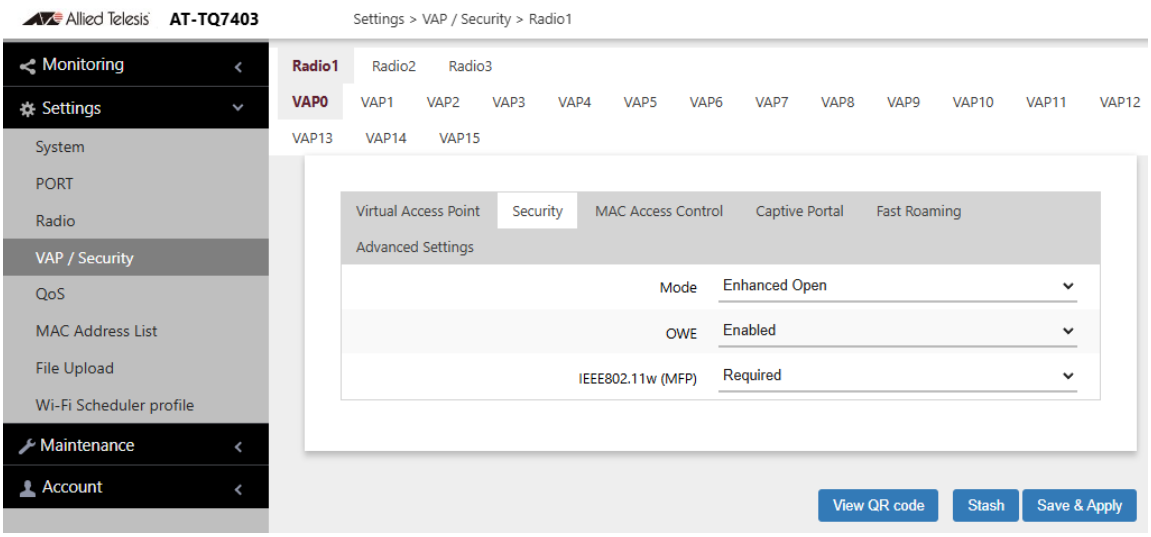

Figure 46. Enhanced Open Security Tab

6. Configure the parameters by referring to Table 24.

Table 24. Enhanced Open Security Tab

Field	Description
Mode	Select **Enhanced Open**.
OWE	Opportunistic Wireless Encryption (OWE) is enabled. No options are available.
IEEE802.11w (MFP)	IEEE 802.11w management frame protection is required. No options are available.

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

Configuring Enhanced Open Transition Mode

The VAPs on Radio1 and Radio2 have the Enhanced Open Transition mode option.

> **Note**
> Radio3 does not have the Enhanced Open Transition mode option.

To configure a VAP for Enhanced Open Transition mode on Radio1 or Radio2, 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. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **Enhanced Open Transition Mode** from the Mode pull-down menu. See Figure 47 as an example.

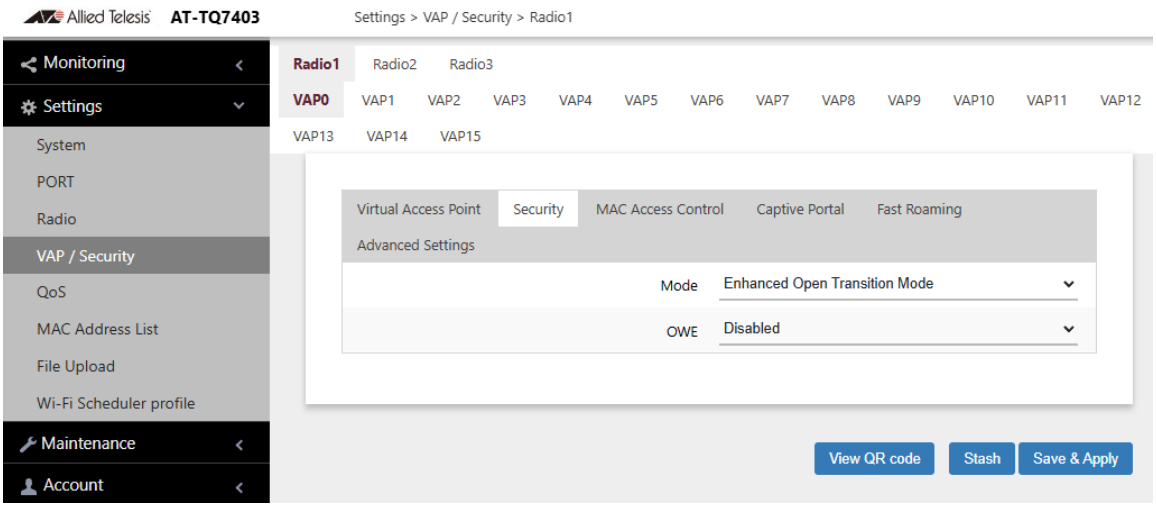

Figure 47. Enhanced Open Transition Mode Tab

6. Configure the parameters by referring to Table 25 on page 105.

Table 25. Enhanced Open Transition Mode Tab

Field	Description
Mode	Select **Enhanced Open Transition Mode**.
OWE	Opportunistic Wireless Encryption (OWE) is disabled. No options are available.

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

Configuring WPA Personal Security

To configure VAPs for WPA Personal (Pre-Shared Key) security, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **WPA Personal** from the Mode pull-down menu. See Figure 48 as an example.

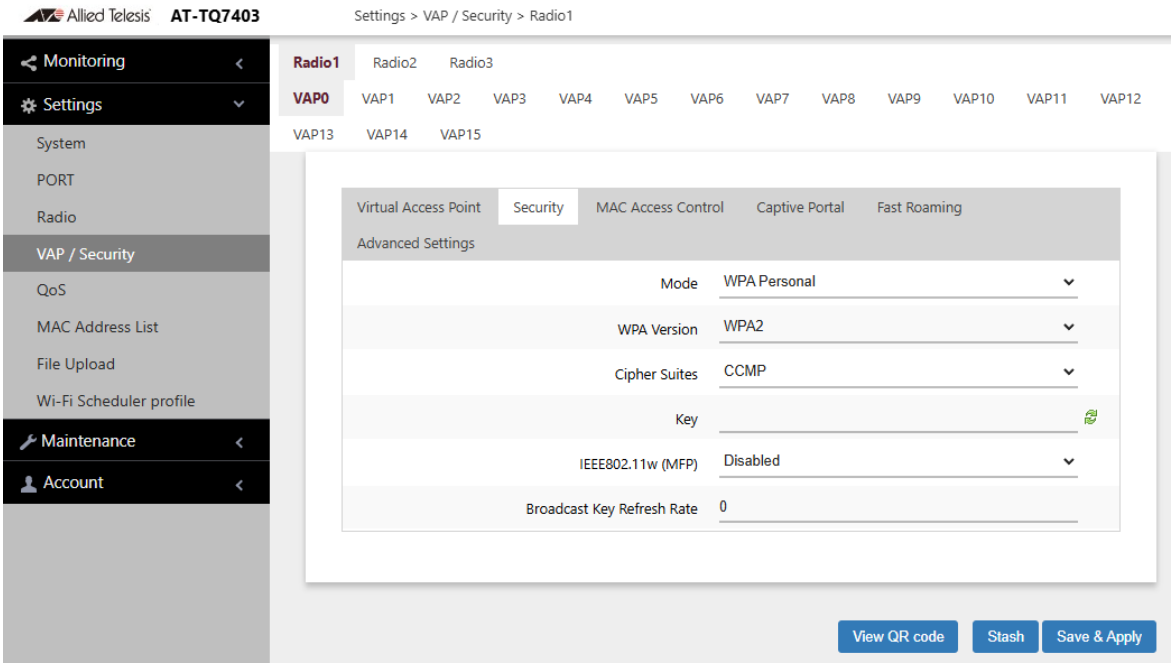

Figure 48. WPA Personal Security Tab

6. Configure the parameters by referring to Table 26 on page 107.

Table 26. WPA Personal Security Tab

Field	Description
Mode	Select **WPA Personal**.
WPA Version	Select the WPA version. The options are listed here: - WPA and WPA2: Select this option if the VAP is to support both WPA and WPA2 clients. - WPA2: Select this option if the VAP is to support WPA2 clients only. This is the default setting. - WPA2 and WPA3: Select this option if the VAP is to support both WPA2 and WPA3 clients. - WPA3: Select this option if the VAP is to support WPA3 clients only.
Cipher Suites	The settings are listed here: - CCMP: This is the only option when the WPA version is WPA2, WPA2 and WPA3, or WPA3. - TKIP and CCMP: This is the only option when the WPA version is WPA and WPA2. 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 26. 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 all the changes later.

Configuring WPA Enterprise Security

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

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 to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **WPA Enterprise** from the Mode pull-down menu. See Figure 49 on page 110 as an example.

Note
You can set WPA Enterprise to the security mode and configure IEEE802.11r as Fast Foaming; however, IEEE802.11r can only be configured using AWC Plug-in.

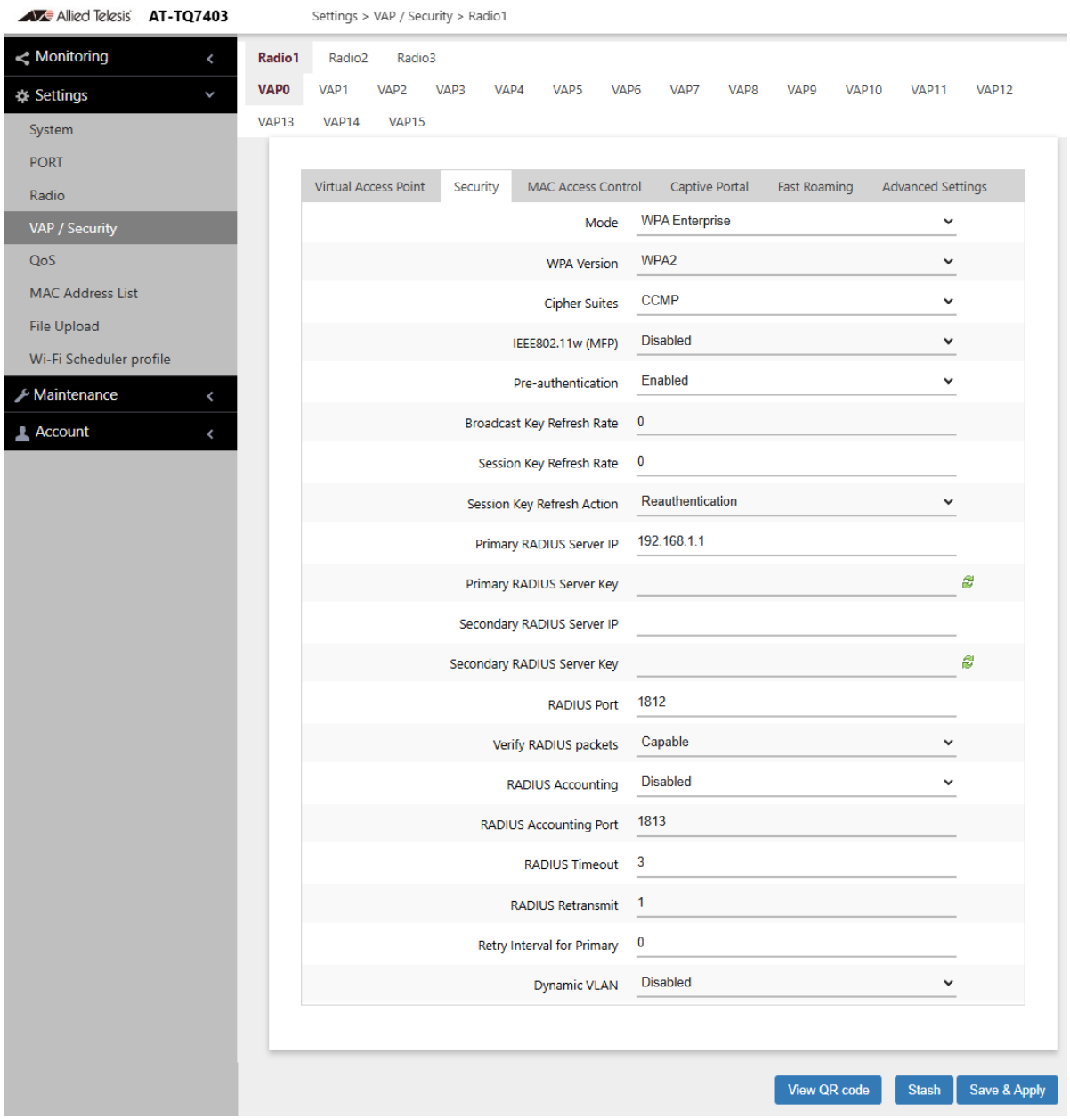

Figure 49. WPA Enterprise Security Tab

6. Configure the parameters by referring to Table 27 on page 111.

Table 27. WPA Enterprise Security Tab

Field	Description
Mode	Select **WPA Enterprise**.
WPA Version	Select the WPA version for the VPA. The options are listed: - WPA and WPA2 - Select this option if the VAP is to support both WPA and WPA2 clients. - WPA2: Select this option if the VAP is to support only WPA2 clients. This is the default setting. - WPA2 and WPA3 - Not supported. - WPA3: Select this option if the VAP is to support only WPA3 clients.
Cipher Suites	The settings are listed here: - CCMP: This is the only option when the WPA version is WPA2, or WPA2 and WPA3. This is the default. - TKIP and CCMP: This is the only option when the WPA version is WPA and WPA2. - 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 27. WPA Enterprise Security Tab (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 VAP clients. The range is 0 to 86400 seconds. The setting 0 (zero), the default, disables the refresh rate.
Session Key Refresh Rate	Enter the interval for refreshing the unicast session key to be sent to the VAP clients. Session keys are unique to each client. The range is 0 to 86400 seconds. The setting 0 (zero), the default, disables the refresh rate.
Session Key Refresh Action	Select the action of the access point when sessions expire. 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.
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.

Table 27. WPA Enterprise Security Tab (Continued)

Field	Description
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 use 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.
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.

Table 27. WPA Enterprise Security Tab (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 then or equal to 29. - both Primary RADIUS and Secondary RADIUS, and the keys are the same, set the values such that “RADIUS Timeout” x “RADIUS Retransmit + 1” 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.
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 all the changes later.

Configuring OSEN Security

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

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 to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **OSEN** from the Mode pull-down menu. See Figure 50 as an example.

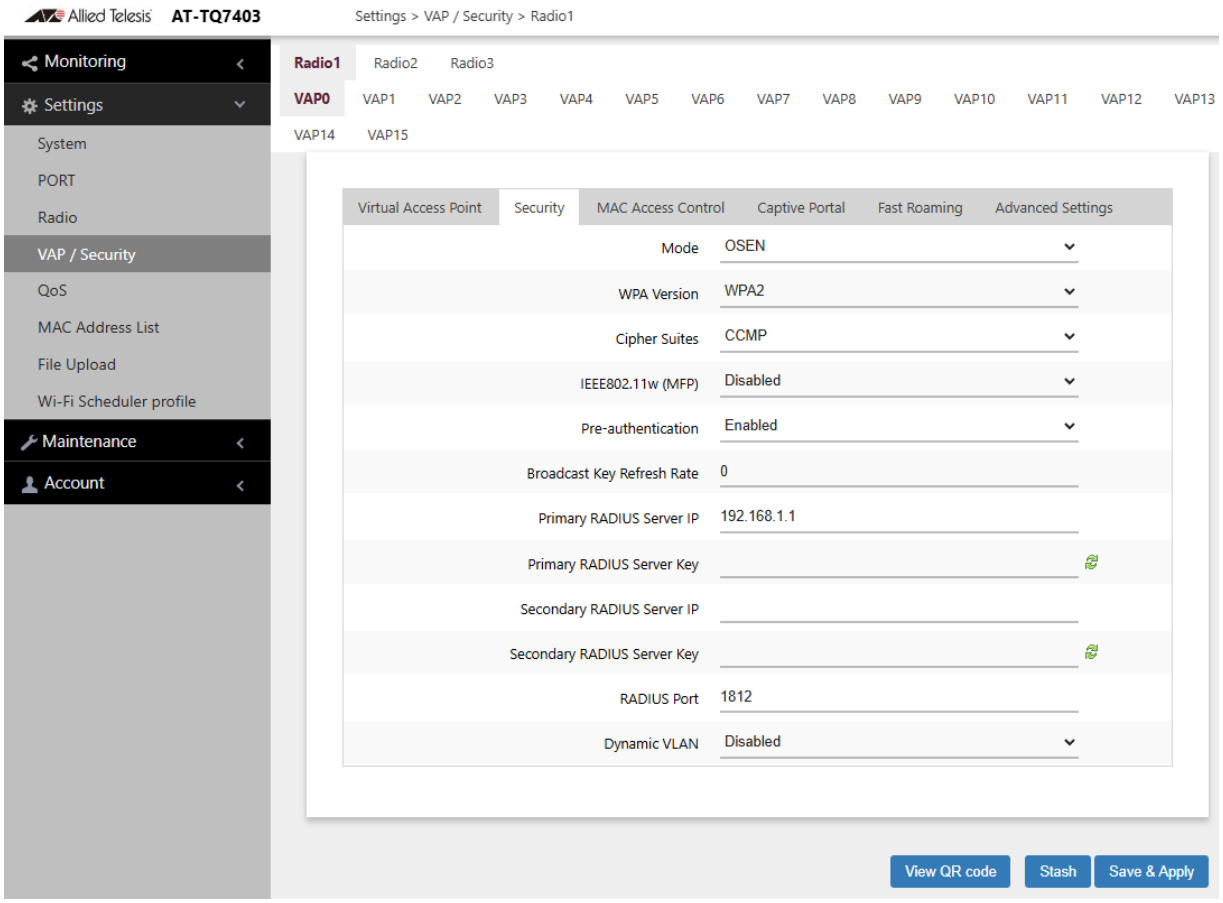

Figure 50. OSEN Security Tab

6. Configure the parameters by referring to Table 28 on page 117.

Table 28. OSEN Security Tab

Field	Description
Mode	Select **OSEN**.
WPA Version	Select the WPA version for the VPA. The options are listed: - WPA and WPA2 - Select this option if the VAP is to support both WPA and WPA2 clients. - WPA2: Select this option if the VAP is to support only WPA2 clients. This is the default setting. - WPA2 and WPA3 - Not supported. - WPA3: Select this option if the VAP is to support only WPA3 clients.
Cipher Suites	The settings are listed here: - CCMP: This is the only option when the WPA version is WPA2, or WPA2 and WPA3. This is the default. - TKIP and CCMP: This is the only option when the WPA version is WPA and WPA2. - GCMP: This is the only option when the WPA version is WPA3. 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 28. OSEN Security Tab (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 VAP clients. The range is 0 to 86400 seconds. The setting 0 (zero), the default, disables the refresh rate.
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 use the same port number. The range is 0 to 65535. The default is 1812.

Table 28. OSEN Security Tab (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 all the changes later.

Configuring Advanced VAP Settings

To configure advanced VAP settings, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0.
4. Select the **Advanced Settings** tab. See Figure 51.

