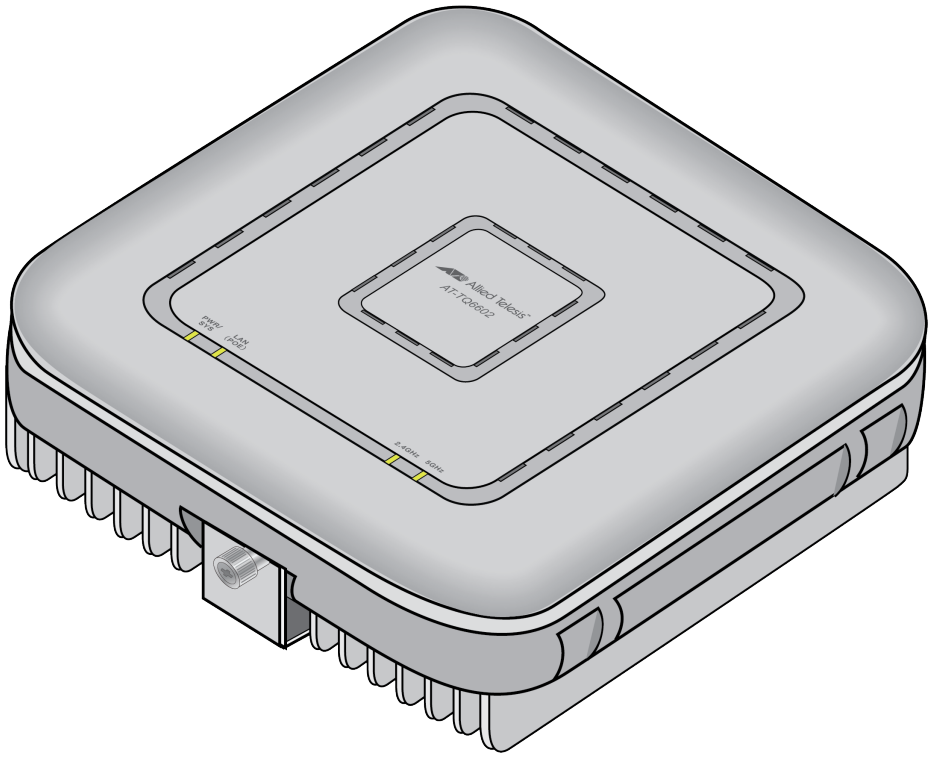
TQ6602

Enterprise-class Wi-Fi 6 802.11ax Indoor Wireless Access Point
with 2.4GHz and 5GHz Radios



Management Software User's Guide

613-002960 Rev.C

Contents

List of Figures

List of Tables

Preface

This guide contains instructions on how to manage the features of the TQ6602 access point with the web browser management interface.

This preface contains the following sections:

Safety Symbols Used in this Document

This document uses the following conventions.

Note
Notes provide additional information.

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

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

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

Contacting Allied Telesis

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

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

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

Chapter 1

Getting Started

Here are the sections in this chapter:

Features

This section lists the features of the access point.

Hardware Features

Here is a list of hardware features:

- One 2.4GHz radio
- One 5GHz radio
- 4x4 MU-MIMO 2.4GHz Internal antennas
- 4x4 MU-MIMO 5GHz Internal antennas
- Transmission beamforming
- One 10/100Mbps/1/2.5/5Gbps Ethernet LAN port with RJ-45 connector
- IEEE 802.3at PoE+ Class 4 powered device
- One Reset button for restoring the default settings
- One On/Off button for the AC/DC power adapter connector
- LEDs for the 2.4GHz and 5GHz radios, Ethernet LAN port, and power
- Ceiling, wall, or table installation
- Kensington lock port
- One Console RJ-45 port for factory use only

Software Features

Here is a list of software features:

Wi-Fi 6 (IEEE802.11ax)

- IEEE802.11a/b/g/n/ac/ax
- Multi-channel (cell operation)
- Channel Blanket (single-channel operation)

  Up to 10 Channel Blanket-enabled VAPs are supported.

Hybrid Operation (Multi-Channel)

- 16 virtual access points (VAPs) per radio and 32 VAPs per access point (Only 11 VAPs can be enabled per radio)
- Quality of Service (QoS) ingress and egress queues
- Control of radio transmission power
- Dynamic frequency selection
- Band steering
- WiFi multimedia (WMM) for prioritizing traffic

- Client filtering by MAC addresses with on-board filter
- Dynamic Host Control Protocol (DHCP) client
- Network Time Protocol (NTP) client
- System log
- Syslog client
- Autonomous Management Framework (AMF) Guest node

Security and Encryption

- Open system
- Shared key authentication
- WPA Personal or Enterprise security with auto, CCMP (AES), or TKIP encryption
- WPA2 Personal or Enterprise security with auto, CCMP (AES), or TKIP encryption
- WPA3 Personal security with CCMP (AES) encryption
- WPA3 Enterprise security with GCMP encryption

Frequency Range and Bandwidth for the 2.4GHz Radio

- 2.412 to 2.472GHz
- 20/40MHz

Frequency Range and Bandwidth for the 5GHz Radio

- 5.150 to 5.250GHz
- 5.250 to 5.350GHz
- 5.500 to 5.720GHz
- 5.745 to 5.825GHz
- 20/40/80MHz

Ethernet LAN Port

- 10Mbps (IEEE 802.3), 100Mbps (IEEE 802.3u), 1000Mbps (IEEE 802.3ab), 2.5Gbps, and 5Gbps (IEEE 802.3bz)
- PoE+ (IEEE 802.3at)
- Flow control (IEEE 802.3x)
- VLAN tagging (IEEE 802.1Q)
- Auto-Negotiation for speed and duplex mode
- Auto-MDI/MDIX at 10/100Mbps

Management Options

- On-board web browser management interface
- Vista Manager EX with Automous Wave Controller (AWC) plug-in
- Vista Manager mini with AWC plug-in
- Autonomous Management Framework (AMF) Security or Security Mini (AMF-Sec mini)

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**
> Allied Telesis supports Google Chrome and Microsoft Edge for this product.

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 Channel Blankets feature on the access point requires Vista Manager EX.

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

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

SNMPv1, SNMPv2c, and SNMPv3

You can use SNMPv1, SNMPv2c, and SNMPv3 to view the parameter settings of the access point. The MIB is available from Allied Telesis website. For instructions on how to configure the access point for SNMP, see "Configuring SNMPv1, SNMPv2c and SNMPv3" on page 44.

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

Starting the First Management Session

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

The default IP address of the access point: 192.168.1.230

If your network has a DHCP server, use the IP address the server assigns it to it to start the management session. For directions, see “Starting a Management Session” on page 26.

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 LAN 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.
- “Starting the First Management Session without a DHCP Server” on page 24

Starting the First Management Session with a Direct Connection

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

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

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

   See the documentation that accompanies your computer for instructions on how to set the IP address.
3. Set the subnet mask on your computer to 255.255.255.0.
4. Power on the access point by doing one of the following:
   - Install a PoE+ injector on the Ethernet cable.
   - Connect an AC/DC adapter to a DC port and Press on the Power button on the access point.
5. Power on the access point with an AC/DC adapter or PoE+ injector.
6. Wait one minute for the access point to initialize its management software.
7. Start the web browser on your computer.
8. 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 26.
9. Enter the user name and password.
   - ❒ User name: manager
   - ❒ Password: friend

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

Starting the First Management Session without a DHCP Server

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

1. To use the PoE feature on the access point, be sure to connect the LAN port to a PoE source device.
2. Connect one end of network cable to the LAN port on the access point and the other end to a port on an Ethernet switch.

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

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

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

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

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

5. Power on the access point by doing one of the following:

   – Connect the LAN port to a PoE+ power sourcing equipment.
   – Connect an AC/DC adapter to the DC port and press the Power button on the access point.
   – Install a PoE+ injector on the Ethernet cable.

6. Wait one minute for the access point to initialize its management software.

7. Start the web browser on your computer.

8. 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 26.

9. Enter the user name and password.

   ❒ User name: manager
   ❒ Password: friend

   Note
   The user name and password are case-sensitive.

10. Click the Login button.

Starting a Management Session

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

Note
If the access point is using its default address 192.168.1.230, see "Starting the First Management Session" on page 23 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.

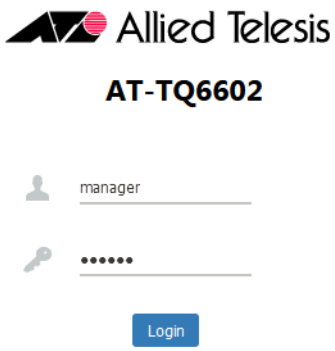


Figure 1. Log On Window

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

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

   The default values are:

   - User name: manager
   - Password: friend

   Note
   The user name and password are case-sensitive.

4. Click the Login button.

Management Windows

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

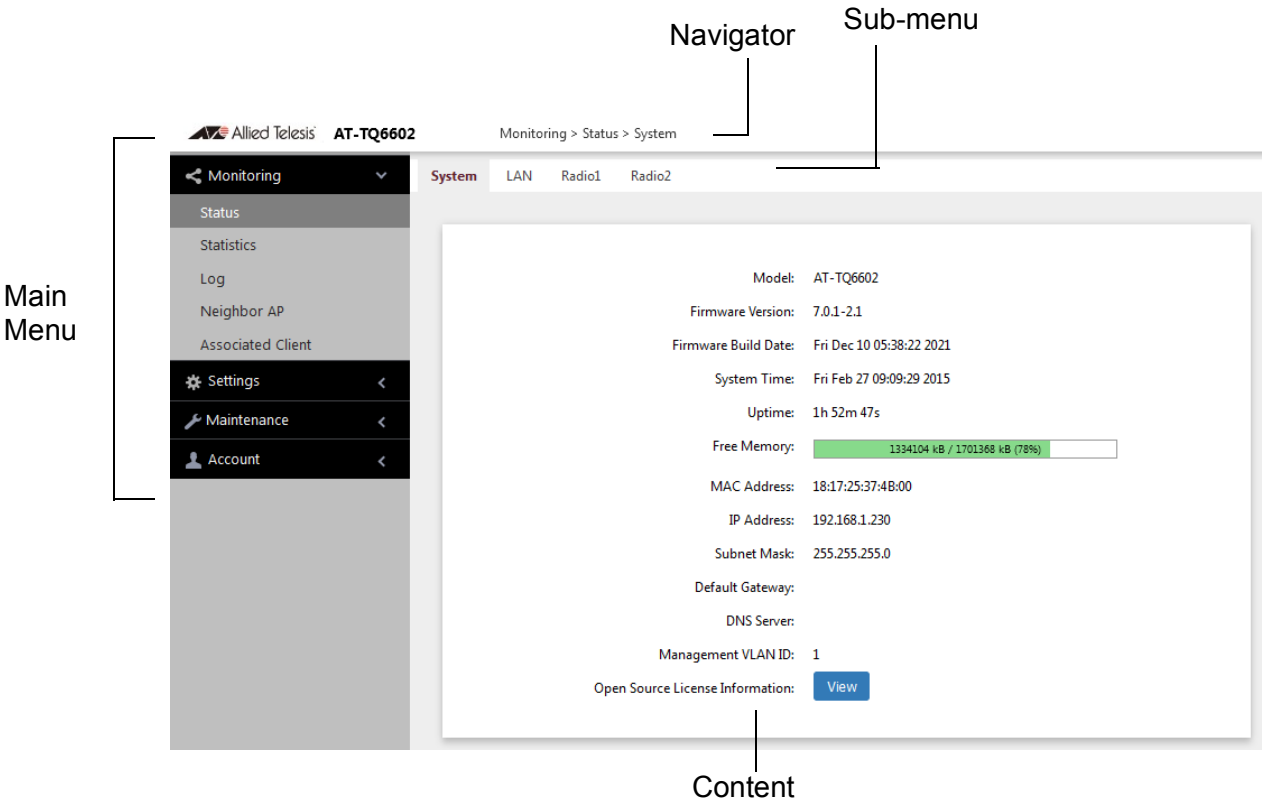


Figure 2. Sample Management Window

Main Menu

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

- Monitoring
- Settings
- Maintenance
- Account

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

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

Figure 3. Main Menu Button

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

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

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

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.

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 66.

   Note
   The country code for units sold in North America, Japan, and 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 128.

3. If you prefer to use HTTPS management sessions, perform "Configuring the Web Browser Interface" on page 126.

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 130.

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. See Figure 4.

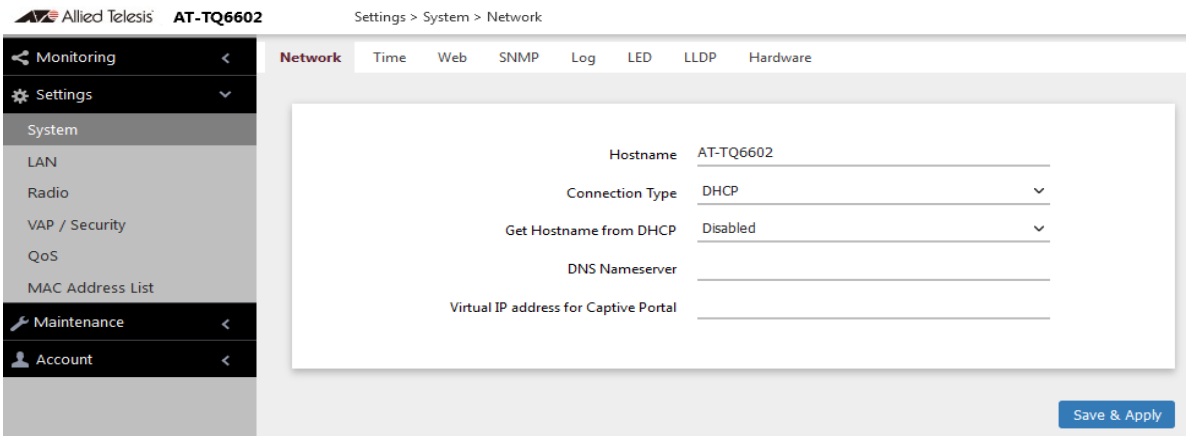


Figure 4. Network DHCP Window

4. Configure the fields by referring to Table 1.

Table 1. 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 TQ6602. - 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.
Get hostname from DHCP	Select one of the following options: - Enabled: When the DHCP server assigns an IP address to the access point, the server assigns a host name as well. - Disabled: The DHCP server does not change the hostname of the access point. This is the default setting.
DNS Nameserver	Enter the IP address of the DNS server. If this field is left blank, the access point tries to obtain the address from the DHCP server. The default is no name.
Virtual IP address for Captive Portal	Assign a virtual IP address to the access point for Captive Portal. Wireless clients use the virtual IP address instead of the access point’s actual IP address to log on to Captive Portal. Hiding the actual IP address increases the security of the network.

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

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

Assigning a Static 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.

