TQ5403 Series

Enterprise-class 802.11ac Wave 2 Wireless Access Points
with 2.4GHz and 5GHz Radios

Version 6.0.1-2.1

AT-TQ5403

AT-TQm5403

AT-TQ5403e

Management Software User's Guide

613-002651 Rev.D

Contents

List of Figures

List of Tables

Preface

This guide contains instructions on how to manage the features of the TQ5403 series access points with the web browser management interface.

The access point models included in this guide are:

- AT-TQ5403
- AT-TQm5403
- AT-TQ5403e

This preface contains the following sections:

Safety Symbols Used in this Document

This document uses the following conventions.

Note
Notes provide additional information.

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

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

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

Contacting Allied Telesis

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

- 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorizations (RMAs), and contact Allied Telesis technical experts.
- USA and EMEA phone support - Select the phone number that best fits your location and customer type.
- Hardware warranty information - Learn about Allied Telesis warranties and register your product online.
- Replacement Services - Submit an RMA request via our interactive support center.
- Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- Software Updates - Download the latest software releases for your product.

For sales or corporate contact information, select your region and country and then go to **www.alliedtelesis.com/contact**.

Chapter 1

Getting Started

Here are the sections in this chapter:

Features

The TQ5403 series wireless access points have the following features:

- One 2.4GHz radio
- Two 5GHz radios
- Eight virtual access points per radio
- WPA Personal and WPA Enterprise with WPA, WPA2, TKIP, and CCMP authentication and encryption
- Static WEP encryption
- MAC address filter for wireless clients
- Multicast rate limiting
- Band steering
- Automatic channel selection
- Adjustable transmission power
- Fast roaming
- Airtime fairness
- Quality of Service
- Wireless Distribution System (WDS) bridges
- Channel blankets (AT-TQ5403 and AT-TQ5403e only)
- DHCP client
- RADIUS accounting with external RADIUS server
- Network Time Protocol client
- HTTP and HTTPS web browser management
- SNMPv1 and v2c management
- Event log
- Syslog client
- LAN1 port: 10/100/1000Base-T Ethernet port with Power over Ethernet (PoE), Auto-Negotiation, and auto MDI/MDIX (AT-TQ5403 and AT-TQm5403 only)
- LAN2 port: 10/100/1000Base-T Ethernet port with Auto-Negotiation and auto MDI/MDIX (AT-TQ5403 and AT-TQm5403 only)
- LAN(PoE) port: 10/100/1000Base-T Ethernet port with IEEE 802.3at PoE+, Auto-Negotiation, and auto MDI/MDIX (AT-TQ5403e only)
- Static link aggregation for LAN1 and LAN2 ports (AT-TQ5403 and AT-TQm5403 only)

- IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), and IEEE 802.3ab (1000Base-T) compliance on LAN1, LAN2, LAN(PoE) ports.
- Outdoor installation on a wall or pole (AT-TQ5403e only)

Table 1 lists the differences among the TQ5403 series access points.

Table 1. TQ5403 Series Access Points Differences

Access Point	Channel Blankets	Maximum Number of Wireless Clients
AT-TQ5403	Supported[1]	200
AT-TQm5403	Not supported	127
AT-TQ5403e	Supported[1]	200

1. Requires Vista Manager EX and Autonomous Wireless Controller (AWC) plug-in.

Management Tools

The access points support the following management tools.

Web Browser

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

Note
The product has been tested with Microsoft Windows Internet Explorer Version 9 or later and Microsoft Edge.

Vista Manager EX and AWC Plug-in

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

Note
The AT-TQ5403 access point requires Vista Manager 2.4 or later. The AT-TQm5403 and AT-TQ5403e access points require Vista Manager 2.5 or later.

Note
The channel blanket feature of the AT-TQ5403 and AT-TQ5403e access points requires Vista Manager EX and the AWC plug-in.

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

- Hostname
- DHCP client or static IP address
- Domain Name Server name
- Timezone
- Daylight savings time
- System date or time
- HTTP and HTTPS modes
- System name, location, and contact

- LLDP PoE negotiation
- Enable or disable the Reset button

SNMPv1, v2c, and v3

You can use SNMPv1, SNMPv2, or SNMPv3 to view the parameter settings of the devices. The MIB is available from the Allied Telesis web site. For instructions on how to configure the unit for SNMP, refer to "Configuring SNMPv1 and v2c" on page 45 and "Configuring SNMP Traps" on page 49.

Note
You cannot use SNMP to change the parameter settings on the access points.

Starting the First Management Session

Note
If you are using the AT-TQ5403 or AT-TQm5403 access point, use the LAN1 port. If you are using the AT-TQ5403e access point, use the LAN(PoE) port.

After you install and power on the access point, it queries the subnet on the LAN1 or LAN(PoE) port for a DHCP server. If a DHCP server responds to its query, the unit uses the IP address the server assigns to it. If there is no DHCP server, the access point uses the default IP address 192.168.1.230.

If your network has a DHCP server, use the IP address the server assigns it to it to start the management session. For directions, refer to “Starting a Management Session” on page 25

If your network does not have a DHCP server, you can start the first management session by establishing a direct connection between your computer and the unit by connecting an Ethernet cable to the Ethernet port on the computer and the LAN1 or LAN(PoE) port on the access point. This procedure requires changing the IP address on your computer to make it a member of the same subnet as the default IP address on the access point.

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

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

- “Starting the First Management Session with a Direct Connection” on page 23. This section is for the AT-TQ5403 and AT-TQm5403 models only.
- “Starting the First Management Session without a DHCP Server” on page 23

Note
The first management session of the access point has to be conducted through the LAN1 or LAN(PoE) port because the default setting for the radios is off.

Starting the First Management Session with a Direct Connection

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

Note
This section is for the AT-TQ5403 and AT-TQm5403 models only.

Note
If the access point is using PoE, you cannot perform this procedure because it requires a direct connection between your computer and the LAN1 port on the access point. If you have the optional power supply, you can connect it to the unit until after you have completed the first management session, or you can perform "Starting the First Management Session without a DHCP Server" on page 23.

1. Connect one end of a network cable to the LAN1 port on the access point and the other end to the Ethernet network port on your computer.
2. Change the IP address on your computer to 192.168.1.*n*, where *n* is a number from 1 to 254, but not 230. Refer to the documentation that accompanies your computer for instructions on how to set the IP address.
3. Set the subnet mask on your computer to 255.255.255.0.
4. Power on the access point.
5. Start the web browser on your computer.
6. Enter the IP address 192.168.1.230 in the URL field of the browser and press the Enter key.

   You should now see the login window, shown in Figure 1 on page 25.
7. Enter "manager" for the user name and "friend" for the password. The user name and password are case-sensitive.
8. Click the Login button.

Starting the First Management Session without a DHCP Server

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

1. To use the PoE feature on the access point, be sure to connect the LAN1 or LAN(PoE) port to a PoE source device.

2. If your network has VLANs, check to be sure that your computer and the access point are connected to ports on the Ethernet switch that are members of the same VLAN. This might require accessing the management software on the switch and listing the VLANS and their port assignments. For example, if the access point is connected to a port that is a member of the Sales VLAN, your computer must be connected to a port that is also a member of that VLAN. If your network is small and does not have VLANs or routers, you can connect your computer to any port on the Ethernet switch.

3. Change the IP address on your computer to 192.168.1.*n*, where *n* is a number from 1 to 254, but not 230. Refer to the documentation that accompanies your computer for instructions on how to set the IP address.

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

5. Power on the access point.

6. Start the web browser on your computer.

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

   You should now see the logon window, shown in Figure 1 on page 25.

8. Enter “manager” for the user name and “friend” for the password. The user name and password are case-sensitive.

9. Click the Login button.

Starting a Management Session

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

Note
If the access point is using its default address 192.168.1.230, refer to "Starting the First Management Session" on page 22 for instructions.

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

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

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

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

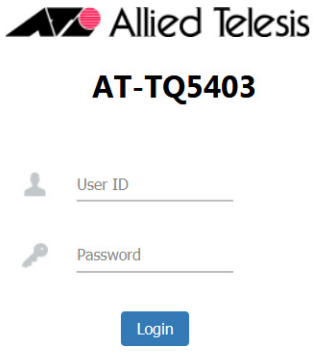

Figure 1. Log On Window

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

3. Enter the user name and password for the unit. The default values are “manager” for the user name and “friend” for the password. The user name and password are case-sensitive.

4. Click the Login button.

Management Windows

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

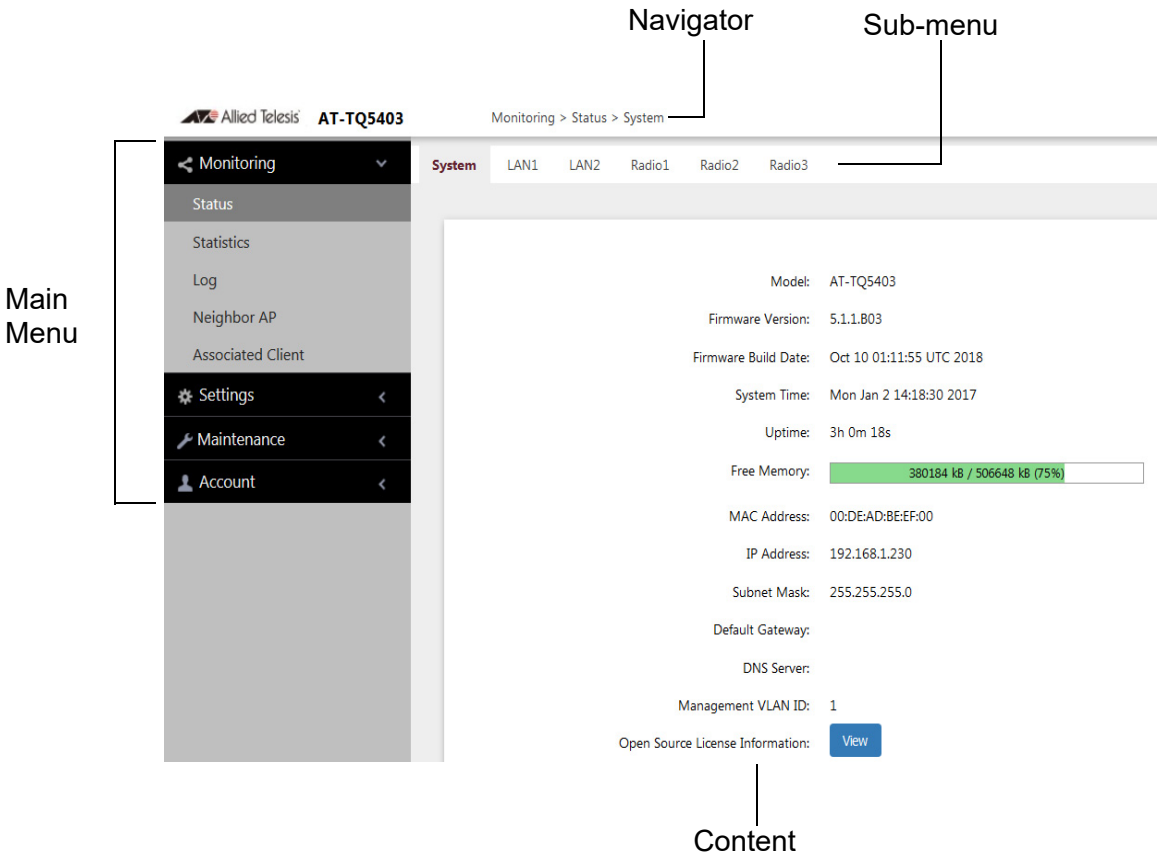

Figure 2. Sample Management Window

Note
The AT-TQ5403e does *not* have LAN2 on the sub-menu.

Main Menu

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

- Monitoring
- Settings
- Maintenance
- Account

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

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

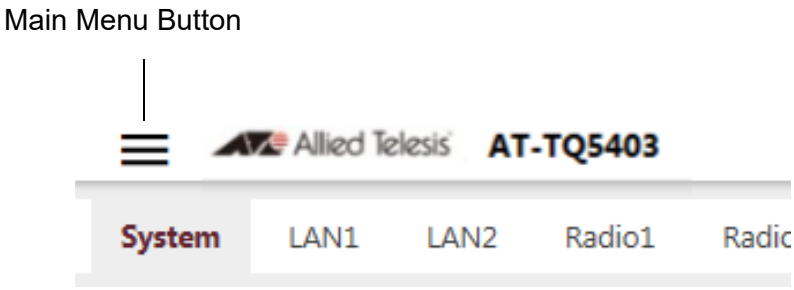

Figure 3. Main Menu Button

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

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

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

Saving and Applying Your Changes

You need to click the **SAVE & APPLY** button to save and activate your changes when you are finished configuring the parameters in a management window. The button is located in the bottom of the windows. When you click the button, the access point immediately activates your changes and saves them in its configuration file. If you change the parameter settings in a window and navigate to a different window without clicking the button, the access point discards your changes.

The access point displays the following messages when you click the **SAVE & APPLY** button:

```
Please wait...
Waiting for changes to be applied...
Changes applied.
```

Ending Management Sessions

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

What to Configure First

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

1. Set the country code. Refer to "Setting the Country Code Setting" on page 76.

   Note
   The country code for units sold in North America, Japan, Canada, Taiwan is preset and cannot be changed.

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

2. Change the manager's login name and password. Refer to "Changing the Manager's Login Name and Password" on page 60.

3. If you prefer to use HTTPS management sessions, perform "Configuring the Web Browser Interface" on page 58.

4. Set the language of the management interface to English or Japanese. The default is English. Refer to "Setting the Language of the Web Browser Interface" on page 62.

5. Activate the LAN2 port to double the bandwidth to your wired network. Refer to "Configuring the LAN2 Port" on page 142.

   Note
   Skip Step 5 if you are using the AT-TQ5403e model because it does not have the LAN2 port.

Chapter 2

Basic Settings

This chapter contains the following procedures:

Assigning a Dynamic IP Address from a DHCP Server

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

If your network does not have a DHCP server or you prefer to manually assign it an IP address, refer to “Assigning a Static IP Address to the Access Point” on page 37.

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. Refer to Figure 4 on page 35.

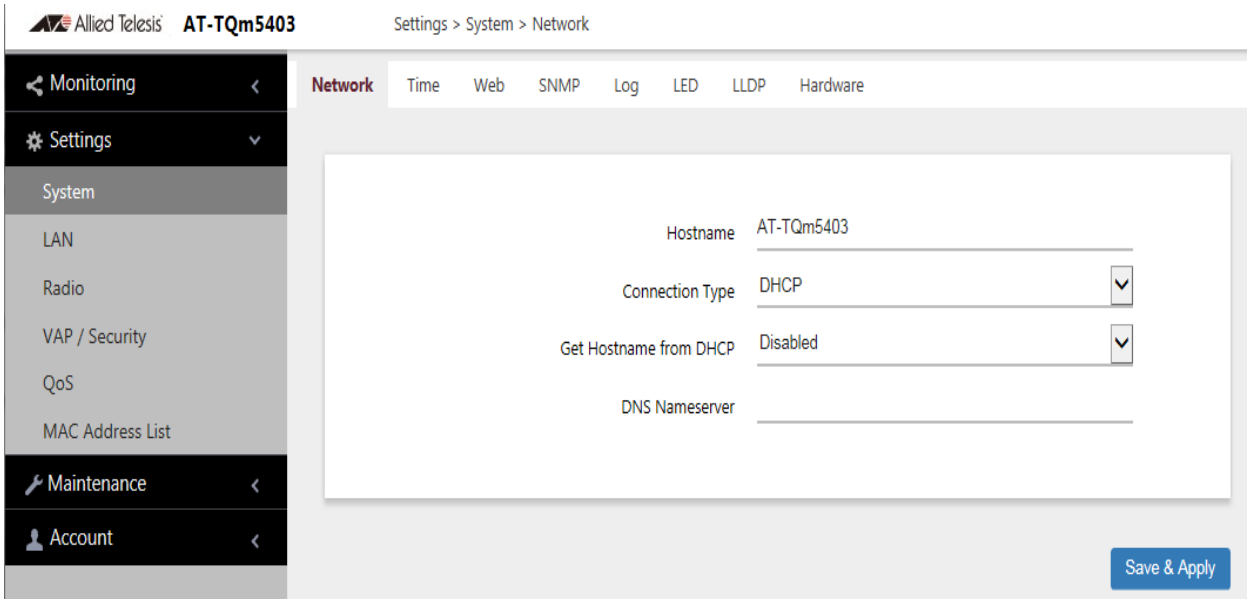

Figure 4. Network DHCP Window

4. Configure the fields by referring to Table 2.

Table 2. Network DHCP Window

Parameter	Description
Hostname	Enter a hostname for the access point. Here are the guidelines: - The hostname can be from 1 to 63 alphanumeric characters. - The hostname cannot contain spaces or any special characters, except hyphens. - The first or last character cannot be a hyphen. - The access point can have only one hostname. - The default is AT-TQ5403, AT-TQm5403, or AT-TQ5403e. - 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 IP Address to the Access Point" on page 37.

Table 2. Network DHCP Window (Continued)

Parameter	Description
Get Hostname from DHCP Server	Control how the access point obtains its hostname. The options are listed here: - Enabled: The access point queries the DHCP server for its hostname. - Disabled: The access point does not query the DHCP server for a hostname. Instead, it uses the entry in the Hostname field in this window.
DNS Name Server	Enter the IP address of the DNS name server. If this field is left blank, the access point tries to obtain the address from the DHCP server. The default is no name.

5. Click the **SAVE & APPLY** button to save and update the configuration.

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

Assigning a Static IP Address to the Access Point

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

If you prefer the access point obtain its IP configuration from a DHCP server on your network, refer to "Assigning a Dynamic IP Address from a DHCP Server" on page 34.

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 5.

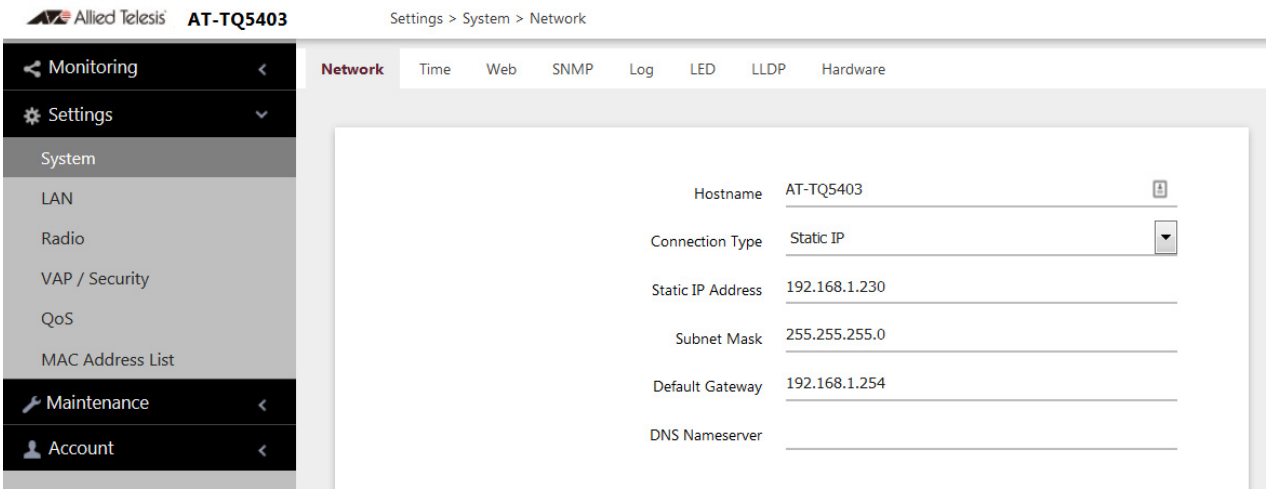

Figure 5. Network Static IP Address Window

4. Configure the field values by referring to Table 3 on page 38.

Table 3. Network Static IP Selection Window

Item Name	Description
Host Name	Enter a host name for the access point. Here are the guidelines: - The host name can be from 1 to 63 alphanumeric characters. - The hostname cannot contain spaces or any special characters, except hyphens. - The first or last character cannot be a hyphen. - The access point can have only one hostname. - The default is AT-TQ5403, AT-TQm5403, or AT-TQ5403e.
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 is 192.168.1.254. 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 and the network portion of the address must be the same as the IP address entered in step 3. You have to assign a default gateway to the access point. If your network does not have a default gateway or you do not want to assign one to the access point at this time, enter an unused IP address of the same network as the IP address.

Table 3. Network Static IP Selection Window (Continued)

Item Name	Description
DNS Name Server	Specify the Domain Name Service name server address. This field is optional The default is no name.

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

To configure the NTP client, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Time** from the sub-menu. Refer to Figure 8 on page 43.
3. From the Set System Time pull-down menu, select **Using Network Time Protocol (NTP)**. The window is updated with new options. Refer to Figure 6.

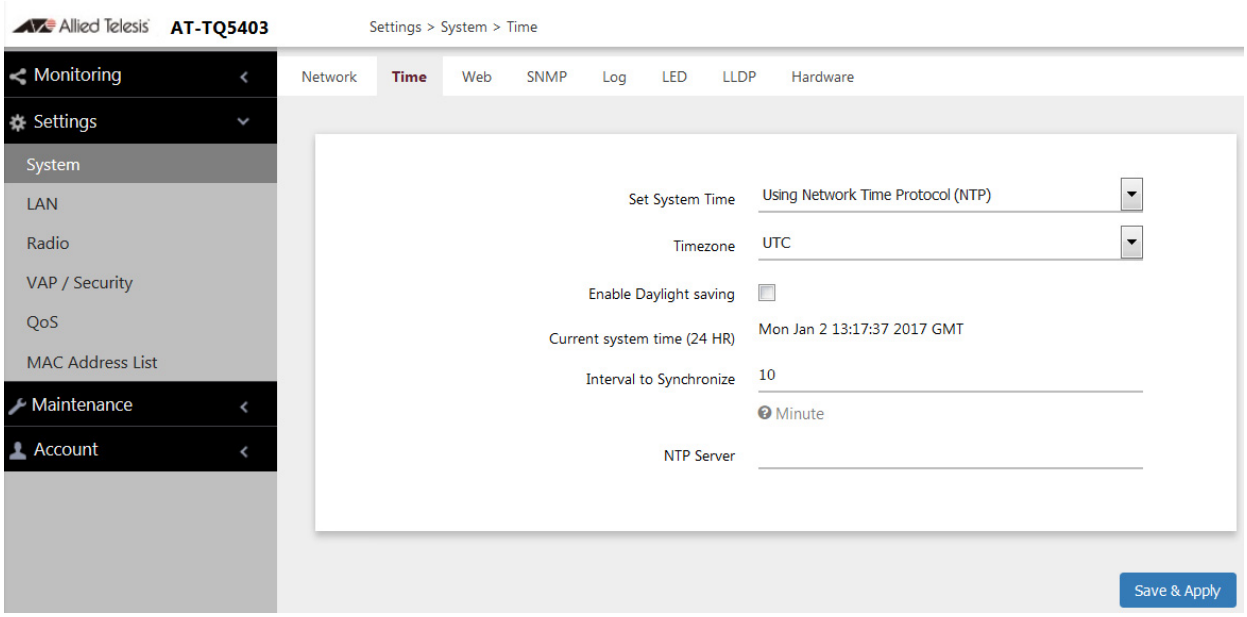

Figure 6. Time Window - NTP Option

4. Configure the fields by referring to Table 4.

Table 4. Time Window - NTP Option

Item Name	Description
Set System Time	Select **Network time protocol (NTP)** to synchronize the date and time of the product with the NTP server. The factory default is Manually.
Timezone	Use this pull-down menu to set the time zone of the location of the access point. If the SNTP server is providing Coordinated Universal Time (UTC), the access point uses the time zone parameter to determine its UTC offset, which is the number of hours its location is ahead or behind UTC. It adjusts the time accordingly.
Enable Daylight Saving	If the location of the access point observes daylight savings time, click the check box for this option. The window displays the fields in Figure 7 on page 42. If the area does not observe Daylight Savings time, leave the check box empty.
Start	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset	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 4. 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 7 contains the settings for Daylight Savings Time.

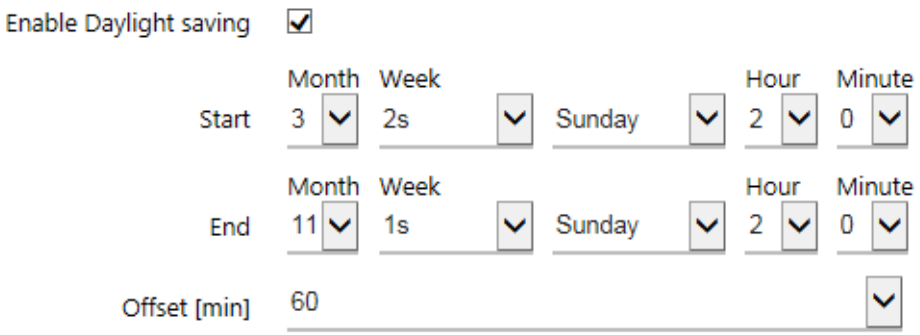

Figure 7. Daylight Savings Time Settings

5. Click the **SAVE & APPLY** button to save and update the configuration.

Manually Setting the Date and Time

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

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

Note
Allied Telesis recommends using a 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 40.

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 8.

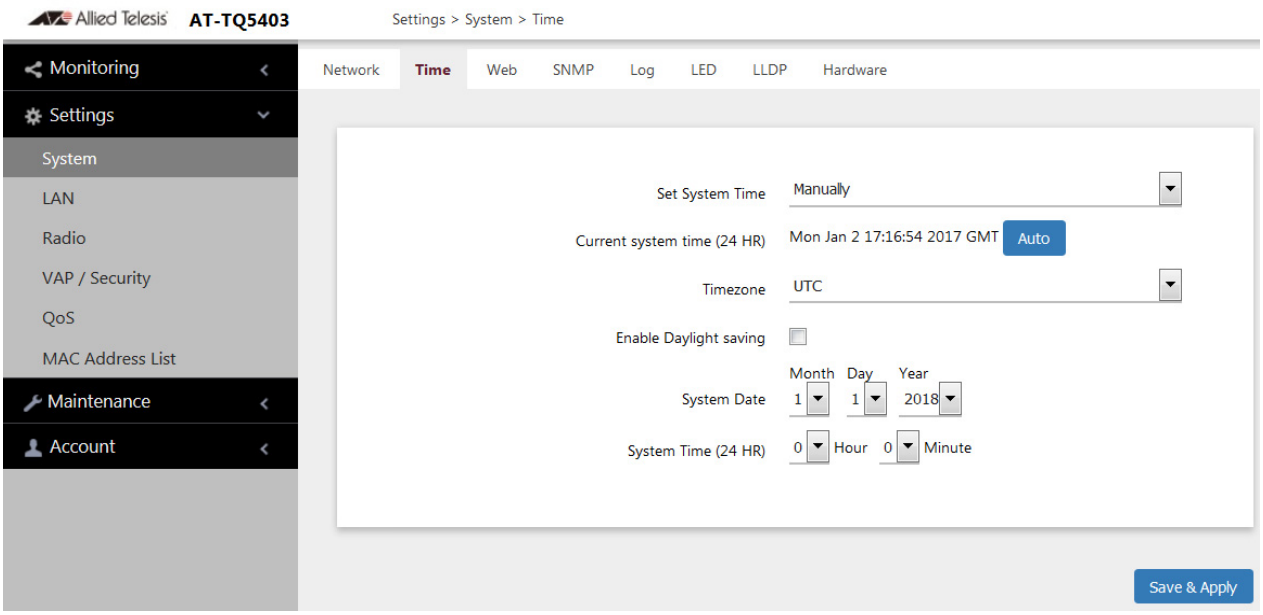

Figure 8. Time Window - Manually Option

3. Configure the parameters by referring to Table 5 on page 44.

Table 5. Time Window - Manually Option

Field	Description
Set System Time	Select **Manually**. This is the default.
Current System Time (24 HR)	Displays the current date and time settings. Click the AUTO button to set the date and time on the access point according to your management workstation.
Timezone	Select the Time Zone of the access point from the pull-down menu.
Enable Daylight Savings	If the location of the access point observes daylight savings time, click the dialog box for the Adjust Time for Daylight Savings parameter. The window displays the fields in Figure 7 on page 42 If the area does not observe Daylight Savings time, leave the check box empty.
Start	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset	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 SNMPv1 and v2c

You can use SNMPv1 and v2c to view the settings and client statistics on the access point, and receive traps. Here are the guidelines:

- You cannot use SNMP to change the settings on the access point.
- The access point does not support SNMPv3.
- The access point has one read-only community string.
- The unit must have an IP address for SNMP management. For instructions, refer to "Assigning a Static IP Address to the Access Point" on page 37 or "Assigning a Dynamic IP Address from a DHCP Server" on page 34.