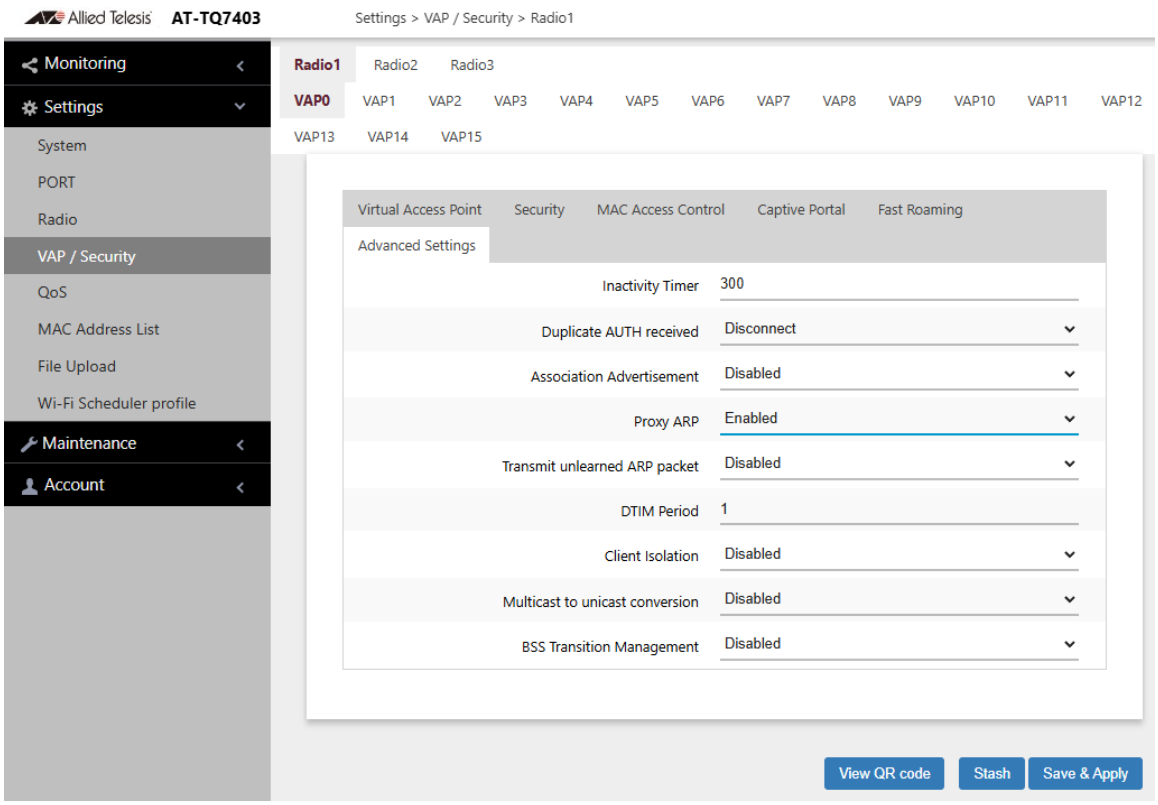

Figure 51. Advanced VAP Settings Window

5. Configure the parameters in Table 29 on page 121.

Table 29. VAP Advanced

Field	Description
Inactivity Timer	Specify time in seconds to close a wireless client session being idle when exceeding the specified time. The range is from 30 to 3600. The default value is 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 “Configuring WPA Personal Security” on page 106. 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 informs other access points of new clients. Other access points on the same subnet must have Association Advertisement enabled to support this feature.

Table 29. 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.
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 efficient though the response is slower. - When the number is lower, the energy saving is less efficient though the response is quicker.

Table 29. VAP Advanced (Continued)

Field	Description
Client Isolation	Enable or disable Client Isolation. The options are: - Disabled: Disables 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.
Pre-allocated Airtime Percentage	**Note** This field is only available when Airtime Fairness is set to Manual on the Advanced Radio Settings page in Figure 37 on page 76. For more information, see the description of Airtime Fairness in Table 18 on page 78. Enter the percentage of the bandwidth of a radio, which you want to allocate as airtime for the VAP. The value must be 0 to 100. The total Airtime Percentages of the VAPs must not exceed 100.
Multicast to unicast conversion	Enable or disable the multicast-to-unicast conversion, which the access point converts received multicast packets to unicast packets when forwarding packets to associated clients. The options are listed here: - Enabled: The access point converts multicast packets to unicast packets and forwards them to associated clients. - Disabled: The function of multicast-to-unicast conversion is disabled. This is the default setting.

Table 29. VAP Advanced (Continued)

Field	Description
BSS Transition Management	Improves performance of a wireless network by sharing information with associated wireless clients. The options are: - Enabled: BSS Transition Management is enabled. - Disabled: BSS Transition Management is disabled. This is the default setting.

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

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 52.

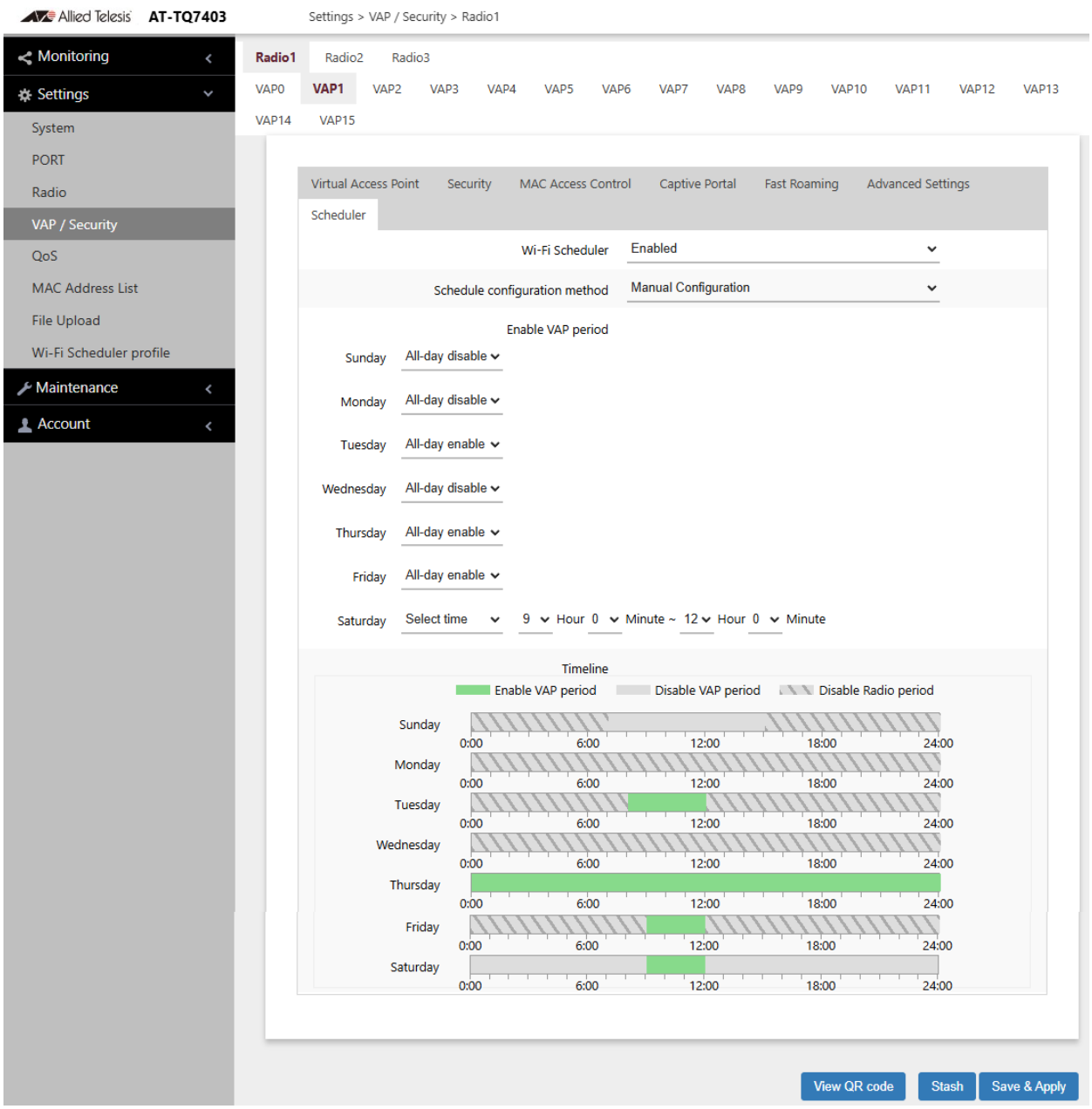

Figure 52. VAP Wi-Fi Scheduler - Manual configuration

2. Configure the parameters by referring to Table 30.

Table 30. 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 53

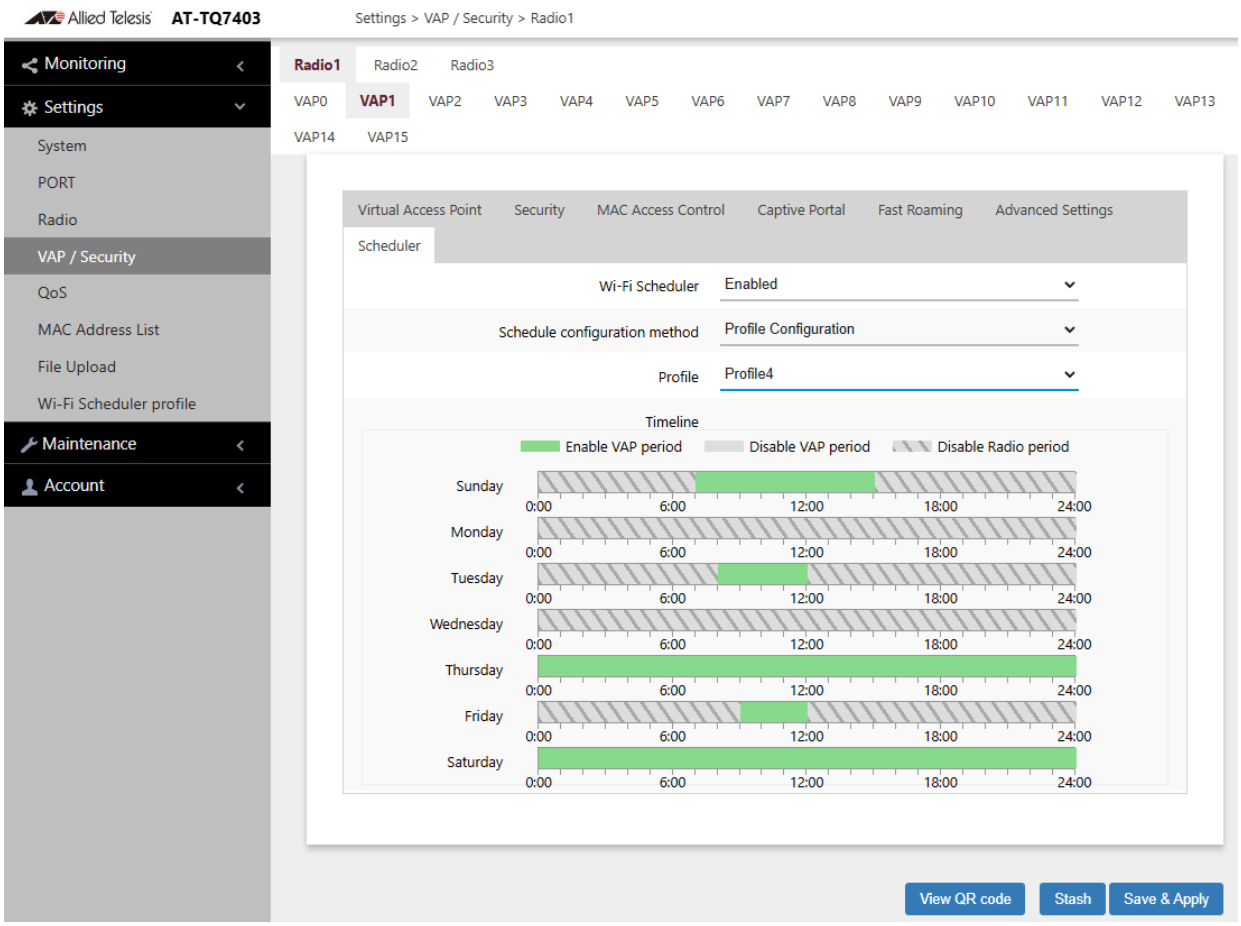

Figure 53. Assigning a Wi-Fi Scheduler Profile to a VAP

2. Configure the parameters by referring to Table 31.

Table 31. 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 31. VAP Wi-Fi Scheduler Settings - 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 -218.
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.

Viewing Fast Roaming

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

Here are the guidelines for Fast Roaming:

- You cannot configure Fast Roaming from the web browser interface. Fast Roaming requires Vista Manager EX and AWC.
- When Security is set to WPA Personal or WPA Enterprise, you can view the parameter values.
- The **View QR code** button is not supported in Fast Roaming.

To view the parameter values for fast roaming clients, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1**, **Radio2**, or **Radio3** from the sub-menu. The default is Radio1.
3. Select a VAP.The default is VAP0.
4. Select the **Fast Roaming** tab. See Figure 54 on page 131.

Note
The Fast Roaming window shown in Figure 54 on page 131 is when the VAP Security is set to WPA Personal or WPA Enterprise.

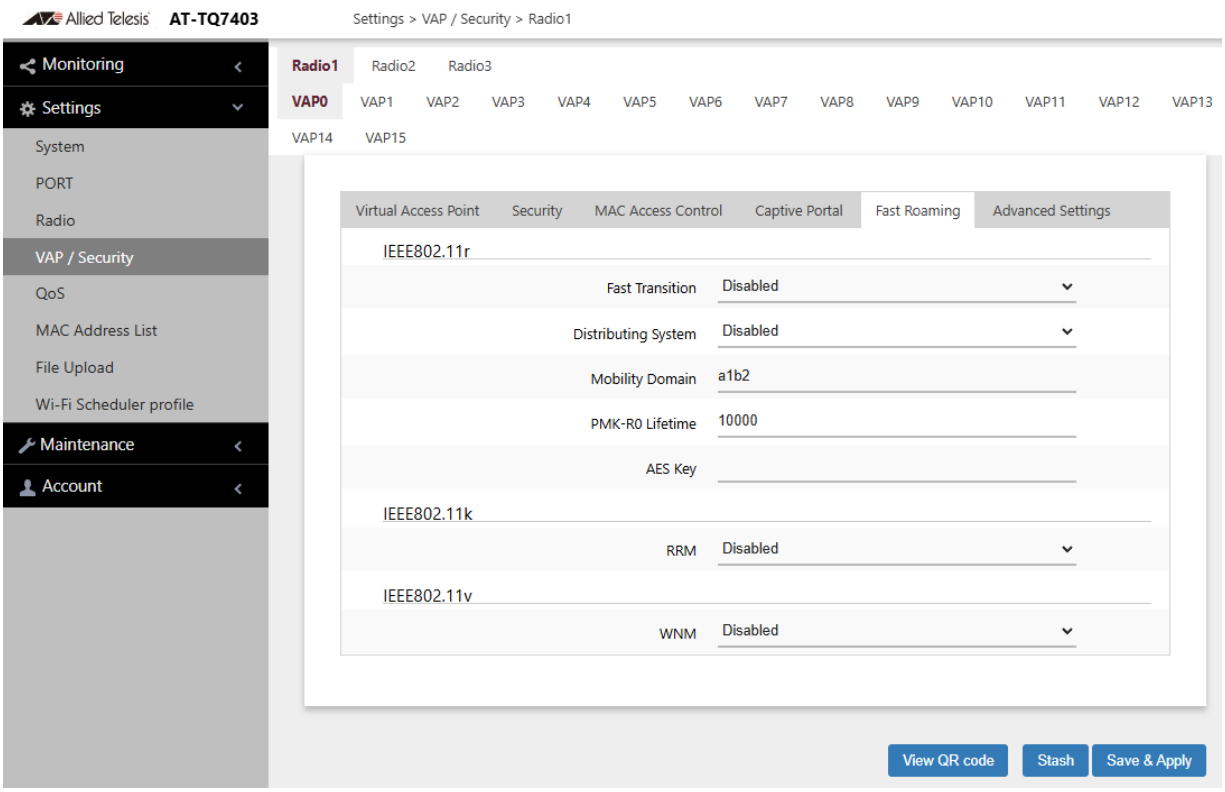

Figure 54. Fast Roaming Window

The parameters for IEEE802.11r are described in Table 32 on page 132.

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.

Note
You can set WPA Enterprise to the security mode and configure IEEE802.11r as Fast Foaming; however, IEEE802.11r can only be configured using AWC Plug-in.

Table 32. 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.
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.

The settings for Fast Roaming IEEE802.11k are:

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

The settings for Fast Roaming IEEE802.11v are:

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

Configuring A Key Holder List

The access point supports adding a Key Holder List for IEEE802.11k/v/r.

Here are the guidelines for configuring a Key Holder List:

- Passpoint must be Enabled to configure a Key Holder List.

  To enable Passpoint, see “Configuring Passpoint” on page 206.

To view the parameter values of the Key Holder List, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1**, **Radio2**, or **Radio3** from the sub-menu. The default is Radio1.
3. Select a VAP.The default is VAP0.
4. Select the **Fast Roaming** tab. See Figure 55 on page 133.

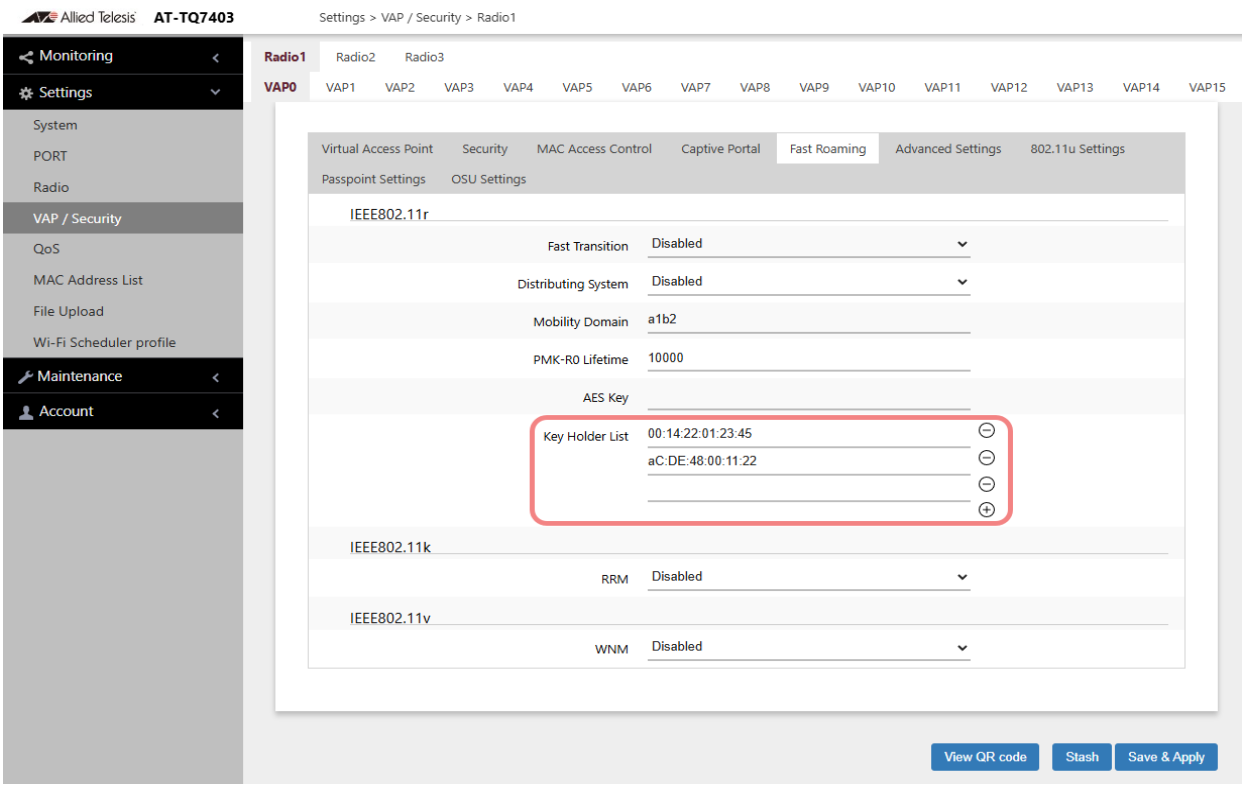

Figure 55. Fast Roaming Window - Key Holder List

The Key Holder List parameters for IEEE802.11r are described in Table 33 below.

Table 33. Key Holder List

Field	Description
Key Holder List	Up to 300 Access Points can be added to the Key Holder List. Enter the BSSID in the following format: XX:XX:XX:XX:XX:XX Letters can be upper or lower case. Use the "plus" button to add more entries and the "minus" button to delete entries. See the examples in Figure 55 on page 133.

Generating Quick Response (QR) Codes for VAPs

You can generate QR codes for the individual VAPs on the access point. Wireless clients can scan the QR codes to join the VAPs without having to manually enter the information.