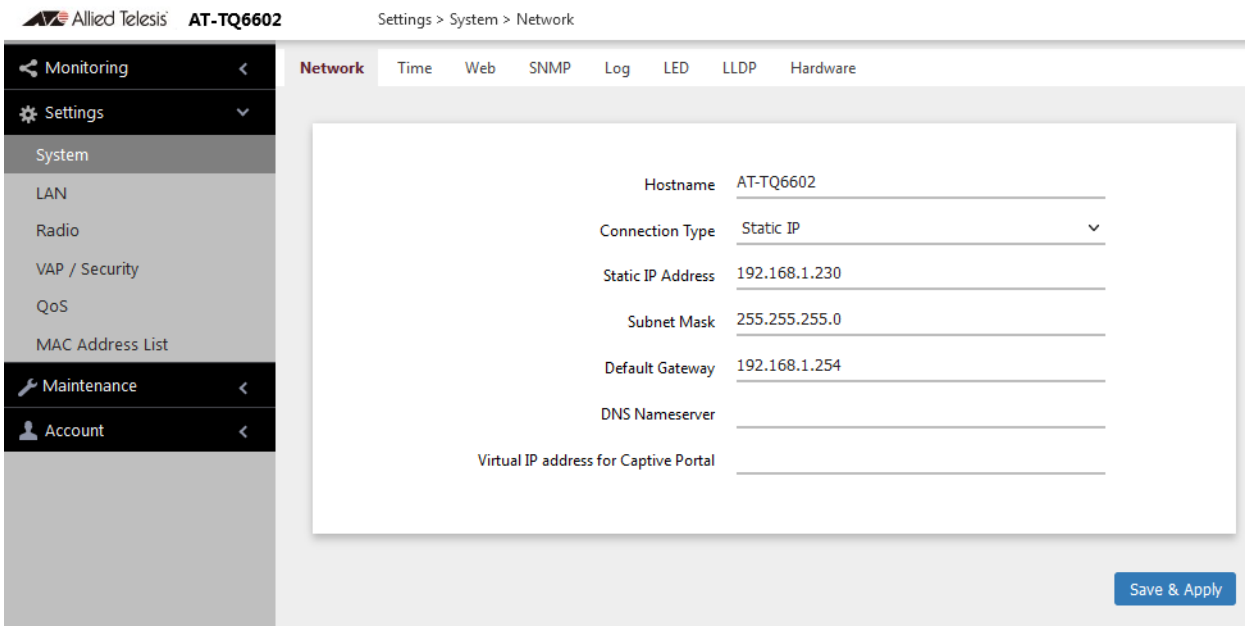


Figure 5. Network Static IP Address Window

4. Configure the field values by referring to Table 2.

Table 2. 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 TQ6602.
Connection Type	Select **Static IP**.
Static IP Address	Enter the new IP address for the access point. The device can have only one IP address. The default is 192.168.1.230.
Subnet Mask	Enter the subnet mask for the IP address. The default is 255.255.255.0.
Default Gateway	Enter the default gateway address for the unit. The default value is 192.168.1.254.
DNS Nameserver	Specify the Domain Name Service (DNS) server address. This field is optional. The default is no name.
Virtual IP address for Captive Portal	Assign a virtual IP address to the access point for Captive Portal. Wireless clients use the virtual IP address instead of the access point's actual IP address to log on to Captive Portal. Hiding the actual IP address increases the security of the network.

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

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

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

Here are the guidelines to using the client:

- You need to know the domain name or 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 42.
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.

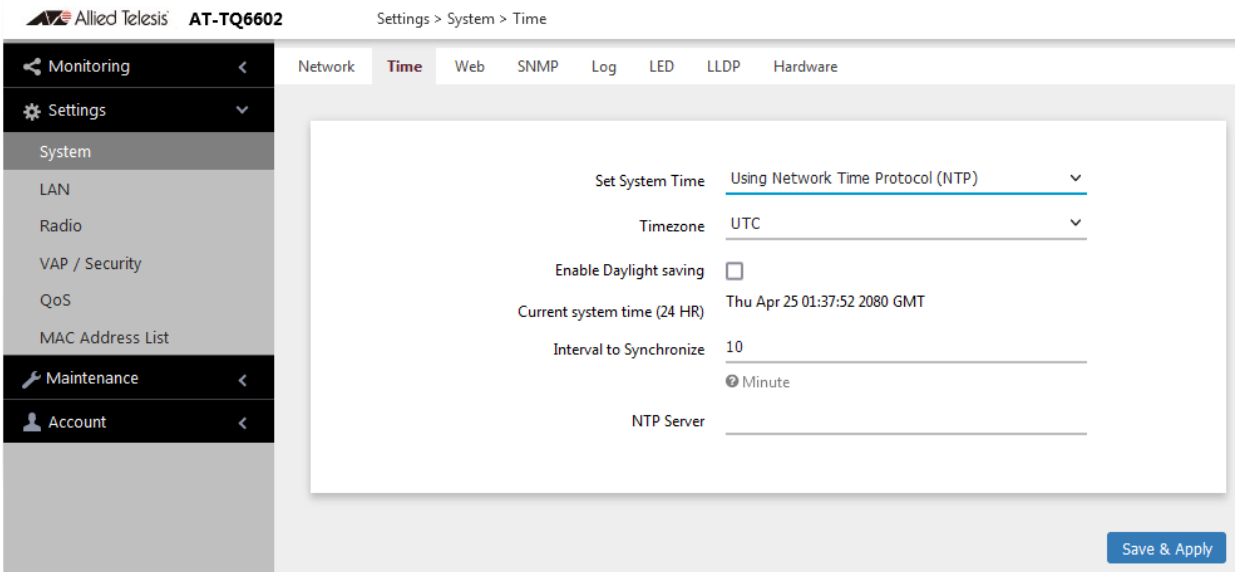


Figure 6. Time Window - NTP Option

4. Configure the fields by referring to Table 3.

Table 3. 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 41. If the area does not observe Daylight Savings time, leave the check box empty.
Start (Daylight Saving)	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End (Daylight Saving)	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset (Daylight Saving)	Use the pull-down menu to select the number of minutes to adjust the time at the start and end Daylight Saving Time. The default is 60 minutes.
Current System Time (24 HR)	Displays the date and time of the access point.
Interval to Synchronize	Enter the interval in minutes at which the access point synchronizes its time with the SNTP server. The range is 1 to 9999 minutes. The default is 10 minutes.

Table 3. 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.

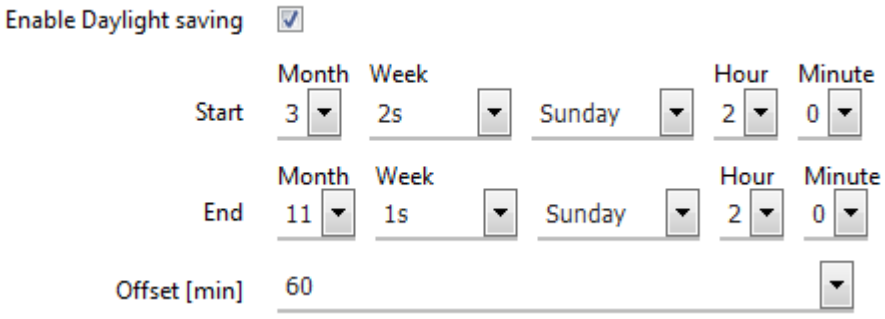


Figure 7. Daylight Savings Time Settings

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 an SNTP server to set the date and time. For instructions, refer to "Setting the Date and Time with the Network Time Protocol (NTP)" on page 39.

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.

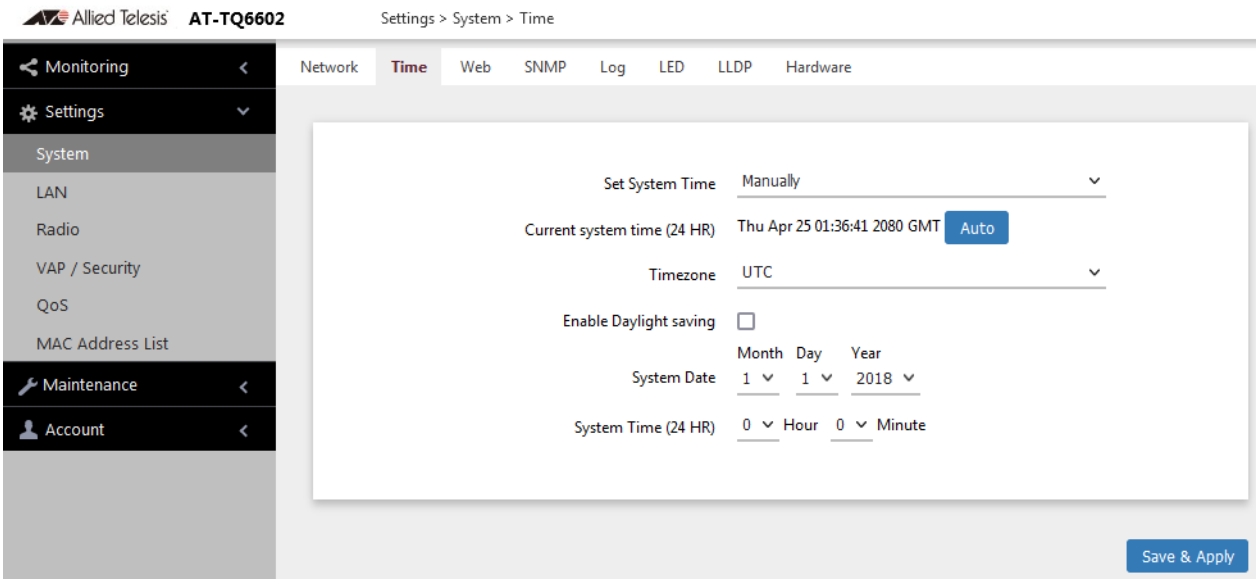


Figure 8. Time Window - Manually Option

3. Configure the parameters by referring to Table 4.

Table 4. 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 41 If the area does not observe Daylight Savings time, leave the check box empty.
Start (Daylight Saving)	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End (Daylight Saving)	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset (Daylight Saving)	Use the pull-down menu to select the number of minutes to adjust the time at the start and end Daylight Saving Time. The default is 60 minutes.
System Date	Use the pull-down menus to set the current month, day, and year.
System Time	Use the pull-down menus to set the current hours and minutes. The hours are in 24 hours. For example, 14 represent 2:00 p.m.

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

Configuring SNMPv1, SNMPv2c and SNMPv3

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

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

  For more information, see"Assigning a Dynamic IP Address from a DHCP Server" on page 34 or "Assigning a Static IP Address to the Access Point" on page 37.

To enable or disable SNMP, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **SNMP** from the sub-menu. Refer to Figure 9.

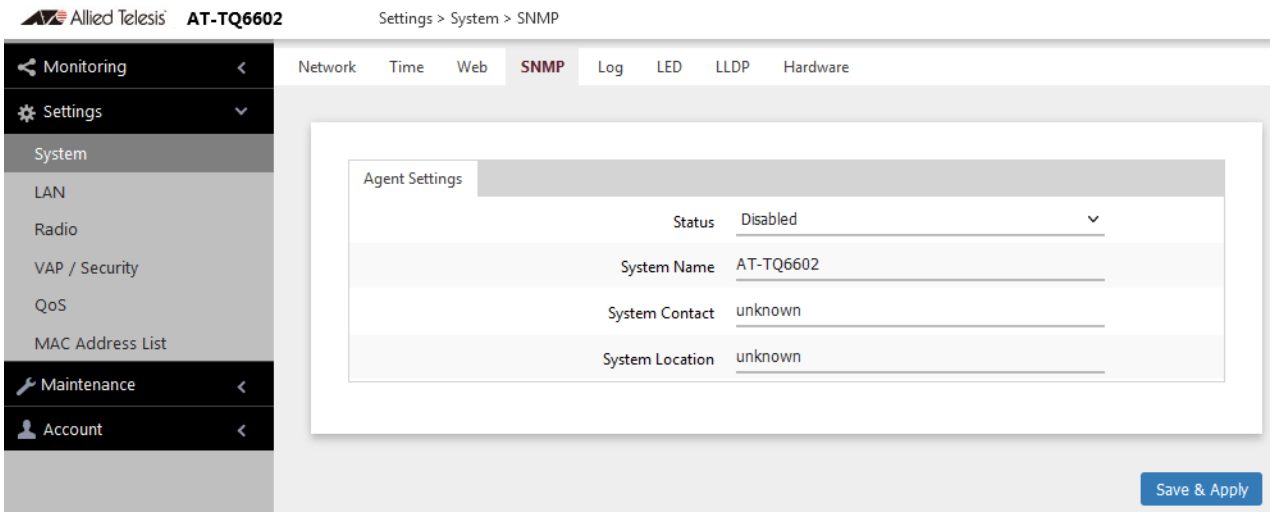


Figure 9. SNMP Window

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

   When Enabled is selected, the SNMPv1 and SNMPv2 or SNMPv3 configuration window appears. See Figure 10 on page 45.

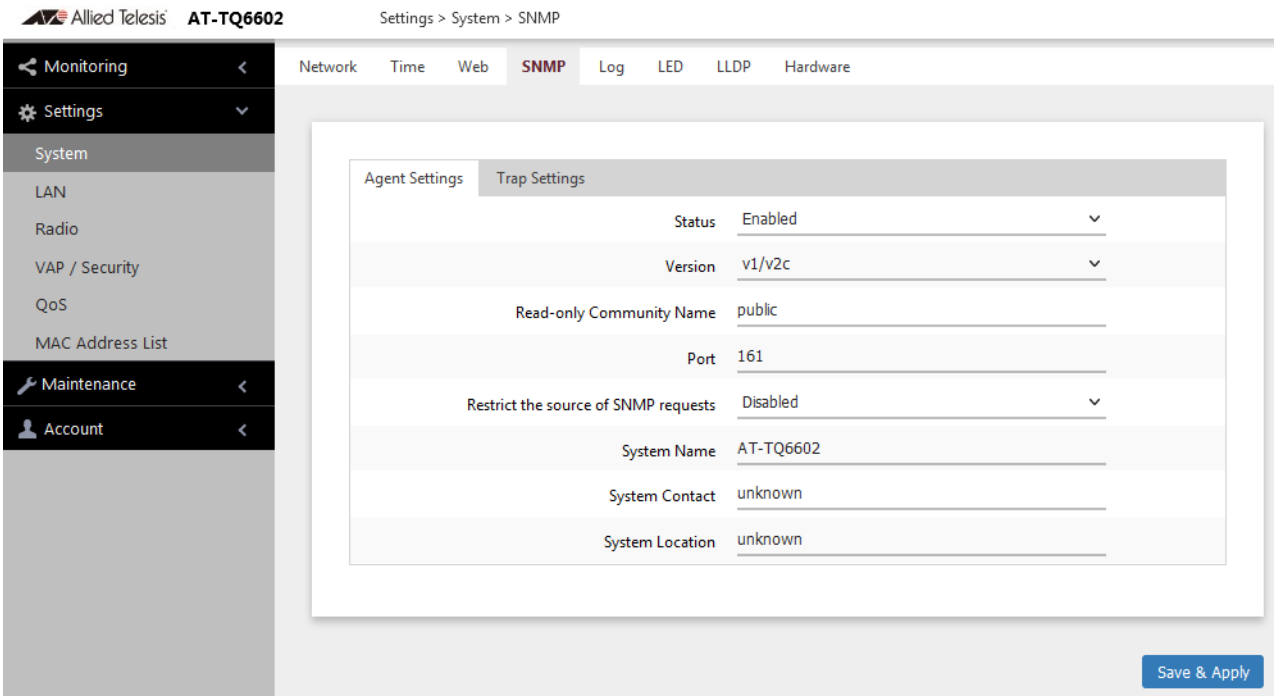


Figure 10. SNMP Window - SNMP Enabled

4. Configure the parameters by referring to Table 5.

Table 5. SNMP Window

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

Table 5. SNMP Window (Continued)

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

Table 5. SNMP Window (Continued)

Field	Description
Only allow from the designated hosts or subnets	Specify management workstations permitted to use SNMP to view the device. This parameter applies only to SNMPv1 and SNMPv2c. Here are guidelines: - You can specify only one value in the field. - You can specify a workstation by its IPv4 address (for example, 192.168.1.5). - You can specify a group of workstations that fall in the same subnet. (for example, 192.168.1.0/24). - You can specify a workstation by its Fully Qualified Domain Name (FQDN). - The default is blank. Observe these guidelines when using an FQDN to specify the workstation: - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters - An FQDN can have up to 253 characters.
System Name	Specify the SNMP system name of the access point. The default is AT-TQ6602.
System Contact	Specify the system administrator name. The system contact can be up to 64 alphanumeric characters. The default is Unknown.
System Location	Specify the location of the device. It can be up to 64 alphanumeric characters. The default is Unknown.