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. Click the **Agent Settings** tab. This is the default tab. Depending on the status or version you are using, one of three screens will appear. Refer to Figure 10, Figure 10 on page 46, or Figure 11 on page 46.

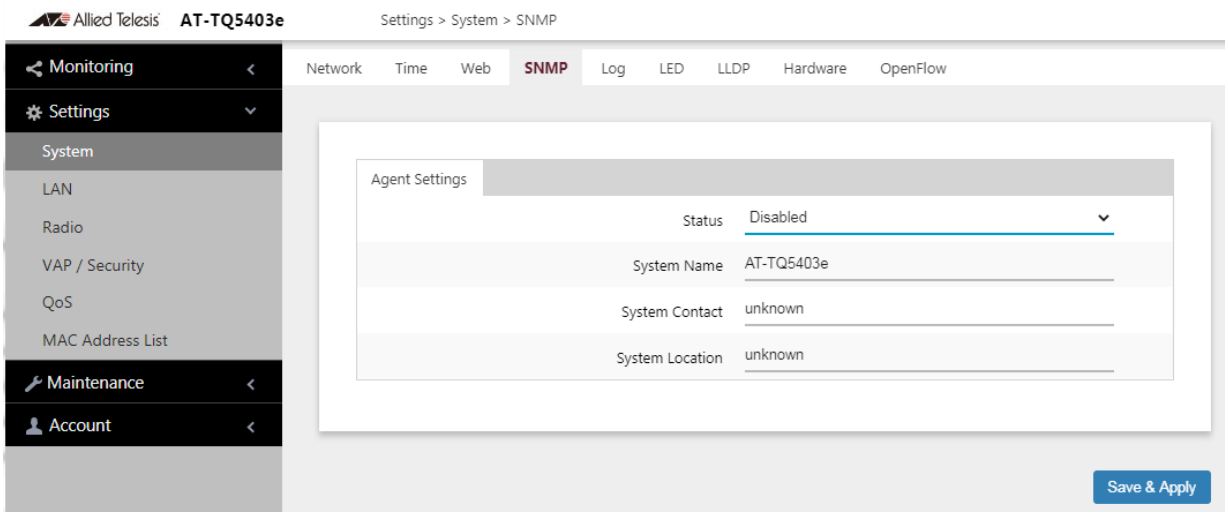

Figure 9. Disabled SNMP Agent Settings Window

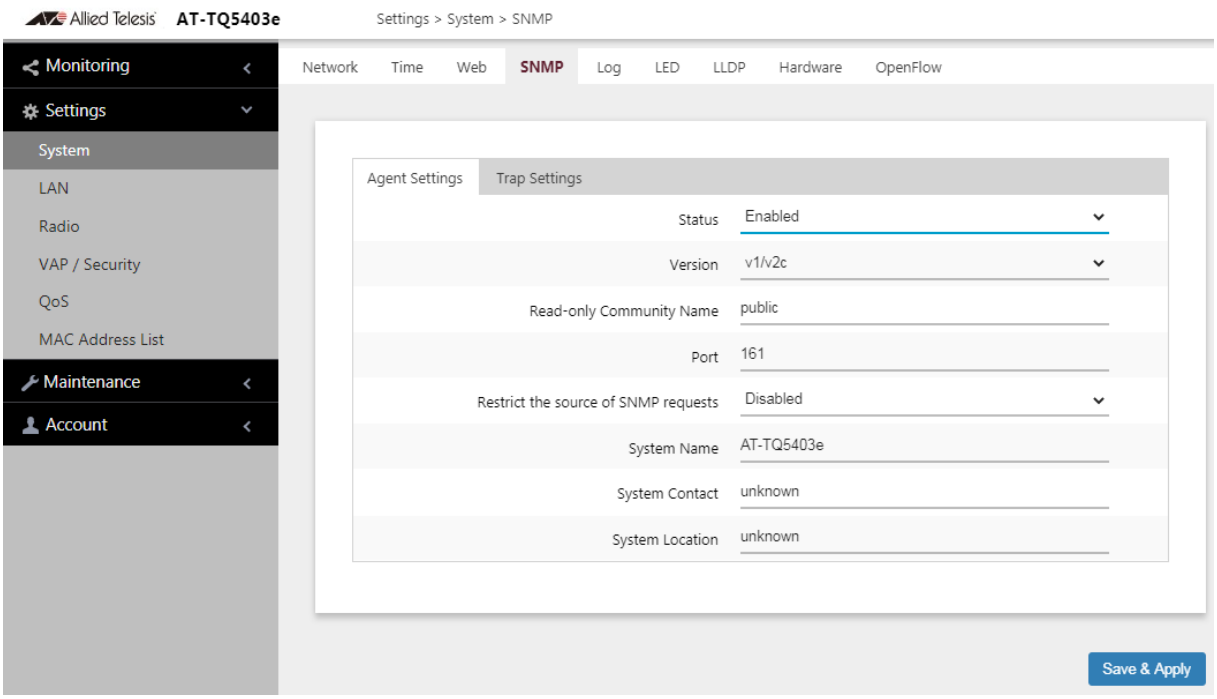

Figure 10. v1/v2c SNMP Agent Settings Window

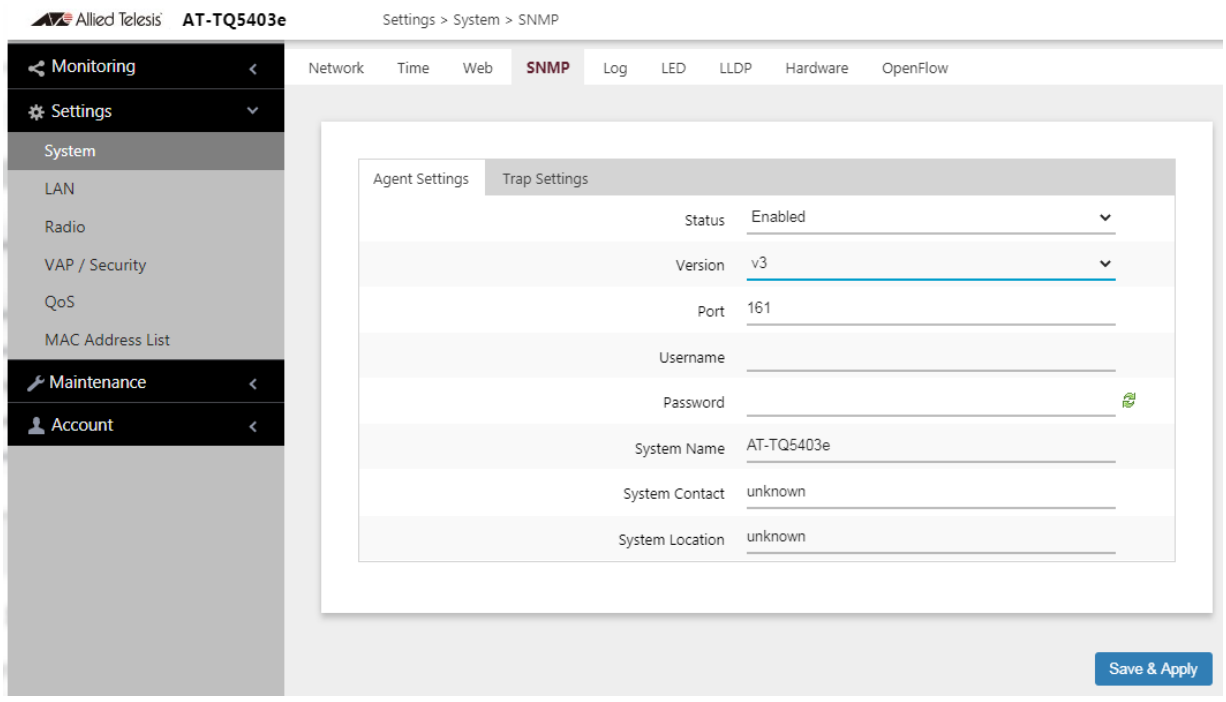

Figure 11. v3 SNMP Agent Settings Window

4. Configure the fields by referring to Table 6 on page 47.

Note
To configure the parameters in the window, you must first set the Status parameter to Enabled. You cannot adjust the settings when Status is Disabled.

Table 6. SNMP Agent Settings 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	Use this option to specify the version number you are using.
Read-Only Community Name	Use this option to specify the community name. Only displayed on "v1/v2" setting.
Restrict the Source of SNMP Requests	Use this option to increase the security of the access point by restricting the use of SNMP to specific subnets or individual workstations. The options are described here: - Enabled: Check this option to restrict the use of SNMP on the access point to only those management stations specified in the next field in the window. - Disabled: Check this option to disable this feature and permit any workstation to use the community string to view the unit. This is the default setting. Only displayed on "v1/v2" setting.
Port	Use this parameter to specify the port number for SNMP. The range is 1 to 65535. The default is 161.

Table 6. SNMP Agent Settings Window (Continued)

Field	Description
Username	Use this field to specify your username. Only displayed on “v3” setting.
Password	Use this field to specify your password. Only displayed on “v3” setting.
Only allow from the designated hosts or subnets	Use this field to identify the management workstations permitted to use SNMP to view the device. This field only applies if you select the Enabled option in the previous field. Here are the guidelines: - You can specify only one value in the field. - You can specify a specific workstation by its IP address (for example,149.23.45.102). - You can specify a subnet by including the subnet mask (for example, 67.101.4.0/24). - You can specify a workstation by its FQDN. - The default is blank. Observe these guidelines when using an FQDN to identify 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-TQ5403, AT-TQm5403, or AT-TQ5403e.
System Contact	Specify the system administrator name. The system contact can be up to 64 alphanumeric characters. The default is Unknown.
System Location	Enter the location of the device. It can be up to 64 alphanumeric characters. The default is Unknown.

5. Click the **SAVE & APPLY** button to save and update the configuration.

Configuring SNMP Traps

To configure the access point to transmit SNMP traps, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **SNMP** from the sub-menu.
3. Click the **Trap Settings** tab. Depending on the version you are using, one of two screens will appear. Refer to Figure 12 or Figure 13 on page 50.

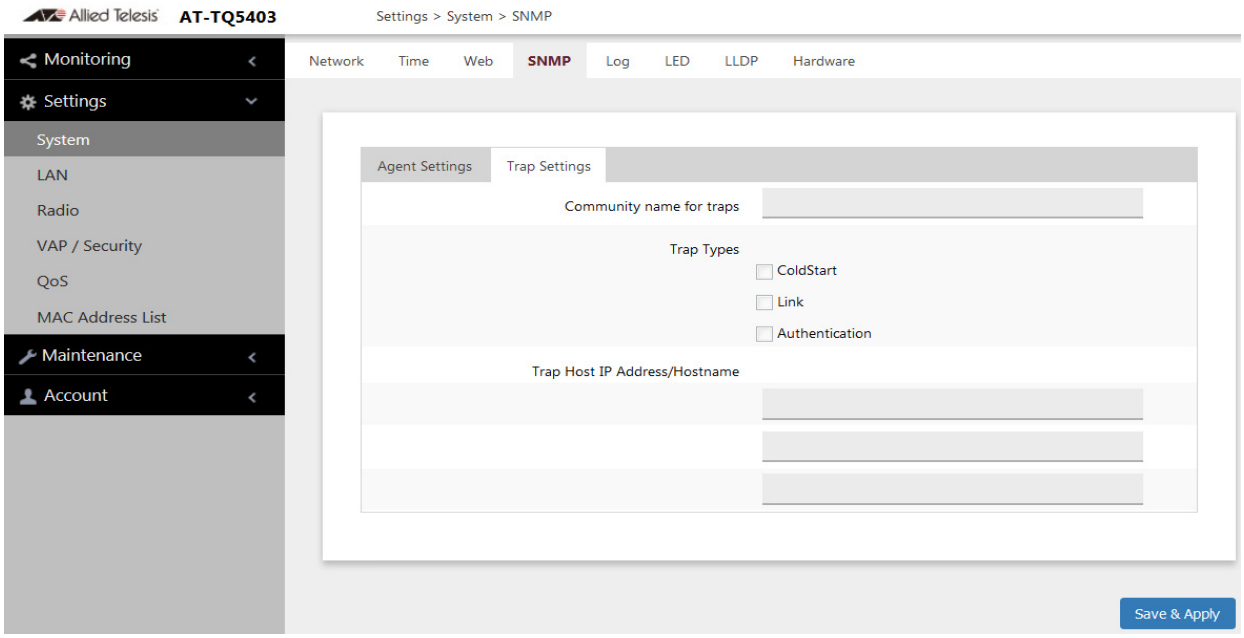

Figure 12. SNMP v1 and v2c Trap Settings Window

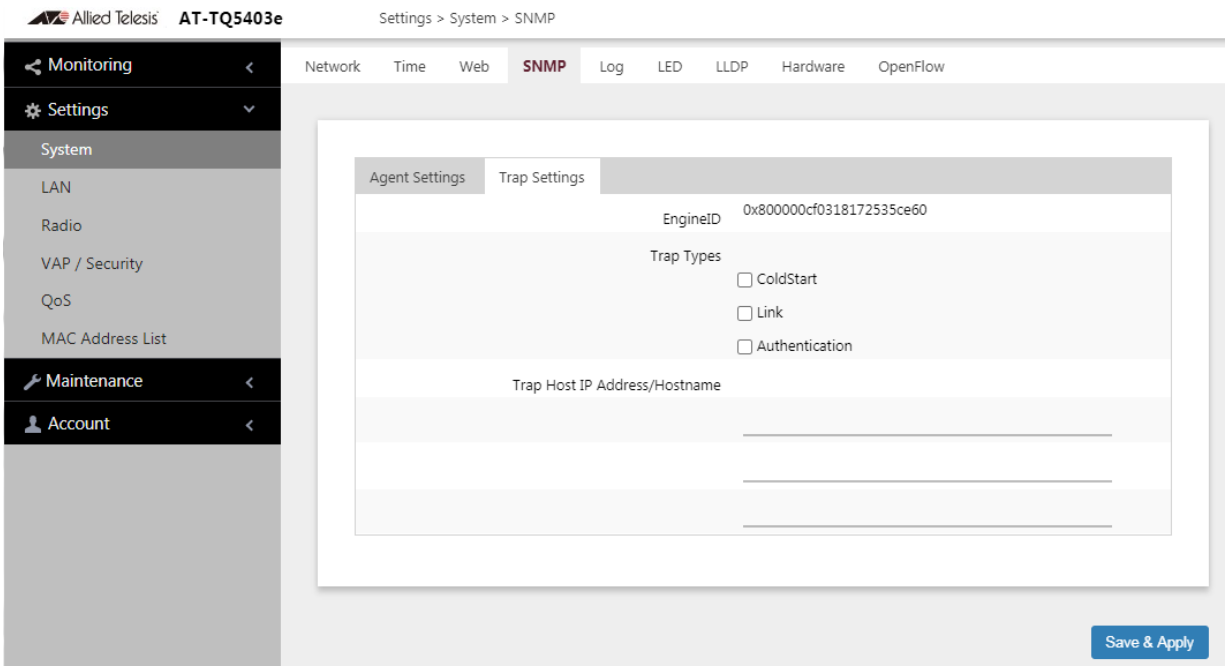

Figure 13. SNMP v3 Trap Settings Window

Note
The Status parameter has to be set to Enabled in the Agent Settings tab before you can configure the parameters in this window. Refer to Table 6 on page 47.

4. Configure the fields by referring to Table 7 on page 50.

Table 7. SNMP Trap Settings Window

Parameter	Description
Community Name for Traps	Use this field to specify the community name the access point is to use to transmit traps. Here are the guidelines: - The community name can be from 1 to 256 alphanumeric characters. - The default is blank. - The name cannot contain any of the following characters: "" (Double quote), '' (single quote), '¥' or '/' (Yen sign or backslash), '&', '<', '>.'

Table 7. SNMP Trap Settings Window (Continued)

Parameter	Description
Trap Types	Select radio button for the trap type you want to generate: - Cold Start - This trap is sent when the SNMP agent started. - Link - This trap is sent when a radio enabled or disabled. - Authentication - This trap is sent when an SNMP authentication fails
Trap Host IP Address / Hostname	Specify the SNMP hosts to receive the traps. Here are the guidelines: - You can specify up to three hosts. - The hosts can be identified by IP addresses or hostnames. - The default is blank. Observe these guidelines when using an FQDN to identify a 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.

5. Click the **SAVE & APPLY** button to save and update the configuration.

Enabling or Disabling the LEDs

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

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

1. Select **Settings** > **System** in the main menu.
2. Select **LED** in the sub-menu. Refer to Figure 14.

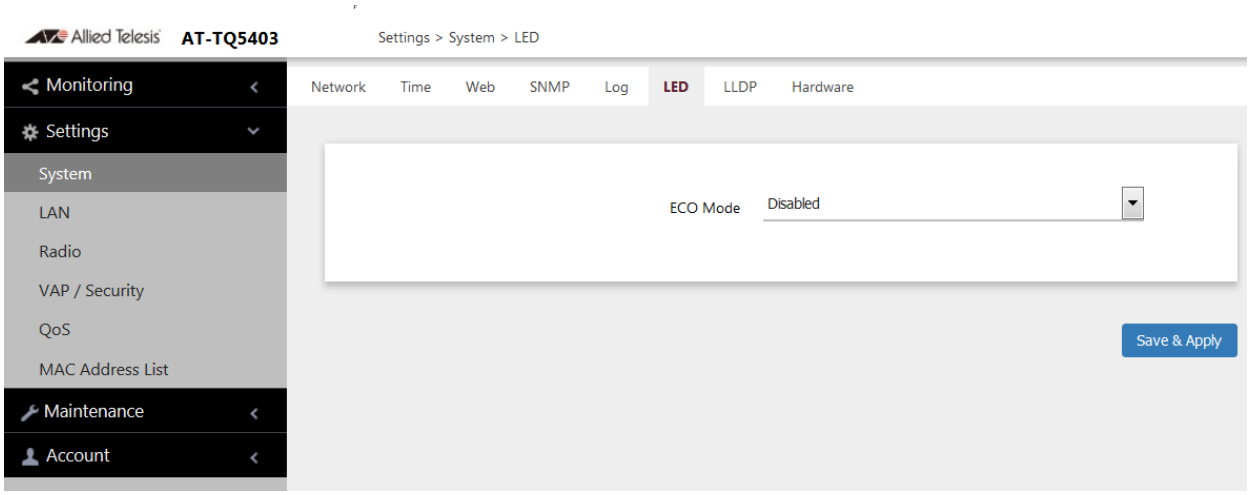

Figure 14. LED Window

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.

Enabling or Disabling the Reset Button

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

The default setting for each model is shown in Table 8.

Table 8. Default Settings for Reset Button

Model	Default Setting for Reset Button
AT-TQ5403	Enabled
AT-TQm5403	Enabled
AT-TQ5403e	Disabled

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

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

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

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

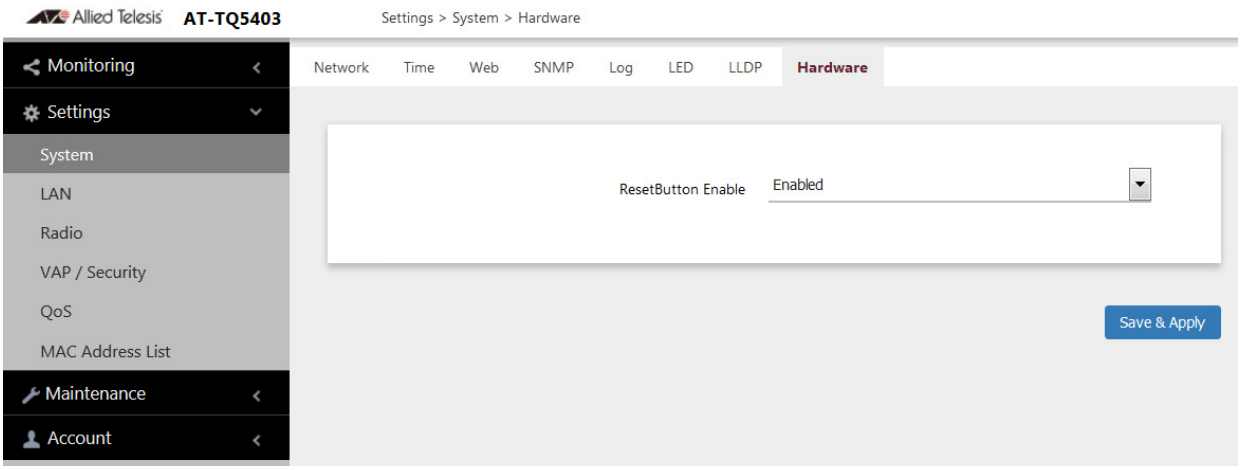

Figure 15. Hardware Window

3. Configure the fields by referring to Table 7 on page 50:
   - ❒ Enabled: The Reset button is enabled.
   - ❒ Disabled: The Reset button is disabled.
4. Click the **SAVE & APPLY** button to save and update the configuration.

Configuring the OpenFlow Protocol

The OpenFlow window in the System main menu is not supported in this release. Refer to Figure 16.

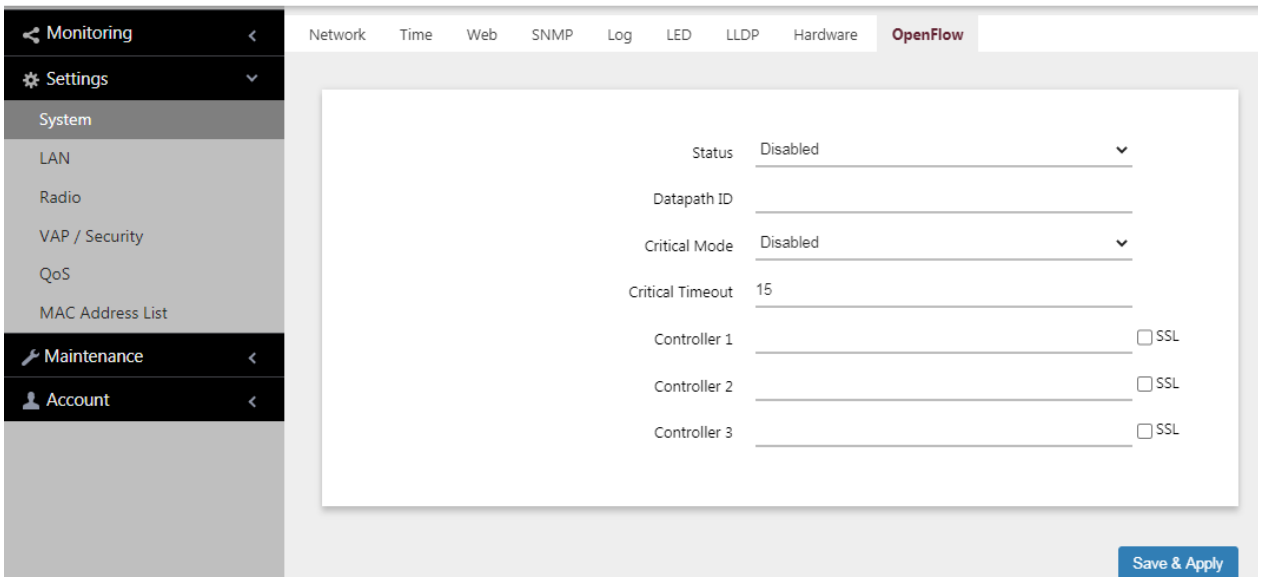

Figure 16. OpenFlow Protocol Window

Chapter 3

Web Browser Interface

This chapter contains the following procedures:

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 17.

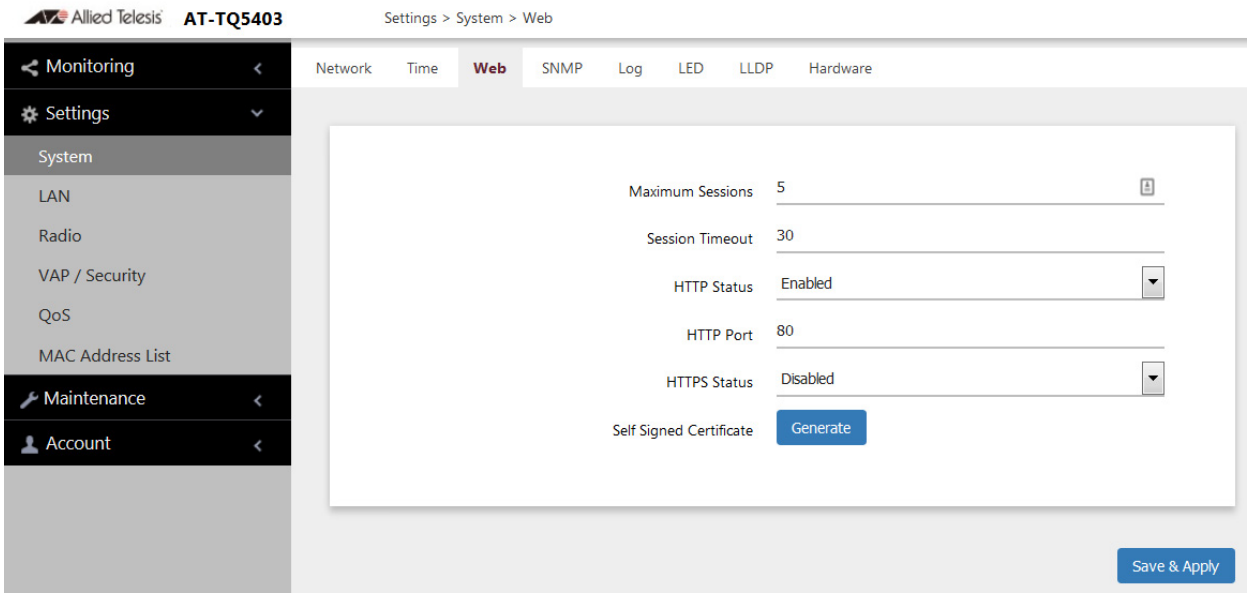

Figure 17. Web Window

3. Configure the fields by referring to Table 9.

Table 9. 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 interval in minutes after which 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.

Changing the Manager's Login Name and Password

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

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

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

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

1. Select **Account** > **User** from the main menu, Refer to Figure 18.

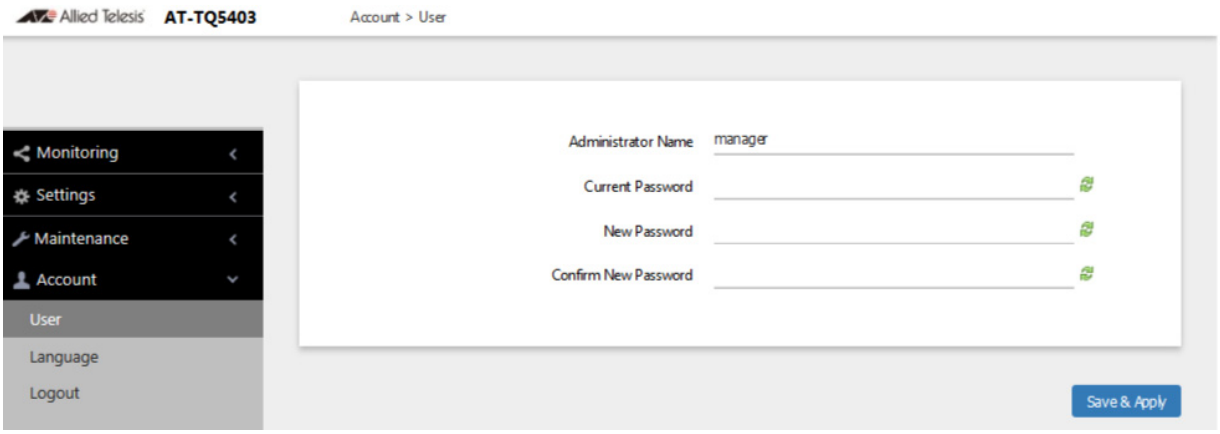

Figure 18. User Window

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

3. To change the password, select the **Current Password** field and enter the account's current password. The default is "friend".