Here are guidelines:

- Codes are generated by clicking the View QR code button in the VAP windows.
- QR codes are not supported on VAPs that use RADIUS servers to authenticate wireless clients.
- A radio has to be enabled for you to generate a QR code.

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

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. See Figure 43 on page 95 as an example.

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

   An example QR code is shown in Figure 56.

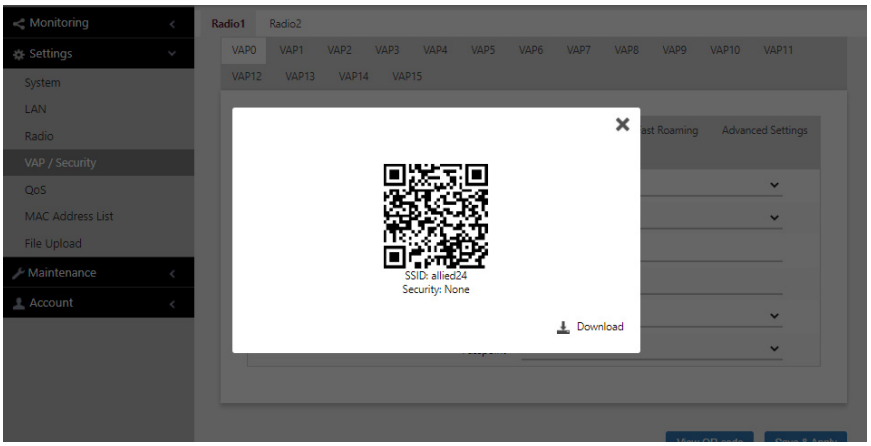

Figure 56. QR Code

6. Download the QR code. The QR code is ready to be used.

Chapter 7

Client MAC Address Authentication

This chapter contains procedures for configuring the access point to authenticate wireless clients by their MAC addresses. The chapter contains the following sections:

Introduction to MAC Address Authentication

The access point has several security tools for protecting your network from unauthorized access. The tools are primarily based on filtering clients based on their MAC addresses:

- MAC Address List: With this security feature, the access point authenticates wireless clients with its internal list of MAC addresses. You configure the list by entering the MAC addresses of the wireless clients that you want the access point is to either accept or reject. The access point has only one internal MAC address list.

  See “Authenticating Clients with the Internal MAC Address List” on page 138.

- External RADIUS server: The access point uses an external RADIUS server to authenticate the MAC addresses of its wireless clients. The access point either accepts or rejects clients based on the addresses you add to the server.

  See “Authenticating Clients with RADIUS Servers” on page 142.

- MAC Address + External RADIUS: This security option combines both the internal MAC address list and an external RADIUS server on your network to authenticate clients.

  See “Authenticating Clients with Both the MAC Address List and RADIUS Servers” on page 148.

- Area: When this security option is activated, wireless clients are authenticated based on their MAC addresses and physical locations in Channel Blankets or multi-channel VAPs. This authentication method requires Vista Manager and the AWC plug-in.

  See the *User Guide: Vista Manager AWC Plug-in*, found under Vista Manager EX Technical Documents in the documentation library.

- Application Proxy: The access point authenticates wireless clients with 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, and designate their network assignments by assigning them VLAN IDs.

  This feature requires AMF Security mini or the AMF Security Controller (AMF-SEC), and Vista Manager EX. It also requires the OpenFlow license on the access point. Application Proxy can only be configured using AWC Plug-in. See the *AMF Security mini User Guide* or *AMF Security Controller User Guide* for more information.

Authenticating Clients with the Internal MAC Address List

This section explains how to configure the access point to authenticate clients based on their MAC addresses, with its internal MAC address list. When a client tries to associate with a VAP, the access point checks the MAC address in the request with the addresses in the list. It either rejects or accepts the request, depending on the list status and whether the MAC address is in the list. Here are the guidelines:

- The access point has only one MAC address list.
- You can enable or disable MAC address authentication on the 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.
- The access point cannot authenticate broadcast or multicast addresses.

Here are the general steps:

- Add the MAC addresses of the clients that the access point is to accept or reject, in the MAC address list. Refer to “Configuring the MAC Address List” next.
- In the same window, specify whether the MAC addresses in the list are of clients to be accepted or rejected.
- Enable MAC address authentication. Refer to “Disabling MAC Address Authentication” on page 153.

Configuring the MAC Address List

To add or delete entries in the MAC address list, perform the following procedure:

1. Select **Settings** > **MAC Address List**. Refer to Figure 57.

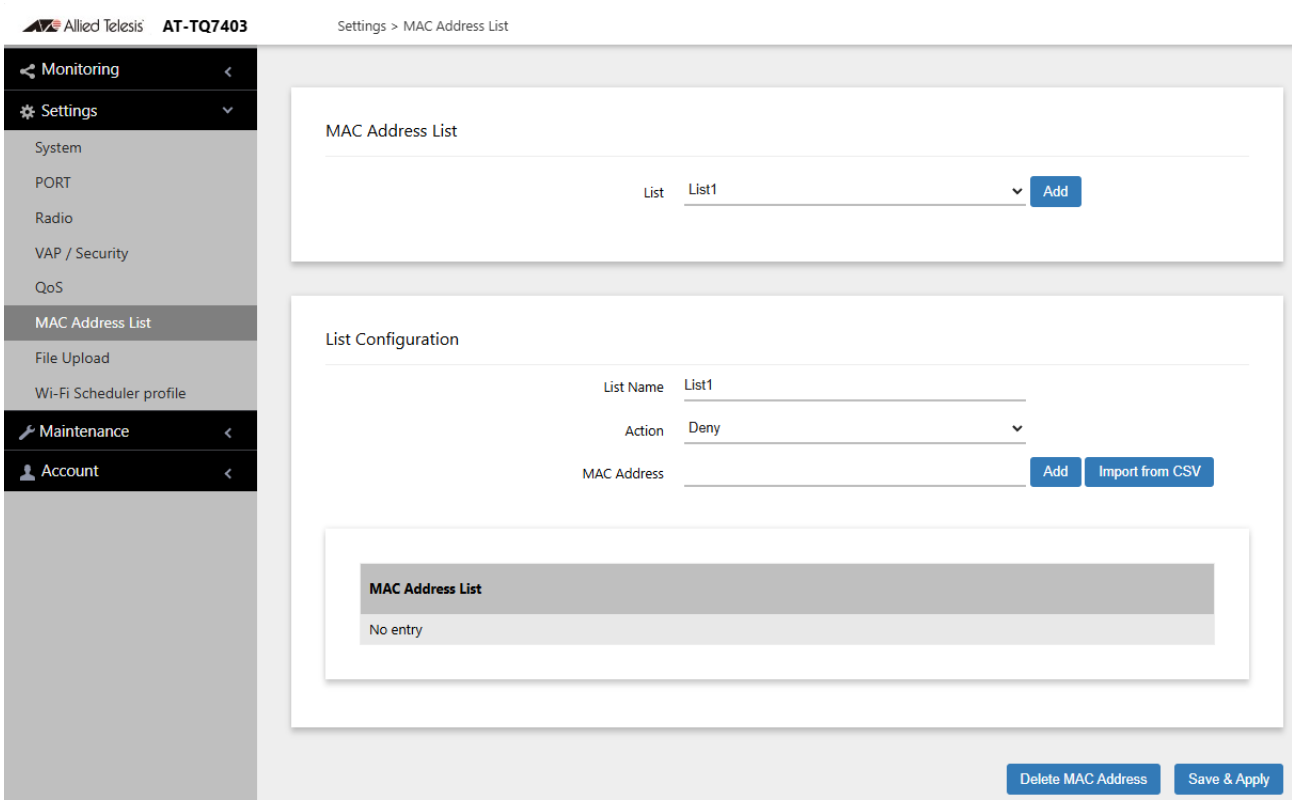

Figure 57. MAC Address List Window

2. In MAC Address List, from the **List** pull-dwn menu, select a list and cllick 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 list, 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 list, and to reject association requests from all other clients.

6. Enter the MAC addresses of the clients the access point is to reject or accept. There are two methods:

   - Click the **MAC Address** field and enter one MAC address in this format xx:xx:xx:xx:xx:xx and click the **Add** button. You can add only one address at a time.
   - Click the **Import from CSV** button to upload an .csv file, containing one or more MAC addresses in the format xx:xx:xx:xx:xx:xx. The addresses must be separated with a comma.

7. Click the **Add** button.

8. To remove addresses from the list, 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.

Enabling MAC Address Authentication with the Internal List

To enable MAC address authentication of the clients on a VAP, with the access point's internal MAC address list, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **MAC Access Control** tab.
5. Select **MAC Address List** from the MAC Access Control pull-down menu. See Figure 58 on page 141.

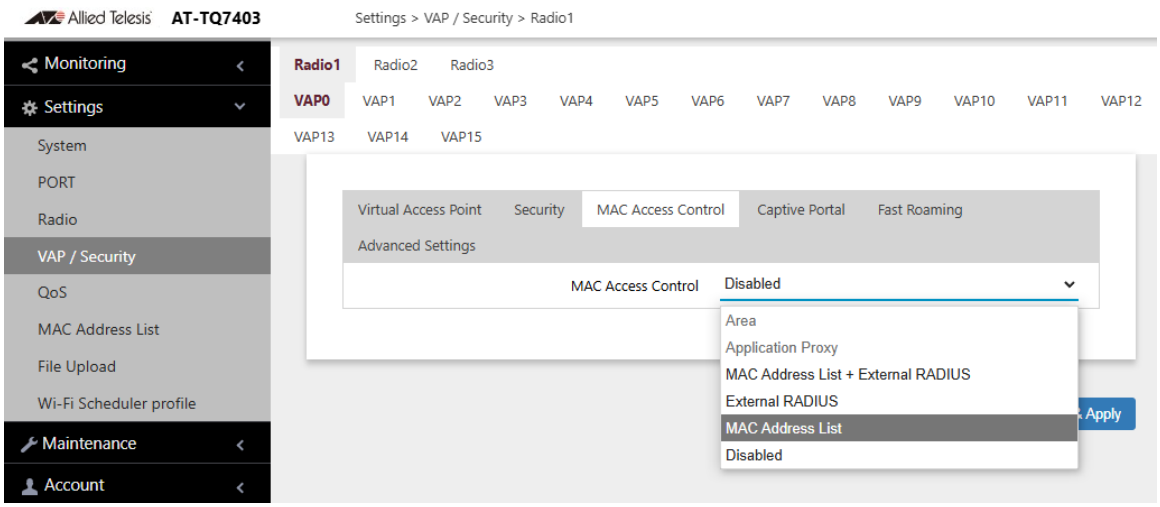

Figure 58. MAC Access Control - MAC Address List

6. From the MAC Address List pull-down, select a list.
7. See

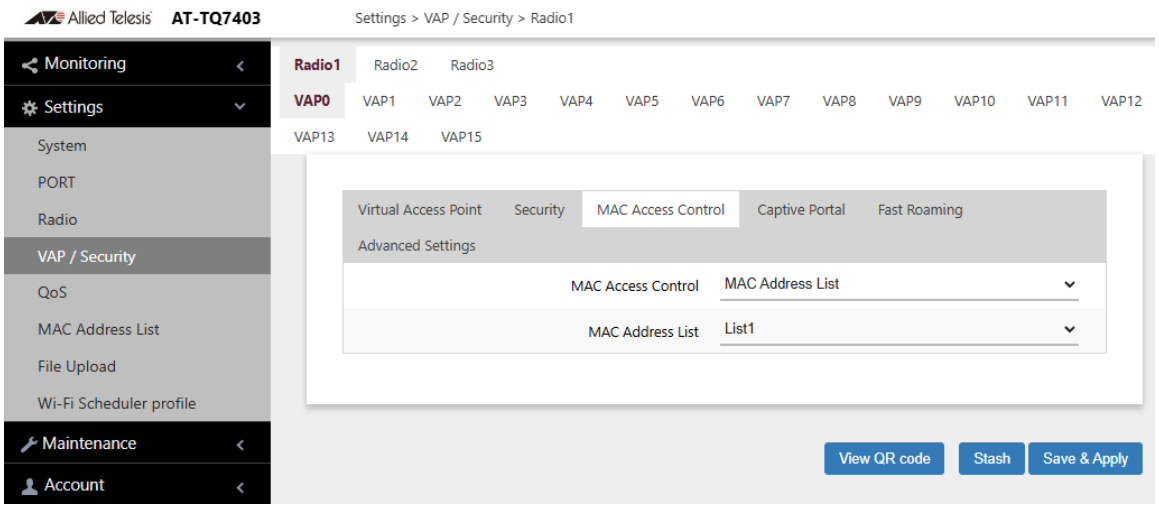

Figure 59. MAC Address List

8. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save all the changes later. MAC address authentication is now active on the VAP.

Authenticating Clients with RADIUS Servers

This section contains the procedures for configuring the access point to authenticate clients on VAPs with external RADIUS servers. The wireless clients are authenticated by their MAC addresses, which the access point sends to the server on the wired network when clients associate with it. You can specify both primary and secondary RADIUS servers.

Guidelines for Configuring the RADIUS Servers

Here are the guidelines to configuring the external RADIUS servers:

- Enter the MAC addresses of the wireless clients of the access point as user names. The MAC addresses function as the user-name attributes of the wireless clients.
- You can enter the addresses in the following formats:
  - Hyphen (nn-nn-nn-nn-nn-nn)
  - Colon (nn:nn:nn:nn:nn:nn)
  - None (nnnnnnnnnnnn)
- To identify the client passwords on the servers, you can use either their MAC addresses or a fixed password that all the clients share. The fixed password is case-sensitive.
- Letters in the MAC addresses should be either all uppercase or lowercase, not both.

Identifying the RADIUS Servers

To identify the RADIUS servers on the access point, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0.
4. Select the **MAC Access Control** tab.
5. Select **External RADIUS** from the MAC Access Control pull-down menu. Refer to Figure 60 on page 143.

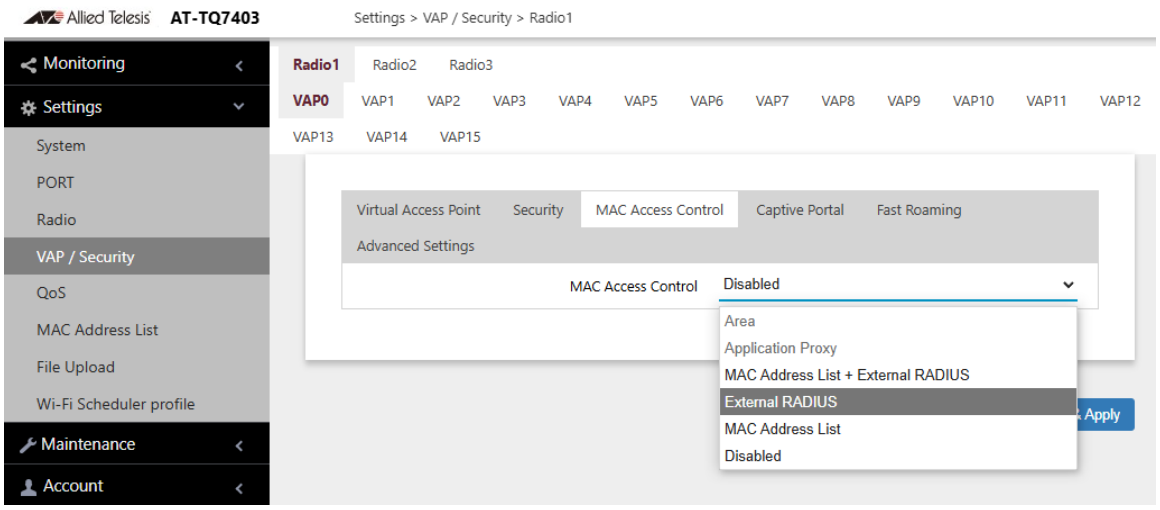

Figure 60. MAC Access Control - External RADIUS

6. Configure the parameters in the External RADIUS window, shown in Figure 61. The parameters are described in Table 34 on page 144.

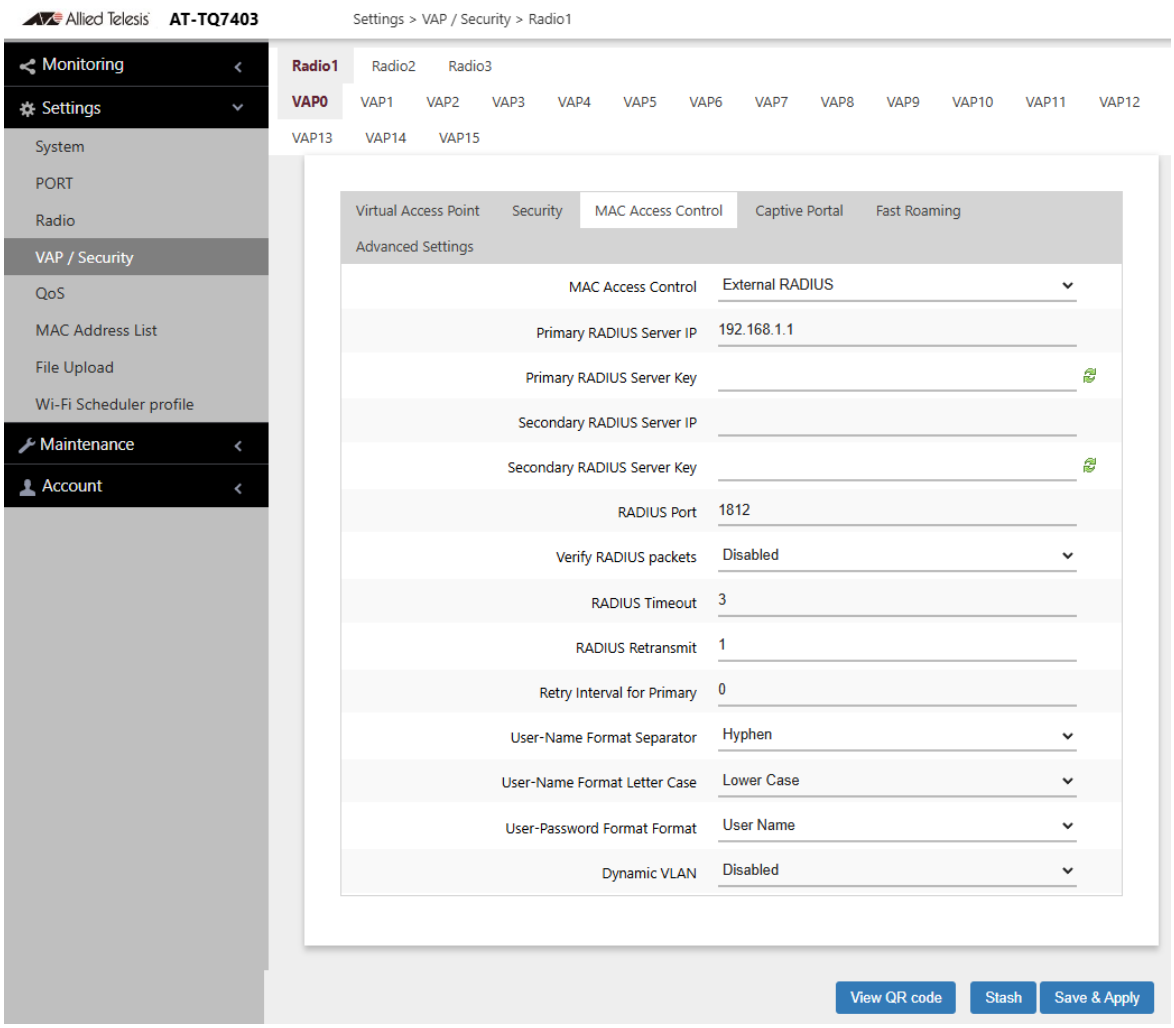

Figure 61. MAC Access Control - External RADIUS Window

Table 34. MAC Access Control - External RADIUS Window

Field	Description
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 of 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 34. MAC Access Control - External RADIUS Window (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 of 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 have 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.