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

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 11.

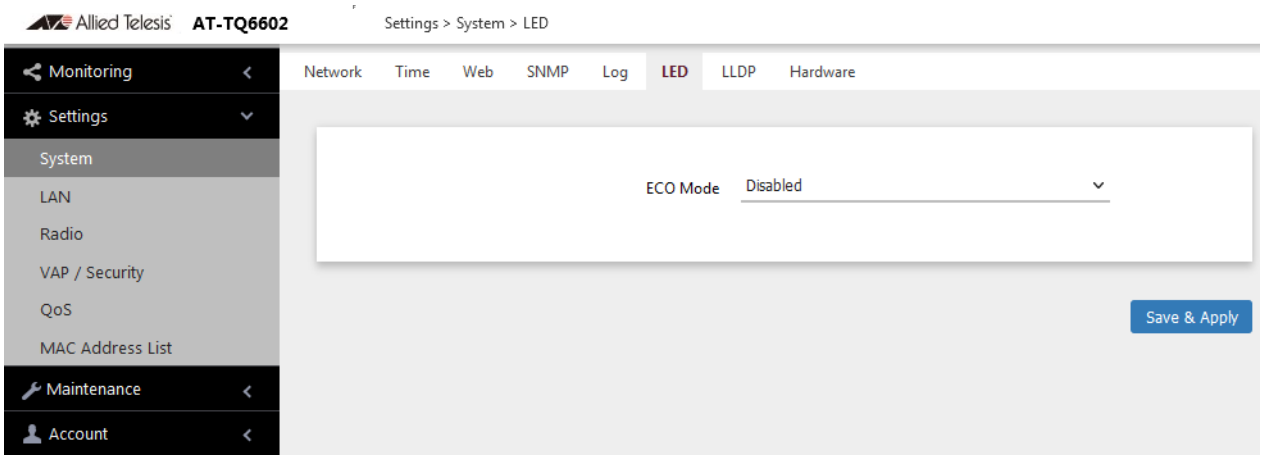


Figure 11. LED Window

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

Configuring PoE Negotiation with Link Layer Discovery Protocol (LLDP)

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

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

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

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

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

Here are guidelines for PoE negotiation with LLDP:

- ❒ The access point must be powered with PoE.
- ❒ The LAN port must be connected to an LLDP-Med device.
- ❒ The LLDP-MED device must be configured for the Extended Power Management TLV.
- ❒ The access point requests 18.8W in the TLV.
- ❒ This feature is optional. The access point can be powered by PoE without enabling this feature.

To enable or disable LLDP PoE negotiation, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **LLDP** from the sub-menu. Refer to Figure 12 on page 50.

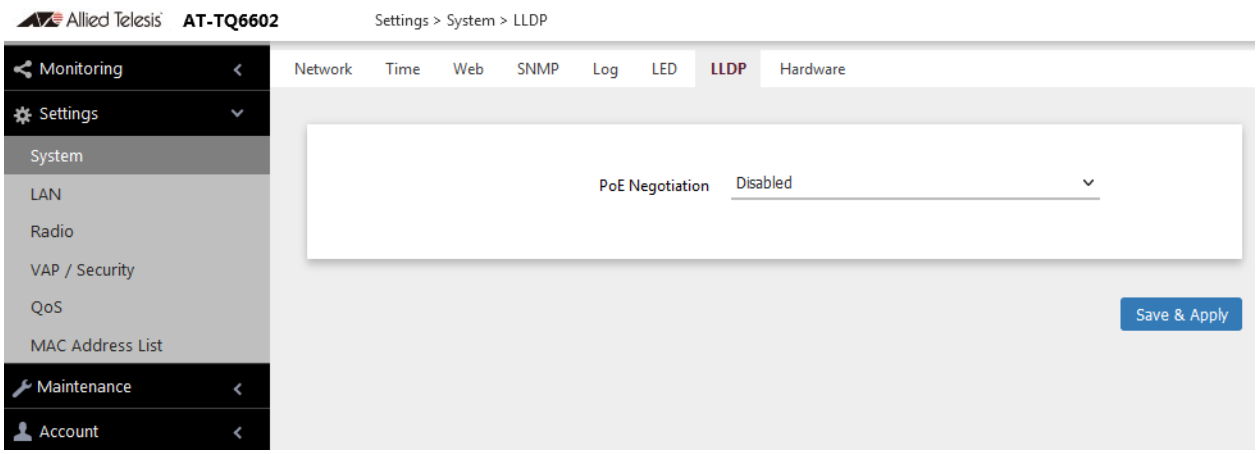


Figure 12. LLDP Window

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

Enabling or Disabling the Reset Button

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

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

> **Note**
> If you disable the Reset button, be sure not to forget the manager account password or the device's IP address. 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 13.

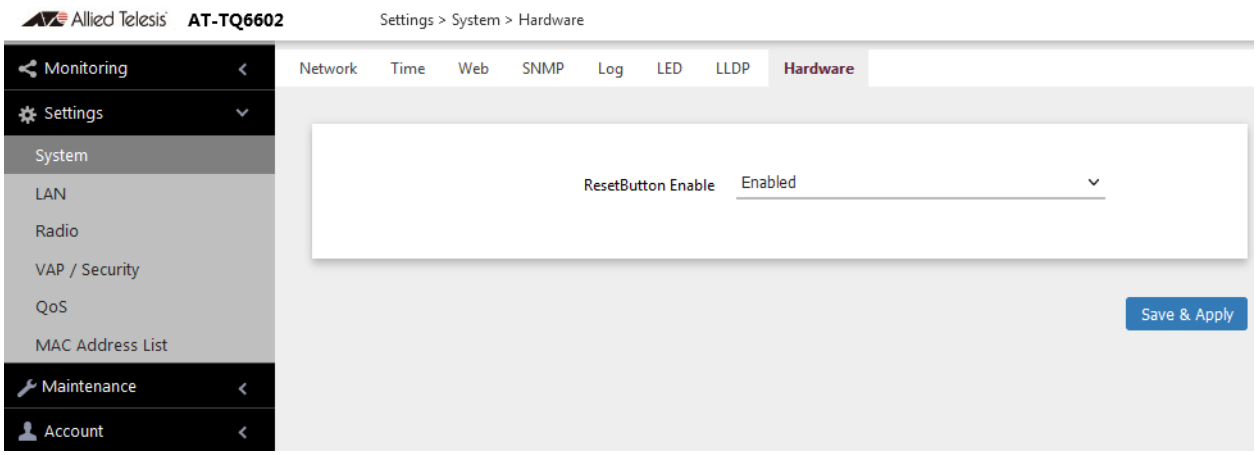


Figure 13. Hardware Window

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

Chapter 3

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 57

Configuring Basic Radio Settings

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

1. Select **Settings** > **Radio**.
2. Select **Radio1** or **Radio2** from the sub-menu. You can configure only one radio at a time.
3. Click the **Basic Settings** tab shown in Figure 14. This is the default tab.

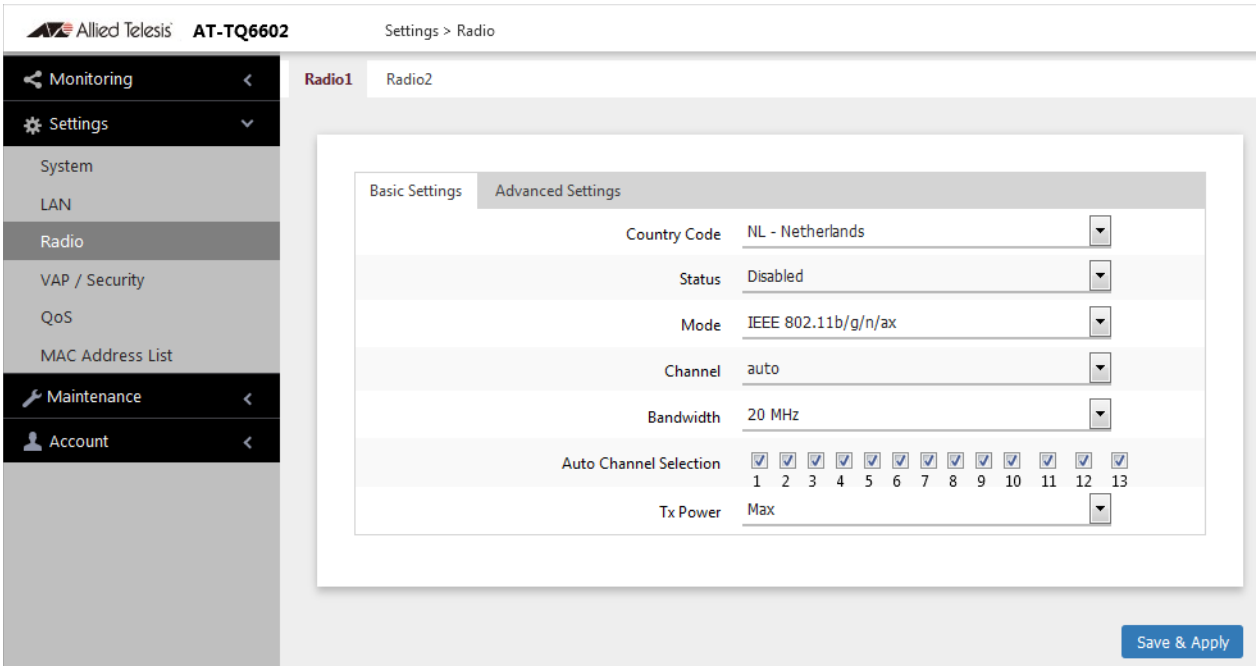


Figure 14. Basic Radio Settings Window

4. Configure the settings by referring to Table 6 on page 55.

Table 6. 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 both radios but it can only be set from Radio1. - The same country code applies to both radios. - Changing the country code disables the radios. - You have to reconfigure the radio settings if you change the country code. - You cannot change the country code on units sold in North America, Japan, or Taiwan.
Status	Activate or deactivate the radio. The selections in the pull-down menu are described here: - Enabled: Activates the radio. - Disabled: Deactivates the radio. This is the default setting.
Mode (Radio1)	Select the communications protocol for Radio1 from the pull-down menu. The selections are listed here: - IEEE 802.11b/g/n/ax: The access point accepts 802.11b, 802.11g, 802.11n,and 802.11ax clients. This is the default for Radio1. - IEEE 802.11b/g: The access point accepts 802.11b and 802.11g clients. Wi-Fi multimedia (WMM) has to be enabled (default) to use IEEE 802.11n or IEEE 802.11ax. Refer to “Configuring QoS Basic Settings” on page 134.

Table 6. Basic Radio Settings Window (Continued)

Field	Description
Mode (Radio2)	Select the communications protocol for Radio2 from the pull-down menu. The selections are listed here: - IEEE 802.11a: The access point accepts 802.11a clients. - IEEE 802.11b/g/n/ax: The access point accepts 802.11b, 802.11g, 802.11n,and 802.11ax clients. This is the default for Radio2. Wi-Fi multimedia (WMM) has to be enabled (default) to use IEEE 802.11n or IEEE 802.11ax. Refer to "Configuring QoS Basic Settings" on page 134.
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. - To view the current active channel, refer to "Displaying Radio Status" on page 62.
Bandwidth (Radio1)	Select the bandwidth for Radio1 from the pull-down menu. The selections for IEEE 802.11b/g/n/ax are listed here: - 20 MHz. This is the default setting. - 40 MHz For IEEE 802.11g/b/n/ax mode, 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 6. Basic Radio Settings Window (Continued)

Field	Description
Bandwidth (Radio2)	Select the bandwidth for Radio2 from the pull-down menu. The available bandwidths for IEEE 802.11a/n/ac/ax are listed here: - 20 MHz. This is the default setting. - 40 MHz - 80 MHz - 80+80 MHz The only bandwidth for IEEE 802.11a is 20 MHz.
Second Channel	Not supported.
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 or Radio2, perform the following procedure:

1. Select **Settings** > **Radio** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. You can configure only one radio at a time.
3. Click the **Advanced Settings** tab. See Figure 15 on page 58.