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

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

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

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

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

Setting the Language of the Web Browser Interface

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

1. Select **Account** > **Language** from the main menu. Refer to Figure 19.

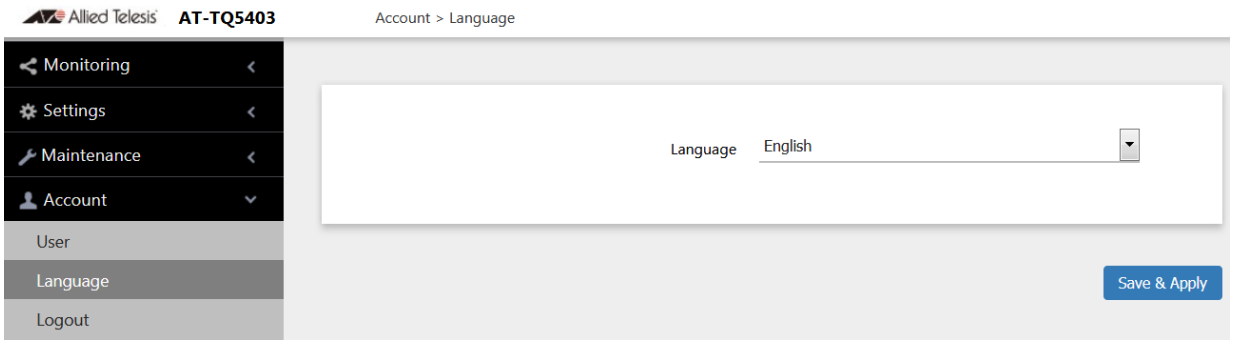

Figure 19. Language Window

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.

Chapter 4

2.4GHz and 5GHz Radios

This chapter has the following procedures:

Configuring the Radios

The radio settings are divided into two groups:

- ❒ “Configuring Basic Radio Settings” next
- ❒ “Configuring Advanced Radio Settings” on page 68

Configuring Basic Radio Settings

To configure the basic settings for Radio1, Radio2, or Radio3, 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. This is the default tab.

   The AT-TQ5403 and AT-TQm5403 access points display a window shown in Figure 20. The AT-TQ5403e access point displays a window shown in Figure 21 on page 65.

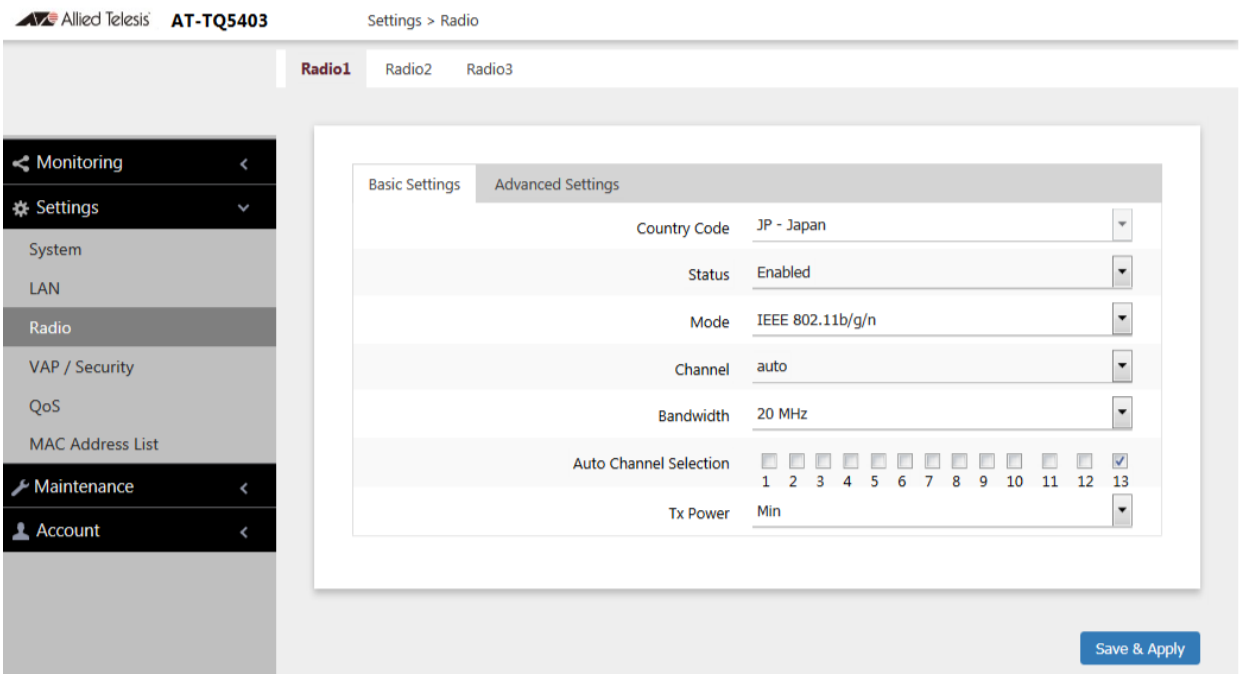

Figure 20. Basic Radio Settings Window on AT-TQ5403and AT-TQm5403

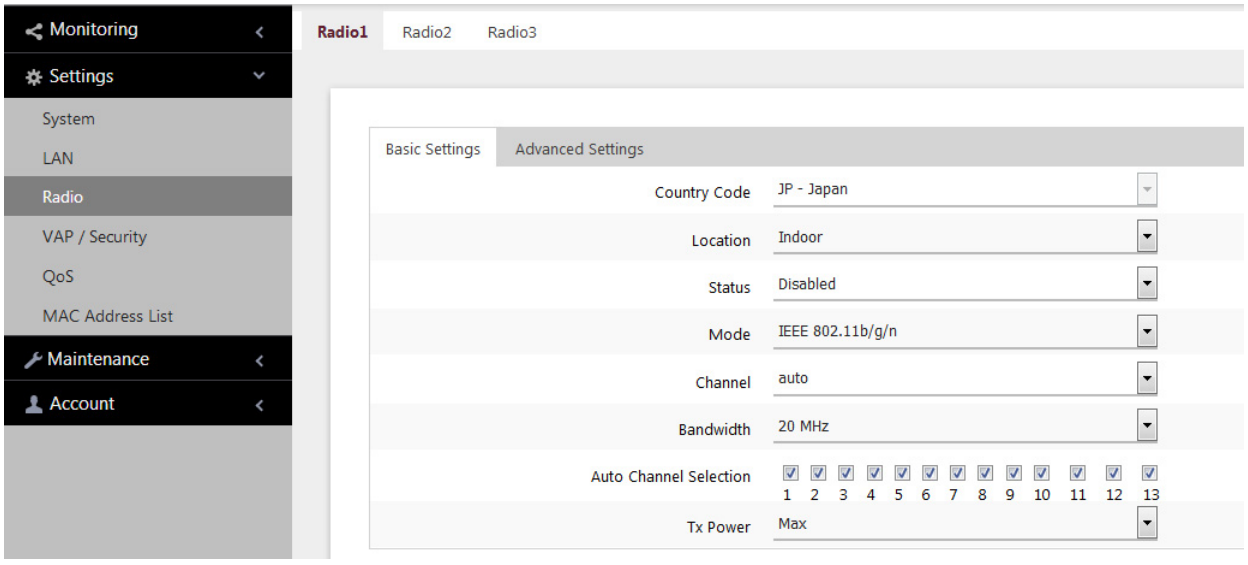

Figure 21. Basic Radio Settings Window on AT-TQ5403e

4. Configure the settings by referring to Table 10.

Table 10. Basic Radio Settings Window

Field	Description
Country Code	Select the country code that applies to your country or region. The country code ensures that the device operates in compliance with the codes and regulations of your region or country. Here are the guidelines: - You can select only one country. - The Country Code parameter is shown in the Basic Settings windows of all three radios but it can only be set from Radio1. - The same country code applies to all three radios. - Changing the country code disables the radios. - You have to reconfigure the radio settings if you change the country code. - You cannot change the country code on units sold in North America, Israel, Japan, Canada, or Taiwan.

Table 10. Basic Radio Settings Window (Continued)

Field	Description
Location (AT-TQ5403e Only)	Select a location where the AT-TQ5403e access point is installed. The selections are: - Indoor: This is the default setting. - Outdoor This can only be set on Radio1, but applies to all three radios. For more information, see “Selecting the Location” on page 77.
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 only 802.11b or 802.11g clients. - IEEE 802.11b/g/n: The access point accepts 802.11b, 802.11g, or 802.11n clients operating at 2.4GHz. This is the default for Radio1.
Mode (Radio2 or Radio3)	Select the communications protocol for Radio2 or Radio3 from the pull-down menu. The selections are listed here: - IEEE 802.11a: The access point accepts 802.11a clients. - IEEE 802.11a/n/ac: The access point accepts 802.11a, 802.11n, and 802.11ac clients operating. This is the default setting for Radio2 and Radio3. Wi-Fi multimedia (WMM) has to be enabled (default) to use IEEE 802.11n or IEEE 802.11ac. Refer to “Configuring QoS Basic Settings” on page 132.

Table 10. Basic Radio Settings Window (Continued)

Field	Description
Channel	Select the channel for the radio from the pull-down menu. Here are the guidelines: - You can select only one channel. - The channels vary by radio, bandwidth, and country. - Select "auto", the default setting, to have the radio select the channel automatically. The access point scans the available channels on the radio and selects the one with the least interference. - If you select Auto, you can use the Auto Channel Selection parameter in this window to restrict the channels from which the access point can choose. - You must set the channel manually when using the Wireless Distribution System (WDS) bridge feature. For information, refer to “WDS Bridge Elements” on page 153. - To view the current active channel, refer to “Displaying Radio Status” on page 73.
Bandwidth (Radio1)	Select the bandwidth for Radio1 from the pull-down menu. The selections for IEEE 802.11n are listed here: - 20 MHz. This is the default setting. - 40 MHz For IEEE 802.11n modes, channel width can be 40 MHz-wide or the legacy 20 MHz-wide. The 40 MHz-wide channel allows for higher data rates, but reduces the number of available channels for other wireless devices. The only bandwidth for IEEE 802.11b/g is 20 MHz.

Table 10. Basic Radio Settings Window (Continued)

Field	Description
Bandwidth (Radio2 or Radio3)	Select the bandwidth for Radio2 or Radio3 from the pull-down menu. The available bandwidths for IEEE 802.11n/ac are listed here: - 20 MHz. This is the default setting. - 40 MHz - 80 MHz The only bandwidth for IEEE 802.11a is 20 MHz.
Auto Channel Selection	Select the channels that the radio can chose 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. - The default is 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, or 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. Refer to Figure 22.

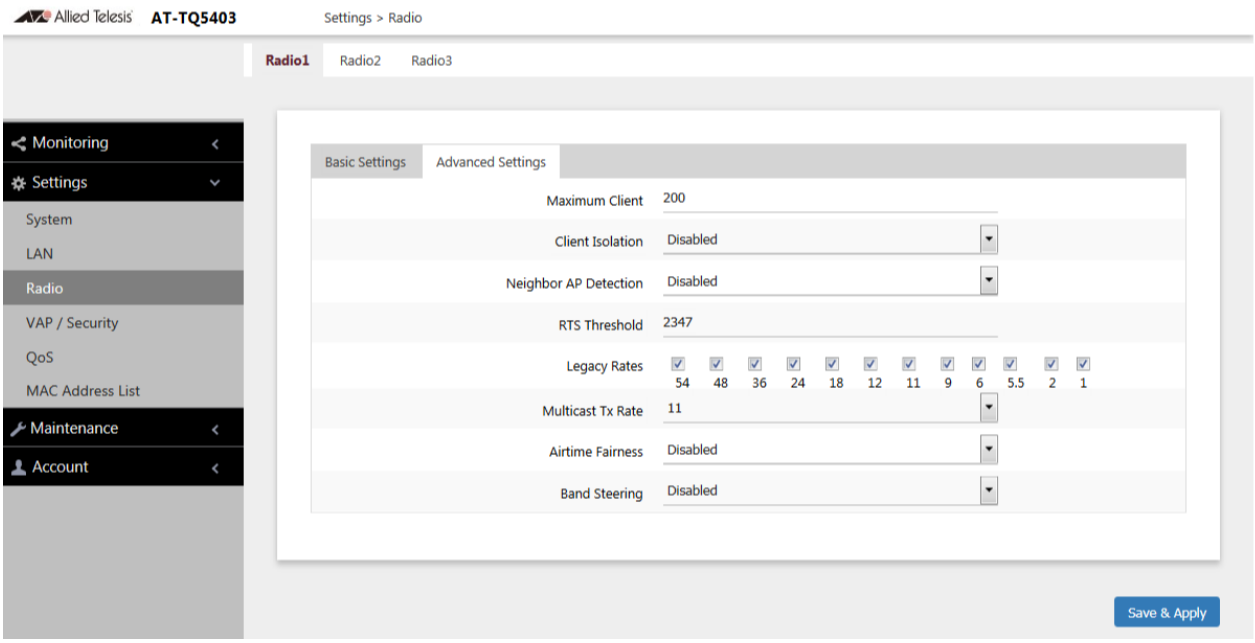

Figure 22. Advanced Radio Settings Window

4. Configure the parameters by referring to Table 11.

Table 11. 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. The guidelines are given here: - The range is 0 to 200 clients. The default is 200 clients. - The AT-TQ5403 access point can support a maximum of 200 clients on all radios at one time. - The AT-TQm5403 access point can support a maximum of 127 clients on all radios at one time. - The AT-TQ5403e access point can support a maximum of 200 clients on all radios at one time.

Table 11. Advanced Radio Settings Window (Continued)

Field	Description
Maximum Clients (continued)	- A radio rejects all clients when the parameter is set to 0. In the following example for the AT-TQ5403 access point, Radio1 is limited to a maximum of 50 clients while Radio2 and Radio3 are permitted up to 75 clients each: - 2.4GHz Radio1 - 50 clients - 5GHz Radio2 - 75 clients - 5GHz Radio3 - 75 clients
Client Isolation	Use this option to enable or disable client isolation. When the feature is enabled, the access point does not allow clients in the same VAP to communicate with each other. However, they can communicate with the wired LAN port and with clients in other VAPs. The feature is typically used to enhance wireless security. For instance, by activating this feature on a publicly accessible access point, you enable clients to communicate with the wired LAN port, but not with each other. The options are listed here: - Enabled: Activates station isolation. The access point does not allow wireless clients of the same VAP to communicate with each other. - Disabled: Deactivates 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. This feature does not apply to WDS. Refer to “Introduction to Wireless Distribution Bridges” on page 150.

Table 11. Advanced Radio Settings Window (Continued)

Field	Description
Neighbor AP Detection	Use this option to control whether the access point listens for neighboring access points. Here are the options: - Enabled: The access point listens for neighboring access points and displays them in the Neighbor AP window. Refer to "Displaying Neighboring Access Points" on page 163. - Disabled: The access point does not listen for neighboring access points. This is the default setting.
RTS Threshold	Specifies the size in octets of MPDUs that initiate a Request to Send (RTS) and Clear to Send (CTS) handshake, in IEEE 802.11b/g. 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	Select the supported and advertised data transmission rates for IEEE 802.11b/g of the radio. Here are the guidelines: - The data rates vary by country. - The default is all data rates are enabled. - Radios are generally more efficient when they advertise subsets of their supported data rates.
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 - 5GHz Radio3: 6Mbps

Table 11. Advanced Radio Settings Window (Continued)

Field	Description
Airtime Fairness	Select Enabled to activate airtime fairness to provide the same communication time (air time) to all connected clients regardless of communication speed. Select Disabled, the default, to turn Airtime Fairness off.
Band Steering	Use this option to enable or disable band steering on the radios. Band steering reduces radio congestion by forcing wireless clients that support both 2.4GHz and 5GHz radios to associate with VAPs on a different radio during periods of traffic congestion. Band steering forces clients to associate with VAPs on a 5GHz radio when there is traffic congestion on the 2.4GHz radio. Conversely, clients are forced to associate with VAPs on the 2.4GHz radio when the 5GHz radios are congested. Here are the guidelines: - Enabling band steering on one radio activates it on all three radios. Conversely, disabling the feature on one radio disables it on all radios. - Ideally, the VAP settings on all radios should be identical. This includes SSID names, VLAN IDs, and security settings. - The default setting is disabled.

5. 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 23 is for Radio1.

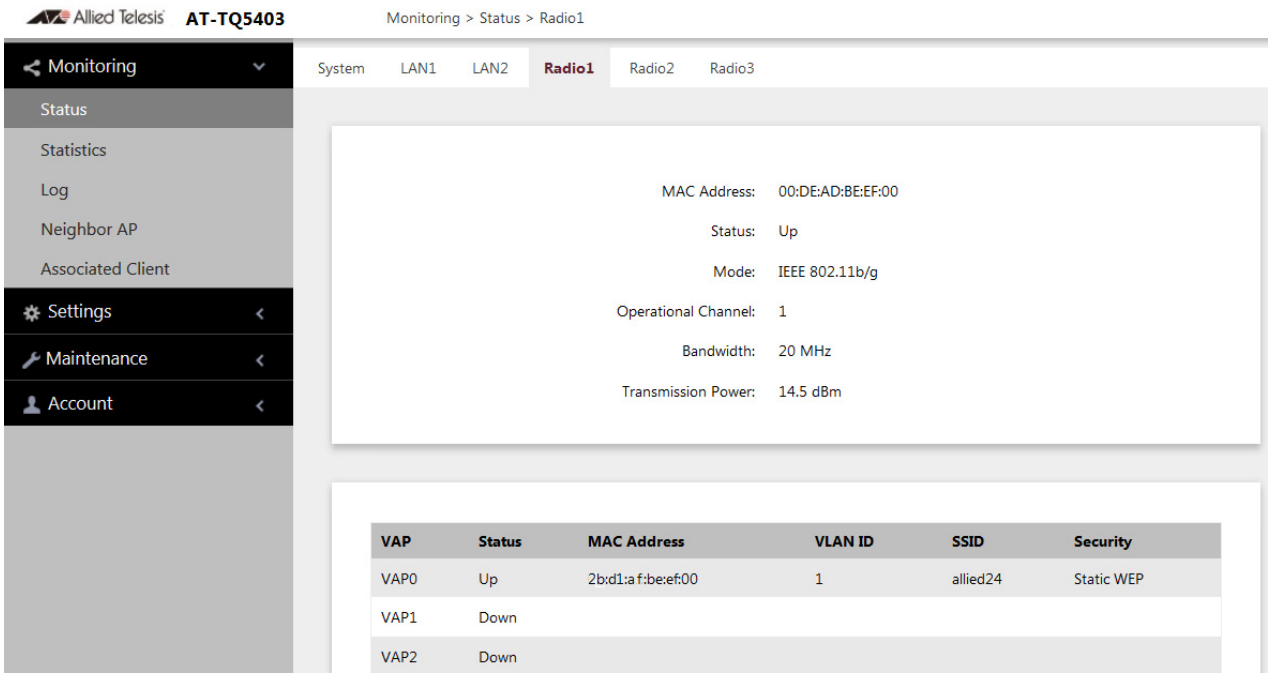

Figure 23. Radio Status Window

Note
The radio status windows for Radio2 and Radio3 include a DFS (Dynamic Frequency Selection) field. For information, refer to "Dynamic Frequency Selection" on page 75.

The fields are defined in Table 12.

Table 12. Radio Status Window

Field	Description
MAC Address	Displays the MAC address of the wireless interface.

Table 12. Radio Status Window (Continued)

Field	Description
Status	Displays the status (up, down) of the wireless interface.
Mode	Displays the current wireless communication mode. Radio1 has these modes: - IEEE 802.11b/g - IEEE 802.11b/g/n Radio2 and Radio3 have these modes - IEEE 802.11a - IEEE 802.11a/n/ac
Operational Channel	Displays the active channel. The channel may have been selected manually or automatically.
Bandwidth	Displays the current bandwidth.
Transmission Power	Displays the transmission power, in dBm.
DFS (Radio2 and Radio3 only)	Displays the status of DFS (Dynamic Frequency Selection). For background information, refer to “Dynamic Frequency Selection” on page 75. The possible states are listed here: - IDLE: DFS is inactive because the radio is using a W52 or W58 channel. Those channels are not used by DFS. - CAC: Channel Availability Check: The radio has selected a W53 or W56 channel and is performing the DFS radar detection period for one minute before beginning to transmit or receive wireless traffic. If no radar is detected, the radio moves to the ISM status. - ISM: In-Service Monitoring: The radio is using a DFS target channel. If radar is detected, it changes the channel. The DFS status changes to IDLE if the new channel is W52 or W58, or to CAC if the new channel is W53 or W56. - OOC: Out Of Channels: The radio has stopped transmitting and receiving client packets because radar signals are detected on all channel candidates. After 30 minutes, it transitions to CAC.

Dynamic Frequency Selection

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

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

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. For background information, refer to "Introduction to Wireless Distribution Bridges" on page 150.

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

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

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

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

Note
To determine whether Radio2 and Radio3 are using DFS channels, refer to "Displaying Radio Status" on page 73.

Setting the Country Code Setting

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 20 on page 64.
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 all three radios, but can only be set from Radio1.
   - ❒ The same country code applies to all three radios.
   - ❒ 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.

Selecting the Location

When your AT-TQ5403e access point is used outdoors, select the Outdoor option in the Location parameter.

Note
The location parameter is available only for the AT-TQ5403e access point.

Guidelines to Changing the Location

Here are the guidelines to changing the location:

- The location parameter is shown in the Basic Settings windows of all three radios but it can only be set from Radio1.
- The same location applies to all three radios.
- The default setting is "Indoor."
- When you use AT-TQ5403e access point in a country that has outdoor channel restrictions and select the Outdoor option in the location parameter, the radio will be disabled.

Warning
Regulatory restrictions prohibit the use of the following frequencies on the 5GHz radio on the AT-TQ5403e access point when the unit is deployed *outdoors*. The restrictions do not apply when the unit is installed indoors:

European Community (CE mark): 5180 to 5240MHz (channels 36 to 48) and 5260 to 5320MHz (channels 52 to 64)

Japan (TELEC mark): 5180 to 5240MHz (channels 36 to 48) and 5260 to 5320MHz (channels 52 to 64)

Australia and New Zealand (RCM): 5180 to 5240MHz (channels 36 to 48) and 5250 to 5350MHz (channels 52 to 64)

Russia (EAC mark): 5150 to 5250MHz (channels 36 to 48) and 5250 to 5350MHz (channels 52 to 64)

Canada (IC mark): 5180 to 5240MHz (channels 36 to 48)

Brazil (ANATEL mark):5150 to 5250MHz (channels 36 to 48)

Mexico (NOM mark): 2412 to 2447MHz (channels 1 to 8)

Changing the Location to Outdoor

To change the location to the Outdoor option, perform the following procedure:

1. Select **Settings** > **Radio**.
2. Select **Radio1** from the sub-menu. The location must be set from Radio1.
3. Click the **Basic Settings** tab. This is the default tab. See Figure 21 on page 65.
4. Select the **Location** pull-down menu and choose the Outdoor option.

   The access point displays the prompt “Do you want to use this AP outdoors? If yes, in case no legal outdoor channel for a radio, this radio will be disabled. Are you sure?”
5. Click OK or Cancel.
6. Click the **SAVE & APPLY** button to save and update the configuration.

Changing the Location to Indoor

To change the location to the Outdoor option, perform the following procedure:

1. Select **Settings** > **Radio**.
2. Select **Radio1** from the sub-menu. The location must be set from Radio1.
3. Click the **Basic Settings** tab. This is the default tab. See Figure 21 on page 65.
4. Select the **Location** pull-down menu and choose the Indoor option.
5. Click the **SAVE & APPLY** button to save and update the configuration.

Chapter 5

Virtual Access Points

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

VAP Introduction

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

- Each radio can have up to eight VAPs. Allied Telesis recommends no more than five VAPs per radio for best performance.
- The VAPs are numbered from 0 to 7.
- You can enable or disable the VAPs individually, except for VAP0, which can only be disabled by disabling its radio.
- The VAP securities are static WEP, Enterprise WPA, and Personal WPA.
- The VAPs of a radio can have different security methods.
- VAPs can have the same or different VLAN IDs.

VAP parameters are divided into these three groups:

- “Configuring Basic VAP Parameters” on page 81
- “Configuring VAP Security” on page 87
- “Configuring VAP Fast Roaming” on page 97

Configuring Basic VAP Parameters

To configure basic VAP settings, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1**, **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 **Virtual Access Point** tab. This is the default tab. The example in Figure 24 shows the settings for VAP0 on Radio1.

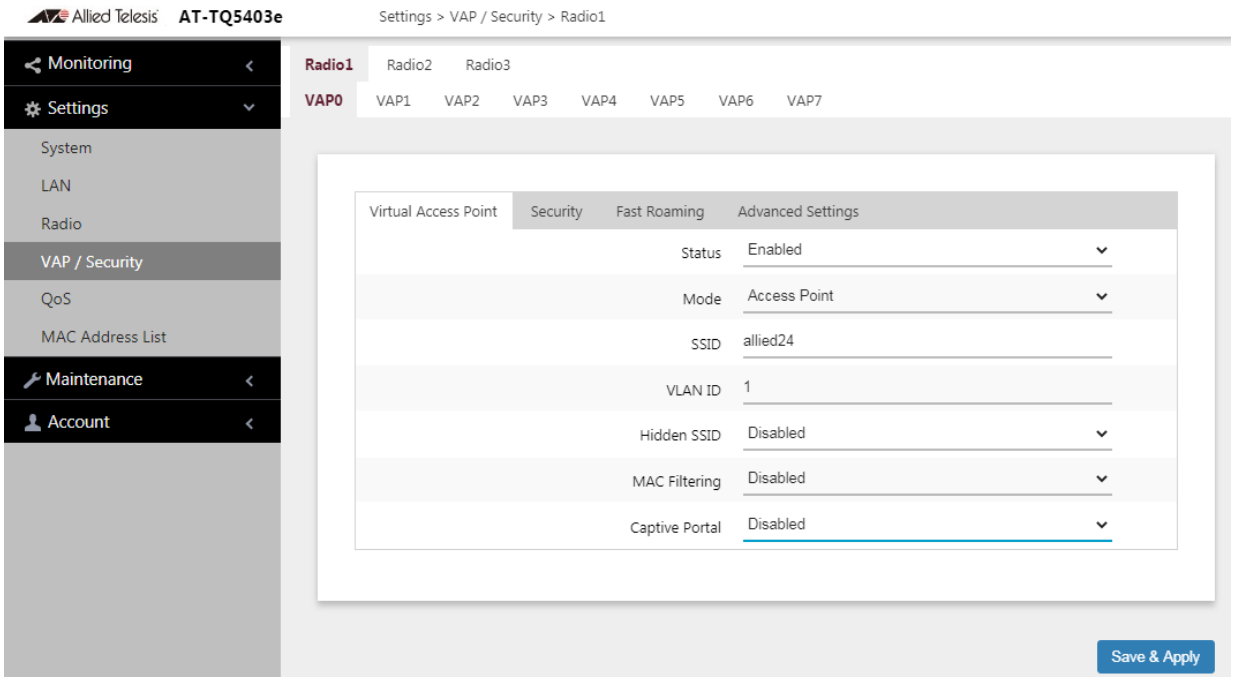

Figure 24. Virtual Access Point Tab

5. Configure the parameters by referring to Table 13 on page 82.

Table 13. 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 VAP7 is disabled. - You cannot disable VAP0. To stop VAP0 from forwarding traffic from wireless clients, you have to disable its radio.