Table 34. MAC Access Control - 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 then or equal to 29. - both Primary RADIUS and Secondary RADIUS, and the keys are the same, set the values such that “RADIUS Timeout” x “RADIUS Retransmit + 1” 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.
User-Name Format Separator	Select the character that separates the octets in the MAC addresses on the RADIUS servers. The choices are listed here: - Hyphen (nn-nn-nn-nn-nn-nn) - Colon (nn:nn:nn:nn:nn:nn) - None (nnnnnnnnnnnn)

Table 34. MAC Access Control - External RADIUS Window (Continued)

Field	Description
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.
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 all the changes later.

8. To generate a QR code, click **View QR code**.

Authenticating Clients with Both the MAC Address List and RADIUS Servers

This section contains the procedure for configuring the access point to authenticate wireless clients on VAPs using both its internal MAC address list and one or two external RADIUS servers. This is configured with the MAC Address List + External RADIUS option in the MAC Address Control tab.

The access point authenticates clients depending on the Allow or Deny setting of the internal MAC address filter, as follows:

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

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

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

General Steps

Here are the general steps to configuring the access point to authenticate wireless clients using both its internal MAC address list and an external RADIUS server:

1. On the RADIUS server, add the MAC addresses of the wireless clients as the user names of the clients. Refer to “Guidelines for Configuring the RADIUS Servers” on page 142.

2. On the access point, add the MAC addresses of the clients to be rejected or accepted, in its internal MAC address filter. Refer to “Configuring the MAC Address List” on page 138.

3. On the access point, identify the RADIUS servers by configuring the MAC Address List + External RADIUS Window. Refer to

Configuring the RADIUS Server Parameters

To identify the RADIUS servers the access point is to use to authenticate clients, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0.

4. Select the **MAC Access Control** tab. See Figure 64 on page 153.

5. Select the **MAC Address List + External RADIUS** option from the MAC Access Control pull-down menu. Refer to Figure 62.

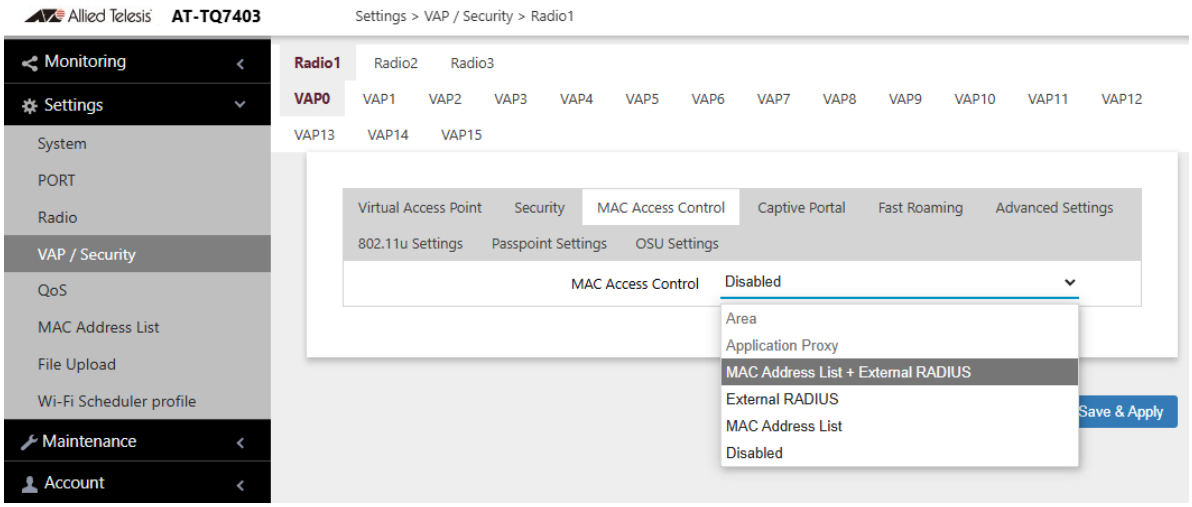

Figure 62. MAC Access Control - MAC Address List + External RADIUS

6. Configure the parameters in the MAC Address List + External RADIUS window, shown in Figure 63 on page 150.

   The parameters are described in Table 34 on page 144.

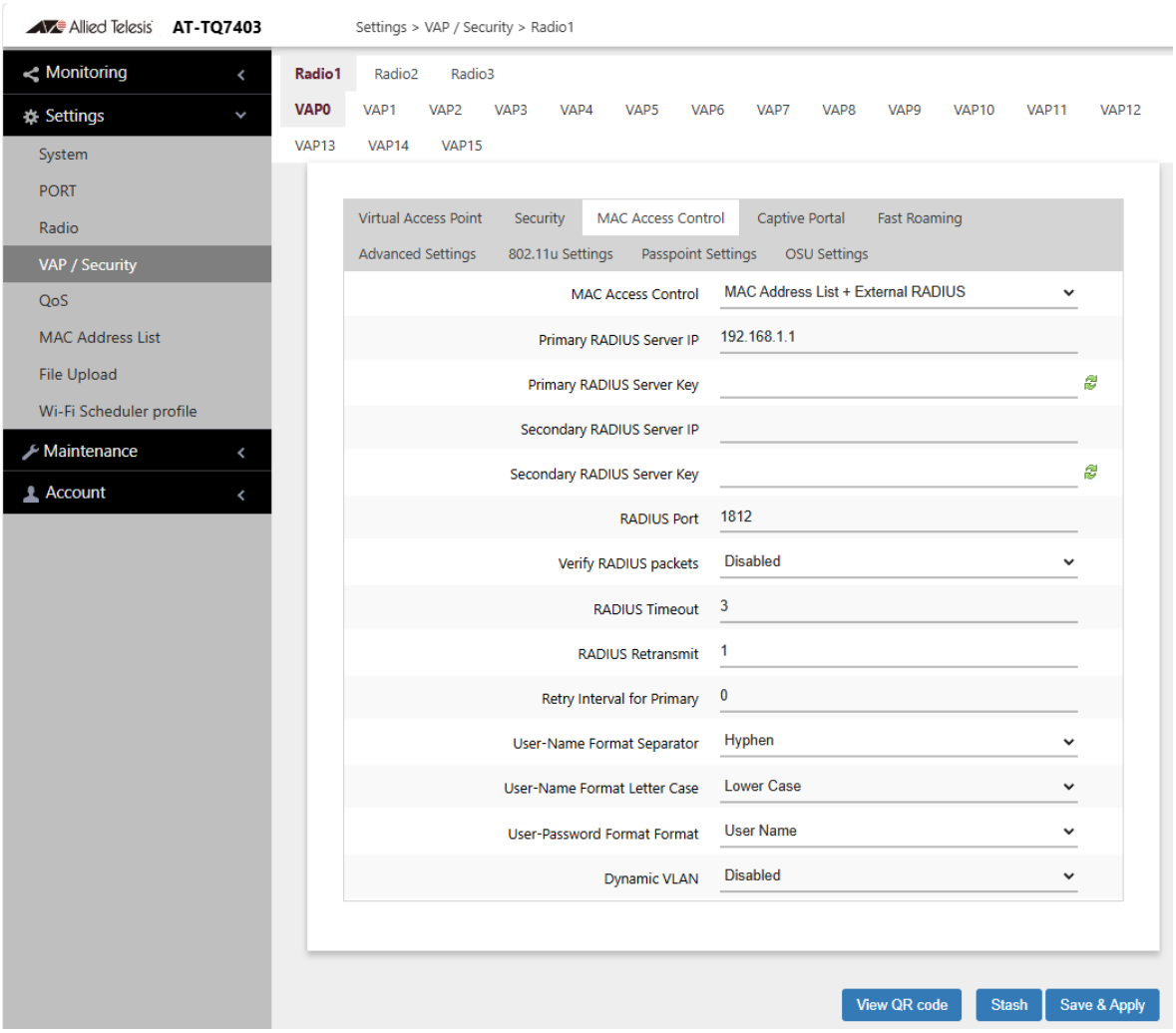

Figure 63. MAC Access Control - MAC Address List + External RADIUS Window

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

8. To generate a QR code, click **View QR code**.

Authenticating Clients by Area with the Vista Manager AWC Plug-in

Wireless networks that use channel blankets to improve wireless performance for roaming clients can add a layer of security with area authentication. This feature, which requires Vista Manager EX version 3.2.1 or later and the AWC plug-in, allows you to restrict access to your wireless network based on the physical locations and MAC addresses of clients.

The MAC Access Control pull-down menu in Mac Access Control tab has an Area selection, as shown in Figure 64 on page 153. However, the feature has to be configured with the AWC plug-in. Refer to the *Vista Manager AWC Plug-In User Guide* for configuration instructions.

Authenticating Clients with an Application Proxy

The MAC Address Control pull-down menu in the MAC Address Control tab has an Application Proxy selection. See Figure 64 on page 153. This option configures the access point to authenticate 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 wireless 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), and Vista Manager EX. Application Proxy can only be configured using AWC Plug-in. See the *AMF Security mini User Guide* or *AMF Security Controller User Guide* for further information.

Disabling MAC Address Authentication

To disable MAC address authentication on VAPs, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **MAC Access Control** tab.
5. Select **Disabled** from the pull-down menu to disable MAC address authentication on the VAP. See Figure 64.

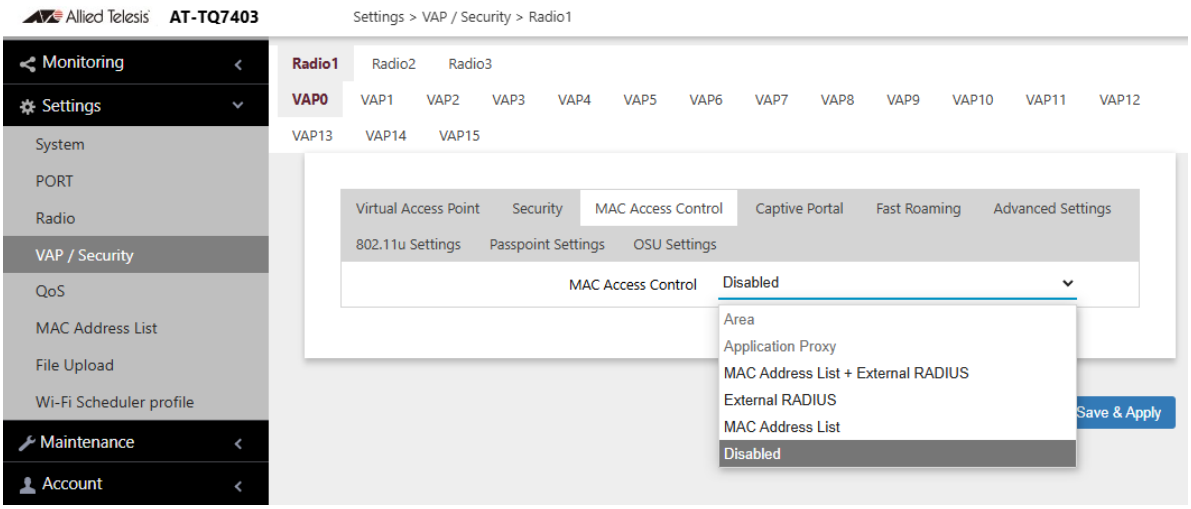

Figure 64. MAC Access Control Tab

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

Chapter 8

Captive Portals

This chapter contains the procedures for configuring Captive Portals on VAPs. As the following sections illustrate, you can configure Captive Portals with or without client authentication and with internal or external web hosting. The chapter contains the following sections:

Introduction to Captive Portals

Captive Portals are web pages 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 and provide information such as their email addresses, prior to allowing access to the networks.

You can configure Captive Portal in the following ways:

- “Disabling Captive Portals on VAPs” on page 175

  No authentication, allowing any wireless client to access to your networks. This is the default.

- “Creating VAPs that Display Introductory Web Pages” on page 156

  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 Server for Wireless Clients” on page 160

  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.

- “Authenticating Clients with RADIUS Servers, and Web Hosting with External URLs” on page 167

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

- “Authenticating Clients with RADIUS Servers, and Web Hosting with Proxy Servers” on page 169

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

- “Authenticating Clients with RADIUS Servers” on page 162

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

Creating VAPs that Display Introductory Web Pages

This procedure explains how to configure VAPs to display introductory web pages to associated clients, without authenticating them. For instance, the web page might contain a network policy or site restriction statement, and an Agree button for clients to click on. To configure VAPs, perform the following procedure:

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 to configure from the next sub-menu.
4. Select the **Captive Portal** tab.
5. Select **Click-Through** from the Captive Portal pull-down menu. See Figure 65.

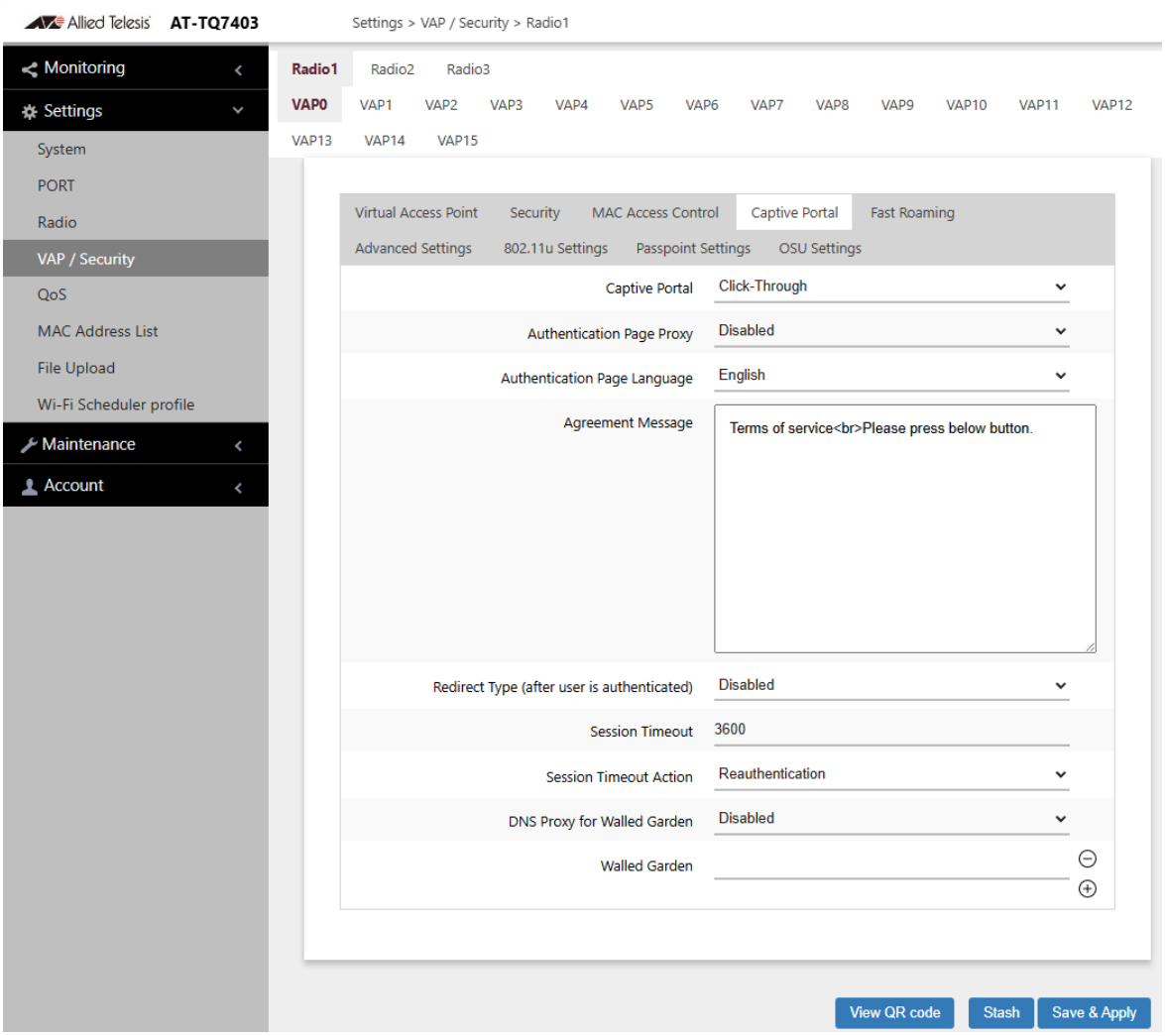

Figure 65. Capital Portal - Click-Through Window

6. Select **Disabled** from the Authentication Page Proxy pull-down menu.
7. Configure the parameters in Table 35.

Table 35. Captive Portal - Click-Through Window

Field	Description
Authentication Page Proxy	Enable or disable Authentication Page Proxy on the Captive Portal: - Enabled: The Captive Portal uses a web server's authentication page via proxy. See "Delegating a Proxy Server for Wireless Clients" on page 160. - Disabled: The Captive Portal uses its own local authentication page in the access point. This is the default setting.
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 as the introductory web page. The text can include HTML formatting and display codes. This field is only available when Authentication Page Proxy is disabled.
Base URL	Enter the URL for an introductory web page on another authentication page proxy server. See "Creating HTML Pages for Proxy Servers" on page 171. This field is only available 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. A welcome.html file that you prepare 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.

Table 35. Captive Portal - Click-Through Window (Continued)

Field	Description
Session Timeout	Specify the time interval in seconds for re-authenticating or disconnecting wireless clients. The default value is 3600 seconds (60 minutes).
Session Timeout Action	Specify the VAP action performed on clients after the session timeout is reached. The options are: - Reauthentication: Re-authenticates clients. This is the default setting. - Disconnection: Disconnects clients.
DNS Proxy for Walled Garden	Enables or disables DNS Proxy for Walled Garden. Disabled is the default.
Walled Garden	Enter the URLs of up to fifty approved HTTP web sites that wireless clients can access through the captive portals on the access point, without having to log on. Wireless clients who access only approved sites are not authenticated. Those who try to access unapproved web sites are shown to a logon window. The feature is supported on all radios, VAPs, and captive portals. 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 green add icon to the right of the last URL field. 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 all the changes later.

Delegating a Proxy Server for Wireless Clients

This procedure explains how to configure VAPs to display web pages on proxy servers to clients, without authentication. To configure the VAPs, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0.
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 66.

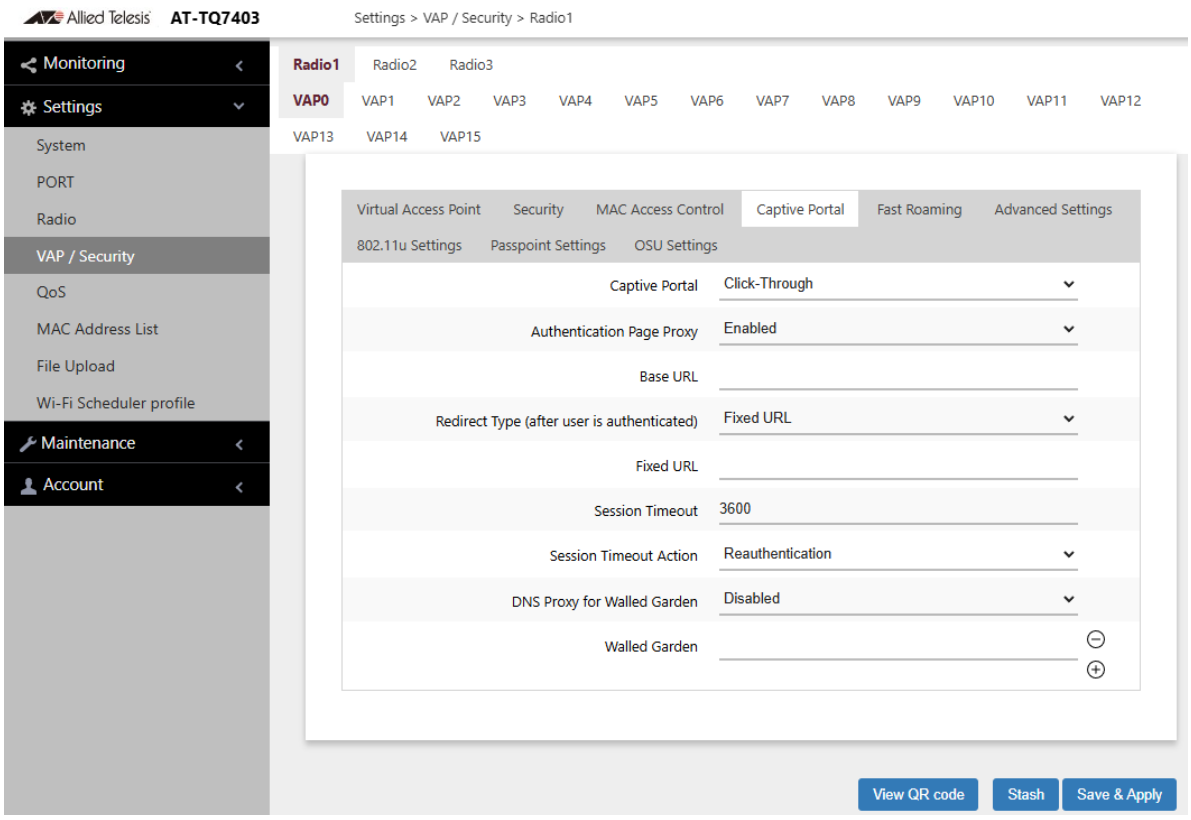

Figure 66. Capital Portal - Click-Through with Authentication Page Proxy Window

7. Specify the URL of your Page Proxy Server in the Base URL field.

8. Configure the remaining parameters by referring to Table 35 on page 158.
9. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save all the changes later.
10. Go to “Creating HTML Pages for Proxy Servers” on page 171.