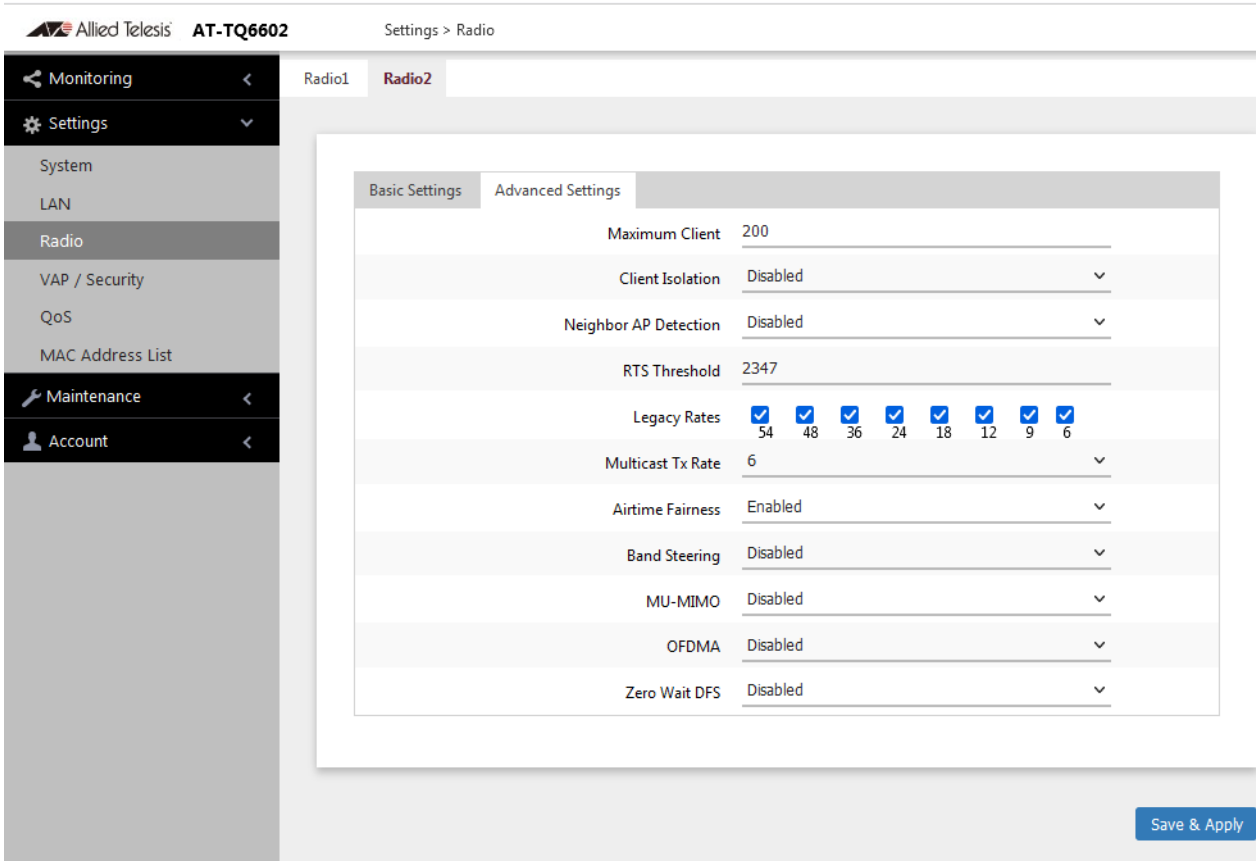


Figure 15. Advanced Radio Settings Window

4. Configure the parameters by referring to Table 7.

Table 7. Advanced Radio Settings Window

Field	Description
Maximum Clients	Use this option to specify the maximum number of wireless clients that a radio will support at one time. You might use the option to control the distribution of clients over the radios. A radio rejects all clients when the parameter is set to 0. The maximum numbers of wireless clients that a radio supports at one time are: - 2.4GHz Radio1 - 320 clients (default setting) - 5GHz Radio2 - 320 clients (default setting)
Client Isolation	Not Supported.

Table 7. 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 Neighbor Access Points” on page 151. - Disabled: The access point does not listen for neighboring access points. This is the default setting.
RTS Threshold	Specify the size in octets of MPDUs, which initiate a Request to Send (RTS) and Clear to Send (CTS) handshake in IEEE802.11b/g. The Range is 0 to 2347. The default is 2347 in octets. When RTS Threshold is 2347, the RTS/CTS function is disabled. Use this parameter to control the use of RTS/CTS handshake 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 frames are send more frequently, which may consume more bandwidth and reduce the throughput; however, more RTS frames may help a network recovery 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

Table 7. Advanced Radio Settings Window (Continued)

Field	Description
Airtime Fairness	Not supported
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 radio is congested. Here are the guidelines: - Enabling band steering on one radio activates it on the other radio. Conversely, disabling the feature on one radio disables it on the other radio. - Ideally, the VAP settings on both radios should be identical. This includes SSID names, VLAN IDs, and security settings. - The default setting is disabled.
MU-MIMO	Multi-user, multiple input, multiple output (MU-MIMO) helps increase the number of simultaneous users a single access point can support. Here are the options: - Disabled: MU-MIMO is disabled. This is the default setting. - Enabled: the access point can support up to 4 wireless clients simultaneously.
OFDMA	Orthogonal Frequency Division Multiple Access (OFDMA) allows the access point to serve multiple wireless clients at the same time by dividing packets into separate bands. Here are the options: - Disabled: OFDMA is disabled. This is the default setting. - Enabled: the access point can serve multiple wireless clients at the same time.
Zero Wait DFS	Not supported.

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** or **Radio2** from the sub-menu. You can view only one radio at a time. The example in Figure 16 is for Radio1.

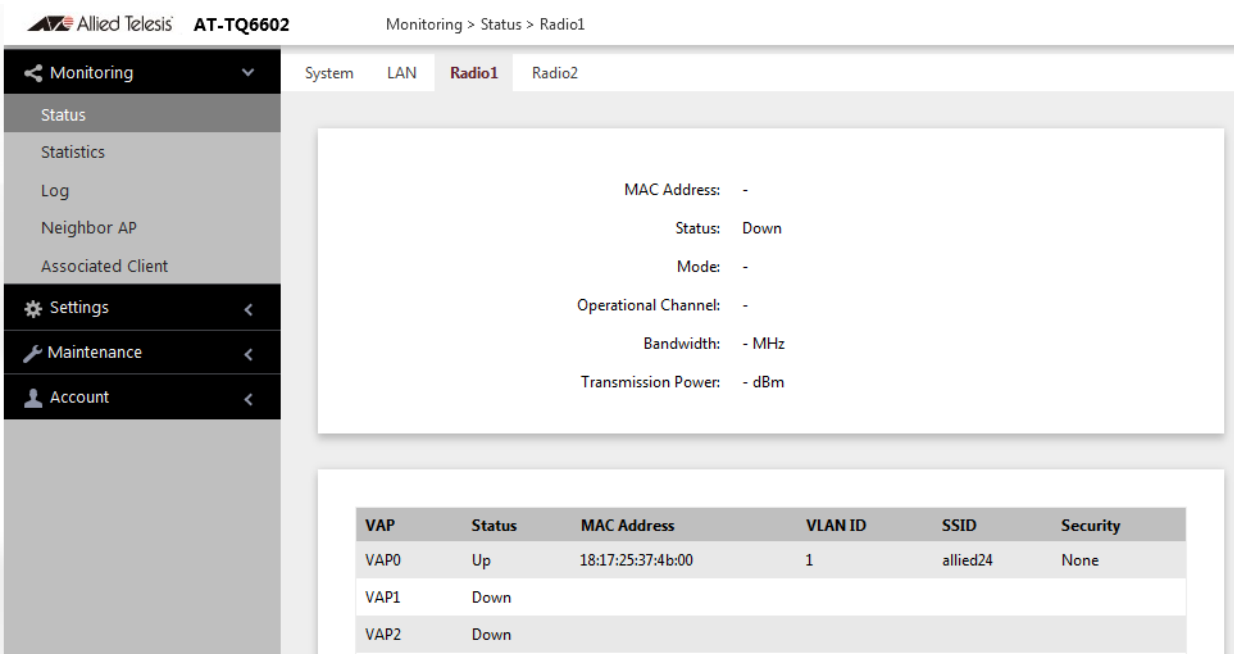


Figure 16. Radio1 Status Window

Figure 17 is an example for Radio2.

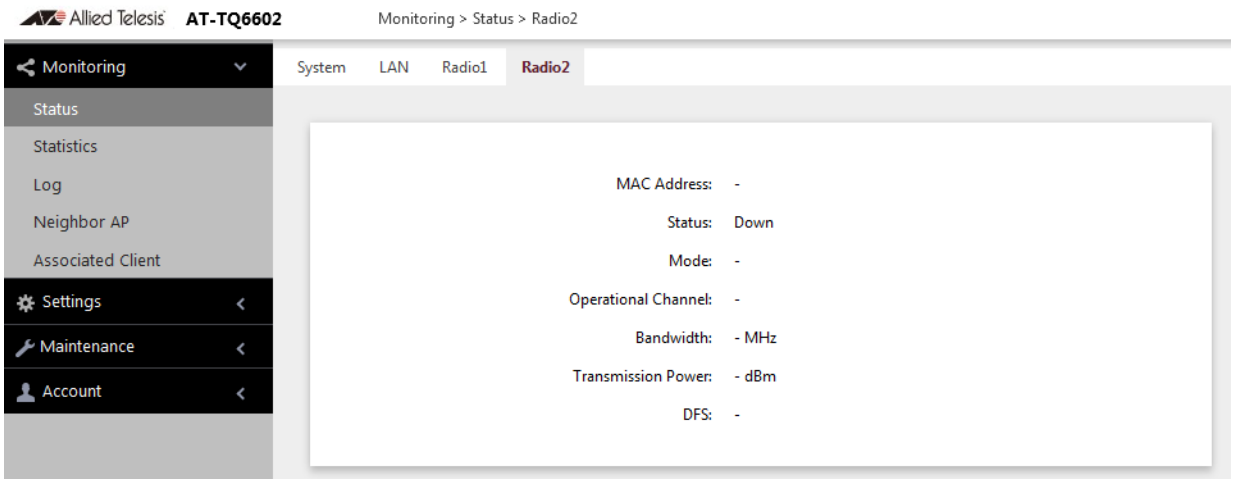


Figure 17. Radio2 Status Window

Note
The radio status window for Radio2 includes a DFS (Dynamic Frequency Selection) field. For more information, see “Dynamic Frequency Selection (DFS)” on page 65.

The fields are defined in Table 8.

Table 8. Radio Status Window

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

Table 8. Radio Status Window (Continued)

Field	Description
DFS (Radio2 only)	Displays the status of DFS (Dynamic Frequency Selection). For background information, refer to "Dynamic Frequency Selection (DFS)" on page 65. 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 wireless traffic because radar signals are detected on all channel candidates. After 30 minutes, the radio moves to the CAC state.

Dynamic Frequency Selection (DFS)

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

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

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

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

Note
To determine whether Radio2 is using a DFS channel, refer to “Displaying Radio Status” on page 62.

Setting the Country Code Setting

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

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

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

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

1. Select **Settings** > **Radio**.
2. Select **Radio1** from the sub-menu. The country code must be set from Radio1.
3. Click the **Basic Settings** tab. This is the default tab. Refer to Figure 14 on page 54.
4. Select the **Country Code** pull-down menu and choose your country or region. Here are the guidelines:
   - ❒ You can select only one country.
   - ❒ The Country Code parameter is shown in the Basic Settings windows of both radios, but can only be set from Radio1.
   - ❒ The same country code applies to Radio2.
   - ❒ Changing the country code disables the radios.
   - ❒ You have to reconfigure the radio settings after changing this parameter.
5. Click the **SAVE & APPLY** button to save and update the configuration.

Chapter 4

Virtual Access Points

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

VAP Introduction

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

VAP parameters are divided into these two groups:

- "Configuring Basic VAP Parameters" on page 69
- "Configuring VAP Security" on page 74

VAP Guidelines

Here are guidelines to configuring VAP:

- Each radio can have up to 16 VAPs.
- The VAPs are numbered from 0 to 15.
- You can enable or disable the VAPs individually, except for VAP0, which can only be disabled by disabling its radio.
- You can enable 11 VAPs per radio.
- The VAP securities are Enterprise WPA and Personal WPA.
- The VAPs of a radio can have different security methods.
- VAPs can have the same or different VLAN IDs.

Configuring Basic VAP Parameters

To configure basic VAP settings, perform the following procedure:

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

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

4. Select the **Virtual Access Point** tab. This is the default tab. The example in Figure 18 shows the settings for VAP0 on Radio1.

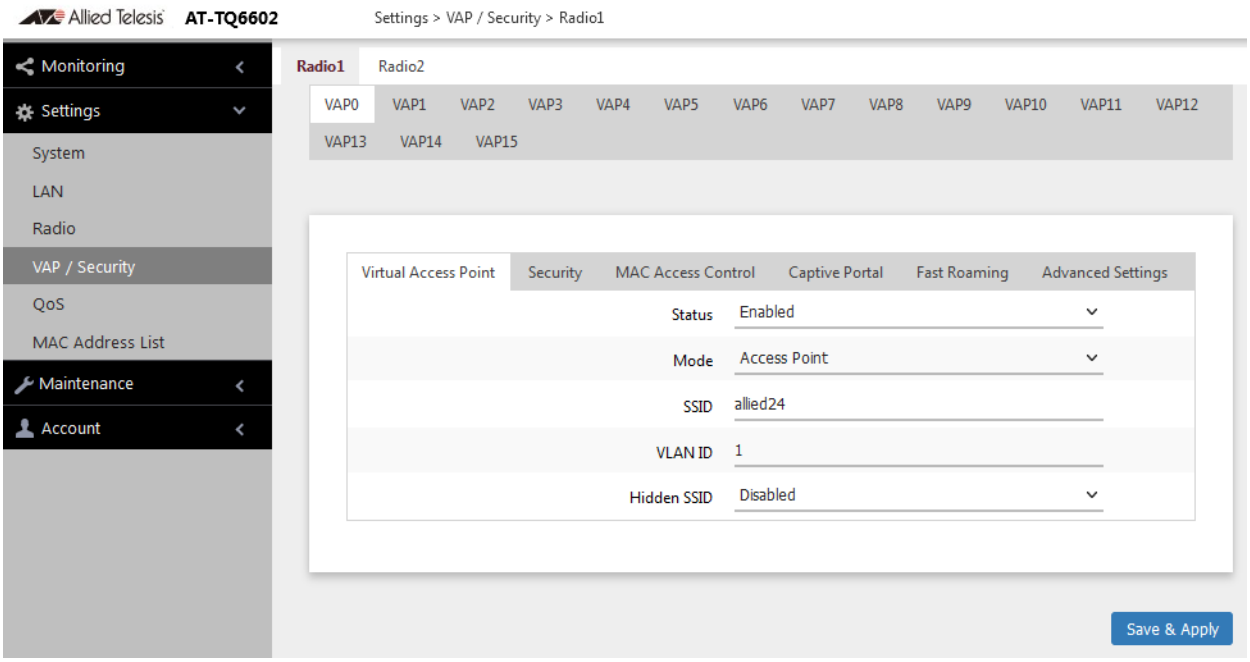


Figure 18. Virtual Access Point Tab

5. Configure the parameters by referring to Table 9 on page 70.

Table 9. Virtual Access Point Tab

Field	Description
Status	Enable or disable the VAP. Here are the guidelines. - A disabled VAP does not forward any ingress or egress traffic. - The default setting for VAP0 is enabled. - The default setting for VAP1 to VAP15 is disabled. - You cannot disable VAP0. To stop VAP0 from forwarding traffic from wireless clients, you have to disable its radio.
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 116. - 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. For background information, refer to "Introduction to Wireless Distribution Bridges" on page 116. **Note** The mode option for VAP1 to VAP15 is only Access Point. - Channel Blanket: Autonomous Wave Control Chanel Blanket (AWC-CB) enables access points with overlapping signals to use the same channel, rather than different channels, for their roaming wireless clients. The mode requires AWC and Vista Manager EX. Refer to the *Vista Manager AWC Plug-in User Guide*. For limitations on the access point, see "Limitations on Channel Blanket" on page 72.