Table 13. Virtual Access Point Tab (Continued)

Field	Description
Mode	Select a mode setting from the pull-down menu. This parameter applies only to VAP0. The menu choices are listed here: - Access Point: Select this mode to have a VAP function as a normal VAP, without WDS bridging. This is the default setting. - WDS Parent: Select this mode to have VAP0 function as the parent in a WDS bridge. A WDS parent access point has its LAN port connected to the wired network. For background information, refer to "Introduction to Wireless Distribution Bridges" on page 150. - WDS Child: Select this mode to have VAP0 function as a child in a WDS bridge. A child access point communicates with the wired network through the parent unit. - AWC-SC Node: Autonomous Wave Control - Smart Connect enables plug-and-play wireless network growth, as new APs only need a power connection, and will then automatically create resilient wireless uplink connections to other APs. Centrally managed by Vista Manager EX. - Channel Blanket (AWC-CB): Select this mode to enable single channel operation. Centrally managed by Vista Manager EX. - SC-Initial: This is the mode for temporarily connecting the AP in the initial setting state with AWC-SC. After the temporary connection, the satellite AP will be joined under the control of AT-Vista Manager EX. Centrally managed by Vista Manager EX. The only mode for VAP1 to VAP7 is Access Point.

Table 13. Virtual Access Point Tab (Continued)

Field	Description
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. ❒ You can assign the same name to more than one VAP. ❒ The default names for VAP0 on Radio1, Radio2, and Radio3 are allied24, allied5-1, and allied5-2, respectively. ❒ The default names for VAP1 to VAP7 are Virtual Access Points 1 to 7.
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 receive their VIDs from a RADIUS server for WPA Enterprise security. VIDs from a RADIUS server override the number in this field.
Hidden SSID	Select whether the access point should advertise the VAP SSID to clients. Here are the options: ❒ Disabled: The access point transmits the SSID to advertise the VAP to clients. This is the default setting. ❒ Enabled: The access point does not advertise the VAP. Clients who want to connect to an unauthorized VAP have to know its name.

Table 13. Virtual Access Point Tab (Continued)

Field	Description
MAC Filtering	Select whether the VAP is to use the MAC filter to control access by wireless clients. For instructions, refer to "Configuring the MAC Address List" on page 99. The options are listed here: ❒ Enabled: The VAP uses the MAC filter to control which wireless clients can connect to it. When wireless clients connect to the VAP, the access point compares their MAC addresses to the addresses in the MAC filter and either accepts or rejects the client traffic depending on the filter settings. ❒ Disabled: The VAP does not use the MAC filter. ❒ Area Authentication: AP allows (or denies) connection to the wireless client based on the estimated location of the wireless client by AT-Vista Manager EX. AP connects wireless clients in the area of AT-Vista Manager EX's floor map. This setting can be set only from AT-Vista Manager EX. ❒ Whitelist Authentication: This feature is not supported. ❒ External RADIUS: Selecting this option displays additional fields. Refer to Figure 25 on page 86. The MAC address filter requires that the Mode setting be Access Point. You cannot use the MAC filter on VAP0 in the WDS Parent or WDS Child mode.

Table 13. Virtual Access Point Tab (Continued)

Field	Description
Captive Portal	Configure Captive Portal. The options are: ❒ Click-Through: See “Requiring Wireless Clients to Click the Agree Button to Access to the Network” on page 119 and “Delegating a Proxy Server to Interact with Wireless Clients” on page 121. ❒ External RADIUS: See “Delegating RADIUS Servers and a Proxy Server” on page 123 and “Delegating RADIUS Servers to Authenticate Wireless Clients” on page 125. ❒ Disabled: When Captive Portal is disabled, any wireless clients can access to your network without authentication or interaction. This is the default setting.
Inactivity Timer	Specify the inactivity timer in seconds. When a wireless client is inactive exceeding the value of the inactivity timer, the client is aged out and needs to associate the wireless network again. The default value is 300 seconds.

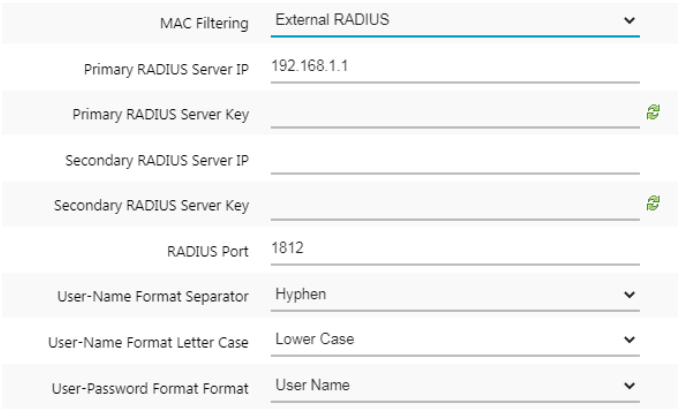

Figure 25. MAC Filtering External RADIUS

6. Click the **SAVE & APPLY** button to save and update the configuration.

Configuring VAP Security

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

No Security

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

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

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1**, **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 **None** from the Mode pull-down menu. This is the default setting. Refer to Figure 26.

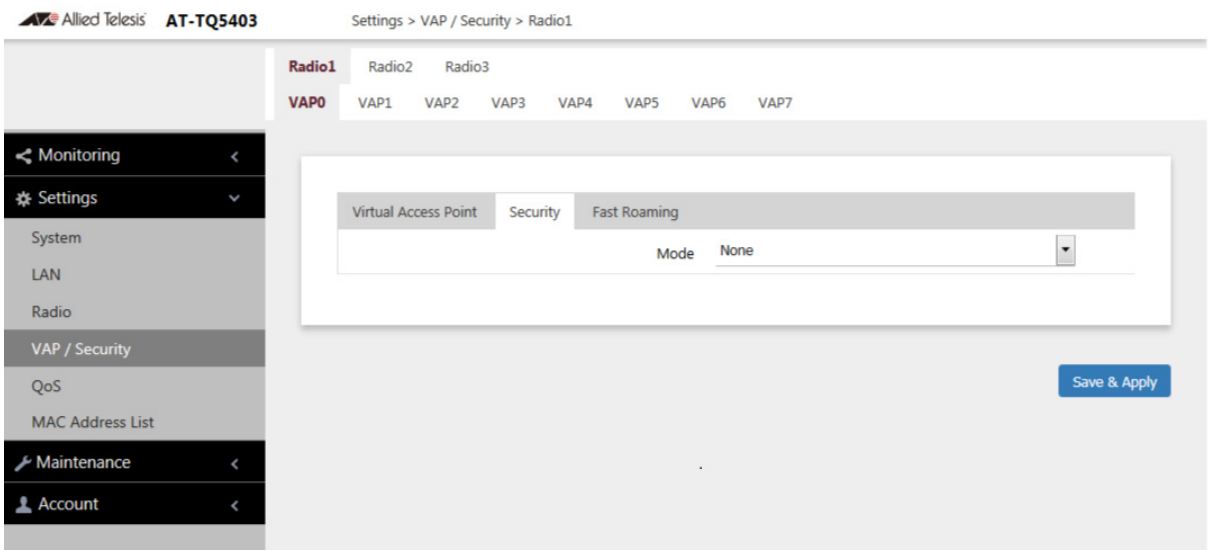

Figure 26. None Selection in the VAP Security Tab

6. Click the **SAVE & APPLY** button to save and update the configuration.

Static WEP

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

> **Note**
> Static WEP is only supported in VAP0 when the mode is IEEE802.11b/g/a. It is not supported in VAP1 to VAP7 nor the VAP0 with IEEE802.11n or ac. See “Configuring Basic Radio Settings” on page 64.

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 **Static WEP** from the Mode pull-down menu. Refer to Figure 28.

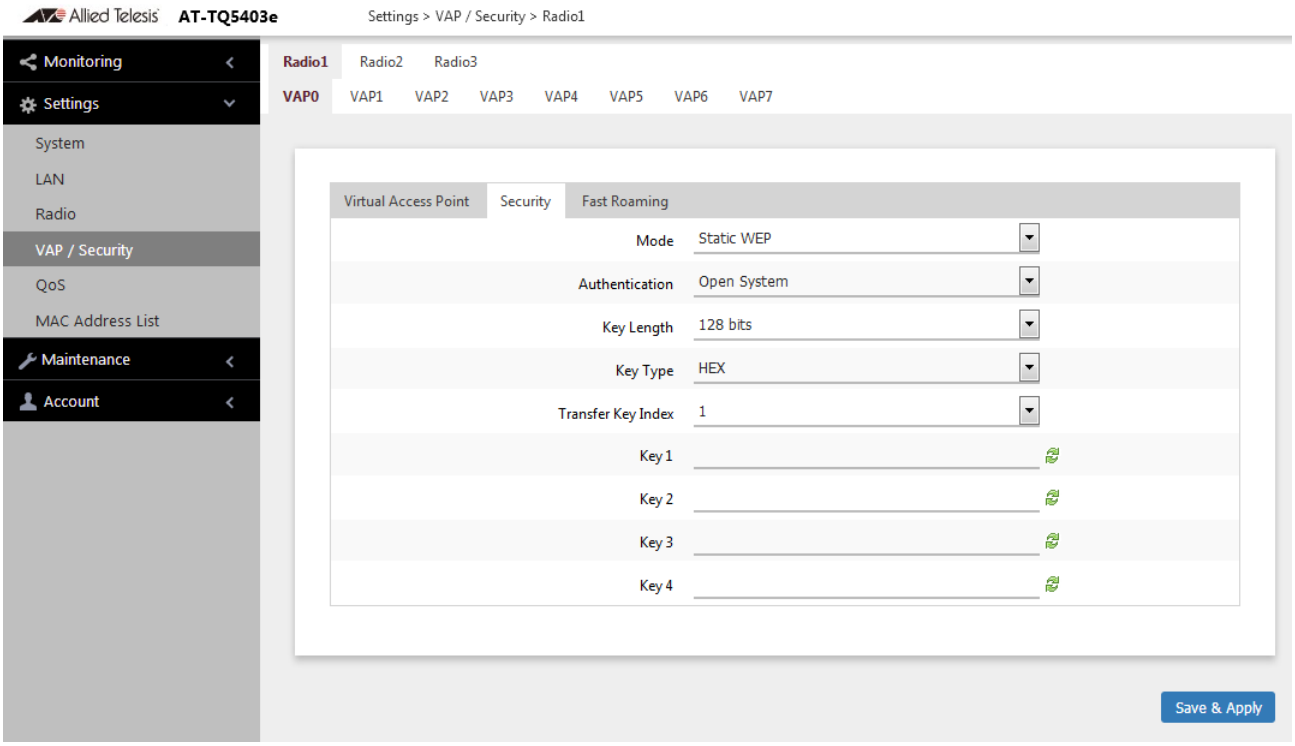

Figure 27. Static WEP Security Tab

6. Configure the parameters by referring to Table 14 on page 89.

Table 14. Static WEP Security Tab

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

Table 14. Static WEP Security Tab (Continued)

Field	Description
WEP Keys	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.

WPA Personal (Pre-Shared Key)

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

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1**, **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. Refer to Figure 28.

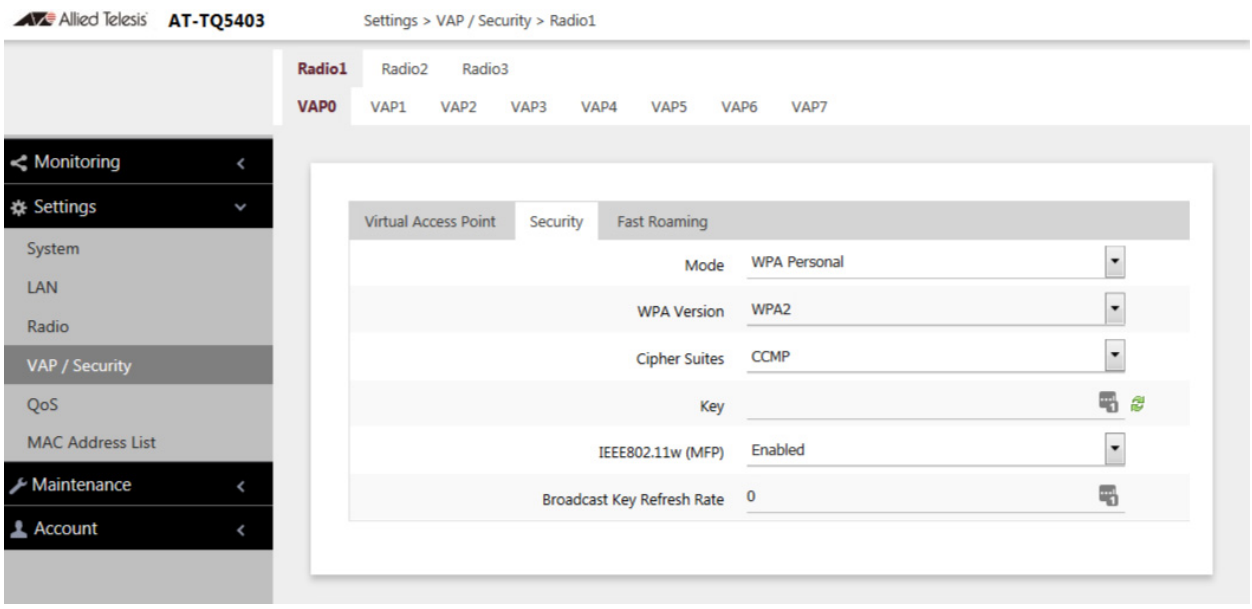

Figure 28. WPA Personal Security Tab

6. Configure the parameters by referring to Table 15.

Table 15. 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 has both WPA and WPA2 clients. - WPA2: Select this option if clients support WPA2, but not WPA. This is the default setting. - WPA2 and WPA3: Select this option if client supports WPA2 and WPA3, but not WPA. - WPA3: Select this option if client supports only WPA3.

Table 15. WPA Personal Security Tab (Continued)

Field	Description
Cipher Suites	Select the cipher suite for the VAP. The options are listed here: - CCMP. This is the default. The CCMP is the only available option when selecting either of the WPA3 options in WPA Version. - TKIP and CCMP When both TKIP and CCMP are selected, 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.
IEEE802.11w (MFP)	Control IEEE 802.11w management frame protection. This feature is only supported with WPA2 as the WPA Version. It is not supported with WPA and WPA2.The options are listed here: - Enabled: Activates management frame protection. This is the default. - Disabled: Deactivates 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.

WPA Enterprise

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

> **Note**
> WPA Enterprise is not available on VAP0 when it is the parent or child of a WDS bridge.

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1**, **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. Refer to Figure 29.

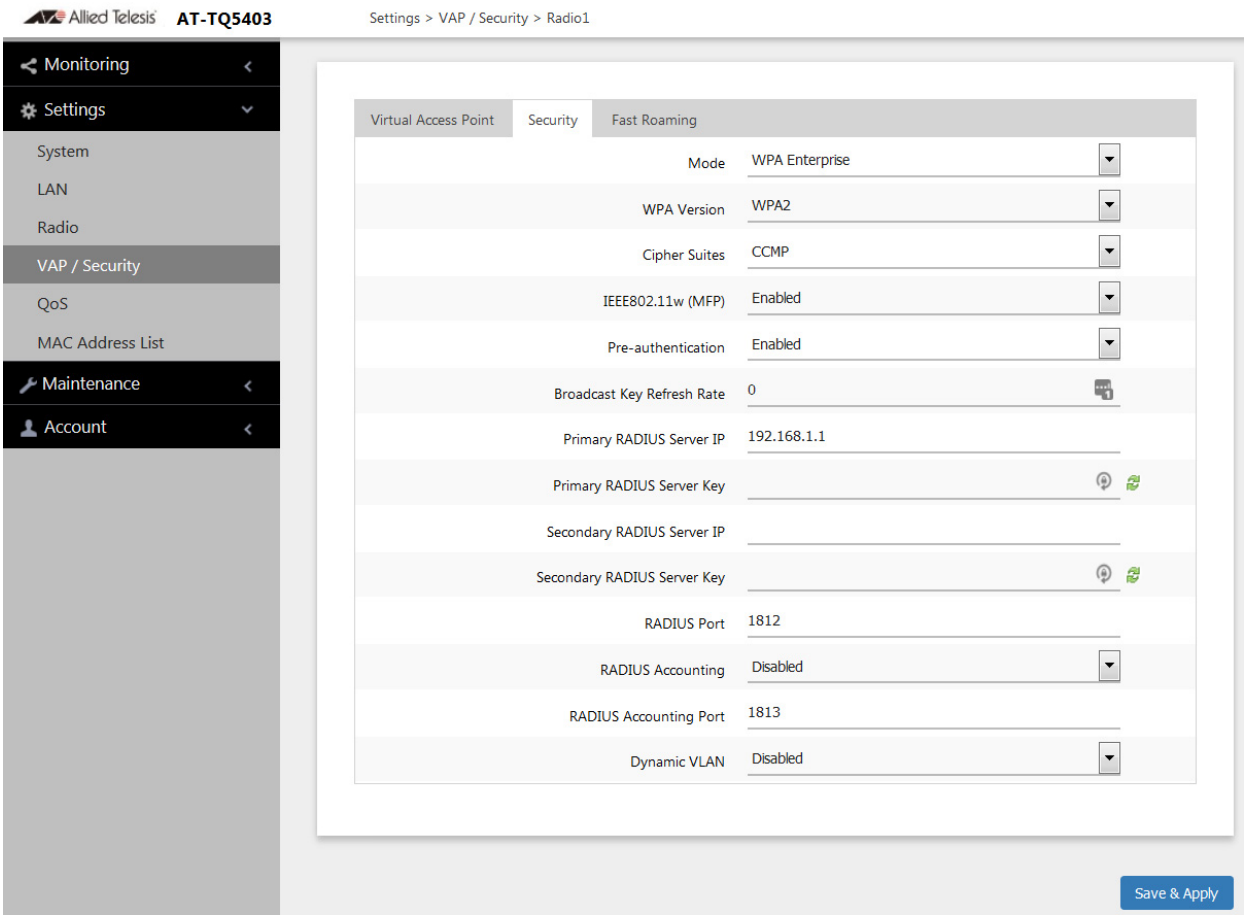

Figure 29. WPA Enterprise Tab

6. Configure the parameters by referring to Table 16 on page 94.

Table 16. WPA Enterprise Tab

Field	Description
Mode	Select **WPA Enterprise**.
WPA Version	Select the WPA version for the VAP. The options are listed - WPA2: Select this option if all the clients support WPA2, but not WPA. This is the default setting. - WPA and WPA2 - Select this option if the VAP has both WPA and WPA2 clients. - WPA3: Select this option if the VAP has WPA3 clients.
Cipher Suites	Select the cipher suite for the VAP, The options are listed here: - CCMP. This is the default. CCMP is the only available option for WPA3. - TKIP and CCMP When both TKIP and CCMP are selected, 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. This feature is only supported with WPA2 as the WPA Version. It is not supported with WPA and WPA2.The options are listed here: - Enabled: Activates management frame protection. This is the default. - Disabled: Deactivates management frame protection. Management frame protection cannot be disabled when WPA3 is selected.

Table 16. WPA Enterprise Tab (Continued)

Field	Description
Broadcast Key Refresh Rate	Enter the interval for updating the key of the broadcast packet to be sent to the wireless clients connected to the VAP. The range is 0 to 86400 seconds. The key is not updated when this parameter is set to 0 (zero). The default is 0.
Primary RADIUS Server IP	Enter the IPv4 address of the primary RADIUS server. The default is 192.168.1.1.
Primary RADIUS Server Key	Enter the shared secret key for the primary RADIUS server. Here are the guidelines: - The key can be up to 128 alphanumeric characters. - It is case-sensitive. - It must be same on the access point and server. - The default is no key.
Secondary RADIUS Server IP	Enter the IPv4 address of a secondary RADIUS server. This field is optional. The access point sends authentication requests to this address if the primary RADIUS server does not respond to requests.
Secondary RADIUS Server Key	Enter the shared secret key for the secondary RADIUS server.
RADIUS Port	Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must be using the same port number. The range is 0 to 65535. The default is 1812.
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 16. WPA Enterprise Tab (Continued)

Field	Description
RADUIS Accounting Port	Enter the RADIUS accounting port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must use the same accounting port number. The range is 0 to 65535. The default is 1813.
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.

Configuring VAP Fast Roaming

The access point supports IEEE 802.11k/v/r for high-speed roaming by wireless clients. Here are the guidelines:

- High speed roaming applies to VAPs with WPA Personal or WPA Enterprise security. It does not apply to no security or Static WEP.
- You can view but not configure the IEEE 802.11r settings with the web browser management interface. Configuring the settings requires Vista Manager EX the AT-Vista Manager EX AWC plug-in.

To configure fast roaming, 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 **Fast Roaming** tab. Refer to Figure 30.

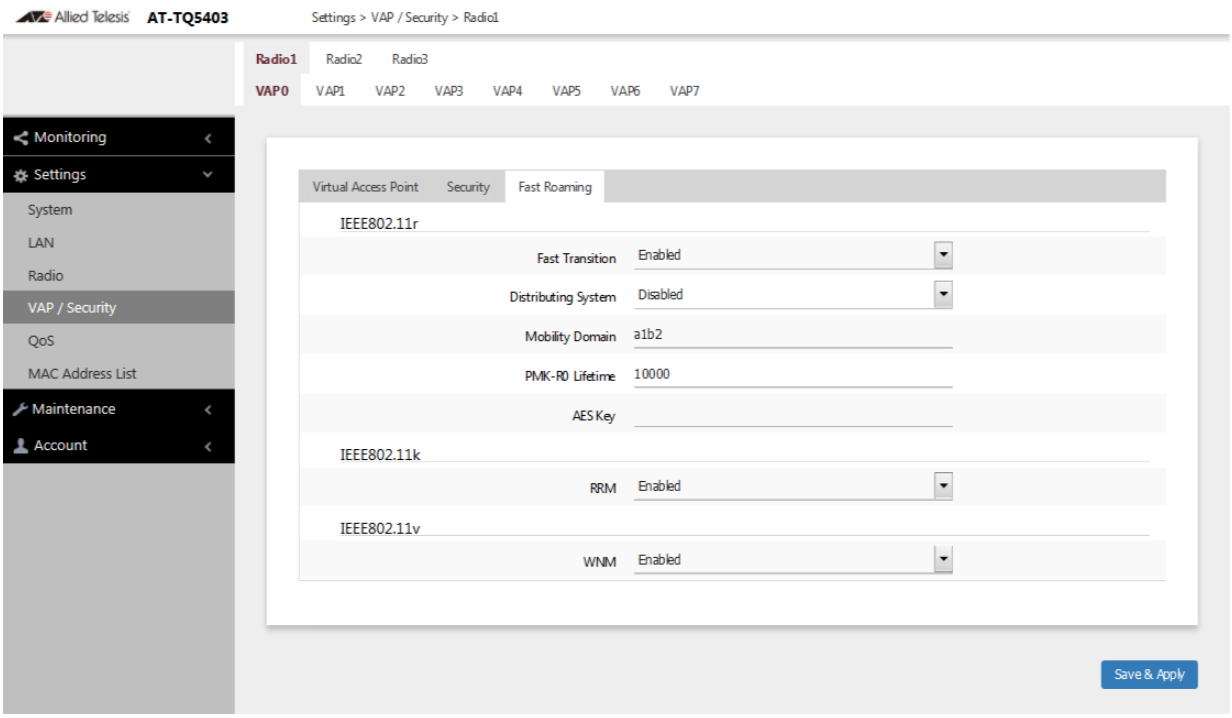

Figure 30. Fast Roaming Window

5. Configure the fields by referring to Table 17 on page 98.

Table 17. Fast Roaming Window

Field	Description
IEEE802.11r Fast Transition Distributing System Mobility Domain PMK-R0 Lifetime AES Key	Refer to the Vista Manager EX and AT-Vista Manager EX AWC documentation for descriptions of these parameters.
802.11k RRM	Select one of the following: - Enabled: Activates IEEE 802.11k Radio Resource Measurement (RRM). - Disabled: Deactivate RRM.This is the default.
802.11v WNM	Select one of the following: - Enabled: Activates IEEE 802.11v Wireless Network Management (WNM). - Disabled: Deactivates WNM. This is the default.

6. Click the **SAVE & APPLY** button to save and update the configuration.

Configuring the MAC Address List

The MAC address filter is used to control which wireless clients can access your network through the VAPs. You configure the filter by entering the MAC addresses of wireless clients whose association requests are to be accepted or rejected by the access point. If you specify the MAC addresses of the permitted nodes, the access point accepts the association requests from the specified clients and rejects requests from all other clients. If you specify the MAC addresses of the denied clients, the device rejects association requests from the specified clients and accepts requests from all other clients.

Here are the guidelines to the MAC address filter:

- The access point has only one MAC address filter.
- You can activate or deactivate the filter on individual VAPs.
- You need to know the MAC addresses of the wireless clients whose association requests the access point is to accept or reject.
- You need to know the VAPs where you want to activate the filtering. Activating filtering on VAPs is described in "Configuring Basic VAP Parameters" on page 81.

To configure the MAC address filter, perform the following procedure:

1. Select **Settings** > **MAC Address List**. Refer to Figure 31.

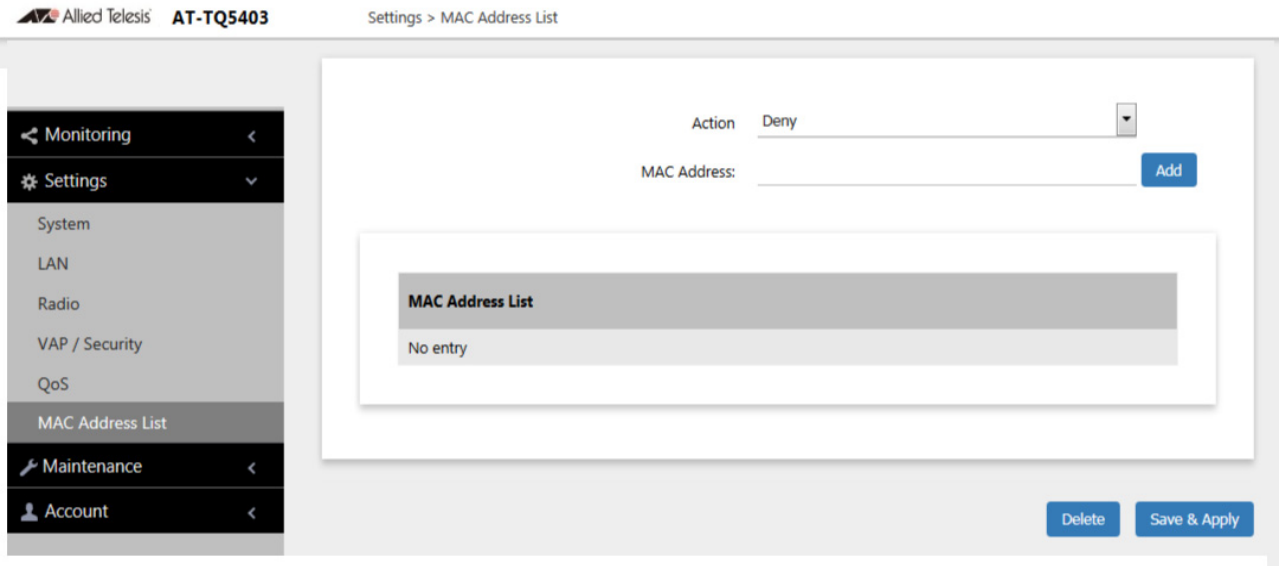

Figure 31. MAC Address List Window

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

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

3. To enter the MAC address of a wireless client the access point is to deny or accept, click the **MAC Address** field and enter the address, in this format xx:xx:xx:xx:xx:xx.

4. Click the **Add** button. You can enter only one address at a time. You cannot enter broadcast or multicast addresses.

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

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

6. Click the **SAVE & APPLY** button to save and update the configuration.

Displaying VAP and LAN Ports Statistics

To view VAP and LAN ports status and statistics, select **Monitoring** > **Statistics** window. Refer to Figure 32.