Authenticating Clients with RADIUS Servers

This procedure explains how to configure VAPs to authenticate clients with RADIUS servers. It does not designate proxy servers to host web pages. To configure VAPs, perform the following procedure:

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 to configure from the next sub-menu.
4. Select the **Captive Portal** tab.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 67.
6. Select **Disabled** from the Authentication Page Proxy pull-down menu.

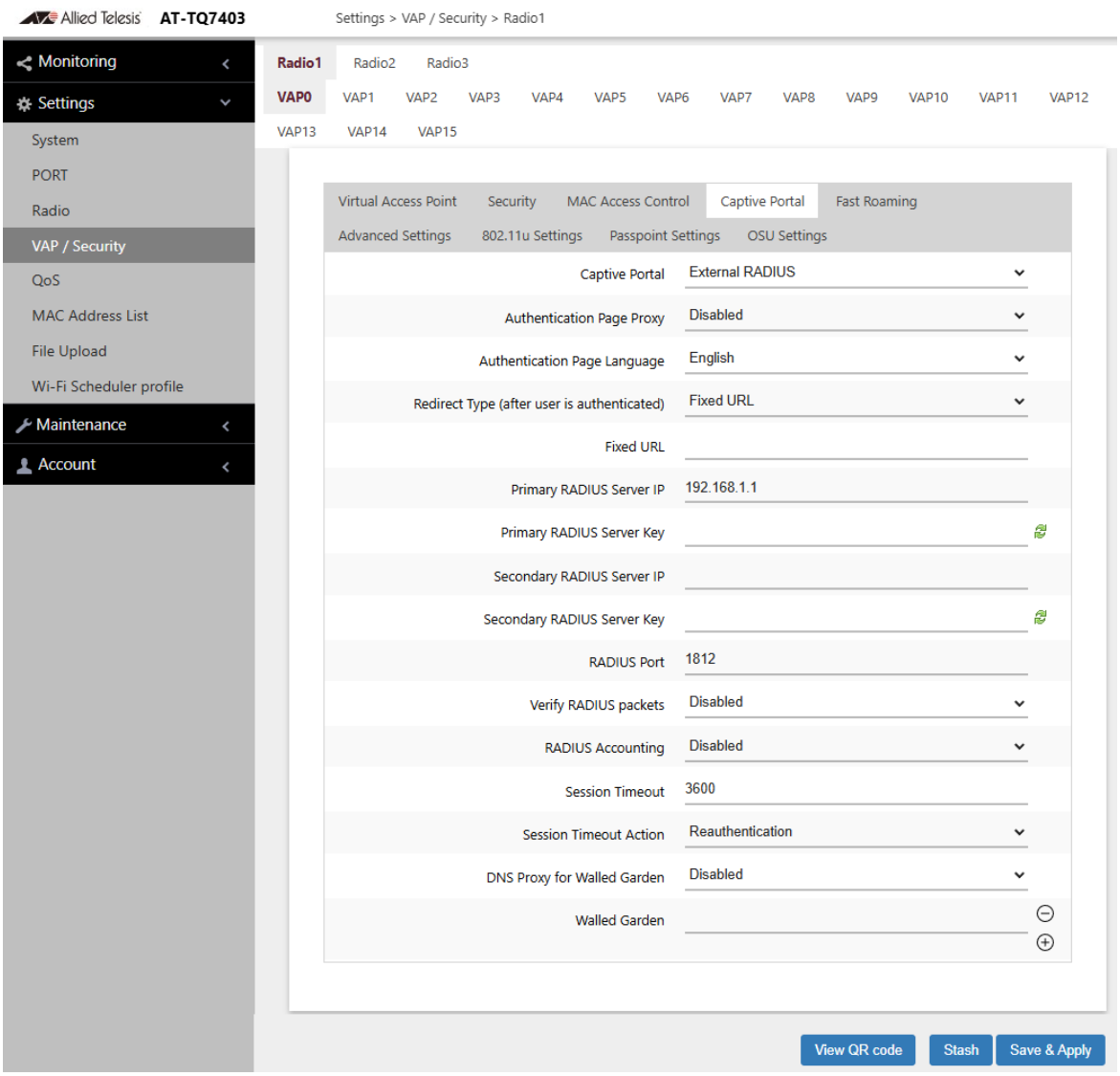

Figure 67. Capital Portal - RADIUS Authentication Window

7. Configure the parameters by referring to Table 36.

Table 36. Captive Portal - RADIUS Authentication Window

Field	Description
Authentication Page Proxy	Enable or disable Authentication Page Proxy on the Captive Portal: - Enabled: The Captive Portal uses a web server's authentication page via proxy. See "Delegating a Proxy Server for Wireless Clients" on page 160. - Disabled: The Captive Portal uses its own local authentication page in the access point. This is the default setting.
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.
Redirect Type (after user is authenticated)	Select the action to occur after 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 initially requested prior to associating with the VAP. - Disabled: Disables redirect. A welcome.html file that you prepare 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.

Table 36. Captive Portal - RADIUS Authentication Window (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 have 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 36. Captive Portal - RADIUS Authentication Window (Continued)

Field	Description
Session Timeout	Specify the time interval in seconds for re-authenticating or disconnecting wireless clients. The default value is 3600 seconds (60 minutes).
Session Timeout Action	Specify the action performed on clients after the session timeout is reached. The options are: - Reauthentication: Re-authenticates clients. This is the default setting. - Disconnection: Disconnects clients.
DNS Proxy for Walled Garden	Enables or disables DNS Proxy for Walled Garden. Disabled is the default.
Walled Garden	Enter the URLs of up to fifty approved HTTP web sites that wireless clients can access through the captive portals on the access point, without having to log on. Wireless clients who access only approved sites are not authenticated. Those who try to access unapproved web sites are shown to a logon window. The feature is supported on all radios, VAPs, and captive portals. 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 green add icon to the right of the last URL field. 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 all the changes later.

Authenticating Clients with RADIUS Servers, and Web Hosting with External URLs

This procedure explains how to configure VAPs to authenticate clients with external RADIUS servers and, once authenticated, redirect them to external web hosting URLs. To configure VAPs, perform the following procedure:

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 to configure from the next sub-menu.
4. Select the **Captive Portal** tab.
5. Select **External Page Redirect** from the Captive Portal pull-down menu. See Figure 68.

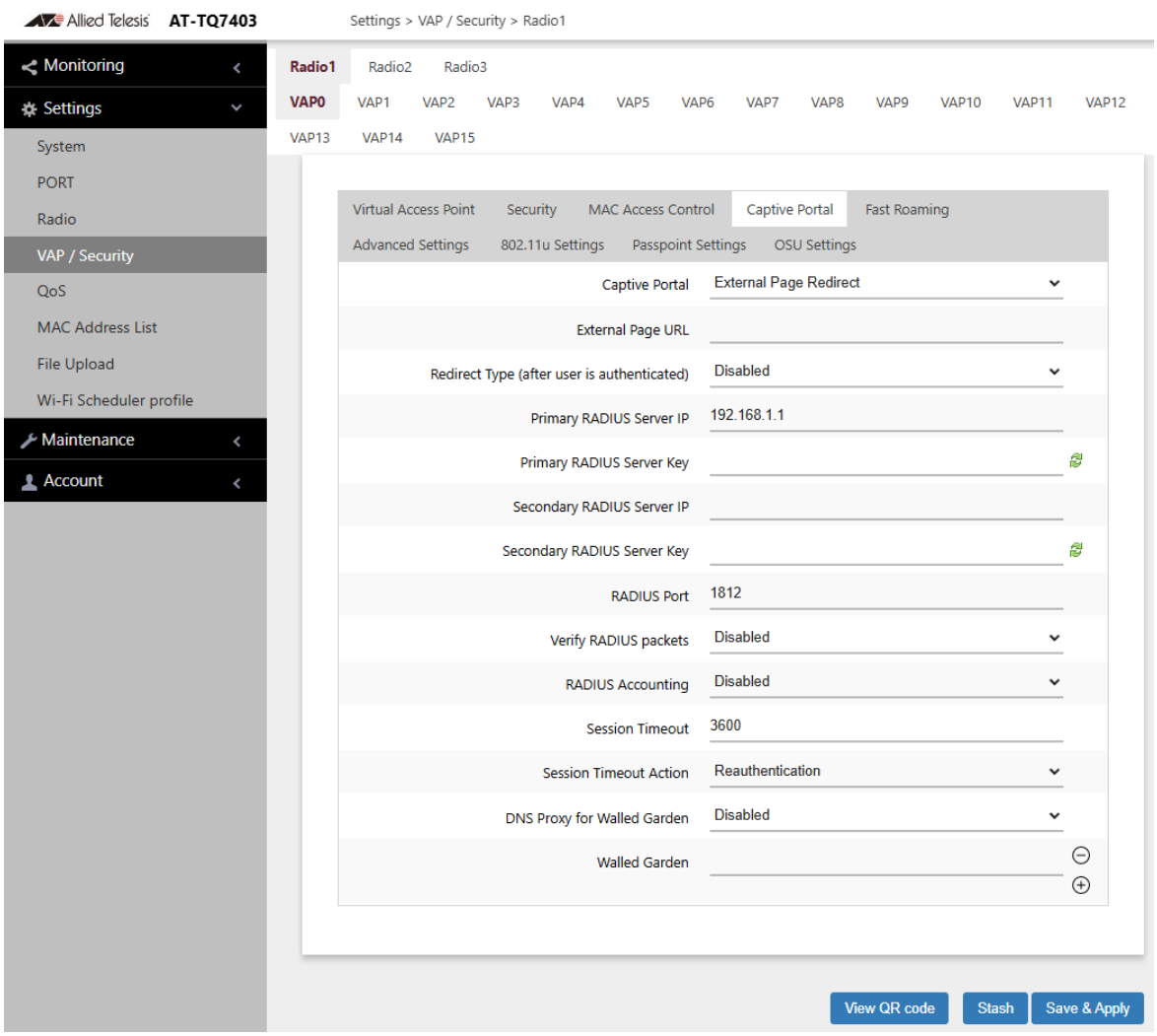

Figure 68. Capital Portal - RADIUS Authentication with External Page URL

6. In the **External Page URL** field, enter the URL to which wireless clients are directed after associating with the VAP. You can specify only one URL.

7. Configure the remaining parameters by referring to Table 36 on page 164.

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

Authenticating Clients with RADIUS Servers, and Web Hosting with Proxy Servers

This procedure explains how to configure VAPs to authenticate clients with RADIUS servers and direct them to web hosting pages on proxy servers. To configure VAPs, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0.
4. Select the **Captive Portal** tab.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 69 on page 170.
6. Select **Enabled** from the Authentication Page Proxy pull-down menu.

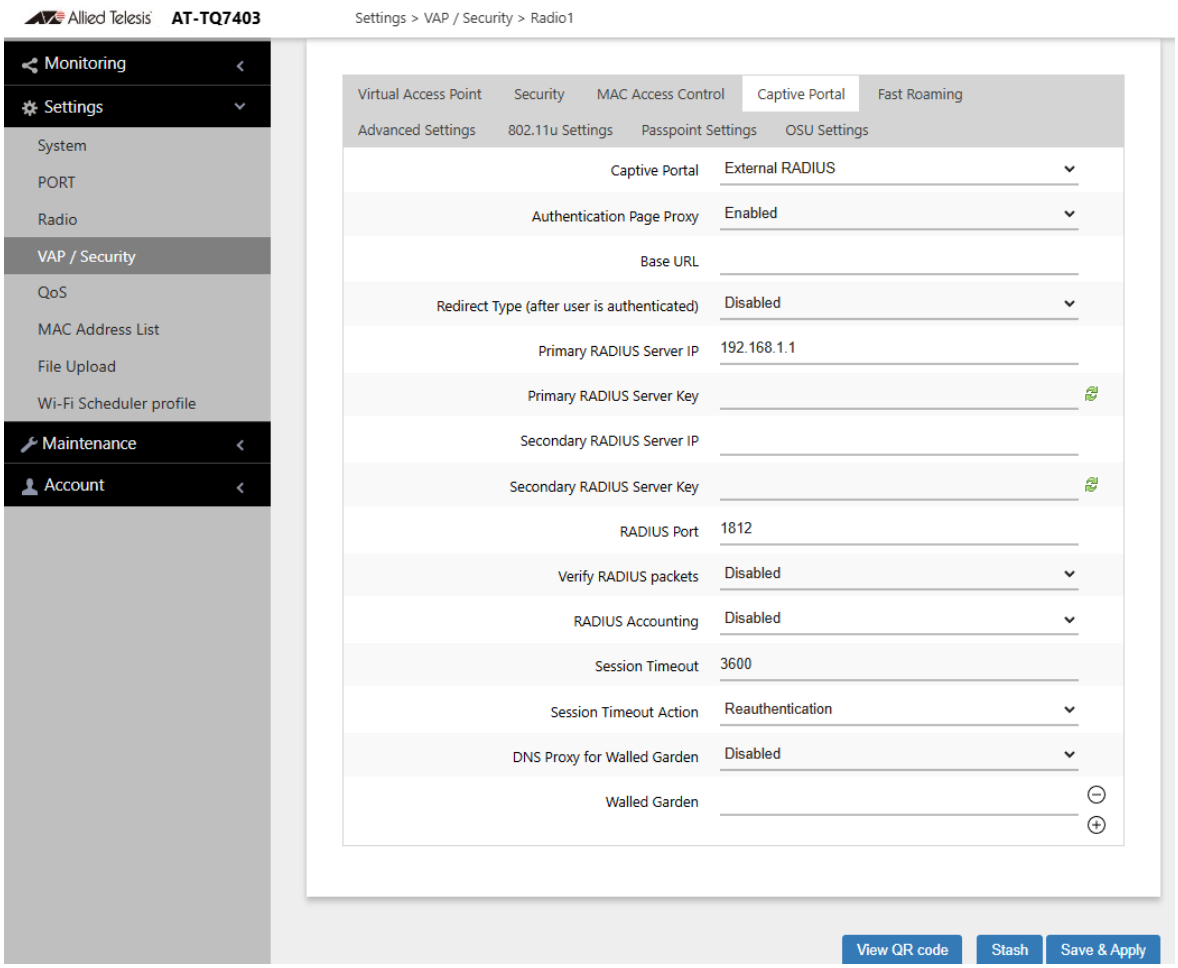

Figure 69. Capital Portal - RADIUS Authentication with Authentication Page Proxy

7. In the **Base URL** field, enter the URL for an introductory web page on an authentication page proxy server. See “Creating HTML Pages for Proxy Servers” on page 171. This field is only available when Authentication Page Proxy is enabled.

8. Configure the remaining table parameters by referring to Table 36 on page 164.

9. Click the **Save & Apply** button to save and update the configuration, or configure other VAPs and save all the changes later.

10. Go to “Creating HTML Login Pages to Authenticate Clients with RADIUS Servers” on page 173.

Creating HTML Pages for Proxy Servers

To host Captive Portals with proxy servers, you need to create the following HTML files on the servers:

- [*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 are the 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 70 on page 172 shows the web page in a web browser.

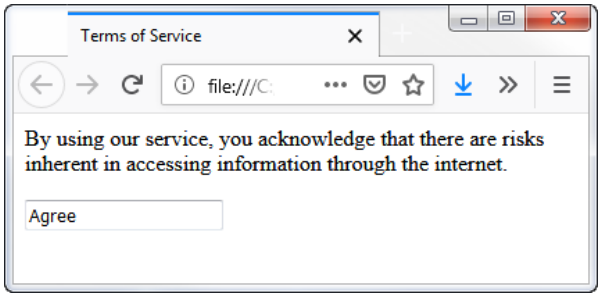

Figure 70. Captive Portal - Terms of Service Page Sample

Creating HTML Login Pages to Authenticate Clients with RADIUS Servers

To configure Captive Portals on VAPs to authenticate clients with RADIUS servers and to host web pages on proxy servers, you have to create the following HTML files on the servers:

- [*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 are 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 71 on page 174 shows the resulting web page.

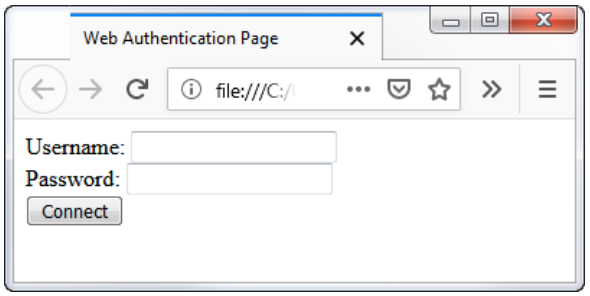

Figure 71. Captive Portal - Login Page Sample

Port Numbers

The following port numbers are used by 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]`

Disabling Captive Portals on VAPs

To disable Captive Portals on VAPs, perform the following procedure:

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 to configure from the next sub-menu. The default is VAP0.
4. Select the **Captive Portal** tab. See Figure 72.

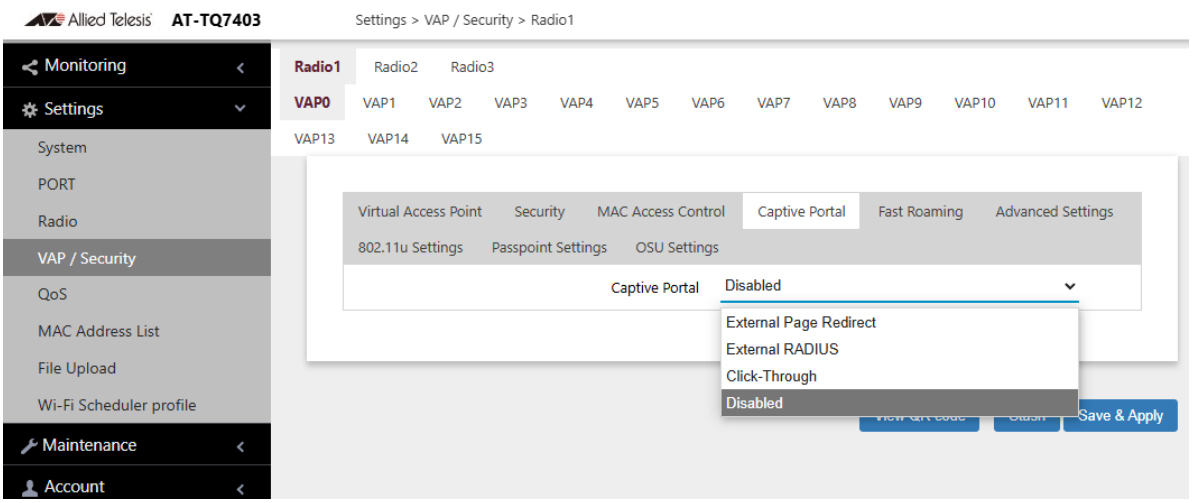

Figure 72. Capital Portal Window

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 all the changes later.