Table 9. 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 except the first and last characters of an SSID. ❒ You can assign the same name to more than one VAP. ❒ The default names for VAP0 on Radio1 and Radio2 are allied24 and allied5, respectively. ❒ The default names for VAP1 to VAP15 are Virtual Access Points 1 to 15.
VLAN ID	Enter a VID for the VAP. Here are the guidelines: ❒ The range is 1 to 4094. ❒ The default is VID 1. ❒ A VAP can have only one VID. ❒ You can assign the same VID to more than one VAP. ❒ This VID is ignored for wireless clients that receive their VIDs from a RADIUS server for WPA Enterprise security. VIDs from a RADIUS server override the number in this field.
Hidden SSID	Select whether the access point should advertise the VAP SSID to clients. Here are the options: ❒ Disabled: The access point transmits the SSID to advertise the VAP to clients. This is the default setting. ❒ Enabled: The access point does not advertise the VAP. Clients who want to connect to a hidden VAP have to know its name.

Table 9. 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 110. 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. ❒ External RADIUS: Authenticates wireless clients with an external RADIUS server. To configure External RADIUS for authentication, see "Configuring VAP Security" on page 74.

6. Select another VAP to configure from the sub-menu and repeat Step 4 and Step 5 if necessary.
7. Click the **SAVE & APPLY** button to save and update the configuration, or configure other VAPs and save the configurations at once later.

Limitations on Channel Blanket

The Channel Blanket feature has the following limitations:

Limitations on the Access Point

- ❒ Band Steer is not supported.
- ❒ Neighbor AP Detection is not supported.
- ❒ Association Advertisement is not supported.

Limitations on the Blanket Radio Interface

- ❒ The value of the RTS Threshold cannot be changed.
- ❒ Airtime is not supported.
- ❒ OFDMA is not supported.
- ❒ MU-MIMO is not supported.

Limitations on Channel Blanket-enabled VAP

- The value of the Broadcast Key Refresh Rate cannot be changed.
- The value of the Session Key Refresh Rate cannot be changed.
- The value of the Session Key Refresh Action cannot be changed.
- RADIUS Accounting is not supported.
- Fast Roaming is not supported.
- Dynamic VLAN is forced to be disabled.
- The Session-Timeout RADIUS attribute is forced to be disabled.
- The value of the Inactivity Timer cannot be changed.
- IEEE802.11w(MFP) needs to be disabled.

Configuring VAP Security

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

- "No Security" on page 74
- "WPA Personal (Pre-Shared Key)" on page 75
- "WPA Enterprise" on page 77

No Security

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

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

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

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

4. Select the **Security** tab.
5. Select **None** from the Mode pull-down menu. This is the default setting. Refer to Figure 19.

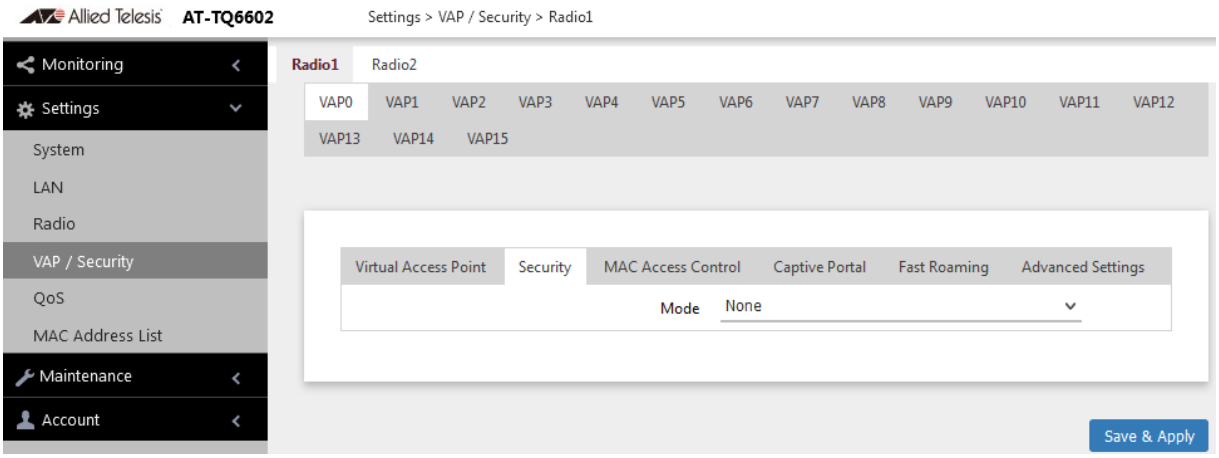


Figure 19. None Selection in the VAP Security Tab

6. Select another VAP to configure from the sub-menu and repeat Step 4 to Step 5 if necessary.

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

WPA Personal (Pre-Shared Key)

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

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

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

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

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

4. Select the **Security** tab.

5. Select **WPA Personal** from the Mode pull-down menu. Refer to Figure 20.

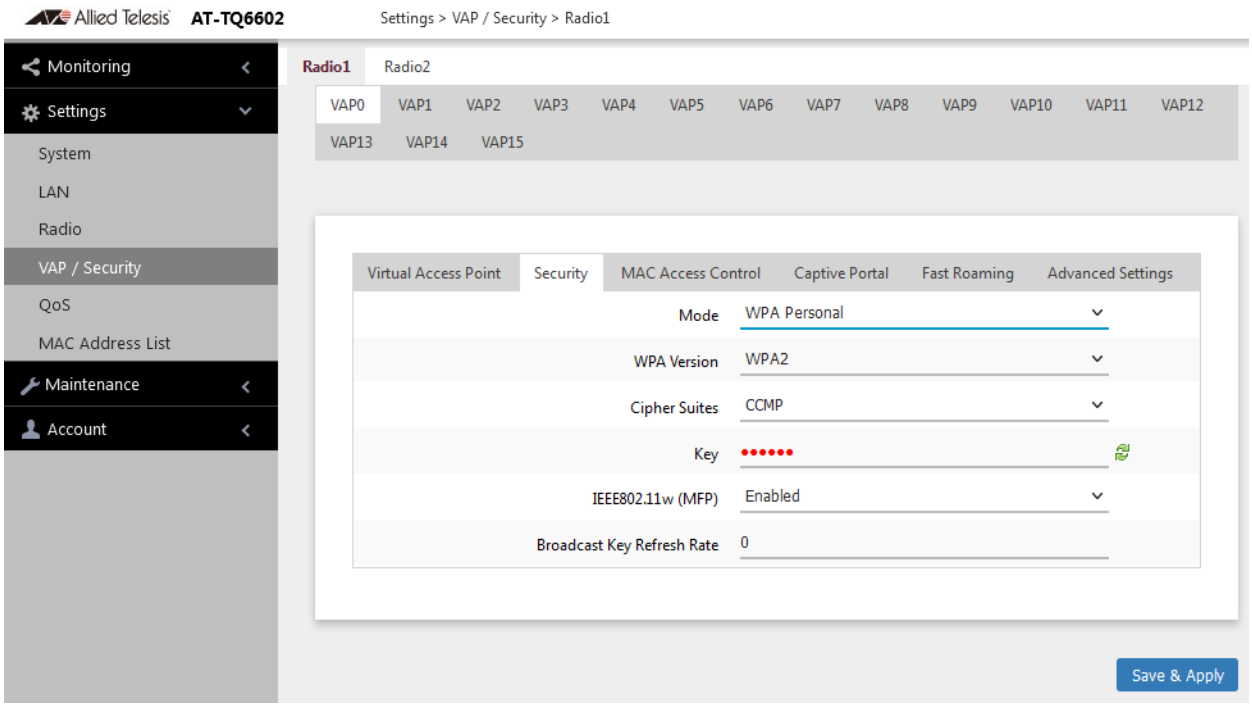


Figure 20. WPA Personal Security Tab

6. Configure the parameters by referring to Table 10.

Table 10. 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 only. This is the default setting. - WPA2 and WPA3: Select this option if the VAP has both WPA2 and WPA3 clients. - WPA3: Select this option if clients support WPA3 only. This is the default setting.
Cipher Suites	Select the cipher suite for the VAP. The options are listed here: - CCMP. This is the default. **Note** When the WPA version is WPA2 and WPA3, or WPA3, CCMP is the only option. - 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.

Table 10. WPA Personal Security Tab (Continued)

Field	Description
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. **Note** When the WPA version is WPA2 and WPA3, or WPA3, Enabled is the only option. - 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. Select another VAP to configure from the sub-menu and repeat Step 4 to Step 6 if necessary.

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

WPA Enterprise

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

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

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

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

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

4. Select the **Security** tab.

5. Select **WPA Enterprise** from the Mode pull-down menu. See Figure 21.

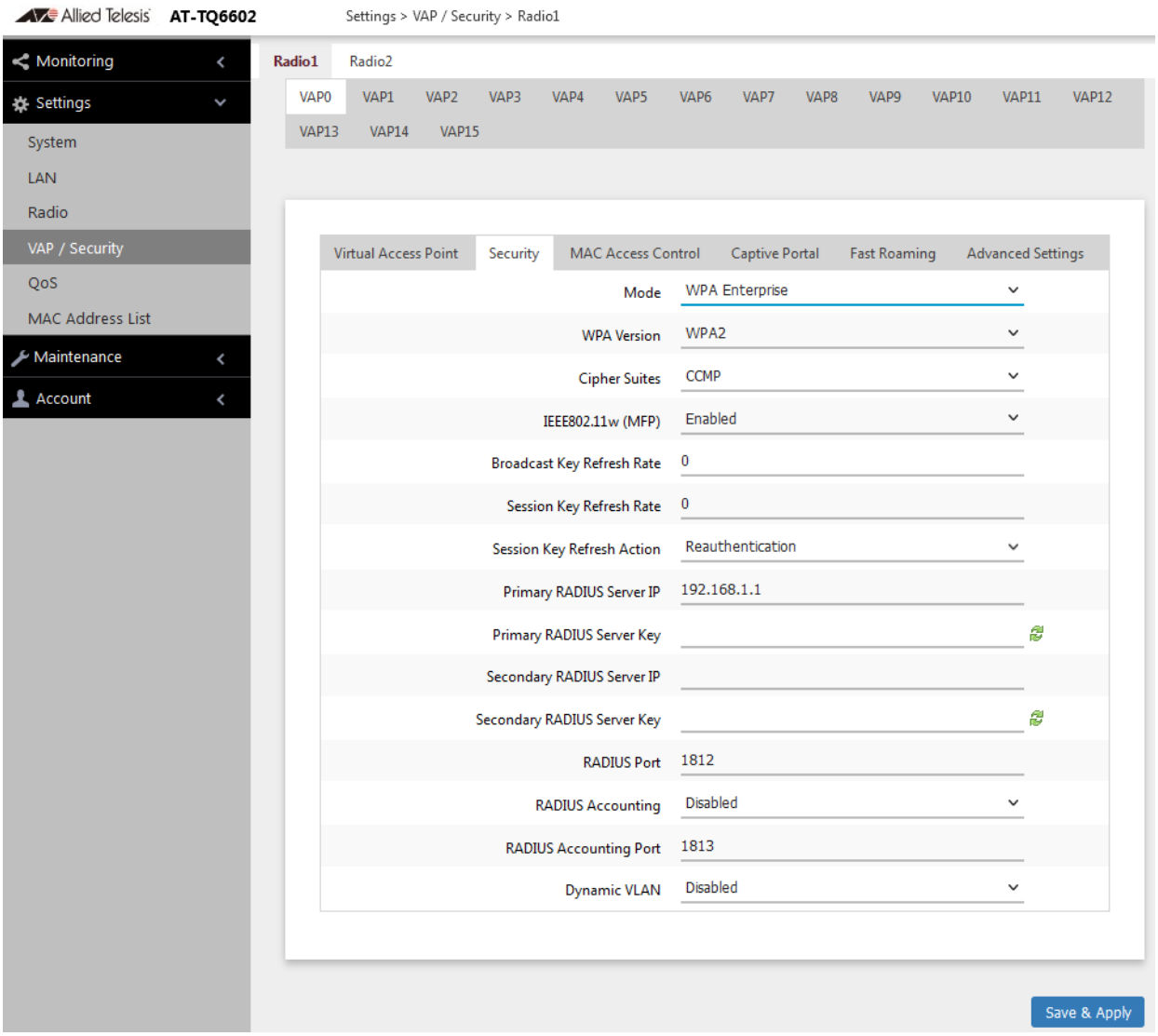


Figure 21. WPA Enterprise Tab

6. Configure the parameters by referring to Table 11 on page 79.

Table 11. WPA Enterprise Tab

Field	Description
Mode	Select **WPA Enterprise**.
WPA Version	Select the WPA version for the VPA. The options are listed: - WPA and WPA2 - Select this option if the VAP has both WPA and WPA2 clients. - WPA2: Select this option if all the clients support WPA2 only. This is the default setting. - WPA3: Select this option if clients support WPA3 only. **Note** WPA3 is supported only on Radio2.
Cipher Suites	Select the cipher suite for the VAP, The options are listed here: - CCMP: This is the default. - TKIP and CCMP - GCMP **Note** When the WPA version is WPA3, GCMP is the only option. 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.

Table 11. WPA Enterprise Tab (Continued)

Field	Description
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. **Note** When the WPA version is WPA3, Enabled is the only option. - Disabled: Deactivates management frame protection.
Broadcast Key Refresh Rate	Enter the interval for updating the key of the broadcast frame to be sent to the wireless clients connected to the VAP. The range is 0 to 86400 seconds. The key is not updated when this parameter is set to 0 (zero). The default is 0.
Session Key Refresh Rate	Enter the interval for refreshing unicast session key to be sent to the wireless clients connected to the VAP. The range is 0 to 86400 seconds. The key is not updated when this parameter is set to 0 (zero). The default is 0.
Session Key Refresh Action	Select an action that the access point takes when a session is expired. The options are: - Reauthentication: Wireless clients are re-authenticated. This is the default setting. - Disconnection: Wireless clients are disconnected.
Primary RADIUS Server IP	Enter the IPv4 address of the primary RADIUS server. The default is 192.168.1.1.
Primary RADIUS Server Key	Enter the shared secret key for the primary RADIUS server. Here are the guidelines: - The key can be up to 128 alphanumeric characters. - It is case-sensitive. - It must be same on the access point and server. - The default is no key.