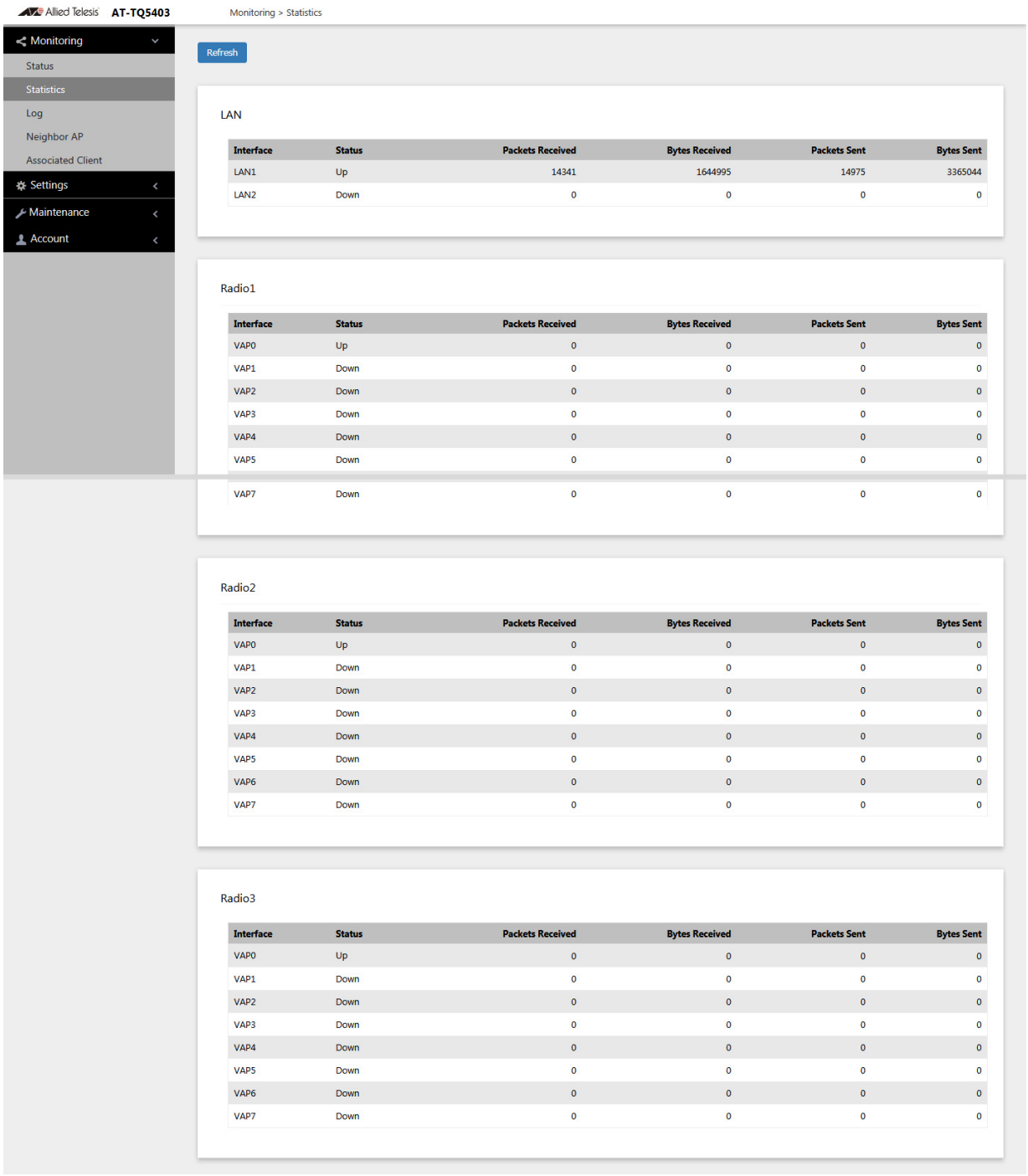

Figure 32. Statistics Window

The columns are defined in Table 18.

Table 18. Statistics Window

Column	Description
Interface	Displays LAN1 and LAN 2 ports, and VAPs 0 to 7.
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.

Advanced Settings

To configure security advanced 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. You can configure only one VAP at a time.
4. Select the **Advanced** tab. This is the default tab. The example in Figure 33 shows the settings for advanced items.

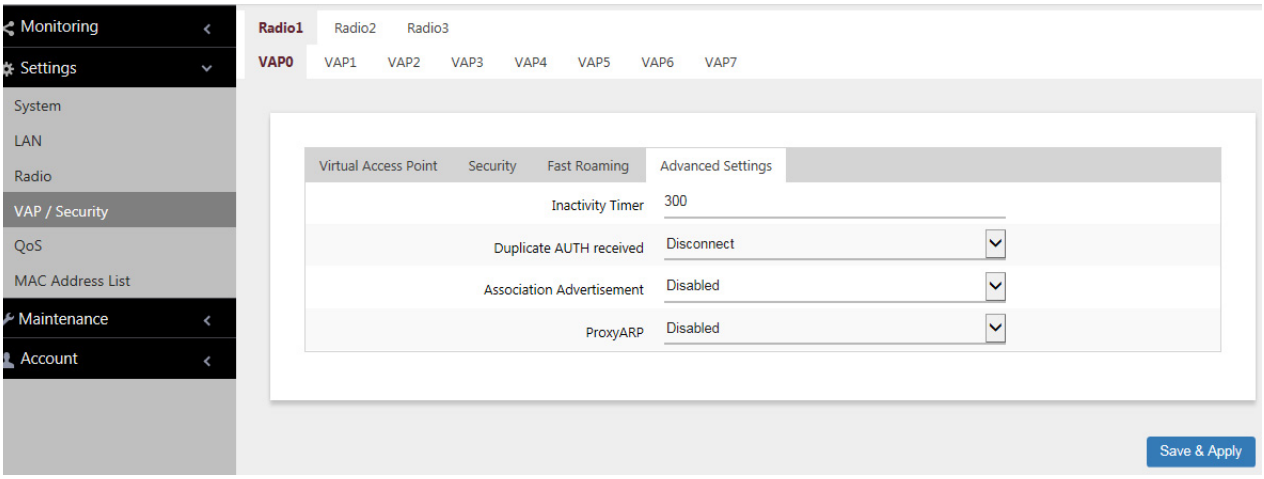

Figure 33. Advanced Settings Tab

5. Configure the parameters by referring to Table 19 on page 103.

Table 19. Advanced Settings Tab

Field	Description
Inactivity Timer	Specifies how long the access point allows inactive wireless clients to remain associated to it. The access point disconnects inactive clients when the timer expires. Here are the guidelines: - The default is 300 seconds. - You can enter only one value.

Table 19. Advanced Settings Tab (Continued)

Field	Description
Duplicate AUTH Received	Controls how the access point responds when it receives authentication requests from wireless clients it has already authenticated. The options are listed here: - Disconnect: The access point responds to duplicate authentication requests by sending deauthentications and disconnecting the clients. This is the default setting. - Ignore: The access point responds to duplicate authentication requests by authenticating the clients again.
Association Advertisement	Controls whether the access point informs other access points of newly associated clients, over the wired network. When the access point associates new clients, it can inform the access points to which the clients were previously connected of the change. This enables access points to update their lists of associated clients more quickly. The options are listed here: - Disabled: The access point does not inform other access points of newly associated clients. This is the default setting. - Enabled: The access point does inform other access points of new clients.
Proxy ARP	This feature is not supported at this time. This option must be set to Disabled.

6. Click the **SAVE & APPLY** button to save and update the configuration.

Generating Quick Response Codes for VAPs

You can now generate Quick Response (QR) codes for the individual VAPs on the wireless access points. Wireless clients can scan the codes to join VAPs on the wireless access points without having to manually enter the information. You can generate QR codes for VAPs that have the following security settings:

- None
- Static WEP / Authentication: Open System / Key Type: HEX or ASCI
- Static WEP / Authentication: Shared Key / Key Type: HEX or ASCI
- WPA Personal / WPA Version: WPA and WPA2
- WPA Personal / WPA Version: WPA2
- WPA Personal / WPA Version: WPA2 and WPA3
- WPA Personal / WPA Version: WPA3

Here are the guidelines:

- Codes are generated by clicking the View QR Code button in the Virtual Access Point windows in the on-board web browser management interface of the TQ5403 Wireless Access Point. Refer to Figure 34 on page 106.
- QR codes are not supported on VAPs that use RADIUS servers to authenticate wireless clients.
- QR codes require firmware v6.0.1-2.1 or later.

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 to configure for the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Configure the VAP settings. Refer to the earlier sections in this chapter.
5. Return to the **Virtual Access Point** tab.
6. Click the **View QR Code** button. Refer to Figure 34 on page 106.

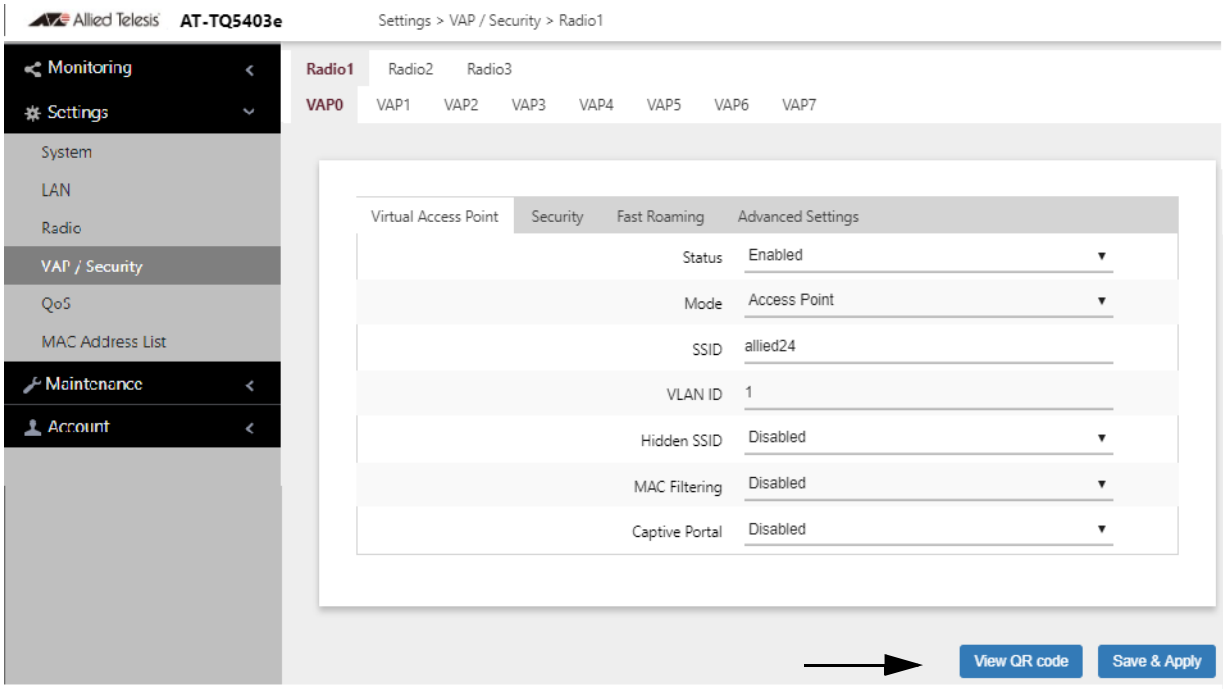

Figure 34. View QR Code Button

Configuring Channel Blankets

In conventional wireless networks, neighboring wireless access points whose transmissions overlap use different channels to avoid interference. Overlapping signals are often required in network environments to ensure that all physical work areas are adequately covered. Conventional wireless networks of multiple channels work best for stationary clients who remain connected to the same wireless access points at all times. They can, however, pose problems for roaming clients. Packets might be lost as clients change channels as they transition between access points. Also, roaming clients may experience slow traffic if, instead of transitioning, they remain connected to their original access points after moving a distance away.

Channel blankets offer a different approach for wireless access points whose transmissions overlap. Rather than having to use multiple channels, they can all use the same channel, thereby forming a single large virtual access point for their wireless clients. This avoids the need for roaming clients to change channels as they transition between access points, thus reducing the chance of lost packets. Channel blankets also reduce the need for complex channel planning.

The access points also support combining multiple channel and channel blanket networks at the same time. This is referred to as hybrid operations. You can implement multiple channel networks for the stationary clients and channel blankets for roaming clients.

Note
Channel blankets require Vista Manager EX and AWC. You have to use AWC to configure access points for channel blankets. For instructions, refer to the *Vista Manager EX and AWC Plug-in User Guide*.

To determine whether a VAP is configured for channel blankets by AWC, 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 from the next sub-menu. The default is VAP0.
4. Select the **Virtual Access Point** tab. This is the default tab.
5. Select the **Mode** pull-down menu. Refer to Figure 35 on page 108:

6. Review the following:

   - If the **Channel Blanket** option in the pull-down menu is inactive (grayed out), the VAP is not configured for channel blankets by AWC.
   - If the **Channel Blanket** option in the pull-down menu is active, then the VAP is configured for channel blankets by AWC.

Note
Selecting **Channel Blanket** displays the BSSID for the channel blanket of the VAP. The value is for viewing purposes only. You have to use AWC to configure channel blankets.

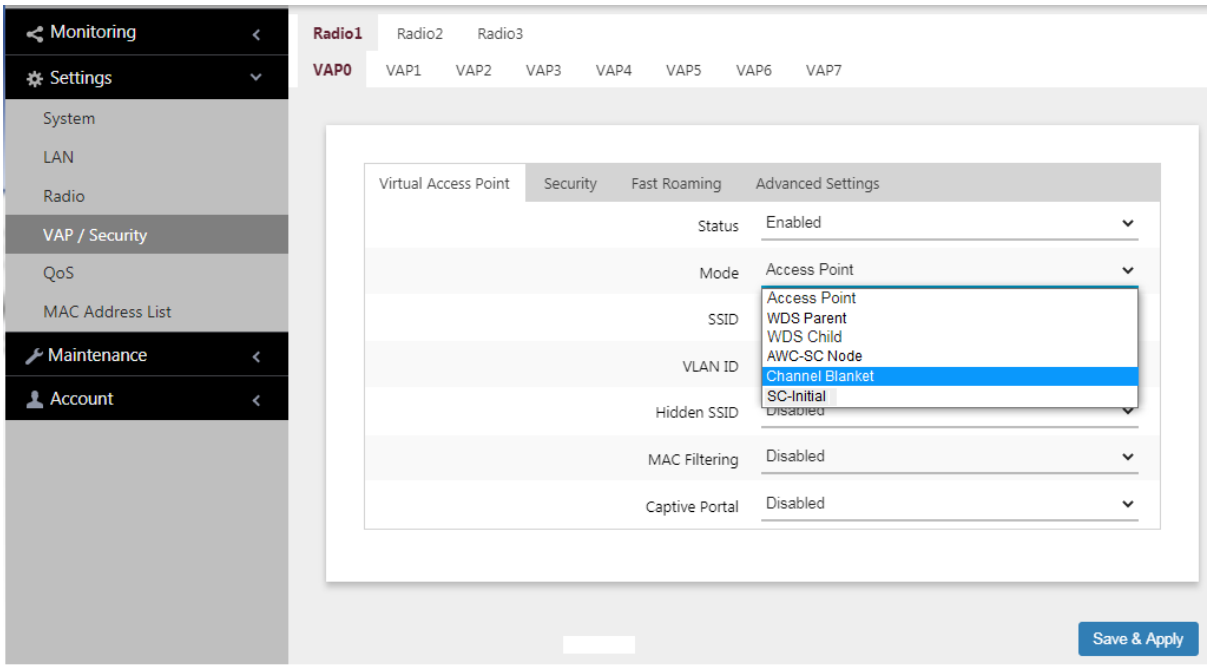

Figure 35. Mode Pull-down Menu

Authenticating Wireless Clients with an External RADIUS Server

The wireless access points have several methods for controlling access by wireless clients to your wireless networks, based on clients' MAC addresses. One method uses the on-board MAC address filter. As described in the User Guides, it allows you to specify the MAC addresses of the wireless clients whose traffic the access points are to either accept or reject. You can apply the filter to the individual VAPs, and so add filtering to those VAPs where it is most needed.

The on-board filter is fine if you have a small number of wireless access points and MAC addresses. But for larger wireless networks, managing and updating the MAC address filters on many access points can be difficult.

Starting with version 5.2.0, you can centralize the list of MAC addresses of the wireless clients on an external RADIUS server. This simplifies management because you only have to manage the list on the server, rather than on the individual access points. When access points receive connection requests from wireless clients, they send the MAC addresses of the clients to the RADIUS server for authentication, and do not allow the clients access to the network until they receive a response from the server.

Note
Once you configure a VAP for RADIUS server authentication, only those wireless clients whose MAC addresses you have added to the server can connect to the VAP.

To configure a VAP to use an external RADIUS server to authenticate wireless 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 for the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Virtual Access Point** tab. This is the default tab.
5. Select **External RADIUS** from the MAC Filtering option. Refer to Figure 36 on page 110:

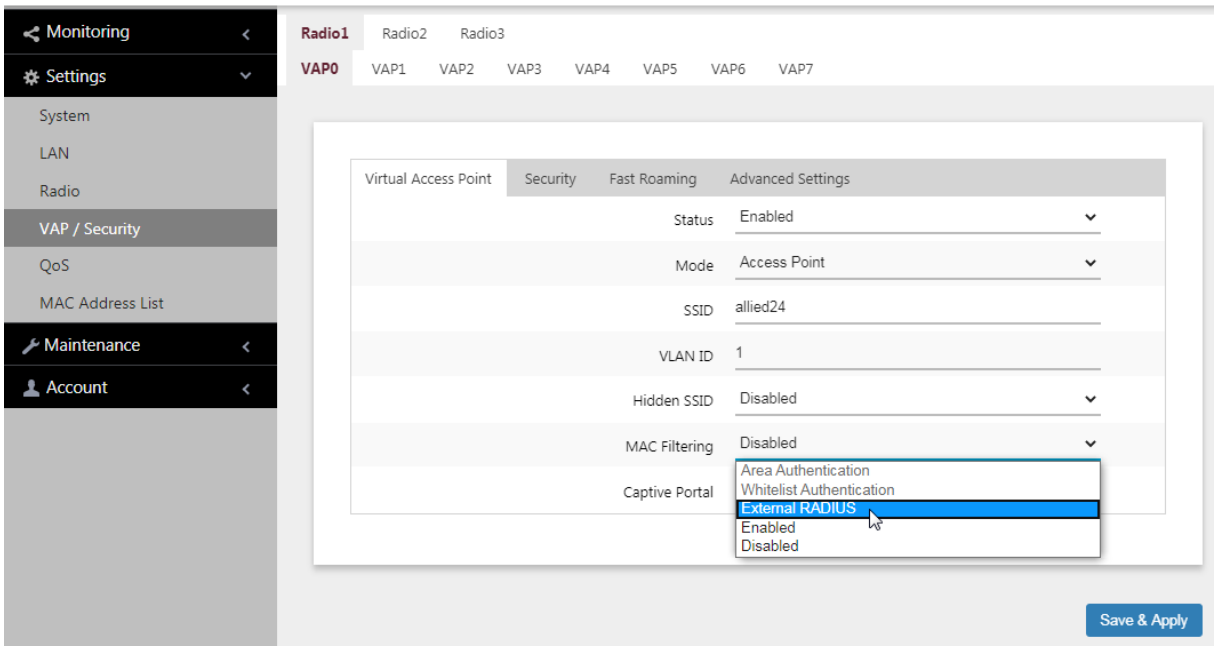

Figure 36. External RADIUS Selection

Selecting External RADIUS displays the additional settings shown in Figure 36.

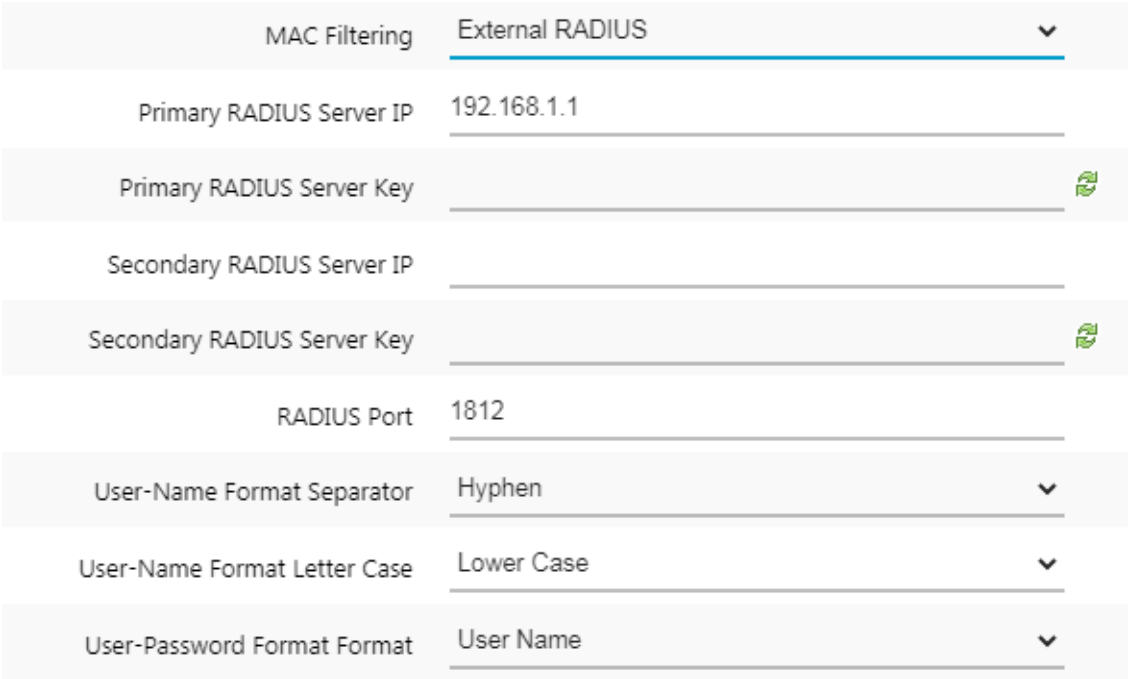

Figure 37. External RADIUS Fields

6. Configure the fields by referring to Table 20.

Table 20: External RADIUS Fields

Parameter	Description
Primary RADIUS Server IP	Enter the IP address of the primary RADIUS server. This field is required. The address has to be entered in the following format: *nnn.nnn.nnn.nnn*
Primary RADIUS Server Key	Enter the secret key of the server. The server key is used by the RADIUS server and access points to encrypt passwords and exchange responses. The key can be up to 64 alphanumeric and symbol characters. This field is required.
Secondary RADIUS Server IP	Enter the IP address of a secondary RADIUS server. This field is optional.
Secondary RADIUS Server Key	Enter the secret key of the server. The key can be up to 64 alphanumeric and symbol characters. This field is optional.
RADIUS Port	Enter the protocol port number for the server. The range is 1 to 65535. The default is 1812. If you specified both primary and secondary servers, both servers have to use the same port number. This field is required.
User-Name Format Separator	Select the character that the wireless access point should use to separate the octets in the MAC addresses it sends to the servers. (The MAC addresses function as the user-name attributes for the wireless clients.) The choices are listed here: - Hyphen (nn-nn-nn-nn-nn-nn) - Colon (nn:nn:nn:nn:nn:nn) - None (nnnnnnnnnnnn)
User-Name Format Letter Case	Specify whether the wireless access point should send the MAC addresses using uppercase or lower 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.

Table 20: External RADIUS Fields (Continued)

Parameter	Description
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. Refer to Figure 38.
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.

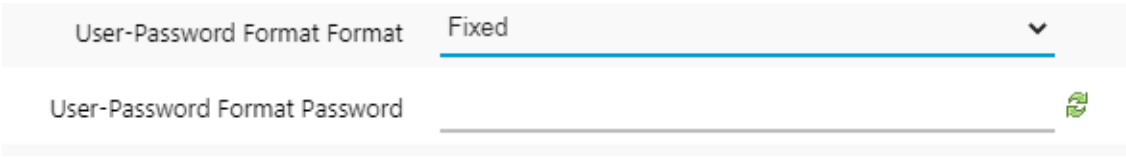

Figure 38. User-Password Format Password

7. Click the **SAVE & APPLY** button to save and update the configuration.

Managing Smart Connect

Smart Connect (SC) is an extension of the wireless distribution system (WDS). The features share similar functions in that they both allow access points to forward traffic directly to each other over wireless connections, as if they were connected with physical Ethernet wires. The features can be used to extend networks into areas where Ethernet cable Installation might be impractical or expensive. Differences between the features include:

- SC requires Vista Manager EX and AWC.
- With WDS, you have to configure the feature on the individual access points. With SC, access points can obtain their operating configurations and form the wireless connections automatically over the wireless connections, without pre-configuration.
- WDS and SC support different numbers of access points. WDS supports a maximum of one parent and three children. For each root unit SC supports up to four connector units, and sixteen terminator units.
- Access points in SC networks are able to dynamically change their wireless paths to the most optimal paths.
- Access points in SC networks are also able to maintain redundant paths for more resilient networks.
- SC requires firmware v6.0.1-1.1 or later.

Note
SC on the TQ5403 access points requires Vista Manager EX and AWC. All configuration steps for SC have to be performed on AWC. For instructions, refer to *Vista Manager EX and AWC Plug-in User Guide*.

To determine whether an access point is currently configured for SC, 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 **VAP0**.
4. Select the **Virtual Access Point** tab. This is the default tab.
5. Select the **Mode** pull-down menu. Refer to Figure 35 on page 108:

6. Review the following:

   - If the **AWC-SC Node** and **SC-Initial** options in the pull-down menu are inactive (grayed out), the access point is not configured for SC by AWC. Consequently, SC is not active on the access point.
   - If the options in the pull-down menu are active, then the access point is configured for SC by AWC.

   Note
   Selecting the AWC-SC Node and SC-Initial options in the Mode menu does not perform any function.

Configuring Area Authentication

Wireless networks that use channel blankets to improve wireless performance for roaming clients can add a layer of security with area authentication. The feature, which requires Vista Manager EX version 3.2.1 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 Filtering pull-down menu in Virtual Access Point tabs has an Area Authentication selection, as shown in Figure 39. However, the feature has to be configured with the AWC plug-in. Refer to the Vista Manager EX version 3.2.1 and AWC plug-in documentation for configuration instructions.

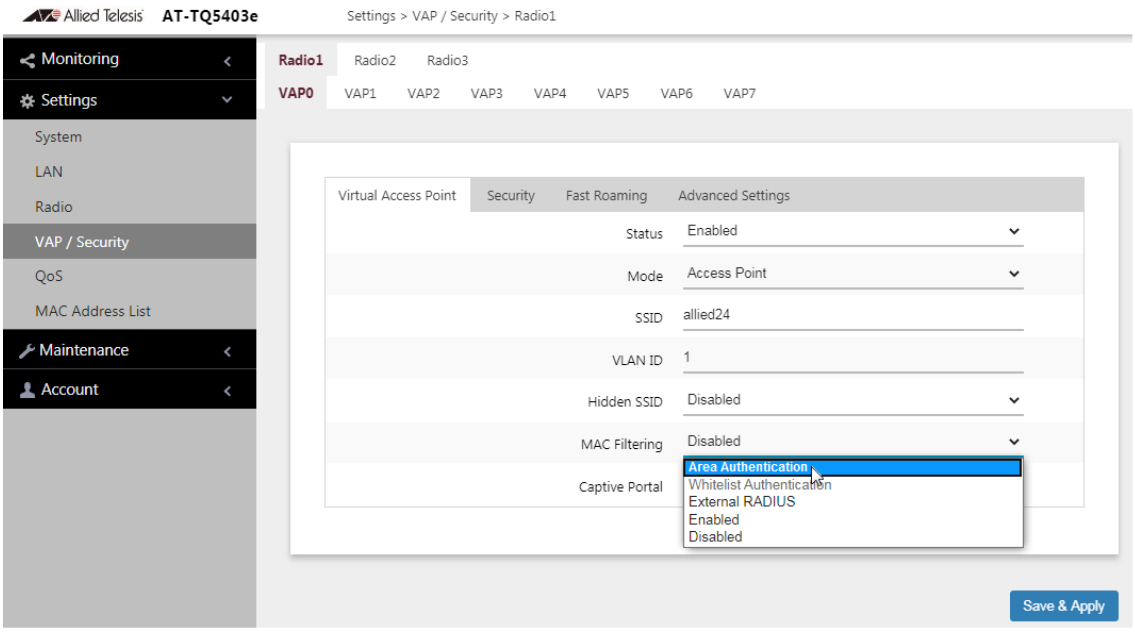

Figure 39. Area Authentication

Configuring Whitelist Authentication

The Whitelist Authentication option in the MAC Filtering pull-down menu in the Virtual Access Port window is not supported in this release. Refer to Figure 40.