Chapter 9

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, **Radio**2, or **Radio3** from the sub-menu. You can configure only one radio at a time. Refer to Figure 73 on page 178.
3. Configure the QoS parameters by referring to the following sections:
   - “Configuring QoS Basic Settings” on page 179
   - “Configuring AP EDCA Parameters” on page 180
   - “Configuring Station EDCA Parameters” on page 183
4. Click the **Save & Apply** button to save and update your configuration.

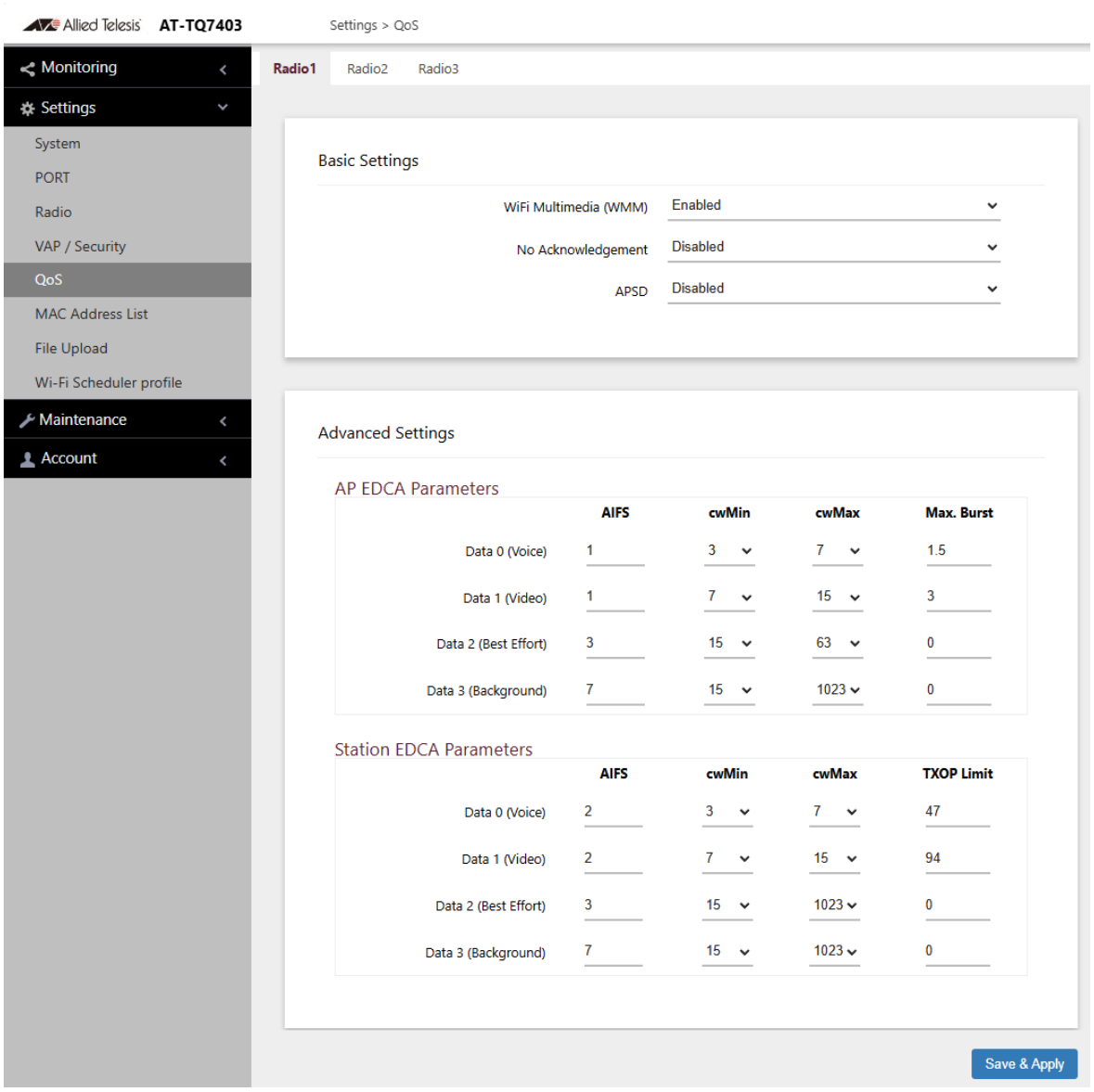

Figure 73. QoS Window

Configuring QoS Basic Settings

The fields for the Basic Settings section are defined in Table 37.

Table 37. 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 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 38 defines the AP EDCA parameters in the QoS window in Figure 73 on page 178.

Table 38. 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 38. 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 38. 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 39 defines the Station EDCA parameters in the QoS window in Figure 73 on page 178.

Table 39. 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 39. 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 39. 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 10

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. It allows units to forward traffic directly to each other over wireless connections, 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 port. 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 74.

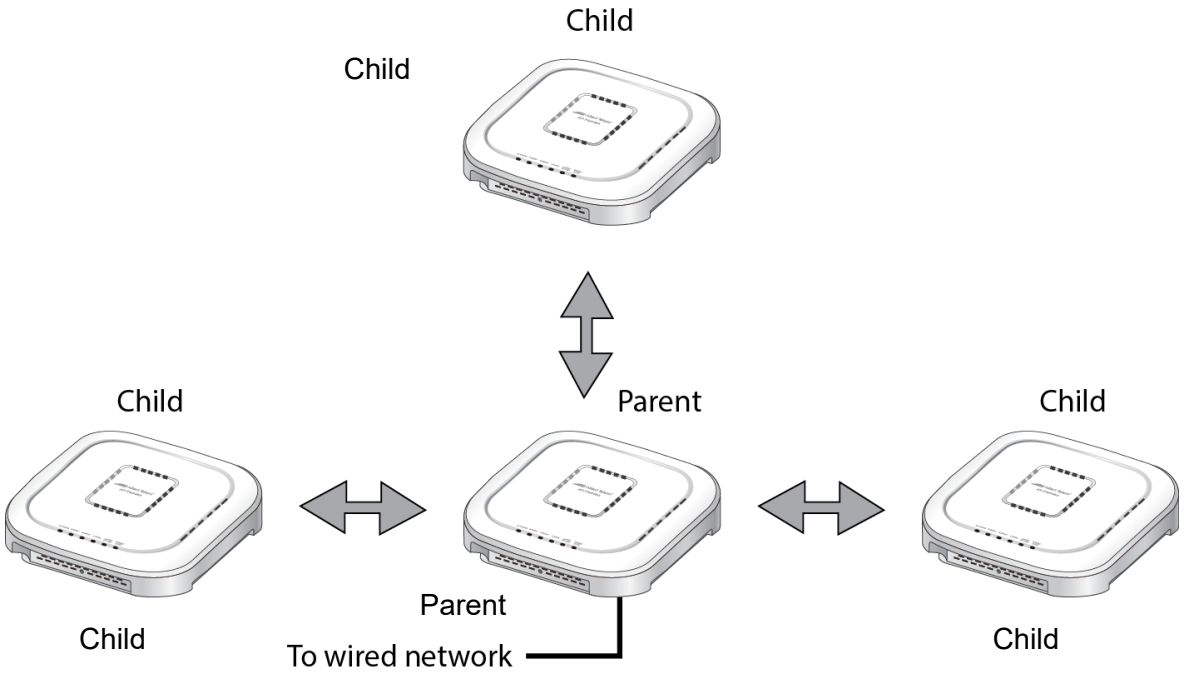

Figure 74. WDS Bridge

When a child receives traffic from a wireless client destined for the wired network, it transmits the traffic over the WDS bridge to the parent, which forwards the packets through the 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, Radio2, or Radio3 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 the other radio 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 75, the parent and children are using Radio2 and channel 40 for the WDS bridge. Wireless clients can access the network using Radio1.

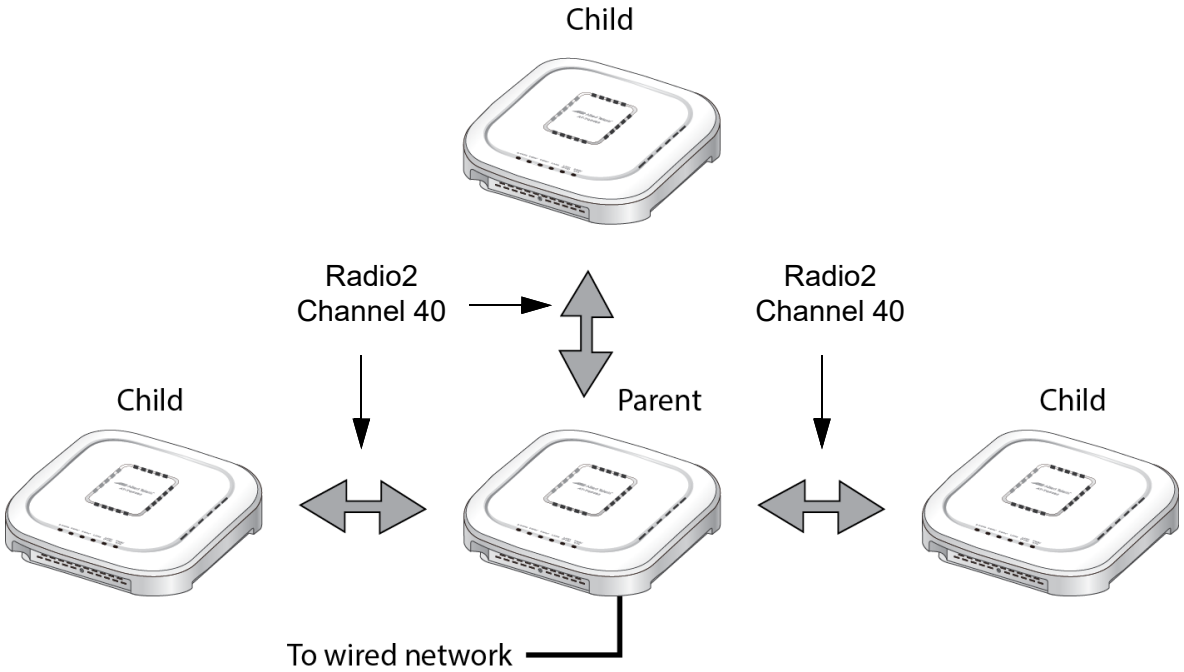

Figure 75. Example of Radio and Channel Assignments in a WDS Bridge

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 76 on page 189 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 Radio1 and channel 10 for their WDS bridge. In contrast, Access Point B and its children are using Radio2 and channel 40.

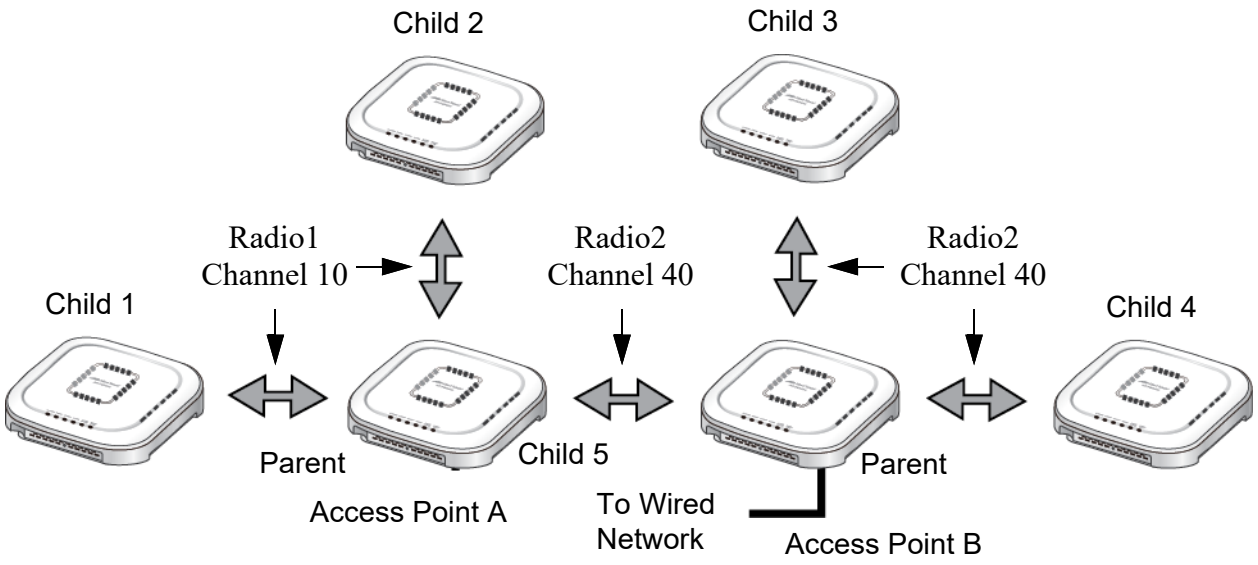

Figure 76. Example of an Access Point as Both Parent and Child

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

Here are the guidelines for the WDS bridge:

- ❒ You can use Radio1, Radio2, or Radio3 for the WDS bridge.
- ❒ 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 74 on page 187.

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 when they detect 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 and 6GHz radios.

Guidelines for WDS Bridges

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 port on the parent is connected to the wired network.
- If two WDS bridges are connected together, as shown in Figure 76 on page 189, you should connect the LAN port 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, Radio2, or Radio3 for the WDS bridge.
- You can use None security or WPA Personal for VAP0 on the selected radio of the bridge. Allied Telesis recommends using WPA Personal for security.
- A WDS bridge must consist of all TQ7403 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 Radio2 for the bridge, Allied Telesis recommends selecting a channel that is not part of dynamic frequency selection (DFS). This is to minimize the chance that the access point 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 the children.
- ❒ You have chosen the radio that the access points will use for the bridges. It can be Radio1, Radio2, or Radio3.
- ❒ 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 for 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.

   See “Configuring Basic Radio Settings” on page 71.

   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, See “Assigning No Security to VAPs” on page 98 or “Configuring WPA Personal Security” on page 106.
4. Select **Settings** > **VAP / Security**.
5. Choose the radio for the WDS bridge by selecting **Radio1**, **Radio2,** or **Radio3** 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 selected 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 35.

Chapter 11

802.11u, Passpoint & OSU

This chapter contains the procedures for configuring 802.11u, Passpoint and OSU. The chapter contains the following sections:

Configuring 802.11u Settings

This section explains how to configure 802.11u for WiFi Certified Passpoint on captive portals. To configure the 802.11u Settings tab, perform the following procedure:

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 to configure for the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **802.11u Settings** tab. See Figure 77 on page 197 and Figure 78 on page 198 which show the Basic and Advanced settings.
5. Configure the fields by referring to Table 41 on page 202.

Note
The table provides a brief description of the fields in the 802.11u Settings tab. For detailed information, refer to *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.*

6. After configuring the tab, click the **Save & Apply** button to save and update the configuration.

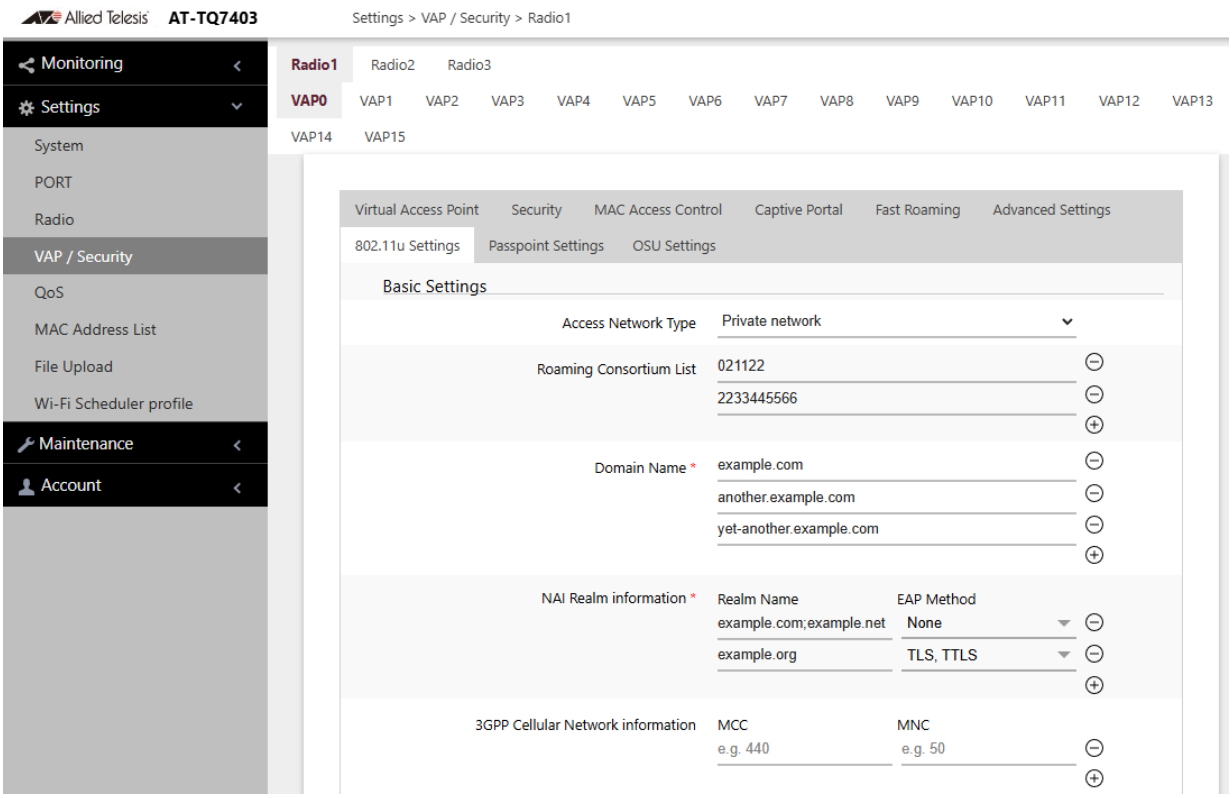

Figure 77. 802.11u Basic Settings

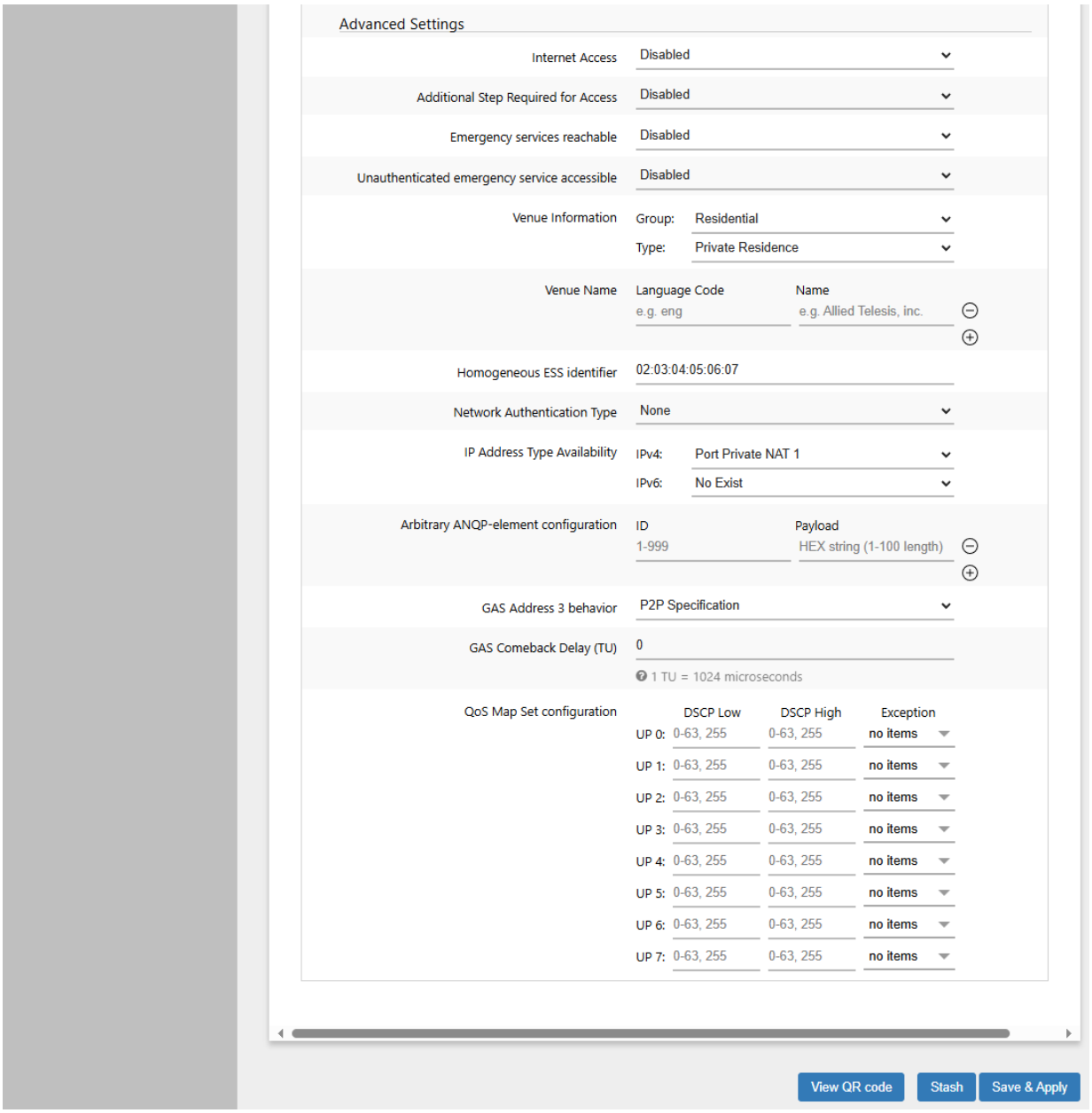

Figure 78. 802.11u Advanced Settings

Table 40. 802.11u Basic Settings

Parameter	Description
Access Network Type	Specifies the access network type ID. 0: Private network – Networks restricted to authorized users only. This is the default. Examples include private or enterprise networks that employ user accounts. Private networks may or may not employ encryption. 1: Guest accessible private network – Private networks that permit temporary access by unauthenticated users. Example includes enterprise networks with guest users. 2: Billing system public network – Public networks accessible to users by paying a fee. Example includes hotel room networks. 3: Free public network – Public networks accessible to all users, without paying a fee. Examples include hotspots at airports and hospitals, and networks provided by cities. 4: Personal device network – Networks for personal devices. Examples include home networks that interconnect personal computers, printers, and wireless access points. 5: Network provided by emergency services – Networks restricted to emergency services. Examples include networks for handling emergency police or firefighting calls, or for transmitting emergency alerts. 14: Test or experimental – Test or experimental networks. Examples include networks at research and development laboratories. 15: Wildcard – Wildcard access networks.