Table 11. WPA Enterprise Tab (Continued)

Field	Description
Secondary RADIUS Server IP	Enter the IPv4 address of a secondary RADIUS server. This field is optional. The access point sends authentication requests to this address if the primary RADIUS server does not respond to requests.
Secondary RADIUS Server Key	Enter the shared secret key for the secondary RADIUS server.
RADIUS Port	Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must be using the same port number. The range is 0 to 65535. The default is 1812.
RADIUS Accounting	Control RADIUS accounting, When accounting is enabled, the access point sends client information, such as usage time, to the RADIUS server. The options are listed here: - Enabled: Activate RADIUS accounting. - Disabled: Deactivate RADIUS accounting. This is the default setting.
RADUIS Accounting Port	Enter the RADIUS accounting port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must use the same accounting port number. The range is 0 to 65535. The default is 1813.
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. Select another VAP to configure from the sub-menu and repeat Step 4 to Step 6 if necessary.

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

Configuring MAC Access Control Settings

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

You have the following options for MAC Access Control:

- "Disabling MAC Access Control" on page 82
- "Authenticating Using RADIUS" on page 83
- "Authenticating Using MAC Address List" on page 86

Disabling MAC Access Control

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

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

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

4. Select the **MAC Access Control** tab. See Figure 22.

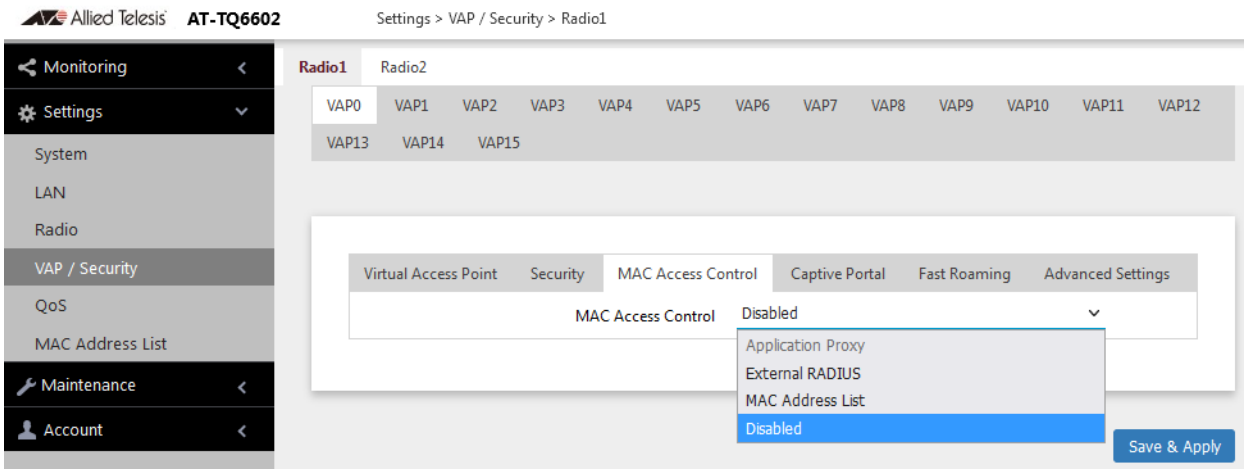


Figure 22. MAC Access Control Tab

5. Select **Disabled** from the MAC Access Control pull-down menu. See Figure 22 on page 82. This is the default setting.

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

Authenticating Using RADIUS

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

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

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

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

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

4. Select the **MAC Access Control** tab. See Figure 22 on page 82.

5. Select **External RADIUS** from the MAC Access Control pull-down menu. See Figure 23 on page 84.

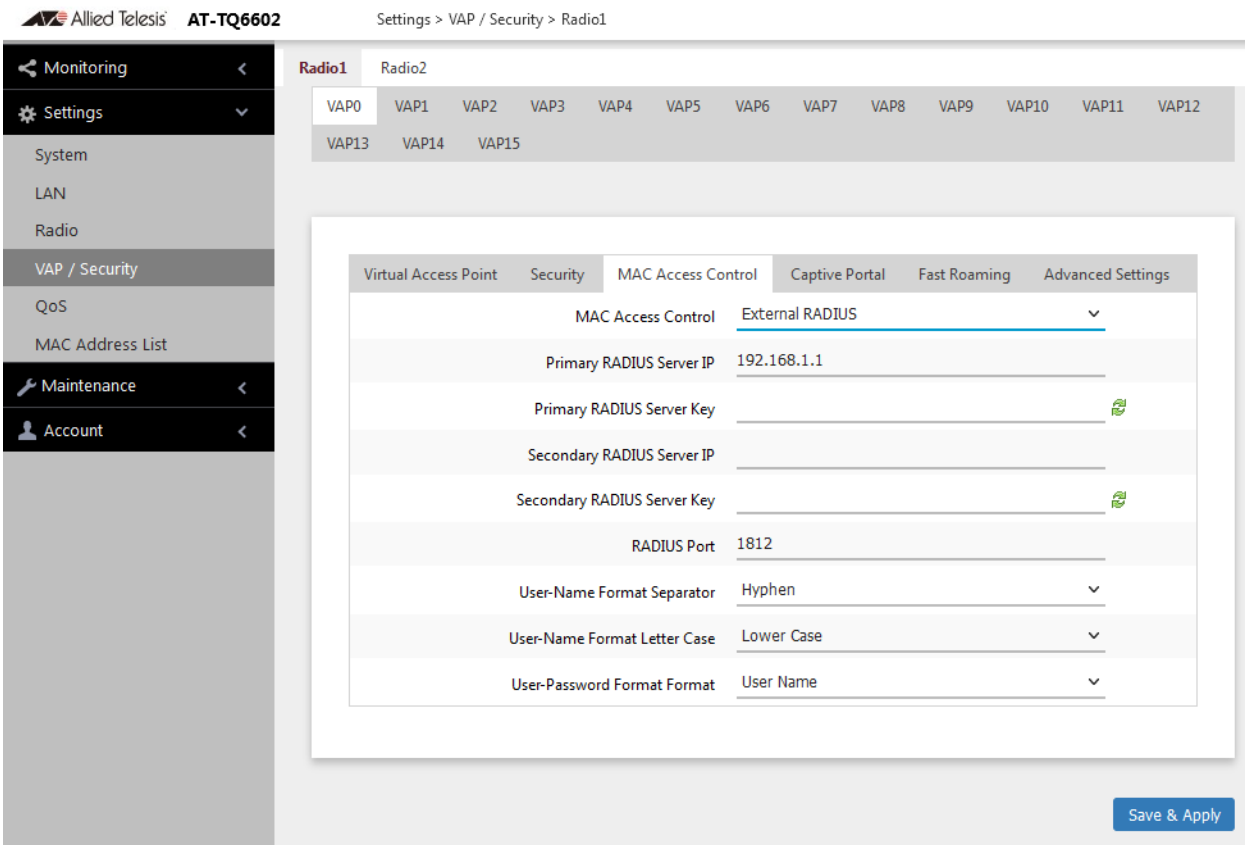


Figure 23. MAC Access Control - External RADIUS Window

6. Configure the parameters by referring to Table 12.

Table 12. External RADIUS Window

Field	Description
MAC Access Control	The options are: - Application Proxy: You need to configure Application Proxy via Vista Manager EX and AWC Plug-in. - External RADIUS: Use a MAC address list form a RADIUS server - MAC Address List: Use a MAC address list stored in the access point. - Disabled
Primary RADIUS Server IP	Enter the IPv4 address of the primary RADIUS server. The default is 192.168.1.1.

Table 12. External RADIUS Window (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.
User-Name Format Separator	Select the character that the access point should use to separate the octets in the MAC addresses it sends to the servers. (The MAC addresses function as the user-name attributes for the wireless clients.) The choices are listed here: - Hyphen (nn-nn-nn-nn-nn-nn) - Colon (nn:nn:nn:nn:nn:nn) - None (nnnnnnnnnnnn)
User-Name Format Letter Case	Specify whether the access point should send the MAC addresses using uppercase or lowercase characters. The options are listed here: - Upper Case: The wireless access point sends the MAC addresses in uppercase characters. - Lower Case: The wireless access point sends the MAC addresses in lowercase characters.

Table 12. External RADIUS Window (Continued)

Field	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 t

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

Authenticating Using MAC Address List

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

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

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

4. Select the **MAC Access Control** tab. See Figure 22 on page 82.
5. Select **MAC Address List** from the MAC Access Control pull-down menu. See Figure 24 on page 87.

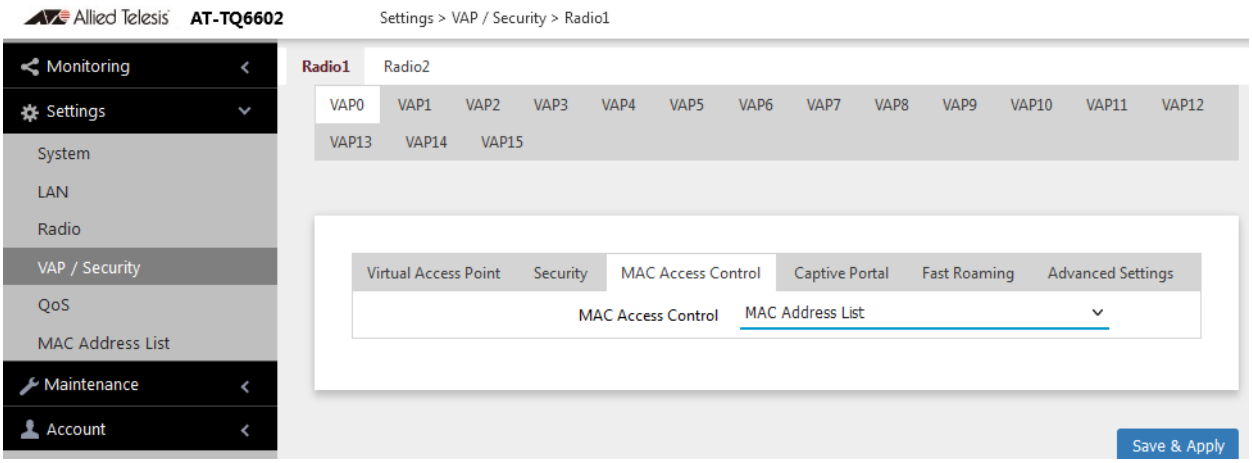


Figure 24. MAC Access Control - MAC Address List Window

Note
You must prepare a MAC address list. See “Configuring the MAC Address List” on page 110.

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

Configuring Captive Portal

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

Captive Portal Options

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

- "No Captive Portal" on page 89

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

- "No Authentication and Web Page Stored in the Access Point" on page 90

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

- "Delegating a Proxy Sever to Interact with Wireless Clients" on page 93

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

- "RADIUS Server for Authentication and External URL for Web Hosting" on page 94

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

- "RADIUS Server for Authentication and Proxy Server for Web Hosting" on page 97

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

- "RADIUS for Authentication and No Proxy Server" on page 99

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

Port Numbers

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

- 8080 for HTTP

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

- 8443 for HTTPS

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

No Captive Portal

To disable Captive Portal, perform the following procedure:

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

   The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

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

4. Select the **Captive Portal** tab. See Figure 25.

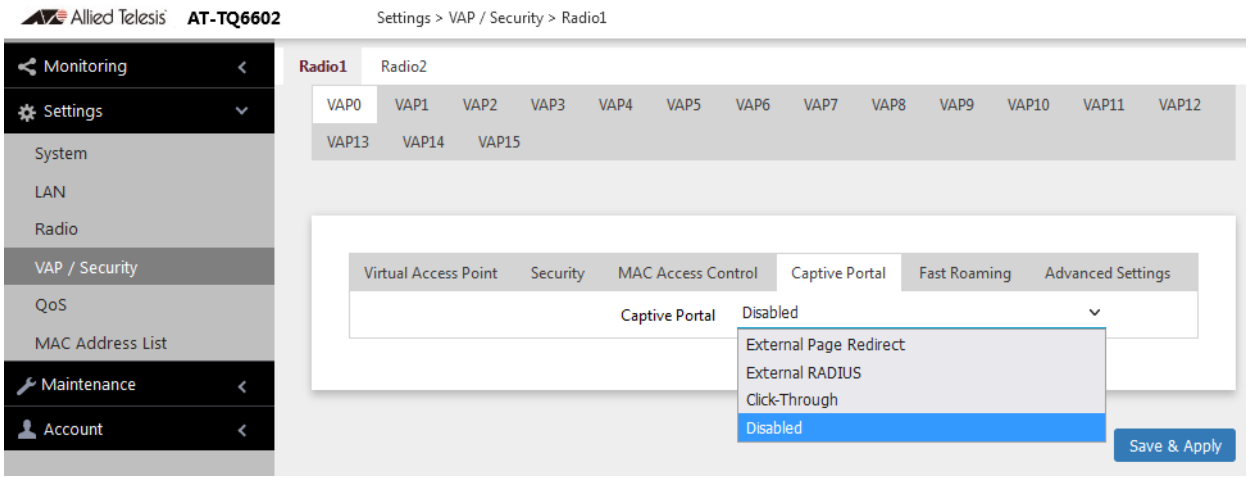


Figure 25. Captive Portal Window

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

   Disabled is the default setting.

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

No Authentication and Web Page Stored in the Access Point

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

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

   The default is Radio1. You can configure only one radio at a time.

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

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

4. Select the **Captive Portal** tab.
5. Select **Click-Through** from the Captive Portal pull-down menu. See Figure 25 on page 89.
6. Select **Disabled** from the Authentication Page Proxy pull-down menu. See Figure 26 on page 91.