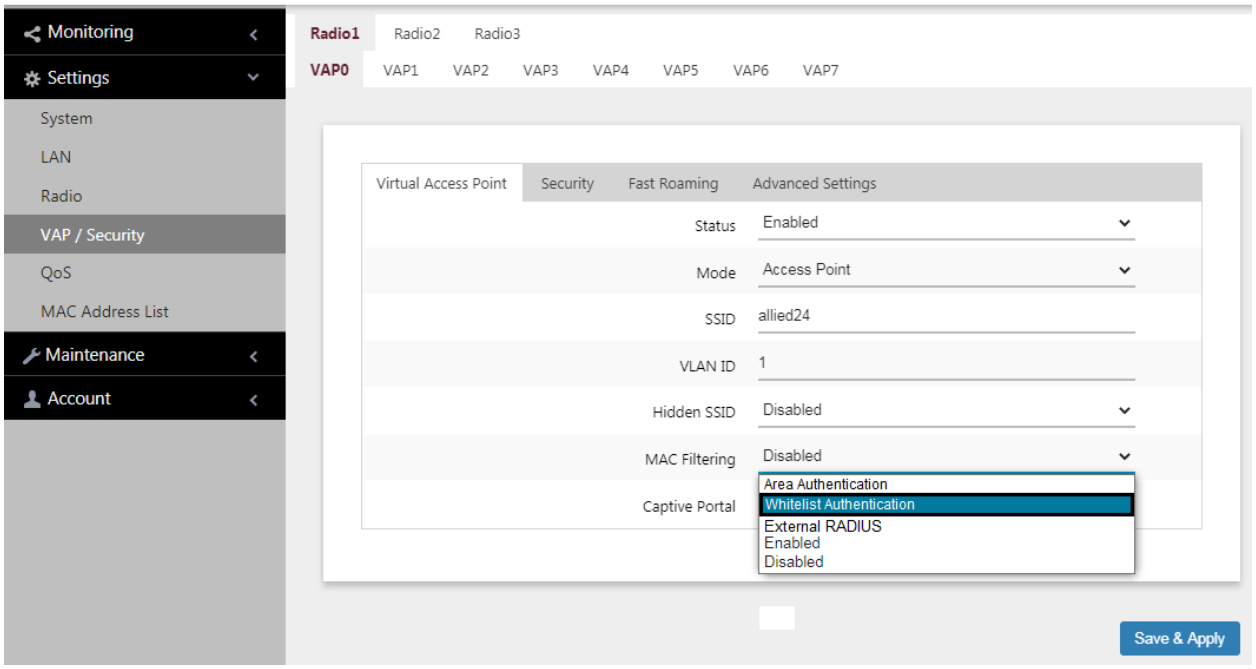

Figure 40. Whitelist MAC Filtering

Chapter 6

Virtual Access Points – Captive Portal

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

Configuring Captive Portal

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

Captive Portal Configurations

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

- Allowing any wireless clients to access to your networks

  When Captive Portal is disabled, any wireless clients can access to your network without authentication or interaction. This is the default setting.

- "Requiring Wireless Clients to Click the Agree Button to Access to the Network" on page 119

  A web page including your message and the Agree button is displayed. Your message is stored on the access point. Wireless clients do *not* go through an authentication process.

- "Delegating a Proxy Server to Interact with Wireless Clients" on page 121

  Interacting with wireless clients is conducted by the proxy server that you specify. The proxy server hosts web pages so that you can create your own web pages and applications if necessary. See "Creating Pages in HTML for a Proxy Server" on page 126.

- "Delegating RADIUS Servers and a Proxy Server" on page 123

  An authentication process is conducted by a RADIUS server that you specify. You also specify a proxy server to host web pages to interact with wireless clients. You can create your own HTML files on the proxy server. See "Creating Login Pages in HTML When External RADIUS is Selected" on page 127.

- "Delegating RADIUS Servers to Authenticate Wireless Clients" on page 125

  An authentication process is conducted by a RADIUS server that you specify. The pre-fixed HTML files stored in the access point are used to interact with wireless clients. You cannot change these HTML files.

Port Numbers

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

- 8080 for HTTP

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

- 8443 for HTTPS

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

Requiring Wireless Clients to Click the Agree Button to Access to the Network

To require wireless clients to click the Agree button to access to the networks, 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 **Virtual Access Point** tab. See the example in Figure 24 on page 81.
5. Select **Click-Through** from the Captive Portal pull-down menu. See Figure 41 on page 120.

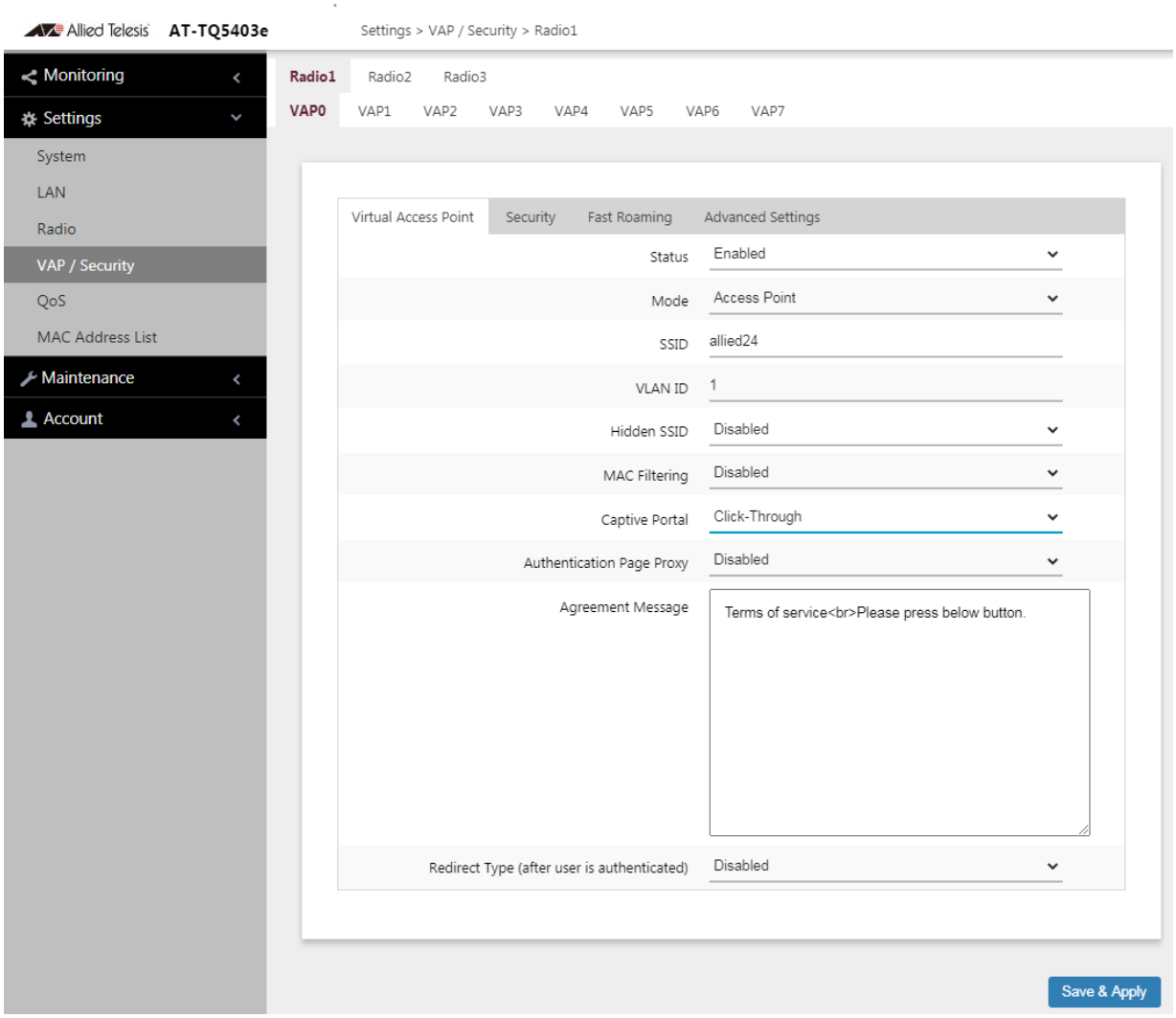

Figure 41. Captive Portal - Click-Through

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

   By default, the Authentication Page Proxy is disabled.

7. Configure the parameters by referring to Table 21.

Table 21. Captive Portal

Field	Description
Authentication Page Proxy	❒ Enabled: The AP uses other web server's Authentication page via proxy with captive portal. ❒ Disabled: AP uses own local Authentication page with captive portal. This is the default. Refer to "Delegating a Proxy Server to Interact with Wireless Clients" on page 121.
Agreement Message	Enter Conditions of Use or other information in the HTML code format to be displayed in the introductory web page.
Redirect Type (after user is authenticated)	Select the following options to control a Web page to be displayed to wireless clients after they are allowed to access to the network. The options are: - Fixed URL: Allows you to specify a URL to redirect to wireless clients. When this option is selected, the Fixed URL field becomes available. - Session Keep: Displays a web page that wireless clients originally requested. - Disabled: Redirect is disabled. The welcome.html that you prepared is displayed. When the Capital 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.
Fixed URL	Specify the URL of a web page. Wireless clients are redirected to the specified web page. To use this field, the Redirect Type must be Fixed URL.

8. Click the **SAVE & APPLY** button to save and update the configuration.

Delegating a Proxy Server to Interact with Wireless Clients

You can delegate a proxy server to conduct authentication or interaction without authentication. The proxy server that you specify hosts web pages so that you must create web pages and applications on the proxy server.

To delegate a proxy server to interact with wireless 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. You can configure only one VAP at a time.
4. Select the **Virtual Access Point** tab. See the example in Figure 24 on page 81.
5. Select **Click-Through** from the Captive Portal pull-down menu. See Figure 42 on page 122.
6. Select **Enabled** from the Authentication Page Proxy pull-down menu. See Figure 42 on page 122.

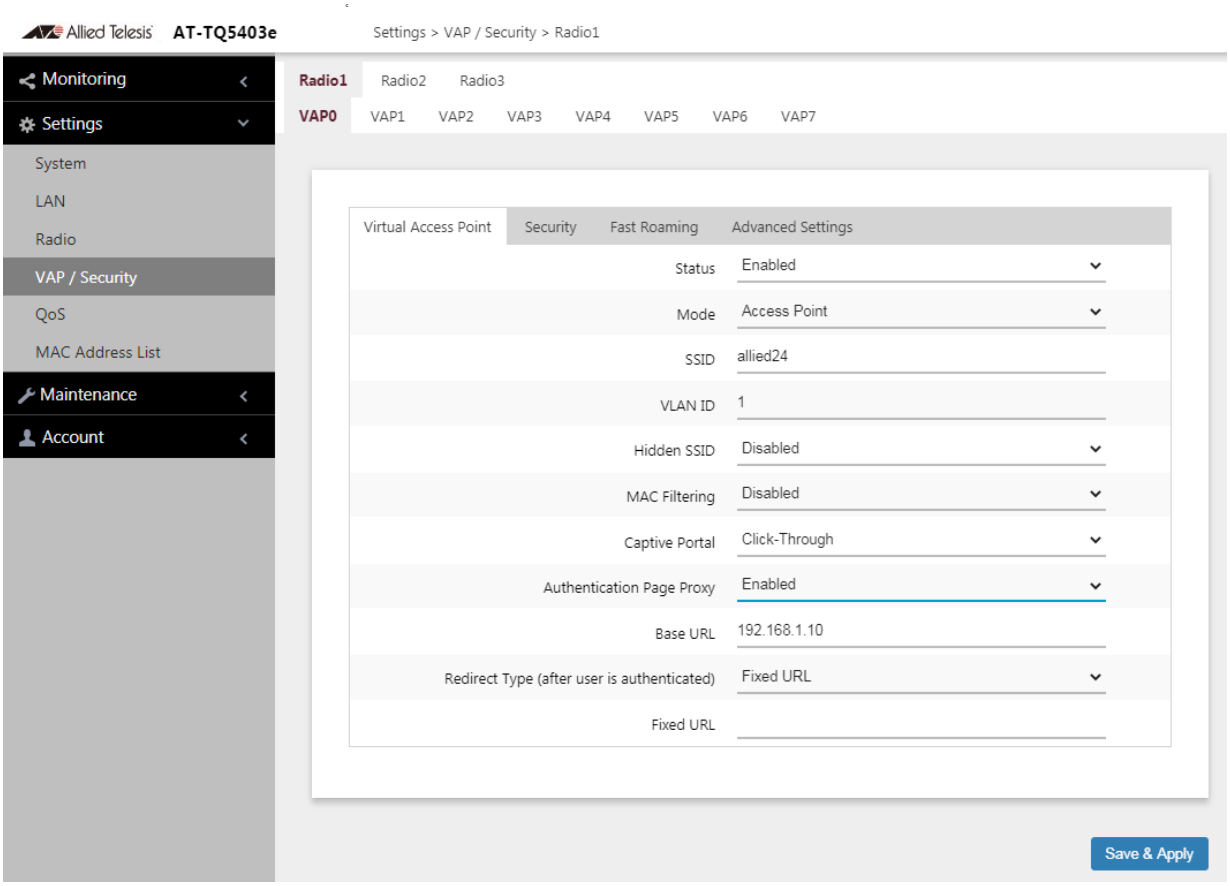

Figure 42. Captive Portal - Using a Proxy Server

7. Specify a URL of your web server in the Base URL field.
8. Specify the Redirect Type field by referring to Table 21 on page 121.
9. Click the **SAVE & APPLY** button to save and update the configuration.

10. Go to "Creating Pages in HTML for a Proxy Server" on page 126 to create the HTML files.

Delegating RADIUS Servers and a Proxy Server

You can delegate RADIUS servers to authentication wireless clients and delegate a proxy server to interaction with these wireless clients. The RADIUS servers authenticate wireless clients. The proxy server hosts web pages so that you can create your own web pages and applications on the proxy server.

To delegate RADIUS servers and a proxy server, perform the following procedure:

To display an authentication page hosted by a RADIUS server when wireless clients access to network resources, 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 **Virtual Access Point** tab. See the example in Figure 24 on page 81.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 43.
6. Select **Enabled** from the Authentication Page Proxy pull-down menu. See Figure 43 on page 124.

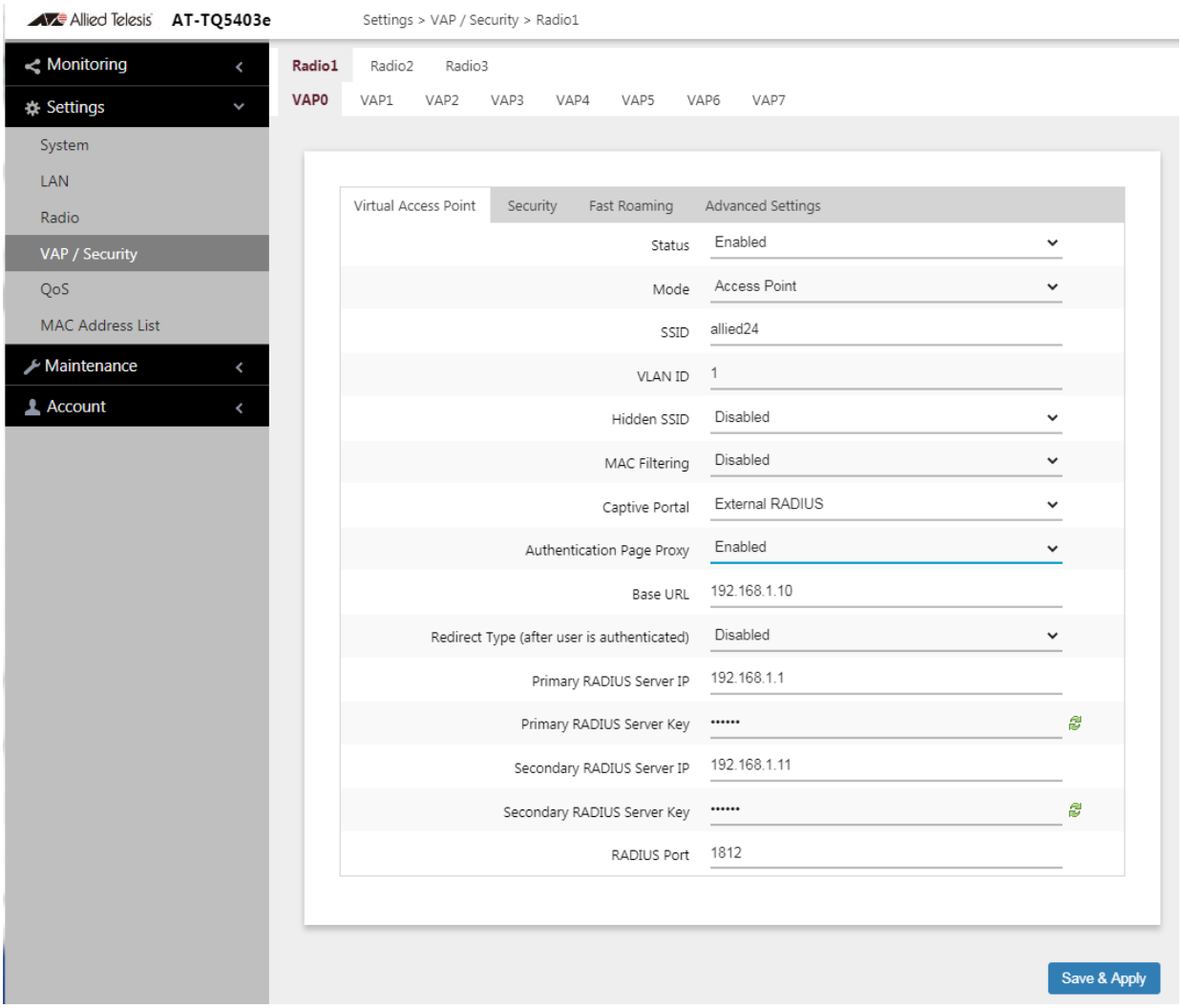

Figure 43. Captive Portal - External RADIUS

7. Configure the parameters by referring to Table 22.

Table 22. Captive Portal - External RADIUS

Field	Description
Authentication Page Proxy	See Table 21 on page 121.
Redirect Type	See Table 21 on page 121.
Primary RADIUS Server IP	Enter the IPv4 address of the primary FADIUS server. The default is 192.168.1.1

Table 22. Captive Portal - External RADIUS (Continued)

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

8. Click the **SAVE & APPLY** button to save and update the configuration.
9. Go to "Creating Login Pages in HTML When External RADIUS is Selected" on page 127 to create the HTML files.

Delegating RADIUS Servers to Authenticate Wireless Clients

You can delegate RADIUS servers to authenticate wireless clients. The pre-fixed HTML files stored in the access point are used to interact with wireless clients.

To delegate RADIUS servers, 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 **Virtual Access Point** tab. See the example in Figure 24 on page 81.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 44.
6. Select **Disabled** from the Authentication Page Proxy pull-down menu. See Figure 44.

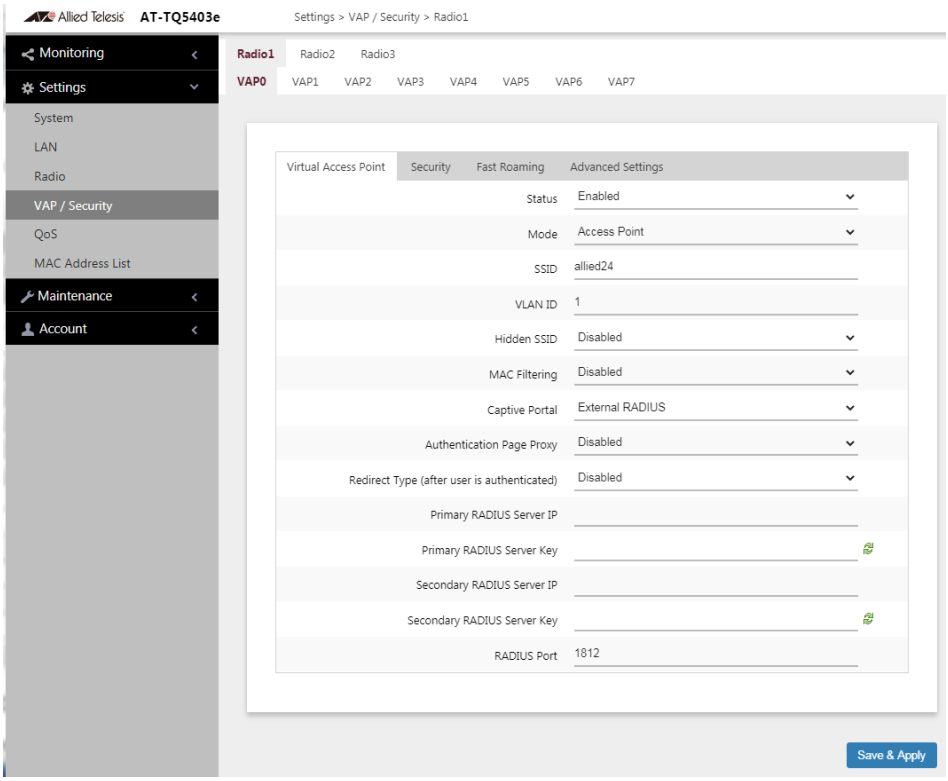

Figure 44. Captive Portal - External RADIUS

7. Configure the parameters by referring to Table 22 on page 124.
8. Click the **SAVE & APPLY** button to save and update the configuration.

Creating Pages in HTML for a Proxy Server

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

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

Requirements for the click_through_login.html and click_through_login_fail.html

Here is a list of requirements:

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

HTML Code and Display Examples of Login Page

The following is an example of HTML code:

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

Figure 45 shows its web page displayed in a web browser.

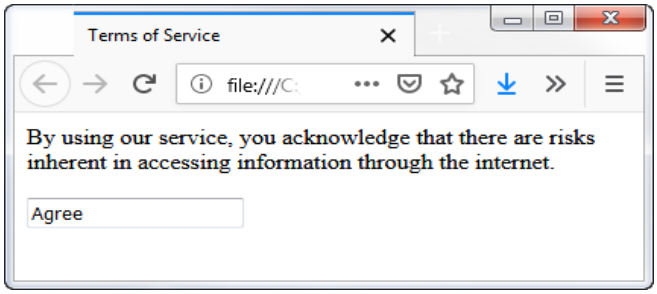

Figure 45. Captive Portal - Terms of Service Page Sample

Creating Login Pages in HTML When External RADIUS is Selected

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

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

Requirements for the radius_login.html and radius_login_fail.html

Here is a list of requirements:

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

HTML Code and Display Examples of Login Page

The following is an example of HTML code:

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

Figure 46 shows its web page displayed in a web browser.

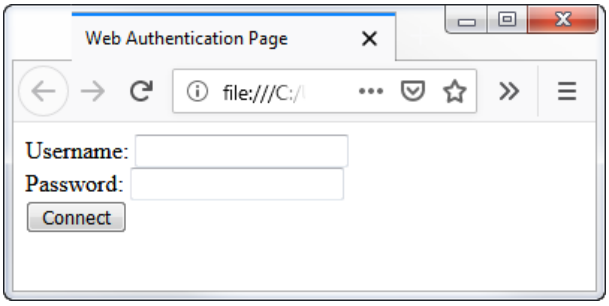

Figure 46. Captive Portal - Login Page Sample

Chapter 7

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 **Radio1**, **Radio2**, or **Radio3** from the sub-menu. You can configure only one radio at a time. Refer to Figure 47 on page 131.
3. Configure the QoS parameters by referring to the following sections:

- “Configuring QoS Basic Settings” on page 132
- “Configuring AP EDCA Parameters” on page 133
- “Configuring Station EDCA Parameters” on page 136

4. Click the **SAVE & APPLY** button to save and update your configuration.

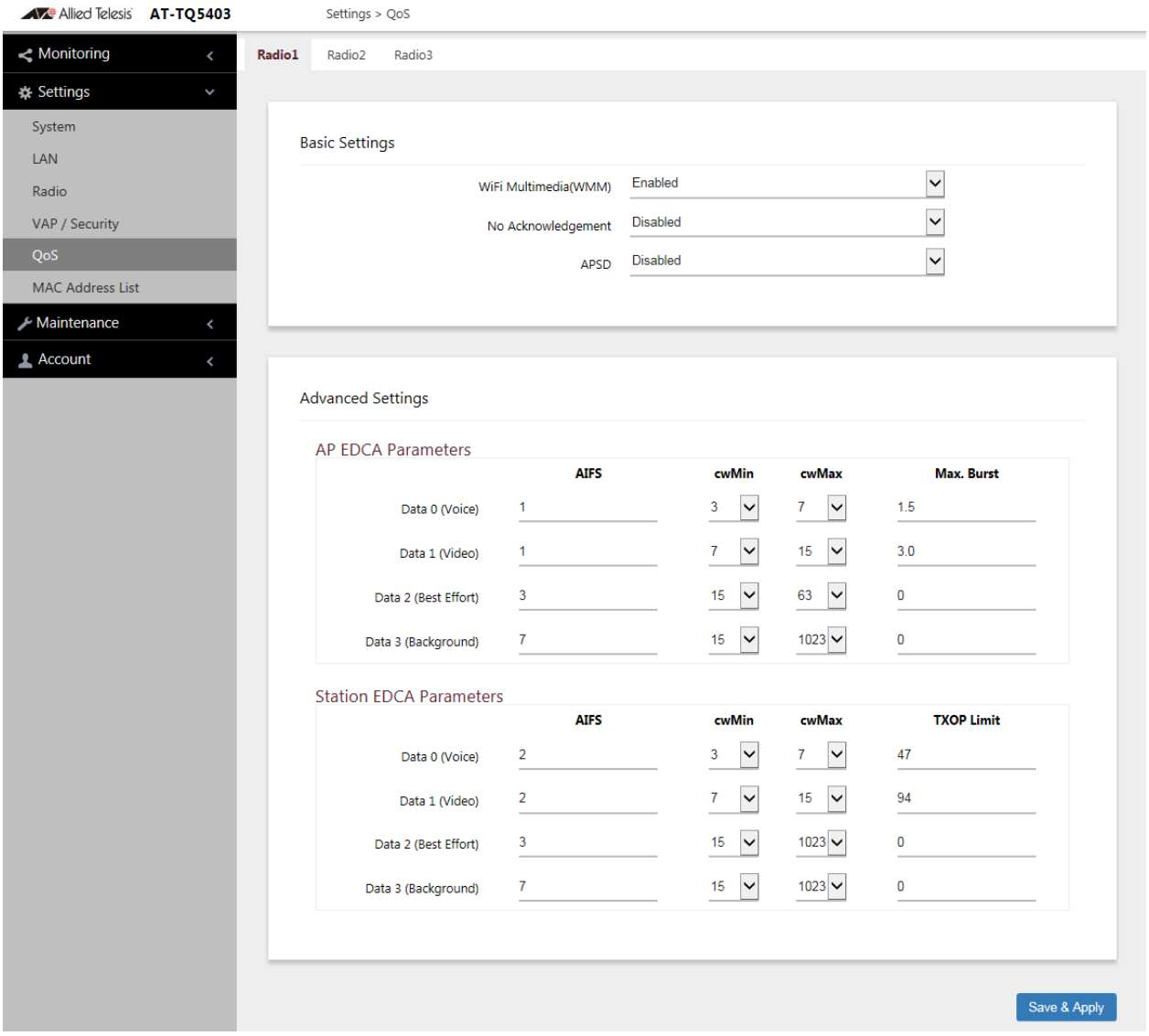

Figure 47. QoS Window

Configuring QoS Basic Settings

The fields for the Basic Settings section are defined in Table 23.

Table 23. QoS Window - Basic Settings

Parameter	Description
WiFi Multimedia (WMM)	Enable or disable QoS prioritizing and coordination. Here are the settings: - 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	Control whether the access point acknowledges frames that have QosNoAck for their service class values from wireless clients. Here are the settings: - Enabled: The access point does not acknowledge frames that have QosNoAck for their service class values. - Disabled: The access point acknowledges frames that have QosNoAck for their service class values. This is the default setting.
APSD	APSD is not supported. It is always disabled.