Table 40. 802.11u Basic Settings (Continued)

Parameter	Description
Roaming Consortium List	Specify the roaming consortium list by Organization Identifiers (OI). The default is blank. Here are the guidelines: ❒ OIs have to be in hexadecimal. ❒ You can add up to 16 identifiers. ❒ Separate multiple OIs with a colon ";". Example: 337135;021122 ❒ OIs must have a minimum of six characters. For OIs with less than six characters, add leading zeros (0). Example: 002122 ❒ OIs must have an even number of characters. For OIs with odd numbers of characters, add a leading zero. Example: 054385
Domain Name	Specifies the domain name in for certificate. When specifying multiple domains, separate them with commas ",". The default is blank.

Table 40. 802.11u Basic Settings (Continued)

Parameter	Description
NAI Realm information	NAI (Network Access Identifier) Realm information is specified in the following format. <Encoding>,<NAI Realm(s)>[,<EAP Method >][,<EAP Method 2>][,...] Encoding Encoding | Explanation 0- NAI Realm written in a format that conforms to IETF RFC 4282. 1 - UTF8 Encodes NAI Realm in a format that does not conform to IETF RFC 4282. NAI Realm(s): NAI Realm separated by semicolons. EAP Method: <EAP Method types>[:<[AuthParam1:Val1]>] [<[AuthParam2:Val2]>][...] Example) 21[2:4][5:7] = Username/Password certification using EAP-TTLS/MSCHAPv2 • EAP Method types: Specify EAP Method types. • AuthParamX, ValY: Auth Param | Val | Authorize Type 2 | 4 | MSCHAPv2. 5 | 7 | UserName/Password authentication. 5 | 6 | Certificate authentication. Example: 0,example.org;example.net,13[5:6],21[2:4][5:7] The default is blank.

Table 40. 802.11u Basic Settings (Continued)

Parameter	Description
3GPP Cellular Network information	Specifies the 802.11u 3rd Generation Partnership Project (3GPP) Cellular Network Code. To enter multiple codes, separate them with colons ";". The default is blank. Here is the format: <MCC1,MNC1>[;<MCC2,MNC2>][;...] ❒ MCC (Mobile Community Code): Specify Country Code (three digits). In Japan it is 440. ❒ MNC (Mobile Network Code): Specify Career Mobile Network Code (two or three digits). Example: [440,XX;440,XX] (XX is Mobile Network Code)

Table 41. 802.11u Advanced Settings

Parameter	Description
Internet Access	Controls whether the VAP permits access to the Internet. Here are the settings: - Enabled: The VAP permits access to the Internet. - Disabled: The VAP does not specify whether it permits access to the Internet. This is the default.
Additional Step Required for Access	Controls whether an additional step is required by the VAP before allowing access. Here are the settings: - Enabled: The VAP specifies that an additional step is required. - Disabled: The VAP does not specify whether an additional step is required. This is the default.
Emergency services reachable	Controls whether the VAP can supply access to higher layer authenticated emergency services. Here are the settings: - Enabled: The VAP can provide access to emergency services. - Disabled: The VAP cannot provide access to emergency services. This is the default.

Table 41. 802.11u Advanced Settings (Continued)

Parameter	Description
Unauthenticated emergency service accessible	Controls whether the VAP can supply access to unauthenticated individuals to emergency services. Here are the settings: - Enabled: The VAP can provide access to unauthenticated individuals to emergency services. - Disabled: The VAP cannot provide access to emergency services. This is the default.
Venue 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.
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.
Arbitrary ANQP-element configuration	Specifies the Access Network Query Protocol (ANQP). Specified when there is an additional designation of Access Network Query Protocol (ANQP)-element. Use the "plus" button to add more entries. - ID: Specify the ID (1-999). The default is blank. - Payload: Specify ANQP payload with 100 characters or less. The default is blank.

Table 41. 802.11u Advanced Settings (Continued)

Parameter	Description
GAS Address 3 behavior	The Generic Advertisement Service (GAS) address setting is in the range of 0~2. Number | Explanation 0 (P2P specification) | When the BSSID included in a GAS Initial request packet is a wildcard BSSID (FF:FF:FF:FF:FF:FF) and the destination MAC address is "Multi cast address and Client not Association" or "Broad cast address", respond using the wildcard BSSID(FF:FF:FF:FF:FF:FF). In all other cases, respond using wireless AP BSSID. 1 (IEEE 802.11 standard) | When the destination MAC address is "Multi cast address and Client not Association" or "Broad cast address", respond using the wildcard BSSID(FF:FF:FF:FF:FF:FF). In all other cases, respond using the wWireless AP BSSID. 2 (Force non-compliant behavior) | In all other conditions, respond with the BSSID of the wireless AP. The default is 0.
GAS Comeback Delay	Specifies the GAS Comeback Time. The range is 0-65535TU (1TU=1024msec). The default is 0.

Table 41. 802.11u Advanced Settings (Continued)

Parameter	Description
QoS Map Set configuration	QoS Map Setting is specified in the following format. Arrange the DSCP exception (DSCP value and user priority value pairs) 0-21 pieces and DSCP range (start DSCP value and end DSCP value pairs) corresponding to user priority 0-7. Arrange them separated by commas. - Specify the DSCP value in the range of 0 to 63 or 255. - If the DSCP range is "255,255", the user priority is not used. Example: If you set the “DSCP range” corresponding to two DSCP exceptions and user priority (UP) 0-7 to the setting values in the following table, the specified value of the QOSMAP 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.

Configuring Passpoint

This feature 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 Passpoint and Hotspot 2.0 services through the wireless access points. The feature is available on all radios, VAPs, and captive portals.

Enabling Passpoint

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

To enable Passpoint, perform the following procedure:

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 to configure from the next sub-menu.

   The default is VAP0. You can configure only one VAP at a time.

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

4. In the **Virtual Access Point** tab, enable Passpoint. See Figure 79 on page 207.

   The **802.11u, Settings**, **Passpoint Settings** and **OSU Settings** tabs will now be visible.
5. Click the **Save & Apply** button to save and update the configuration, or click **View QR code** to generate a QR Code.

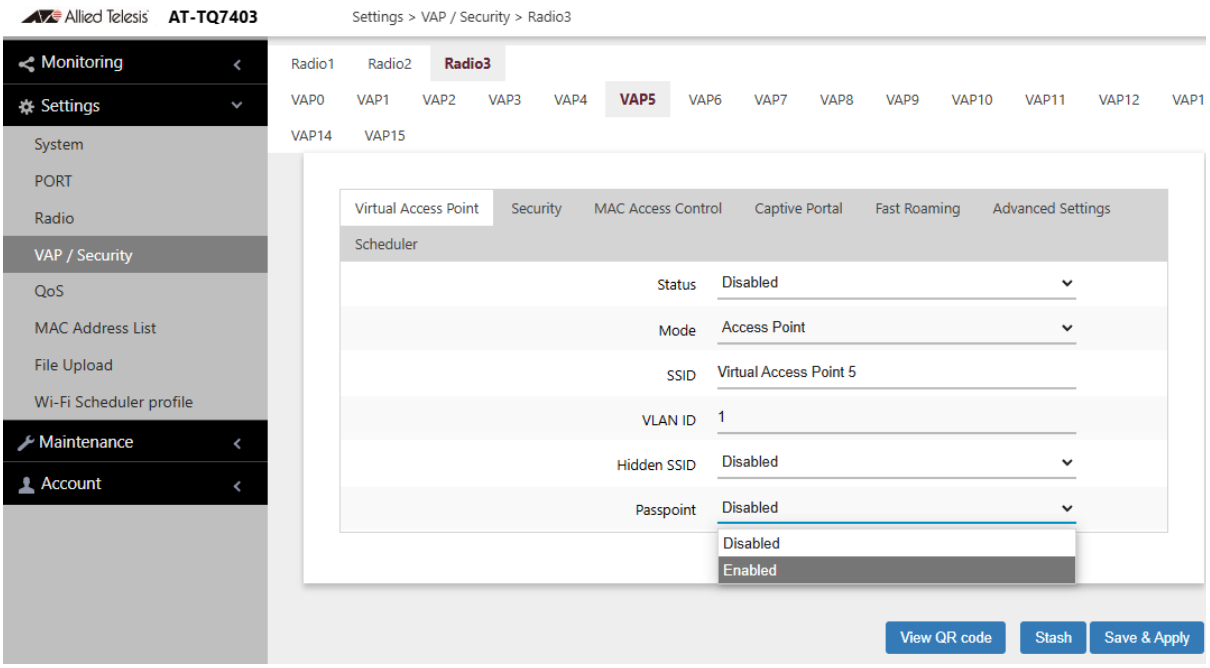

Figure 79. Enable/Disable Passpoint

Configuring Passpoint

To configure Passpoint perform the following:

1. Select the **Passpoint Settings** tab. See Figure 80 on page 208.
2. Configure the fields by referring to Table 42 on page 208.
3. Click the **Save & Apply** button to save and update the configuration, or click **View QR code** to generate a QR Code.

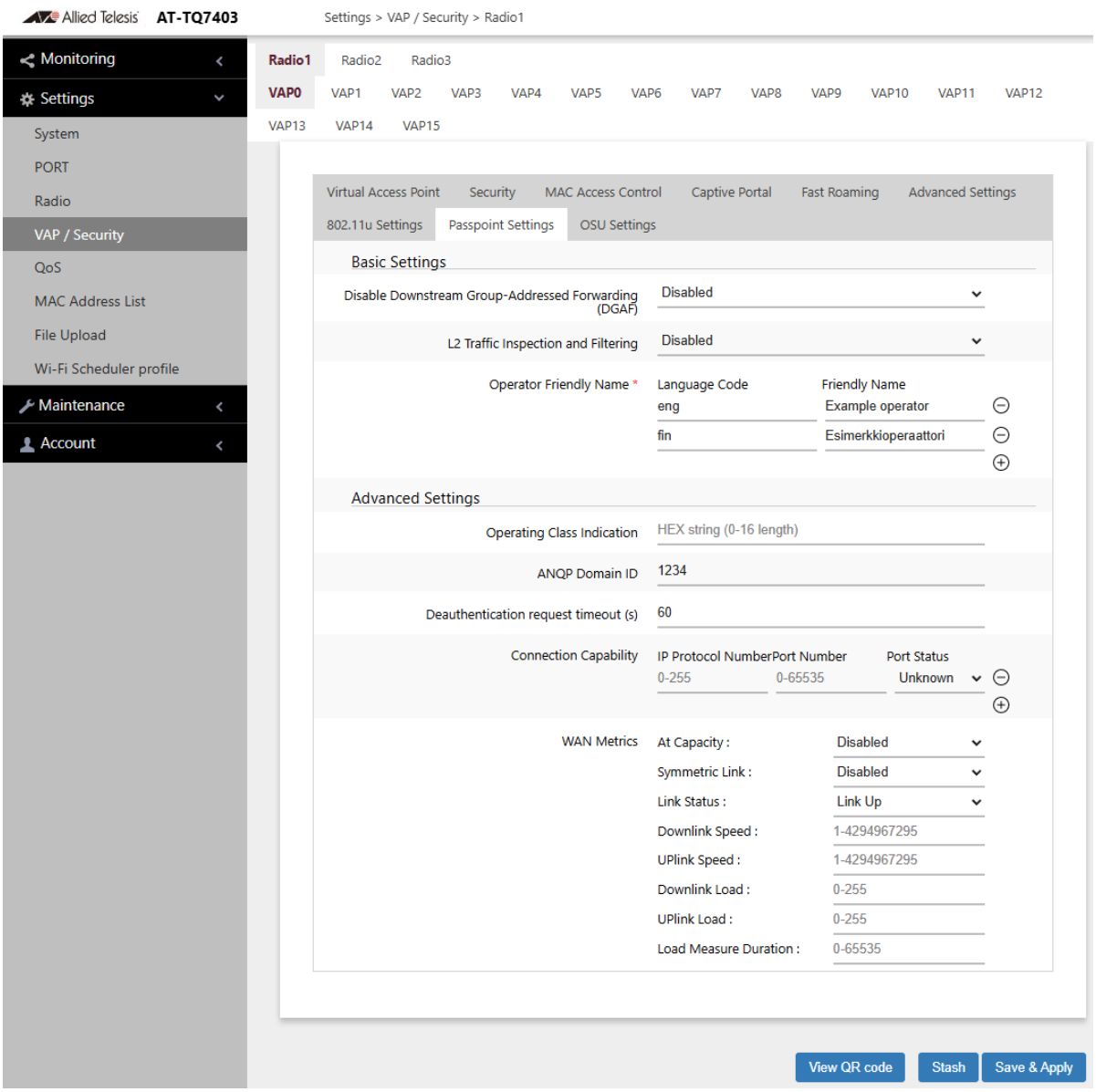

Figure 80. Passpoint Settings

Table 42: Passpoint Settings

Parameter	Description
Disable Downstream Group-Addressed Forwarding (DGAF)	Enables or disables sending of multicast and broadcast frames: - Enabled: Does not send multicast and broadcast - Disabled frames: Sends multicast and broadcast frames. This is the default.

Table 42: Passpoint Settings

Parameter	Description
L2 Traffic Inspection and Filtering	Enables or disables traffic between VAPs Layer 2 traffic (ARP, ICMP, TDLS). - Enabled: Discards Layer 2 traffic (ARP, ICMP, TDLS) between VAPs. - Disabled: Does not discard Layer 2 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".
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.

Table 42: Passpoint Settings

Parameter	Description
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.
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.

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 enable Passpoint, see “Enabling Passpoint” on page 206.

To configure the OSU settings, perform the following procedure:

1. Select the **OSU Settings** tab and enable OSU Status. See Figure 81 on page 212.

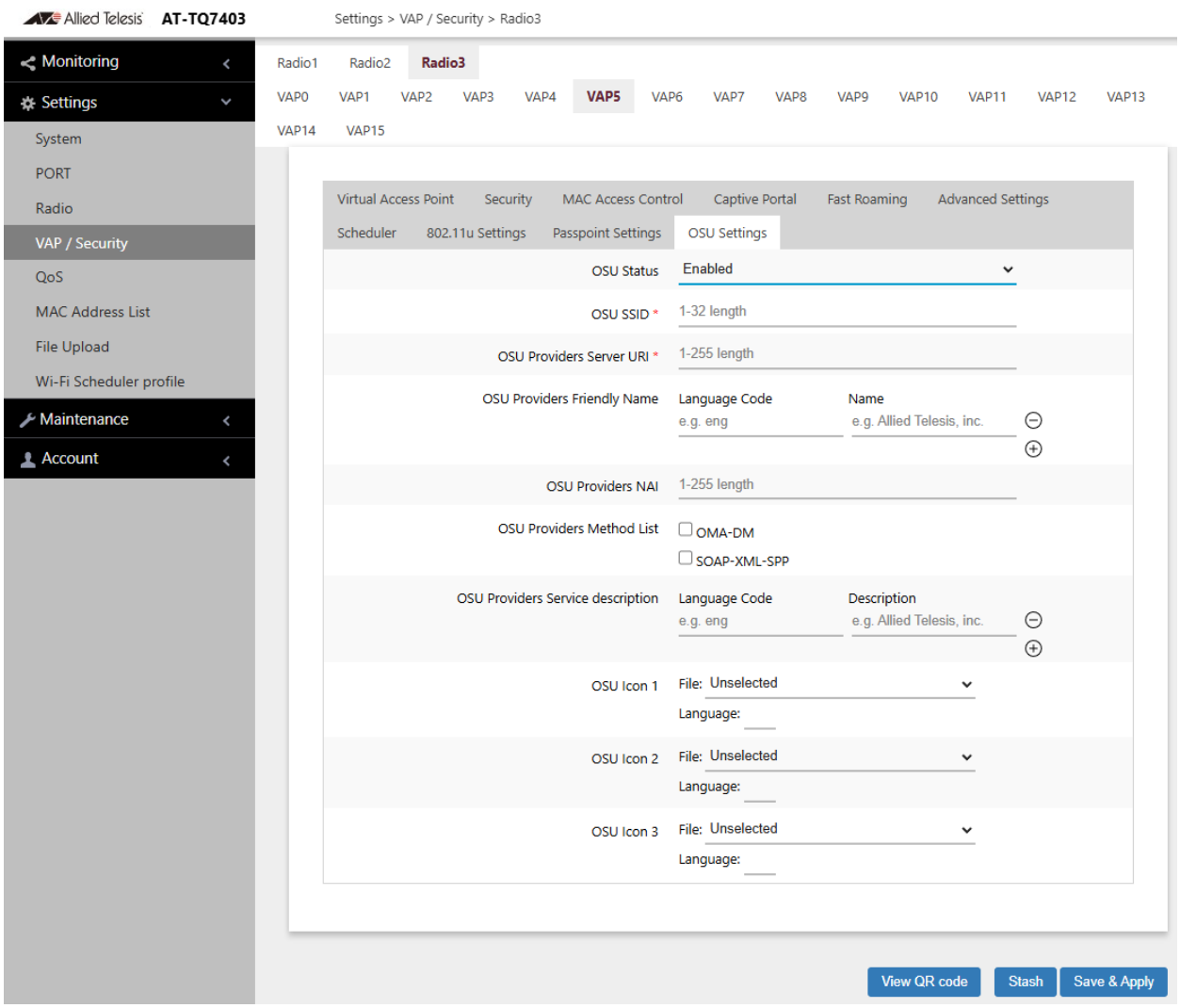

Figure 81. OSU Settings Window

2. Configure the parameters by referring to Table 43.

Table 43. 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.
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.
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.