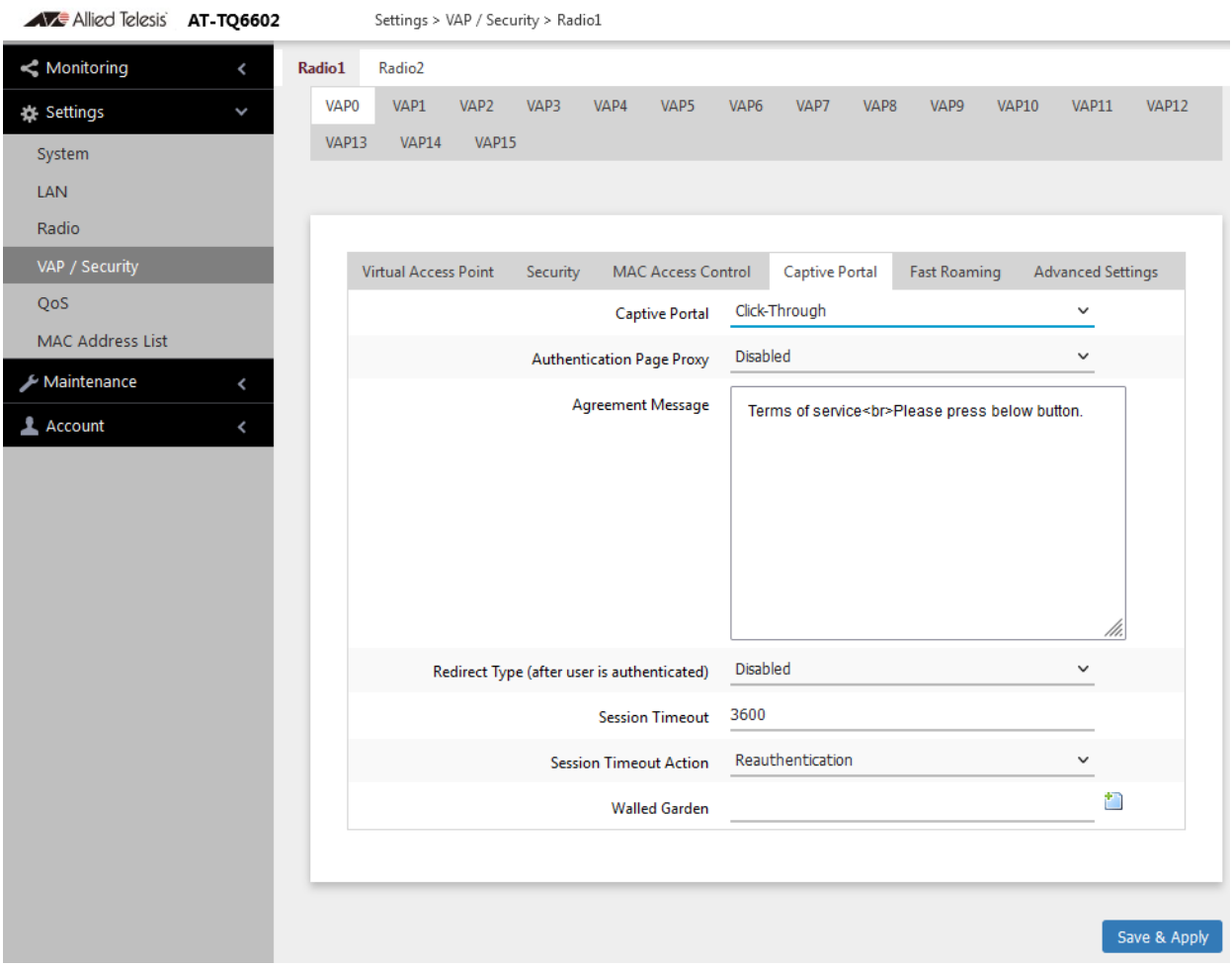


Figure 26. Captive Portal Window - Click-Through

7. Configure the parameters described in Table 13.

Table 13. Captive Portal - Click-Through

Field	Description
Authentication Page Proxy	Enable or disable Authentication Page Proxy on the Captive Portal: - Enabled: The access point uses other web server's authentication page via proxy with Captive Portal. - Disabled: The access point uses its own local authentication page with Captive Portal. This is the default setting.

Table 13. Captive Portal - Click-Through (Continued)

Field	Description
Agreement Message	Enter Conditions of Use or other information to display the introductory web page. The text can include HTML formatting and display codes.
Redirect Type (after user is authenticated)	Select the action to occur after the clients click the Agree button. The options are listed here: - Fixed URL: Directs clients to a specified web page. Selecting this option displays the Fixed URL field. - Session Keep: Directs clients to the web page they requested prior to the click-through window. - - Disabled: Disables redirect. The welcome.html file that you prepared is displayed. When the Captive Portal field is Click-Through and the Authentication Proxy Page is Disabled, the welcome page on the access point is displayed. This is the default setting.
Session Timeout	Enter time in seconds to allow wireless clients to connect to the access point. The maximum duration is 86400 seconds.
Session Timeout Action	Select an action when the session is timeout. The options are: - Re-authentication - Re-authenticates wireless clients. - Disconnection: Disconnect wireless clients.
Walled Garden	Enter the URLs of up to fifty approved HTTP web sites that wireless clients can access through the captive portals on the access point, without having to log on. Wireless clients who access only approved sites are not authenticated. Those who try to access unapproved web sites are shown to a logon window. The feature is supported on all radios, VAPs, and captive portals. To add the first HTTP web site, enter it in the empty field. You can identify a site by its fully qualified domain name (FQDN), IPv4 address, or IPv4 address and mask (e.g 32.134.45.0/24). When using FQDN, do not include "HTTP://". To add more URL addresses, click the green add icon to the right of the last URL field. You can enter up to fifty sites.

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

Delegating a Proxy Sever to Interact with Wireless Clients

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

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

   The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

   Note
   You can configure multiple VAPs without saving each VAP configuration page. You can save multiple VAP configurations all at once by clicking the **SAVE & APPLY** button.
4. Select the **Captive Portal** tab.
5. Select **Click-Through** from the Captive Portal pull-down menu.
6. Select **Enabled** from the Authentication Page Proxy pull-down menu. See Figure 27 on page 94.

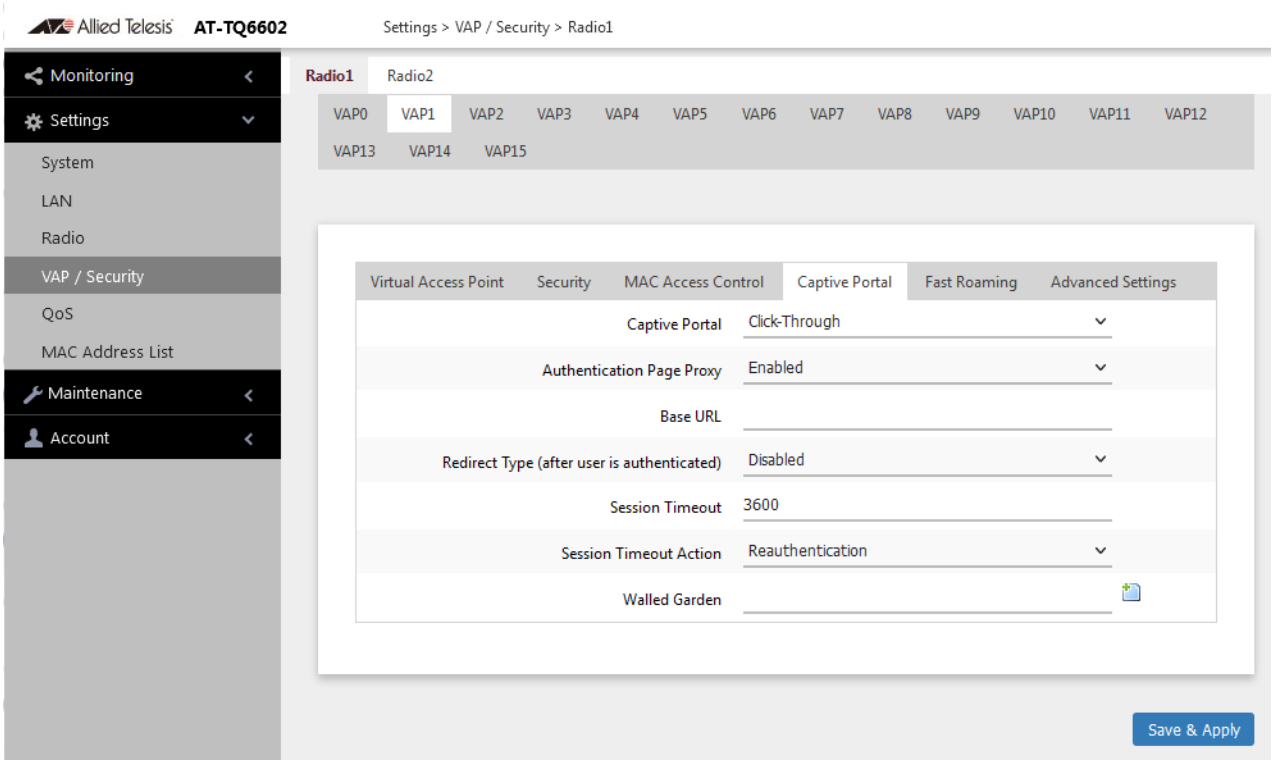


Figure 27. Captive Portal - Click-Through and Authentication Page Proxy

7. Specify the URL of your Page Proxy Server in the Base URL field.
8. Configure the rest of parameters by referring Table 13 on page 91.
9. Click the **SAVE & APPLY** button to save and update the configuration, or configure other VAPs and save the configurations at once later.
10. Go to "Creating Pages in HTML for a Proxy Server" on page 101.

RADIUS Server for Authentication and External URL for Web Hosting

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

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

   The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

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

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

5. Select **External Page Redirect** from the Captive Portal pull-down menu. See Figure 28.

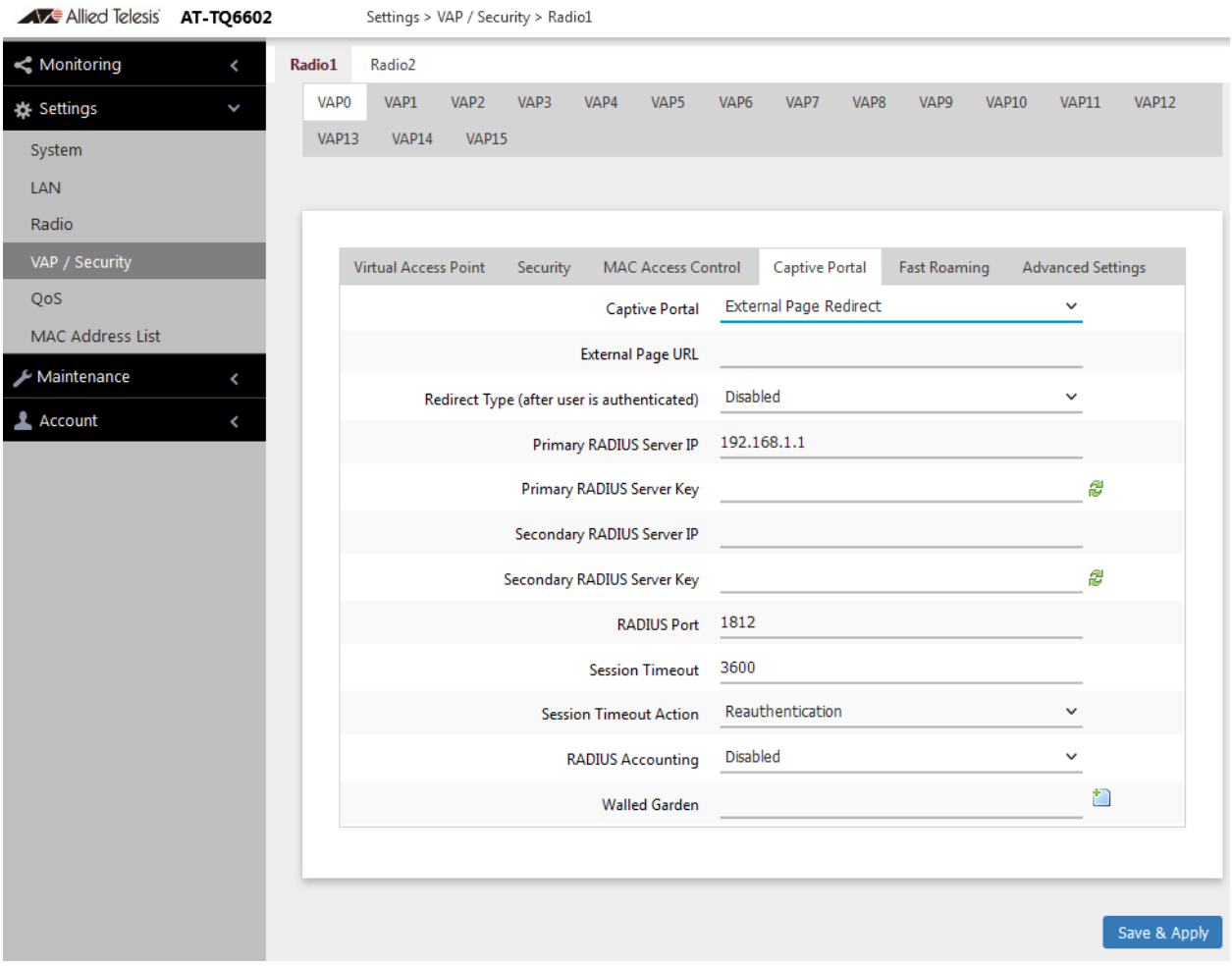


Figure 28. Captive Portal - External Page Redirect Window

6. Configure the parameters described in Table 14 on page 96.

Table 14. Captive Portal - External Page Redirect

Field	Description
External Page URL	Enable or disable Authentication Page Proxy on the Captive Portal: - Enabled: The access point uses other web server's authentication page via proxy with Captive Portal. - Disabled: The access point uses its own local authentication page with Captive Portal. This is the default setting.
Redirect Type (after user is authenticated)	See Table 13 on page 91.
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.a

Table 14. Captive Portal - External Page Redirect (Continued)

Field	Description
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.
Walled Garden	See Table 13 on page 91.

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

RADIUS Server for Authentication and Proxy Server for Web Hosting

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

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

   The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0.

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

4. Select the **Captive Portal** tab.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 29 on page 98.
6. Select **Enabled** from the Authentication Page Proxy pull-down menu. See Figure 29 on page 98.

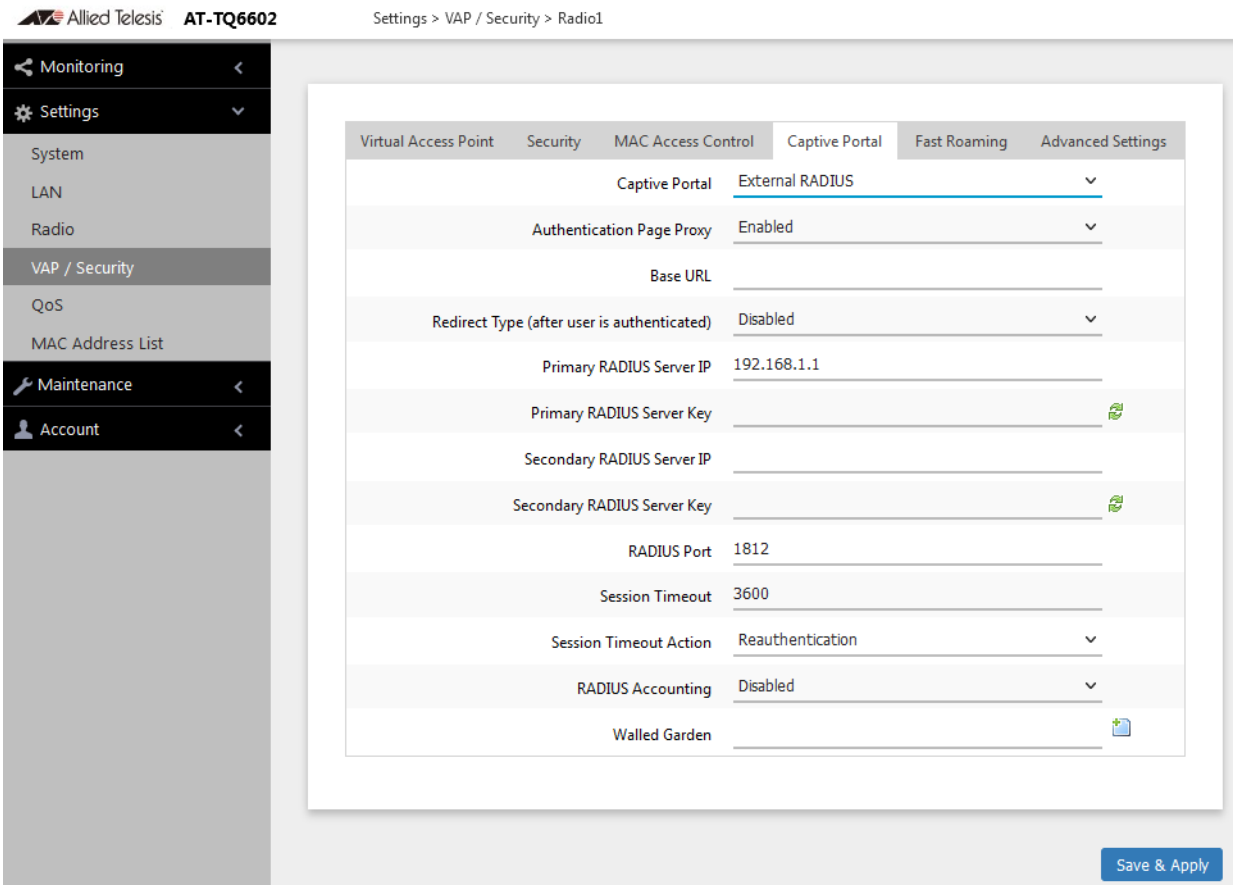


Figure 29. Captive Portal - RADIUS and Authentication Page Proxy

7. Configure the parameters described in Table 15.

Table 15. Captive Portal - RADIUS and Authentication Proxy

Field	Description
Base URL	Specify the URL of the Authentication Page Proxy.
Redirect Type (after user is authenticated)	See Table 13 on page 91.
Primary RADIUS Server IP	Table 14 on page 96.
Primary RADIUS Server Key	Table 14 on page 96.
Secondary RADIUS Server IP	Table 14 on page 96.