Configuring AP EDCA Parameters

Table 24 defines the AP EDCA parameters in the QoS window in Figure 47 on page 131.

Table 24. 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 24. 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 24. 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 25 defines the Station EDCA parameters in the QoS window in Figure 47 on page 131.

Table 25. 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 25. 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 25. 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 8

LAN1 and LAN2 Ports

This chapter describes the following procedures:

Configuring the Management VLAN

Here are the guidelines to setting the management VLAN:

- When the management VLAN is disabled, the default setting, the access point handles untagged packets as members of VLAN 1.
- When the management VLAN is enabled and set to VID 1, the default VID, the access point accepts only tagged packets and discards all untagged packets.
- When Management VLAN Tag is enabled and Management VLAN ID is a value other than 1, packets from wireless clients on VAPs with the VID 1 are handled as untagged packets. This is also true for packets from clients that are dynamically assigned the VID 1 from a RADIUS server.

Note
Changing the management VLAN might end your management session.

To configure the management VLAN, perform the following procedure:

1. Select **Settings** > **LAN** from the main menu. Refer to Figure 48.

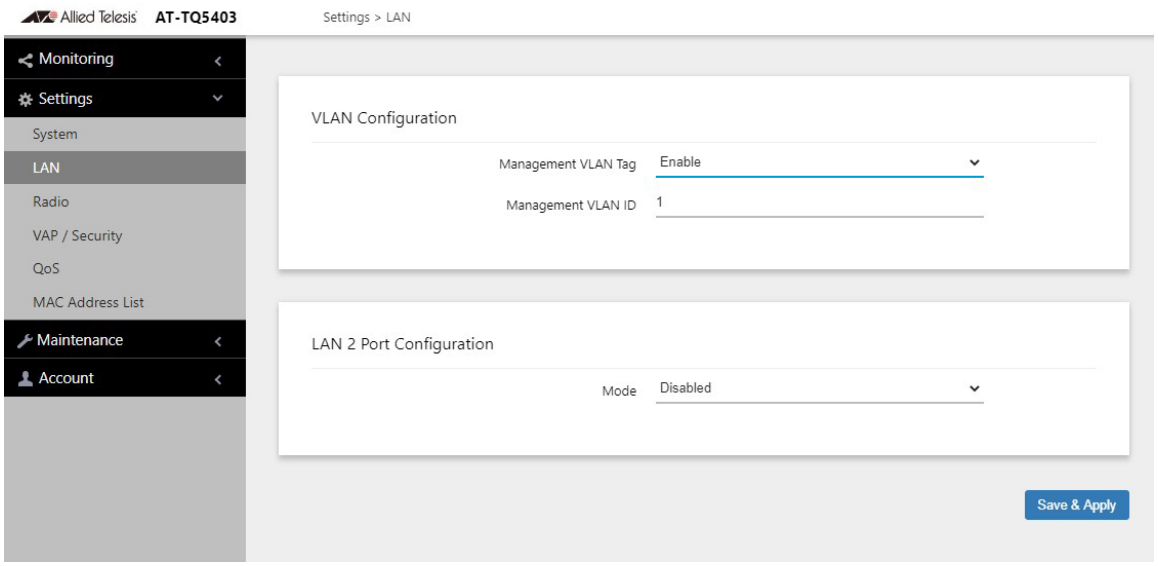

Figure 48. LAN Settings Window

Note
The AT-TQ5403e access point does *not* have the Link Aggregation section on the LAN Settings window shown in Figure 48.

Note
The LAN 2 Port Configuration section is explained in "Configuring the LAN2 Port" on page 142.

2. Configure the settings by referring to Table 26.

Table 26. LAN Settings Window - VLAN Configuration Section

Parameter	Description
Management VLAN Tag	Select one of the following: - Enabled: Activates the management VLAN. - Disabled: Deactivates the management VLAN.
Management VLAN ID	Enter a VLAN ID if Management VLAN Tag is set to Enabled. Here are the guidelines: - You can enter only one VID. - The range is 1 to 4094. - The default is 1. - This field is hidden when Management VLAN Tag is disabled.

3. Click the **SAVE & APPLY** button to save and update the configuration.

Configuring the LAN2 Port

Note
The explanation for the LAN2 in this section applies only to the AT-TQ5403 and AT-TQm5403 access points. The AT-TQ5403e access point does *not* have a LAN2 port.

The wireless access point has two Ethernet ports, labeled LAN1 and LAN2. You use the ports to connect the wireless access point to your wired network. Here are their basic properties:

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

Static Link Aggregation

You can double the bandwidth between the wireless access point and your wired network by combining LAN1 and LAN2 ports into a static LAG. A static LAG functions as a single logical link between the wireless 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 wireless access point maintains connectivity to the wired network over the remaining link. Refer to Figure 49.

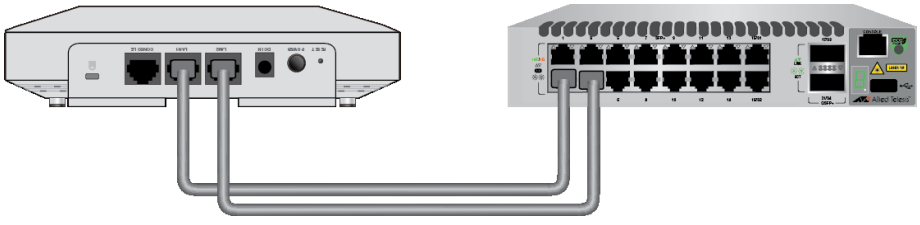

Figure 49. LAN1 and LAN2 Ports in a Static LAG

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

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

- You have to configure the two ports on the network device as a static LAG.
- You activate the static LAG for LAN1 and LAN2 ports with the on-board web browser management interface.

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

Cascade Mode

The LAN2 port also 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 50.

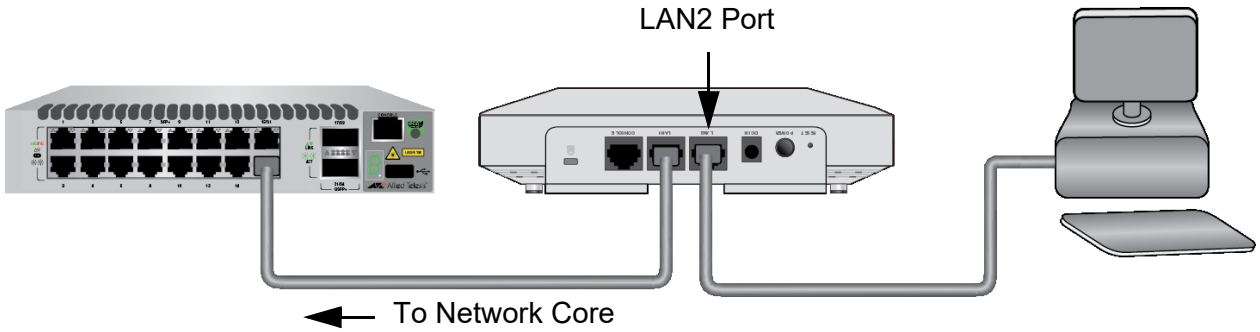

Figure 50. LAN2 Port in Cascade Mode with an End Node

It can also be a networking device such as a switch, router, or media converter. Refer to Figure 51.

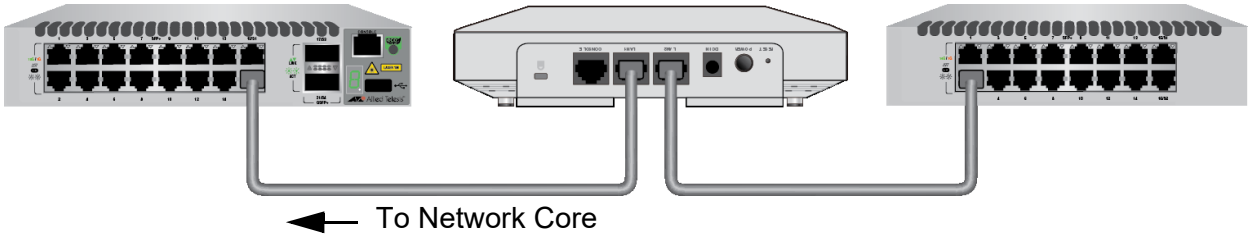

Figure 51. LAN2 Port in Cascade Mode with a Networking Device

Here are the Cascade mode guidelines:

- The Cascade mode requires firmware version 6.0.1-2.1 or later.
- You set the Cascade mode with the on-board web browser management interface.

- ❒ The Cascade mode is not supported with Vista Manager EX and the AWC plug-in.
- ❒ Do not connect both LAN1 and LAN2 ports to the same network device when the LAN2 port is in the Cascade mode.

To configure the LAN2 port, perform the following procedure:

1. Select **Settings** > **LAN** from the main menu. Refer to Figure 48 on page 140.

   The window has two sections. The LAN2 port is controlled with the LAN2 Port Configuration section. For information on the VLAN Configuration section, refer to “Configuring the Management VLAN” on page 140.

2. From the Mode pull-down menu in the LAN2 Port Configuration section configure the settings by referring to Table 27.

Table 27. LAN Settings Window - LAN2 Port Configuration Section

Parameter	Description
Mode	Select one of the following: - Disabled: Disables LAN2 port. - Static LAG: Combines LAN1 and LAN2 ports into a static LAG. - Cascade: Activates the Cascade mode on LAN2 port so that you can use the port to connect another device to your network

3. Click the **SAVE & APPLY** button to save and update your configuration.

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

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

Configuring PoE Negotiation with Link Layer Discovery Protocol

The feature described in this section is applicable when the access point is powered by Power over Ethernet and the LAN1 port is connected to a network device that supports Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED).

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) allow Ethernet network devices to receive and/or transmit device-related information 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 the feature guidelines:

- ❒ The access point has to be powered with PoE.
- ❒ The LAN1 port has to be connected to an LLDP-MED device.
- ❒ The LLDP-MED device has to be configured for the Extended Power Management TLV.
- ❒ The access point transmits the Extended Power Management TLV only on LAN1 port.
- ❒ The access point requests 18.8W in the TLV.
- ❒ This feature is optional. You do not have to use it to power the device with PoE.

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 52.

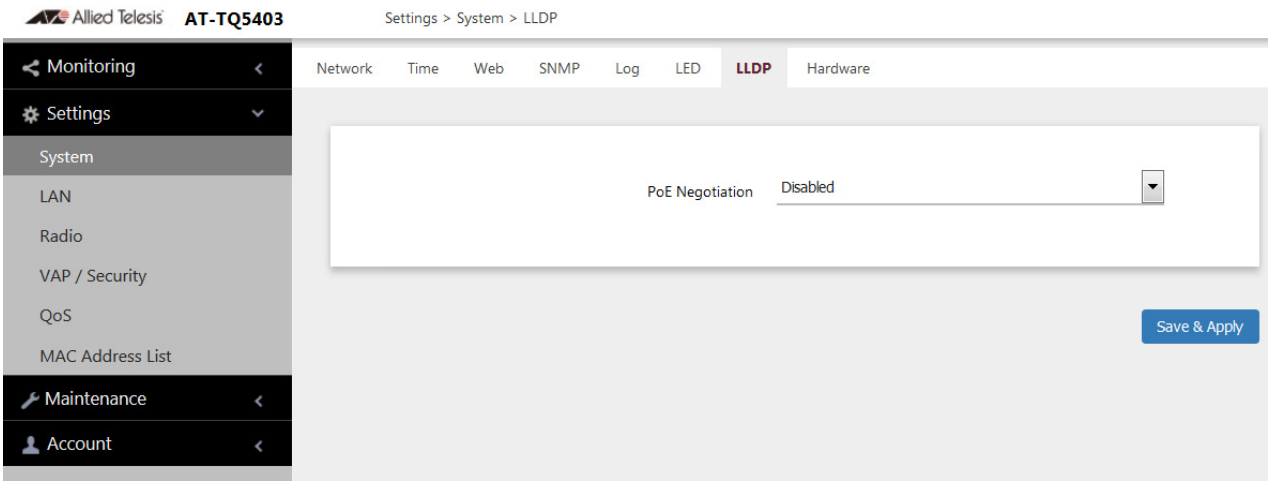

Figure 52. LLDP Window

3. Select one of the following from the **PoE Negotiation** pull-down menu.

   - Enabled: Enables PoE negotiation. The access point transmits the Extended Power Management TLV on the LAN1 port.
   - Disabled; Disables PoE negotiation. This is the default.

4. Click the **SAVE & APPLY** button to save and update your configuration.

   If you enabled the feature, the access point sends Extended Power Management TLVs to the LLDP-MED device connected to the LAN1 port.

Displaying the Status of LAN1 and LAN2 Ports

To display the status of the LAN1 and LAN2 ports, perform the following procedure:

> **Note**
> The AT-TQ5403e access point does *not* have a LAN2 port.

1. Select **Monitoring** > **Status** from the main menu.
2. Select **LAN1** or **LAN2** from the sub-menu. Figure 53 shows the LAN1 port status window.

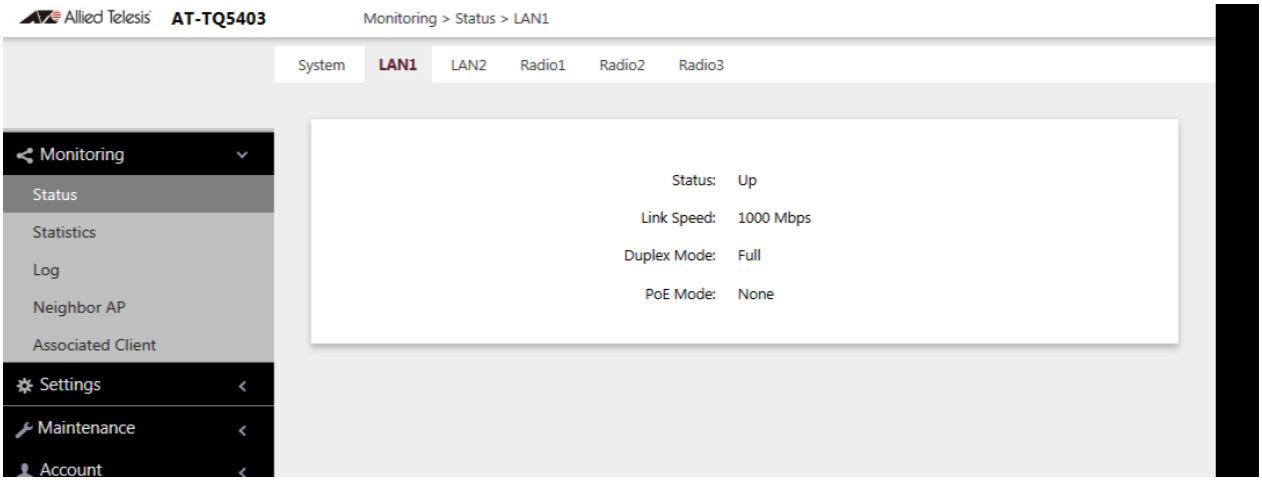

Figure 53. LAN1 Window

Figure 54 shows the LAN2 port status window.

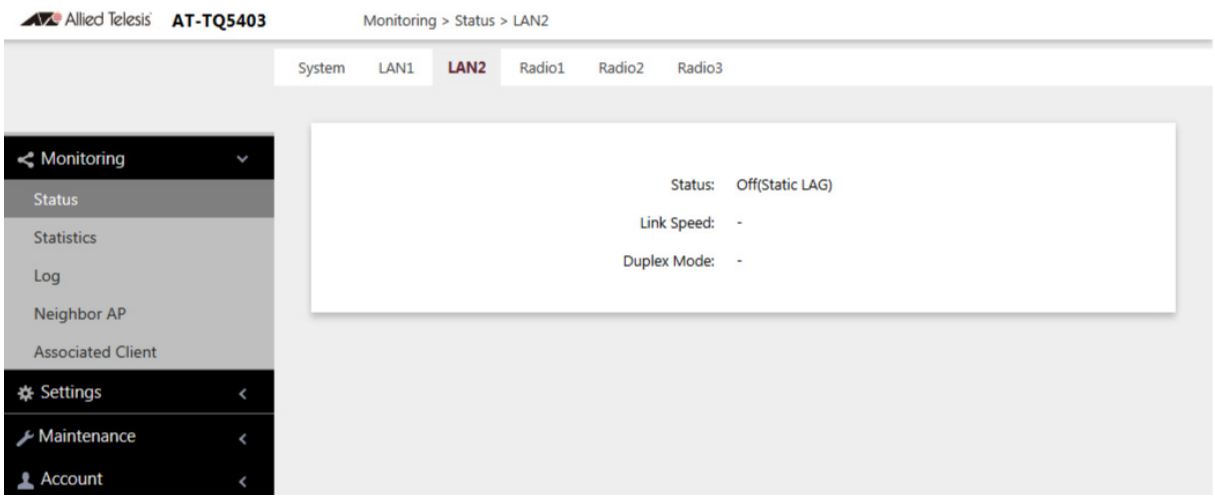

Figure 54. LAN2 Window

The fields are defined in Table 28.

Table 28. LAN1 or LAN2 Window

Item Name	Description
Status (LAN1 port)	Displays the status of the LAN1 port. The possible states are listed here: - Up: The port has established a link with a network devices, such as an Ethernet switch or router. - Down: The port has not established a link with a network device.
Status (LAN2) (AT-TQ5403 and AT-TQm5302 only)	Displays the status of the LAN2 port: - Off: The port is disabled. - Static LAG: The LAN1 and LAN2 ports are functioning as a static LAG. - Cascade: The LAN2 port is operating in the Cascade mode. For further instructions, refer to “Configuring the LAN2 Port” on page 142.
Link Speed	Displays the speed of the link (10 Mbps, 100 Mbps, 1000 Mbps).
Duplex Mode	Displays the duplex mode of the port, as follows: - Full: Full-duplex. - Half: Half-duplex.
PoE Mode (LAN1 port)	Displays the PoE status on the LAN1 port, as follows: - IEEE 802.3af, IEEE 802.3at: The access point is powered by PoE. - None: The access point is powered by an external adapter.

Chapter 9

Wireless Distribution System Bridges

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

Introduction to Wireless Distribution Bridges

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

A WDS bridge consists of one parent and up to three children. The parent is connected to the wired network through its LAN ports. The children function as wireless clients of the parent, communicating with the wired network over the WDS bridge to the parent. An example of a parent with three children is shown in Figure 55.

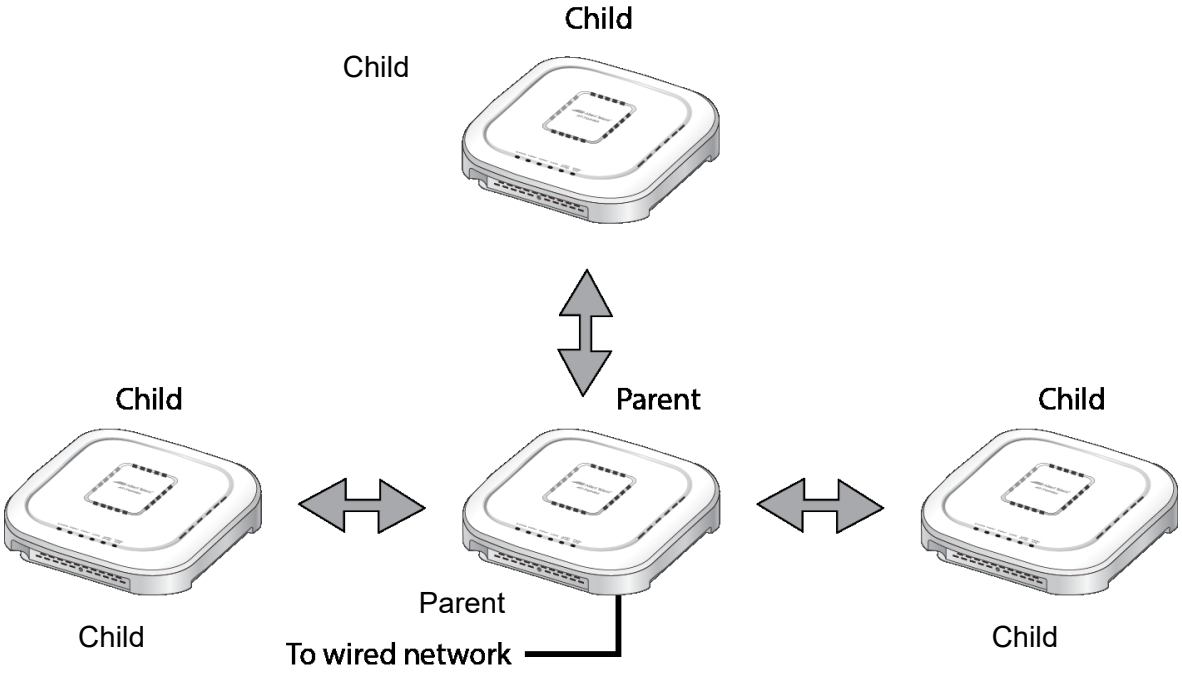

Figure 55. WDS Bridge

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

A WDS bridge consists of a radio and a radio channel. You can use Radio1, 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 other radios to access the network. Additionally, because the access points have to use the same channel,

you have to select the channel manually, instead of using the default auto channel setting. In the example in Figure 56, the parent and children are using Radio2 and channel 40 for the WDS bridge. Wireless clients can access the network using either Radio1 or Radio3.

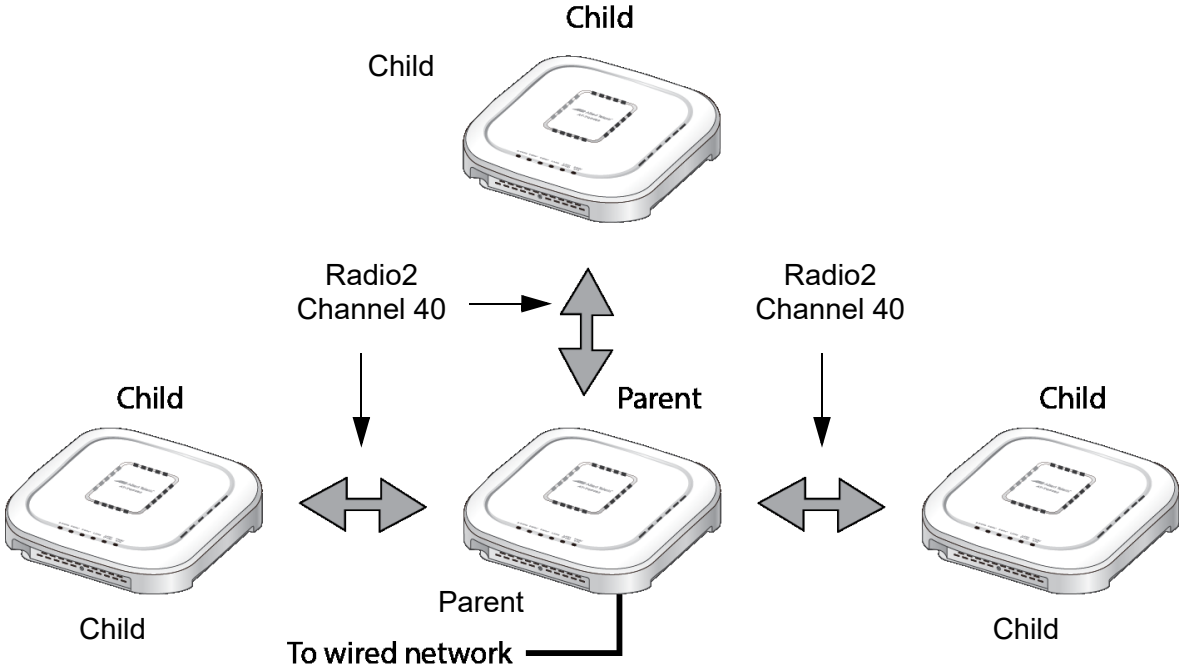

Figure 56. Example of Radio and Channel Assignments in a WDS Bridge

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 57 on page 152 is an example. Access Point A is functioning as the parent to children 1 and 2 in one WDS bridge, and as child 5 to Access Point B in another bridge. In contrast, Access Point B is functioning solely as a parent, in this case to children 3, 4, and 5, which is Access Point A.

Each WDS bridge has to use a different radio and channel. This is illustrated in the example where Access Point A, as parent, and children 1 and 2 are using Radio 1 and channel 10 for their WDS bridge. In contrast, Access Point B and its children are using Radio2 and channel 40. It should be noted that since Access Point A is acting as both parent and child, two of its radios are being used for WDS bridges, leaving only one radio to support wireless clients.

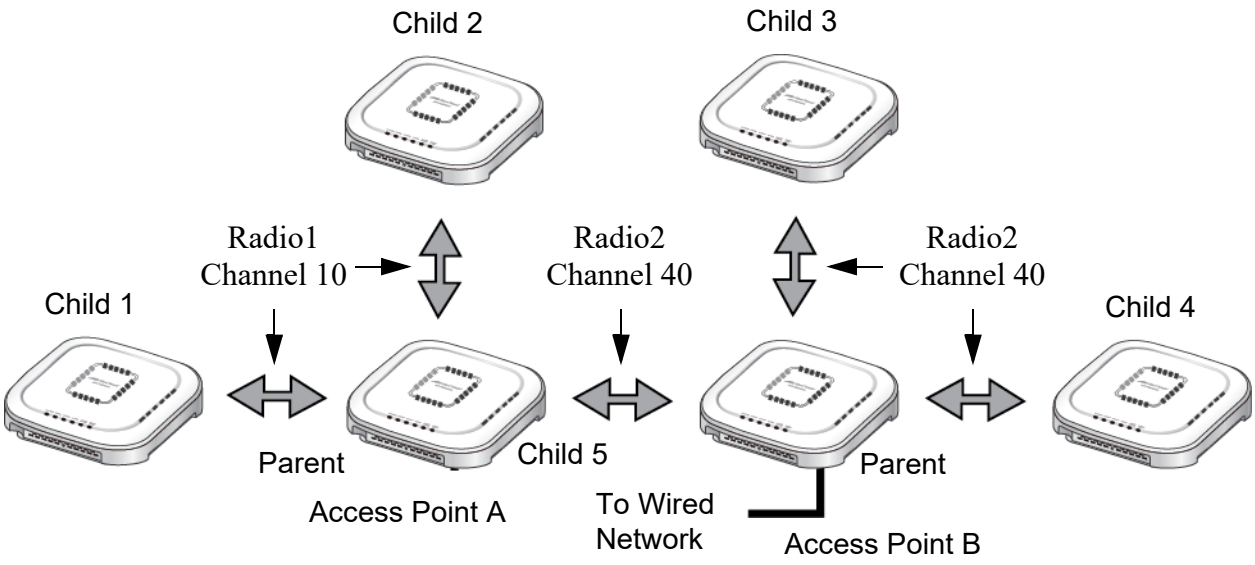

Figure 57. Example of an Access Point as Both Parent and Child

Here are important rules to observe when linking WDS bridges together as shown in Figure 57:

- 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.
- Allied Telesis does not recommend linking together more than two WDS bridges. The LAN ports on the parent connected to the wired network might not be able to efficiently handle the traffic load of wireless clients of more than two bridges.

WDS Bridge Elements

This section describes the various elements of a WDS bridge.

Radio

You can use Radio1, Radio2, or Radio3 for a WDS bridge. Here are the guidelines:

- The access points must all use the same radio for a bridge.
- The selected radio should only be used for a WDS bridge. It should not be used by wireless clients.
- A bridge uses VAP0 on the selected radio.
- VAP1 to VAP7 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 VAP7 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 55 on page 150.

Security

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

- No encryption
- WPA Personal

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

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.