Table 43. OSU Settings (Continued)

Field	Description
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.
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 215.

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

Chapter 12

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.

To upload OSU icon files to the access point, perform the following procedure:

1. Select **Settings** > **File Upload** from the main menu. See Figure 82.

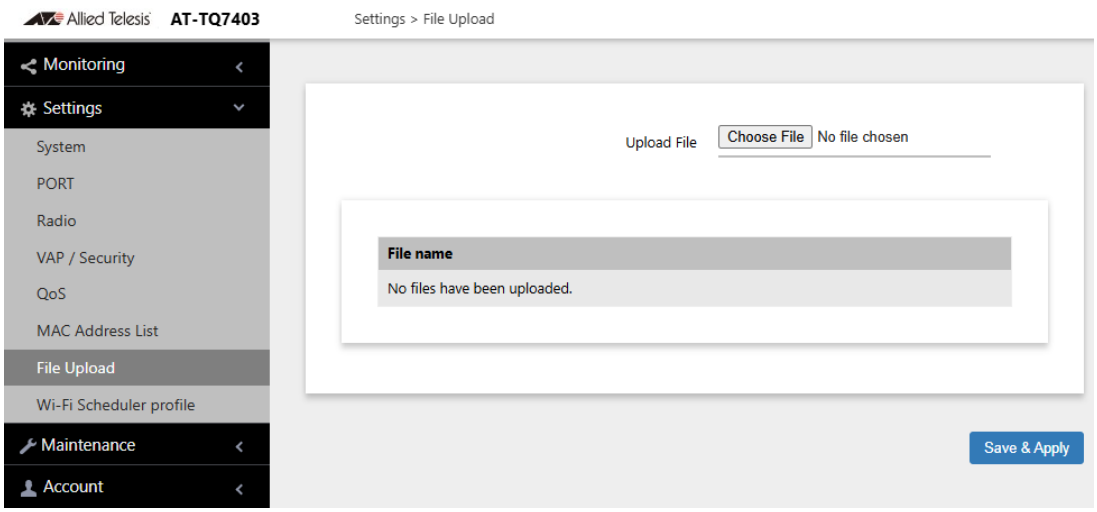

Figure 82. File Upload Window

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 13

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 the following sections for how to configure a Radio or a VAP:

For Radio Wi-Fi Scheduler see “Configuring Wi-Fi Scheduler” on page 82.

For VAP Wi-Fi Scheduler see .

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 83.

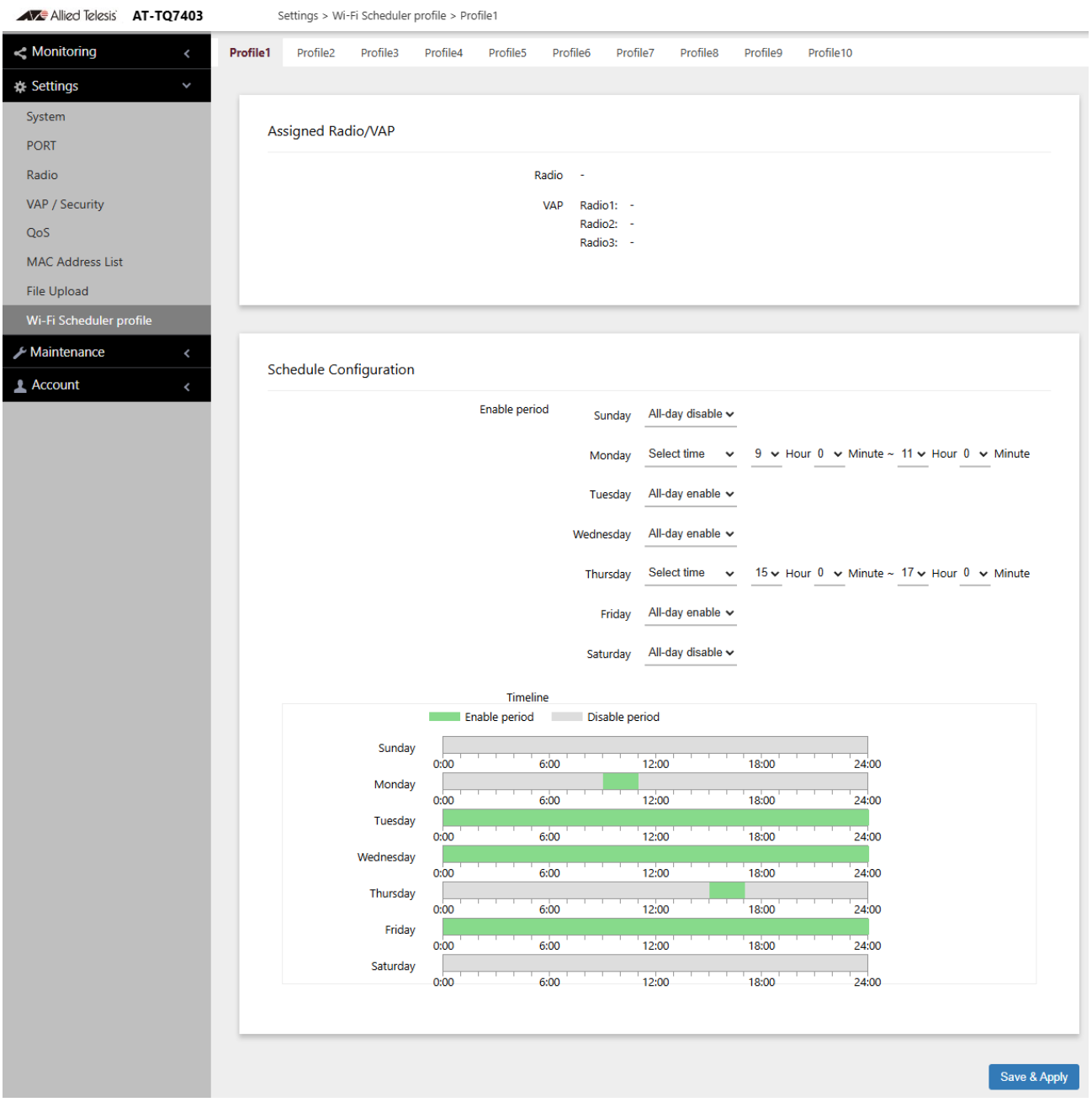

Figure 83. Wi-Fi Scheduler profile settings

2. Select a **Profile** (from 1 to 10).
3. Configure the parameters by referring to Table 44, “Wi-Fi Scheduler profile settings”.

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 14
Maintenance

This chapter has the following procedures:

Downloading the Access Point's Configuration File 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. See Figure 84.

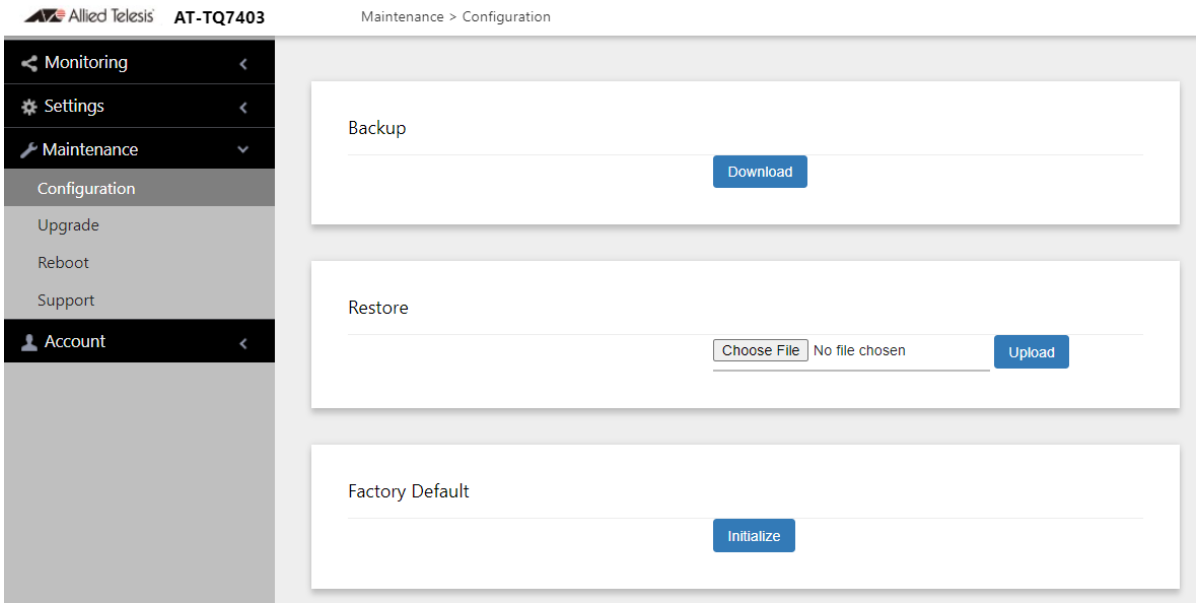

Figure 84. Configuration Window

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 suffix ".txt" must be added to the filename.

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 Access Point’s Configuration File to Your Computer” on page 221.
- 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 84 on page 221.
2. Click the **Choose File** button in the Restore section of the window and select the configuration file on your management workstation or network server to restore to the access point.
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 84 on page 221.
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 17.

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. See Figure 85 on page 225.

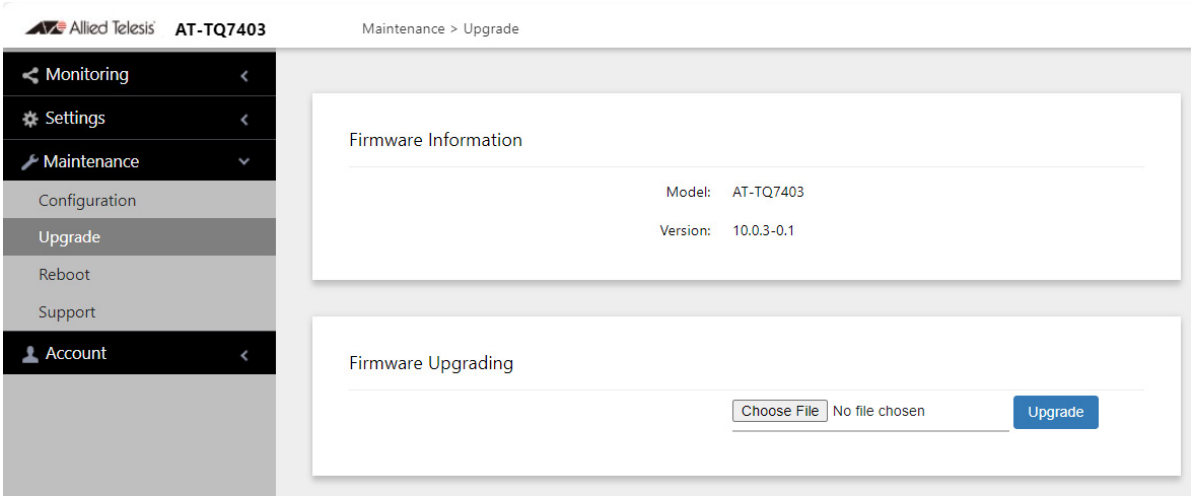

Figure 85. Upgrade Window

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

2. Click the **Choose File** button in the Firmware Upgrading section 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. See Figure 86.

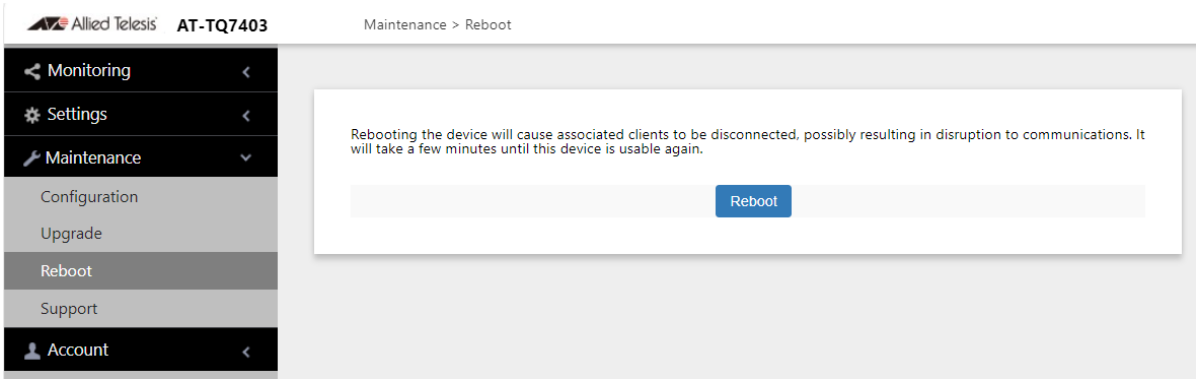

Figure 86. Reboot Window

2. Click the **Reboot** button.

   The access point displays a confirmation prompt.

3. Click **OK** button to reboot the access point or **Cancel** to cancel the procedure.

   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. See Figure 87.

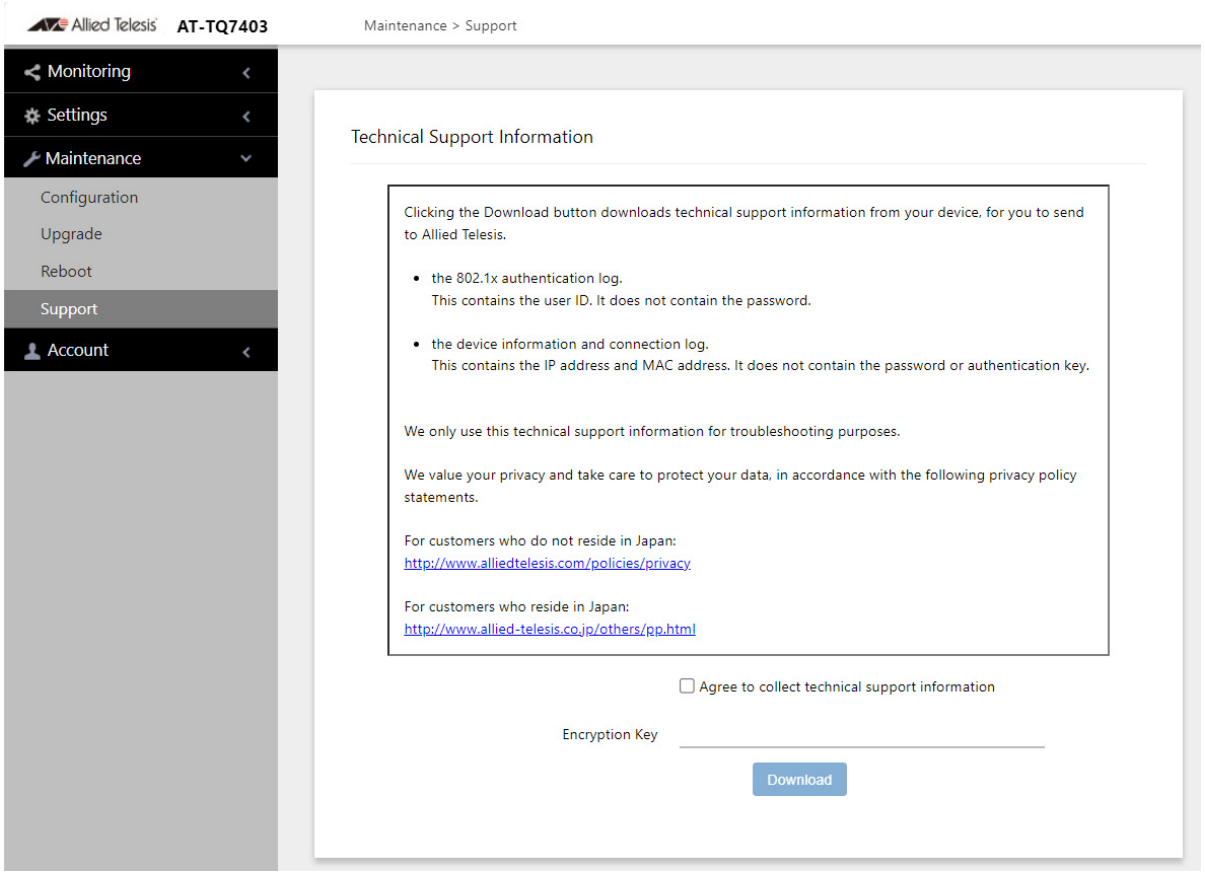

Figure 87. Support Window

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.

   Here are the guidelines:

   - ❒ This step is optional.
   - ❒ The key can be up to 32 alphanumeric characters.
   - ❒ The key 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 and encryption key to your Allied Telesis technician.

Chapter 15

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.

Here are guidelines on changing the login name and password:

- Default login name: manager
- Default password: friend
- The access point can have only one manager account.
- Changing the name and password does not affect your current management session.
- 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 88.

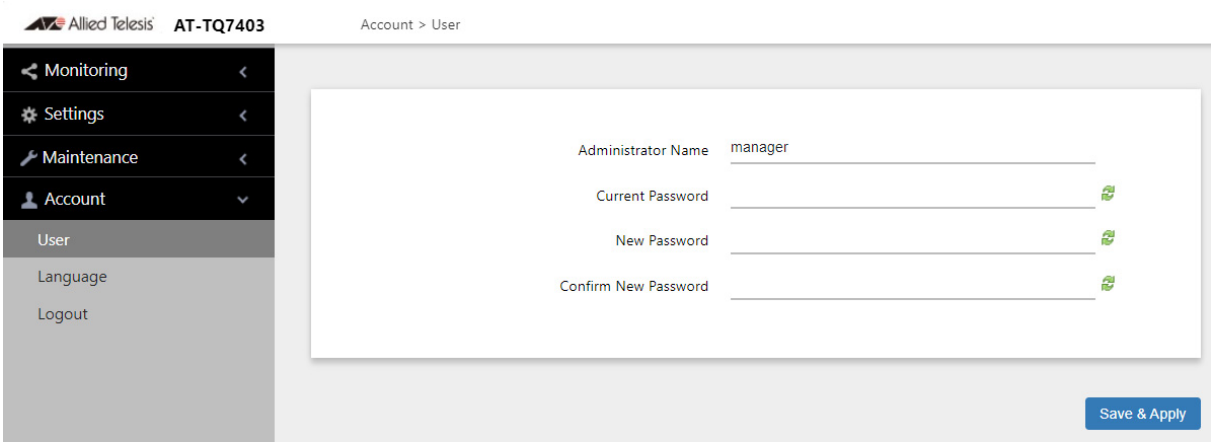

Figure 88. User Window

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.

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

   Here are the guidelines:

   - Default password: friend
   - To display the password as either alphanumeric characters or asterisks, click the green, double arrow symbol.

4. Select the **New Password** field and enter a 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 89.

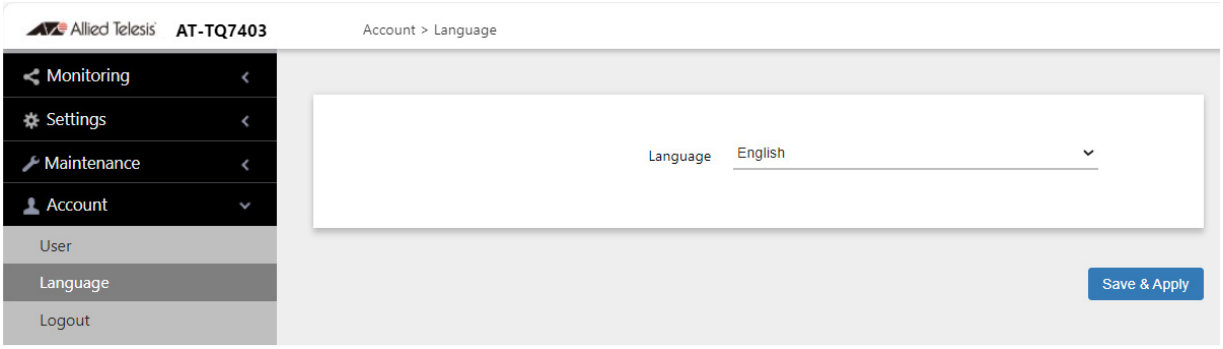

Figure 89. Language Window

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.