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

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

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

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

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

Guidelines

Here are the guidelines for WDS bridges:

- A WDS bridge can have from two to four wireless access points.
- One access point is the parent and the others are children.
- The LAN ports on the parent are connected to the wired network.
- If two WDS bridges are connected together, as shown in Figure 57 on page 152, you should connect the LAN ports on only one parent to the wired network. Connecting the LAN ports on both access points might form a loop in the network topology.
- The LAN ports on children should not be connected to the wired network.
- You can use Radio1, Radio2, or Radio3 for the WDS bridge.
- You can use no security (none) or WPA Personal security for VAP0 on the selected radio of the bridge. Allied Telesis recommends using WPA Personal security.
- A WDS bridge can have both AT-TQ5403 and AT-TQm5403 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 or Radio3 for the bridge, Allied Telesis recommends selecting a channel that is not part of dynamic frequency selection. This is to minimize the chance that the access points have to change channels and break the WDS bridge due to radar signals.
- A WDS bridge uses VAP0 on the selected radio as the communications link. The VAP should not be used by wireless clients. All other VAPs on the radio are disabled.
- An access point can be a parent in one bridge and a child in another. However, it cannot be a parent or child in more than one bridge.
- The WDS bridge feature on these access points is not compatible with the same feature on other products from Allied Telesis or other companies.

Preparing Access Points for a WDS Bridge

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

- ❒ You have selected the access points for the bridge.
- ❒ You have decided which access point will be the parent and which will be the children.
- ❒ You have chosen the radio that the access points will use for the bridges. It can be Radio1, 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 security.

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

1. Start a management session.
2. On the selected radio for the bridge, set the mode and channel. Refer to “Configuring Basic Radio Settings” on page 64. Here are the guidelines:
   - ❒ You can use any available radio mode for the bridge, but the radios in the different access points must use the same mode.
   - ❒ You can use any available channel, but the devices must use the same channel. Do not use the Auto setting.
3. Configure the security setting for VAP0 on the radio. The security setting can be none or WPA Personal. For instructions, refer to “Configuring VAP Security” on page 87.
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. From the Mode pull-down menu, select either **WDS Parent** or **WDS Child**. This can only be set on VAP0.
8. Click the **SAVE & APPLY** button to save and update the configuration.

Note
The access point disables VAPs 1 to 7 on the same radio.

9. 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 164.

Chapter 10

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 58.

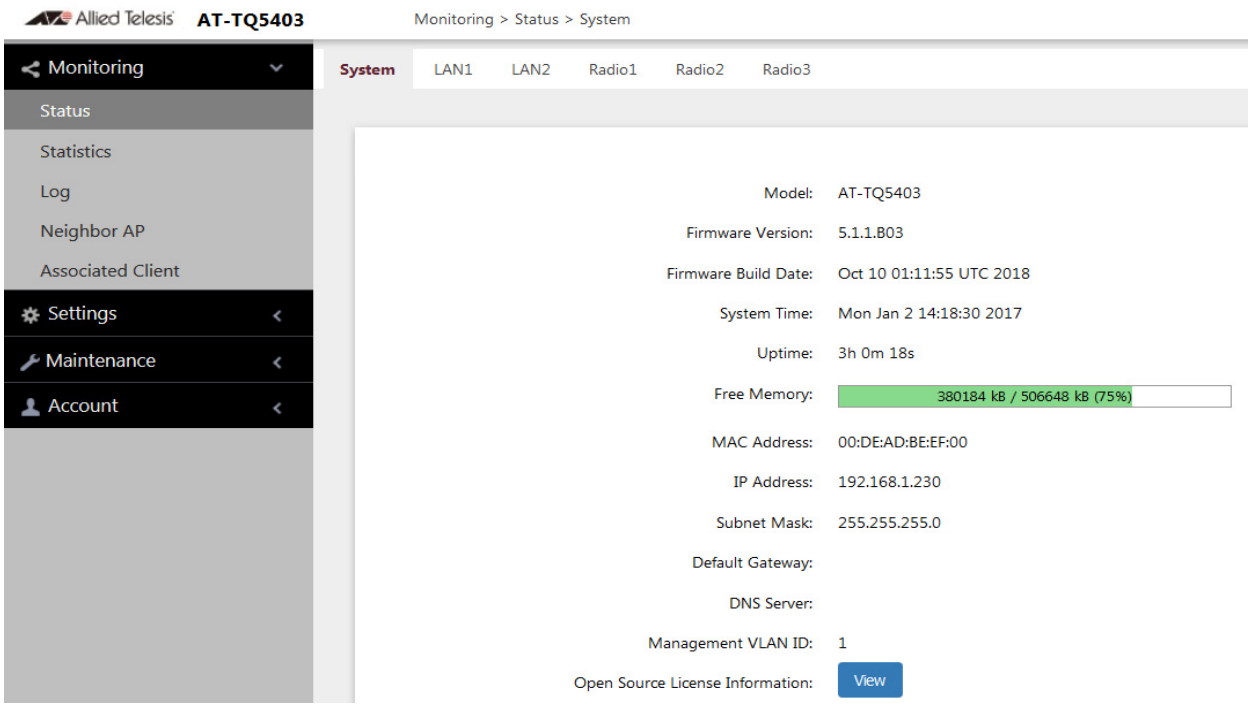

Figure 58. System Window

The fields are defined in Table 29.

Table 29. System Window

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

Table 29. 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 43 or "Setting the Date and Time with the Network Time Protocol (NTP)" on page 40.
Uptime	Displays the number of hours, minutes, and seconds that have elapsed since the unit was last reset or powered on.
Free Memory	Displays the amount of free memory in the access point, as follows: - The first value is the total amount of unused memory, in KB. - The second value is the total amount of memory, in KB. - The last number in parentheses is the percentage of total memory that is free.
MAC Address	Displays the MAC address of the access point and radio 1. Radios 2 and 3 have different MAC addresses. You cannot change the MAC addresses.
IP Address	Displays the IP address of the access point. To set this value, refer to "Assigning a Dynamic IP Address from a DHCP Server" on page 34 or "Assigning a Static IP Address to the Access Point" on page 37.
Subnet Mask	Displays the subnet mask. To set this value, refer to "Assigning a Dynamic IP Address from a DHCP Server" on page 34 or "Assigning a Static IP Address to the Access Point" on page 37.
Default Gateway	Displays the default gateway address. The default gateway is an IP address of an interface on a router or other Layer 3 routing device. It specifies the first hop to reaching the subnets or networks where your management devices, such as management workstations and syslog servers, reside. The access point can have only one default gateway. To set this value, refer to "Assigning a Dynamic IP Address from a DHCP Server" on page 34 or "Assigning a Static IP Address to the Access Point" on page 37.

Table 29. System Window (Continued)

Item Name	Description
DNS Name Server	Displays the current DNS name server address. Refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 34 or “Assigning a Static IP Address to the Access Point” on page 37.
Management VLAN ID	Displays the management VLAN ID. The default is 1. Refer to “Configuring the Management VLAN” on page 140.
Open Source License Information	When you click the **View** button, displays open source license information.

Displaying Neighboring Access Points

To view information about other access points that the access point has detected, select **Monitoring** > **Neighbor AP**, Refer to Figure 59.

Note
This feature requires activating the Neighbor AP Detection option on the radios, as explained in "Configuring Advanced Radio Settings" on page 68.

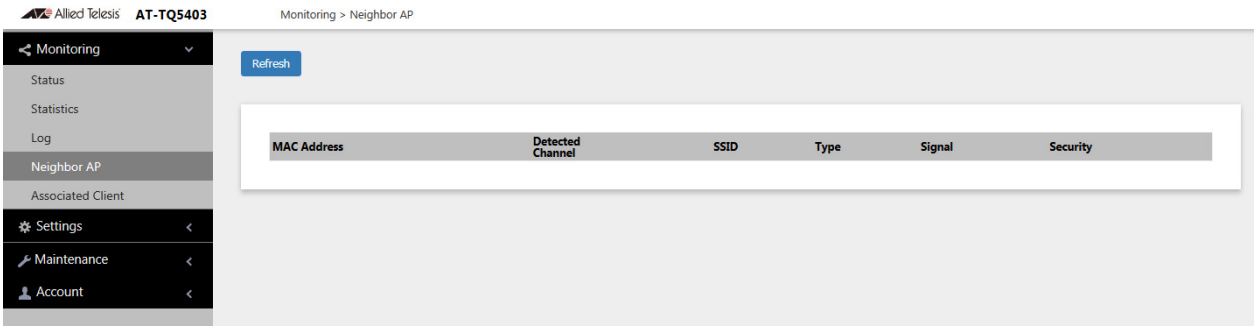

Figure 59. Neighbor AP Window

The columns are described in Table 30.

Table 30. Neighbor AP Window

Column	Description
MAC Address	Displays the MAC address of the detected VAP.
Detected Channel	Displays the detected radio channel.
SSID	Displays the network name (SSID) of the detected VAP.
Type	Displays the wireless mode as AP or Adhoc.
Signal	Displays the intensity of the received signal in a four-level bar graph icon. Point to the icon displays dB (dBm).
Security	Displays the security status of the detected VAP.

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 60.

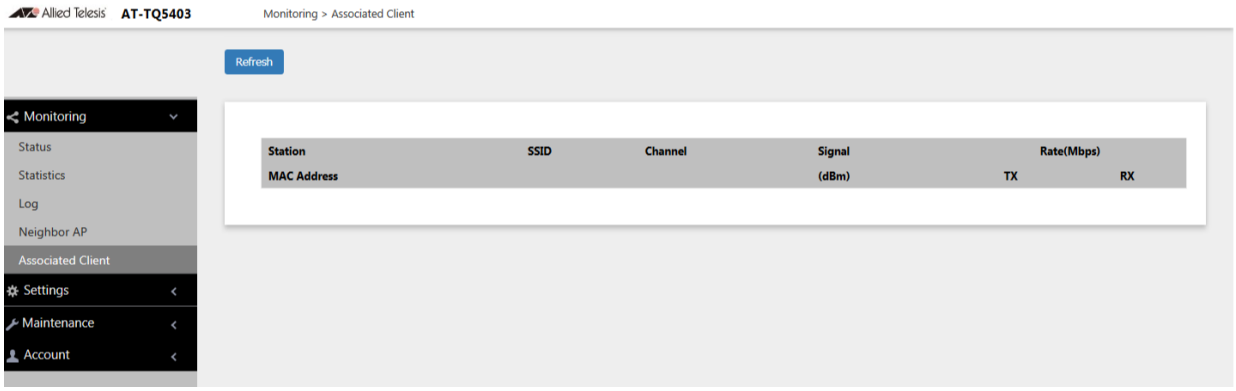

Figure 60. Associated Client Window

The columns are defined in Table 31.

Table 31. Associated Client Window

Column	Description
MAC Address	Displays the MAC addresses of associated clients.
SSID	Displays the network name (SSIDs) to which the client is connected.
Channel	Displays the radio channel the client is using.
Signal	Displays the strength of the signal from the client.
Rate (Mbps)	Displays the transmission (Tx) and reception (Rx) rates in Mbps.

Chapter 11

System Log

This chapter describes the system log in the following sections:

Displaying the System Log

A wireless access point is a complex piece of network equipment that includes both hardware and software components. Multiple software features operate simultaneously, interoperating with each other and processing large amounts of network traffic. It is often difficult to determine exactly what is happening when an access point appears not to be operating normally, or what happened when a problem occurred.

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 they provide can help you identify and solve system problems.

The messages are divided into the eight severity levels listed in Table 32:

Table 32. 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.

At its default setting, the log displays all messages. You can restrict the log to display only certain messages by adjusting the Severity parameter in the syslog client. Refer to “Sending Log Messages to a Syslog Server” on page 168.

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 168.

To view the system log, select **Monitoring** > **Log**, Figure 61 on page 167 is an example.

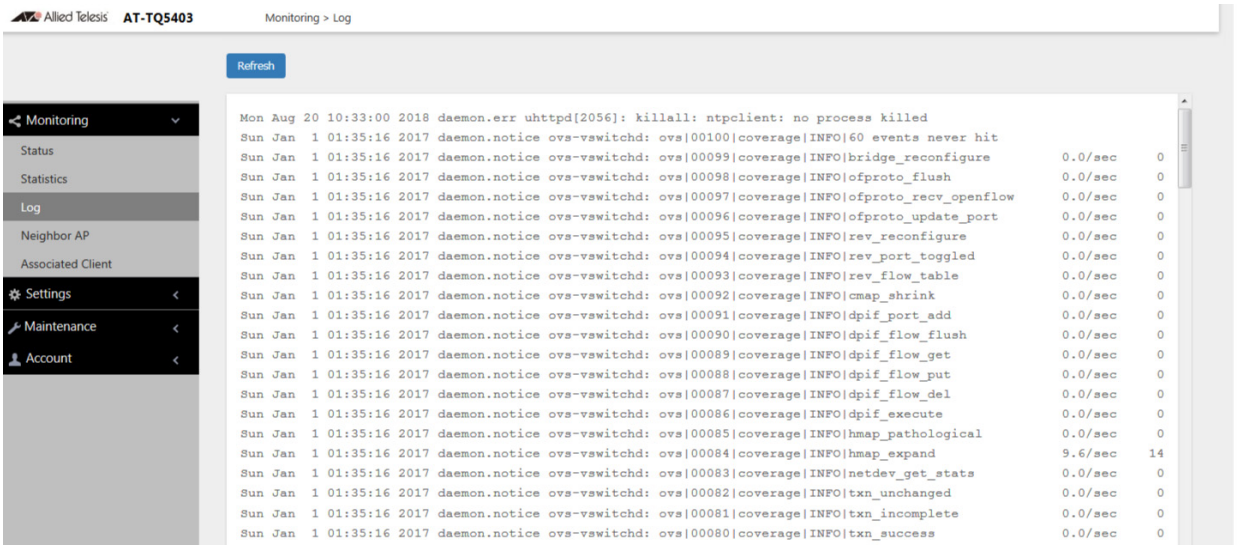

Figure 61. Log Window for Event Messages

Sending Log Messages to a Syslog Server

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

1. Select **Settings** > **System** from the main menu.
2. Select **Log** from the sub-menu. Refer to Figure 62.

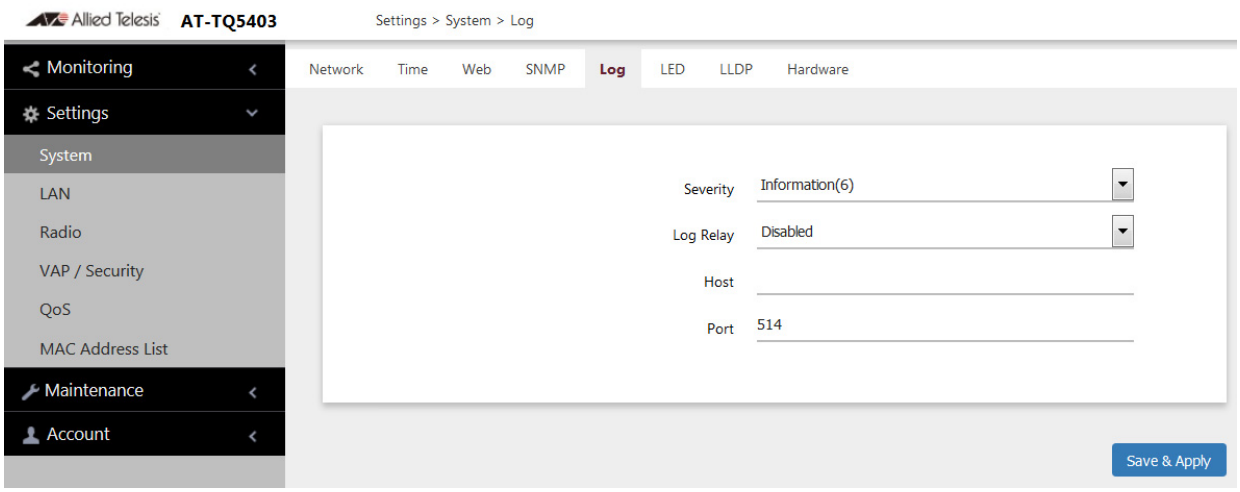

Figure 62. Log Window for Syslog Client

3. Configure the fields by referring to Table 33.

Table 33. Log Window for Syslog Client

Field	Description
Severity	Select the severity of messages the access point is to display in the log file and transmit to the syslog server. The severity levels are listed in Table 32 on page 166. Here are the guidelines: - You can specify only one severity level. - The severity level applies to both the messages displayed in the log file and transmitted to a syslog server. - The selected level includes that level and all numerically lower (higher severity) messages. For example, selecting level 3, error, designates system messages levels 0 to 3. - The default is level 7, debug. This is the highest value; it designates all messages.

Table 33. Log Window for Syslog Client (Continued)

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

4. Click the **SAVE & APPLY** button to save and update the configuration.

Chapter 12
Maintenance

This chapter has the following procedures:

Downloading the Configuration of the Access Point to Your Computer

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

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

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

1. Select **Maintenance** > **Configuration** from the main menu. Refer to Figure 63.

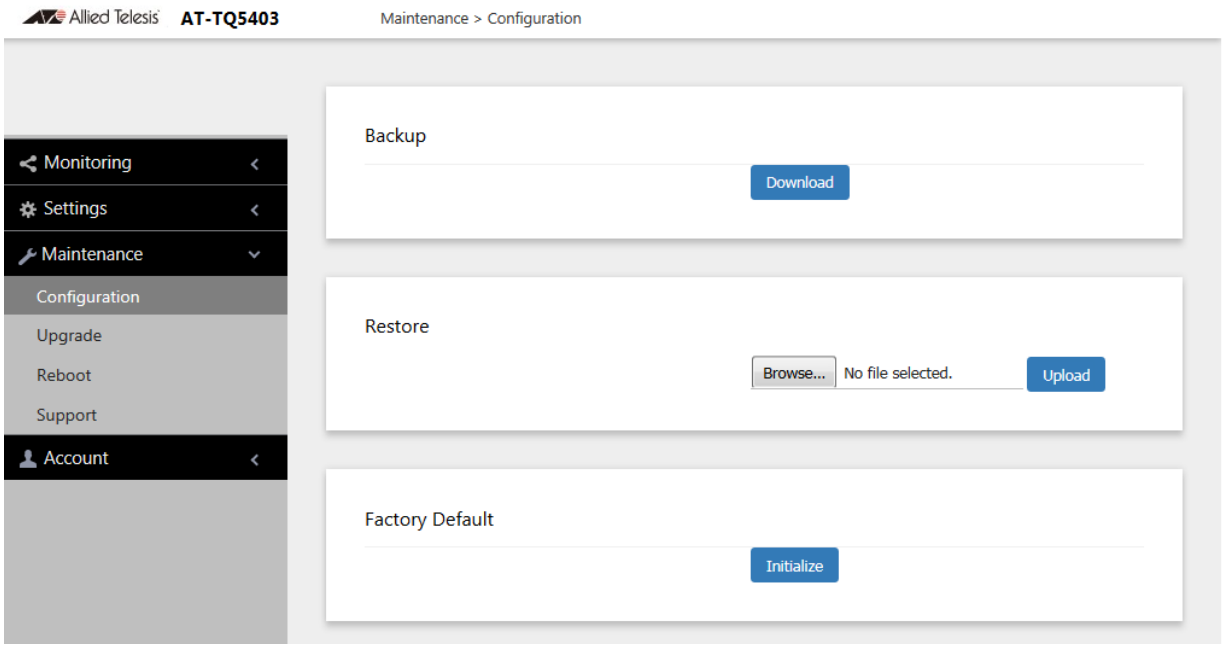

Figure 63. Configuration Window

2. Click the **Download** button in the Backup section of the window.
3. When prompted, click the **Browse** button and select the folder or directory in which to store the file on your management workstation or network server.

4. If desired, change the filename of the configuration file. The filename suffix must be "txt".

5. Click the **Save** button.

   The access point downloads a file with its configuration to your management workstation, which stores it in the designated folder.

Restoring a Configuration to the Access Point

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

- ❒ You can only restore configuration files that are created with “Downloading the Configuration of the Access Point to Your Computer” on page 172.
- ❒ 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 63 on page 172.
2. Click the **Browse** button in the Restore section of the window and select the configuration file to restore to the access point from your management workstation or network server.
3. Click the **Open** button.
4. Click the **Upload** button.
5. Wait one minute for the access point to upload the file and reboot.
6. To resume managing the unit, establish a new management session.

Restoring the Default Settings to the Access Point

This procedure explains how to restore the default settings on the access point. Please 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 LAN1 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 63 on page 172.
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 22.

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 access point during the firmware upgrade.

Caution
The access point does not forward network traffic while it uploads the management software from your computer and writes it to flash memory. To minimize the disruption of the upgrade procedure to network operations, you should perform it only during periods of low traffic activity, such as during non-business hours.

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

1. Select **Maintenance** > **Upgrade** from the main menu. Refer to Figure 64 on page 177.

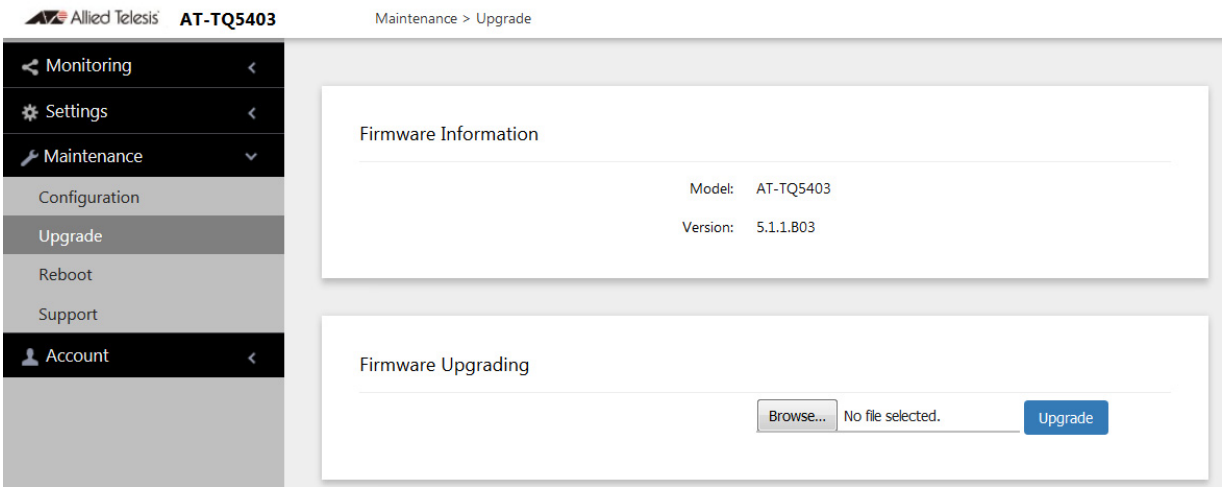

Figure 64. Upgrade Window

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

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

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

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

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

Rebooting the Access Point

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

Caution
The access point does not forward network traffic while it reboots. Some network traffic may be lost.

To reboot the access point, perform the following procedure:

1. Select **Maintenance** > **Reboot** from the main menu. Refer to Figure 65.

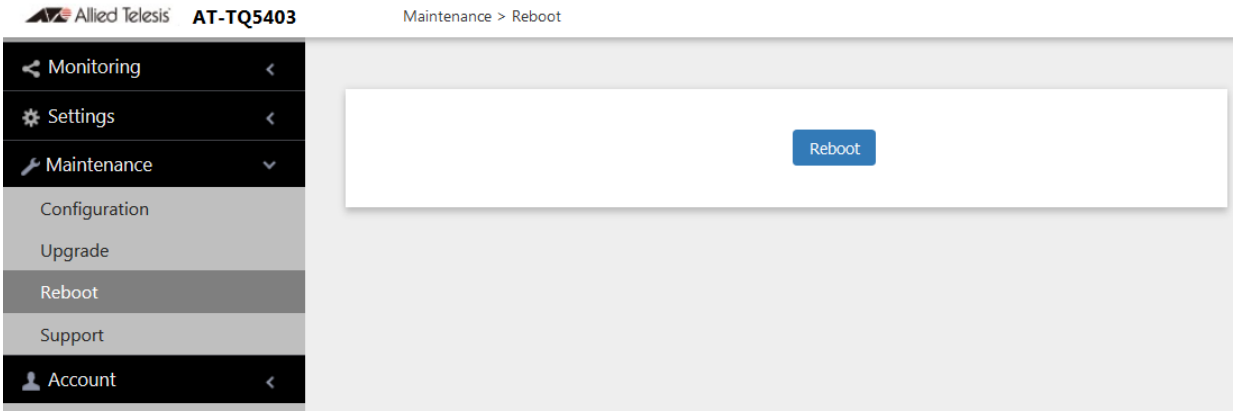

Figure 65. Reboot Window

2. Click the **Reboot** button.

   The access point displays a confirmation prompt.

3. Click **OK**.

   Your current management session is interrupted.

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

Sending Technical Support Information to Allied Telesis

If you contact Allied Telesis for technical assistance with the access point, you may be instructed to perform this procedure. It has the access point send to Allied Telesis technical and operational information that technicians can use to troubleshoot problems with the device.

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

To send technical support information to Allied Telesis, perform the following procedure:

1. Select **Maintenance** > **Support** from the main menu. Refer to Figure 66.

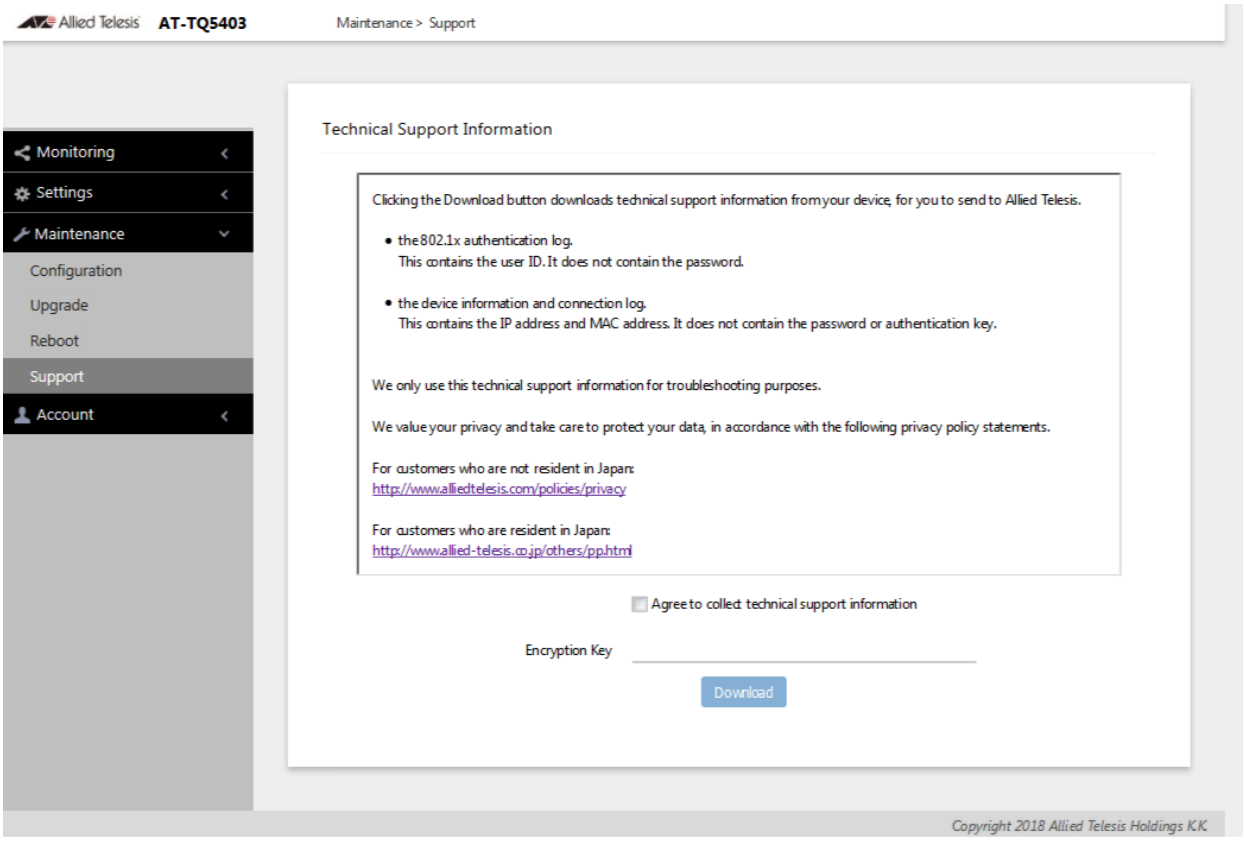

Figure 66. Support Window

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 give Allied Telesis, Inc. permission to collect the technical support information.

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

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

5. Click the **Download** button.

   The access point transmits the file.