Table 15. Captive Portal - RADIUS and Authentication Proxy (Continued)

Field	Description
Secondary RADIUS Server Key	Table 14 on page 96.
RADIUS Port	Table 14 on page 96.
Session Timer	See Table 13 on page 91.
Session Timeout Action	See Table 13 on page 91.
RADIUS Accounting	Table 14 on page 96.
Walled Garden	See Table 13 on page 91.

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

9. Go to “Creating Pages in HTML for a Proxy Server” on page 101.

RADIUS for Authentication and No Proxy Server

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

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

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

   The default is Radio1. You can configure only one radio at a time.

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

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

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

5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 29 on page 98.

6. Select **Disabled** from the Authentication Page Proxy pull-down menu. See Figure 30 on page 100.

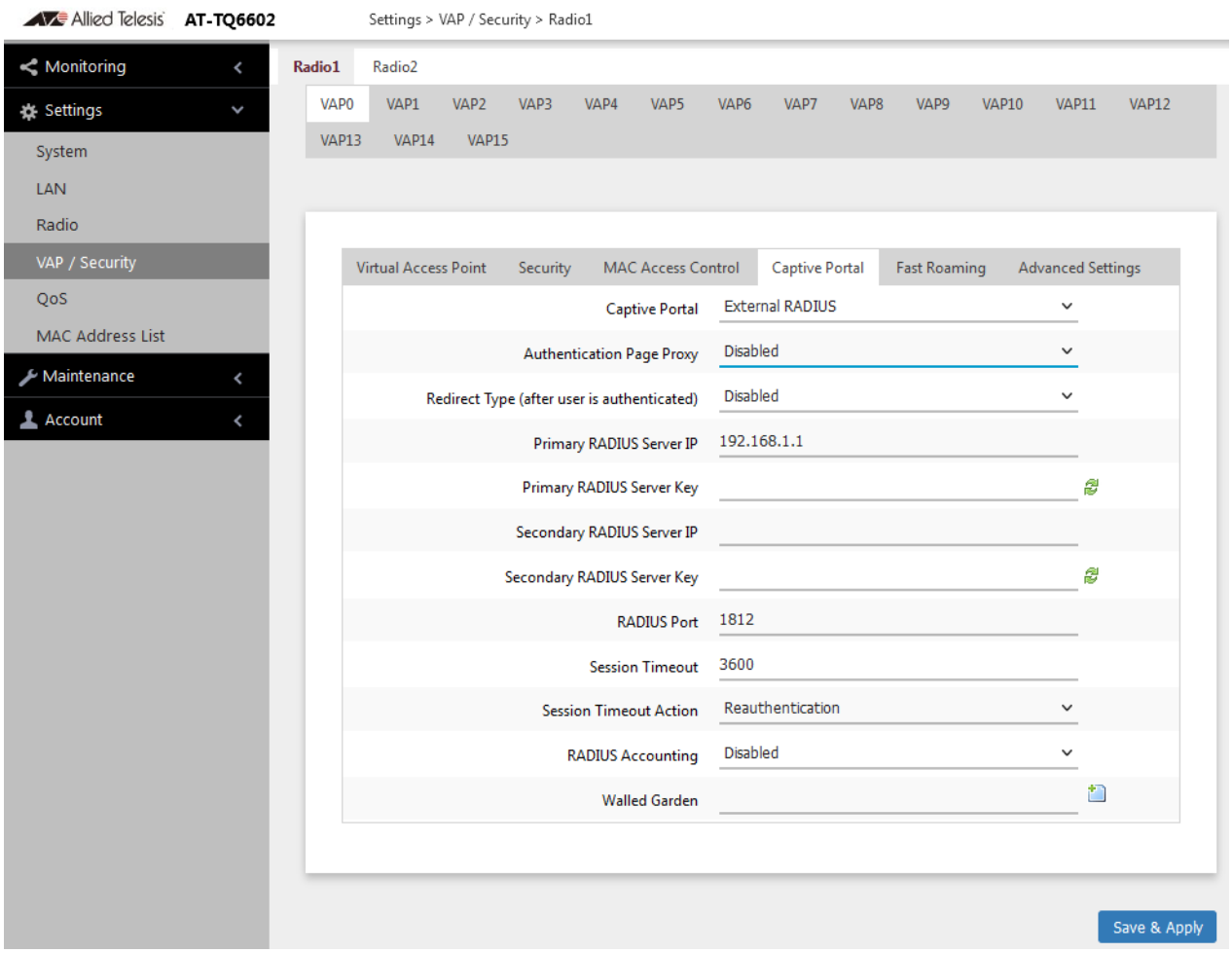


Figure 30. Captive Portal - RADIUS and No Proxy Window

7. Configure the parameters described in Table 16.

Table 16. Captive Portal - RADIUS and No Proxy

Field	Description
Redirect Type (after user is authenticated)	See Table 13 on page 91.
Primary RADIUS Server IP	Table 14 on page 96.
Primary RADIUS Server Key	Table 14 on page 96.
Secondary RADIUS Server IP	Table 14 on page 96.

Table 16. Captive Portal - RADIUS and No Proxy (Continued)

Field	Description
Secondary RADIUS Server Key	Table 14 on page 96.
RADIUS Port	Table 14 on page 96.
Session Timer	See Table 13 on page 91.
Session Timeout Action	See Table 13 on page 91.
RADIUS Accounting	Table 14 on page 96.
Walled Garden	See Table 13 on page 91.

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

9. “Creating Login Pages in HTML When External RADIUS is Selected” on page 102.

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 31 shows its web page displayed in a web browser.

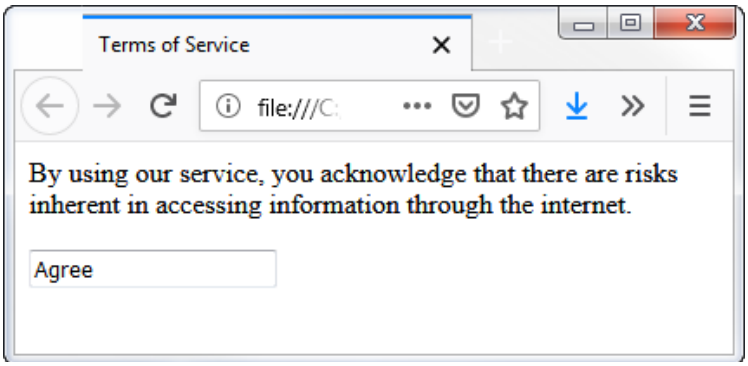


Figure 31. Captive Portal - Terms of Service Page Sample

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 31 shows its web page displayed in a web browser.

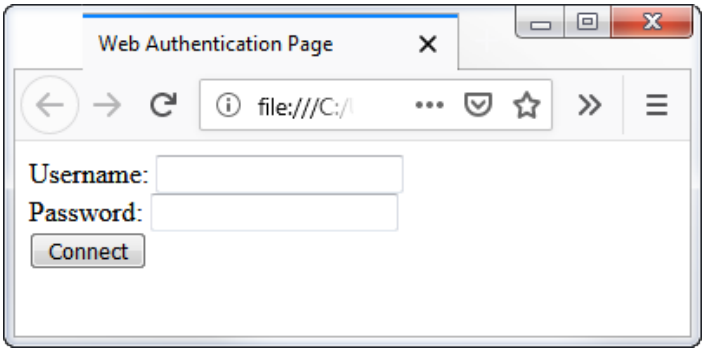


Figure 32. Captive Portal - Login Page Sample

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.
- You can view but not configure the IEEE 802.11r settings with the web browser management interface. Configuring the settings requires AWC and Vista Manager EX.
- IEEE802.11r, configured by AWC and Vista manger EX, applies to VAPs with WPA Enterprise security only.
- IEEEE802.11r does not apply to VAPs with the WPA version setting including WPA3.

To configure Fast Roaming, perform the following procedure:

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

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

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. See Figure 33 on page 105.

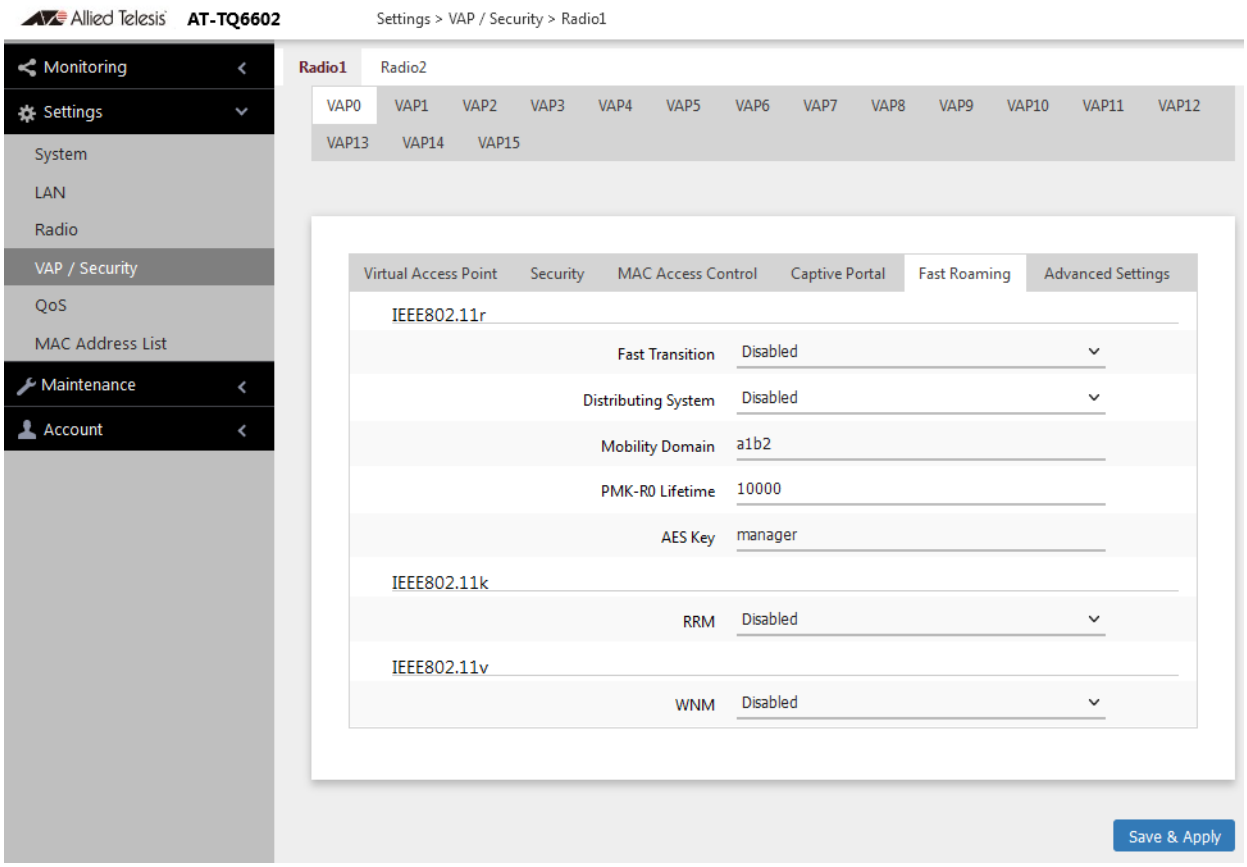


Figure 33. Fast Roaming Window

5. Configure the parameters by referring to Table 17.

Table 17. Fast Roaming Tab

Field	Description
IEEE802.11r	
Fast Transition	Select one of the following: - Enabled: When a wireless client is roaming, pre-authentication to a new access point is done before the wireless client switches to the new access point. - Disabled: Fast Transition is disabled.

Table 17. Fast Roaming Tab (Continued)

Field	Description
Distributing System	Select one of the following: - Enabled: Pre-authentication to a new access point that a wireless client acquires is done through the current access point. - Disabled: Pre-authentication to a new access point that a wireless client acquires is done through the new access point.
Mobility Domain	Specify a mobility domain ID. The mobility domain is a scope of the network in which Fast Transition is supported in a group of access points, which share pre-authentication keys. Mobility Domain is up to four alphanumeric characters.
PMK-R0 Lifetime	Specify the interval in minutes before PMK-R0 is refreshed. The range is 1 to 65535.
AES Key	Specify a key to generate RMK-R0. When this field is empty, RMK-R0 is generated based on MSK or WPA security key depending upon the security setting.
IEEE802.11k RRM	Select one of the following: - Enabled: IEEE802.11k Radio Resource Measurement (RRM) is enabled. - Disabled: IEEE802.11k Radio Resource Measurement (RRM) is disabled. This is the default setting.
IEEE802.11v WNM	Select one of the following: - Enabled: IEEE802.11v Wireless Network Management (WNM) is enabled. - Disabled: IEEE802.11v Wireless Network Management (WNM) is disabled. This is the default setting.

6. Select another VAP to configure from the sub-menu and repeat Step 4 to Step 5 if necessary.

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

Configuring Advanced VAP Settings

To configure advanced VAP settings, perform the following procedure:

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default iVAP0.

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

4. Select the **Advanced** tab. See Figure 34.

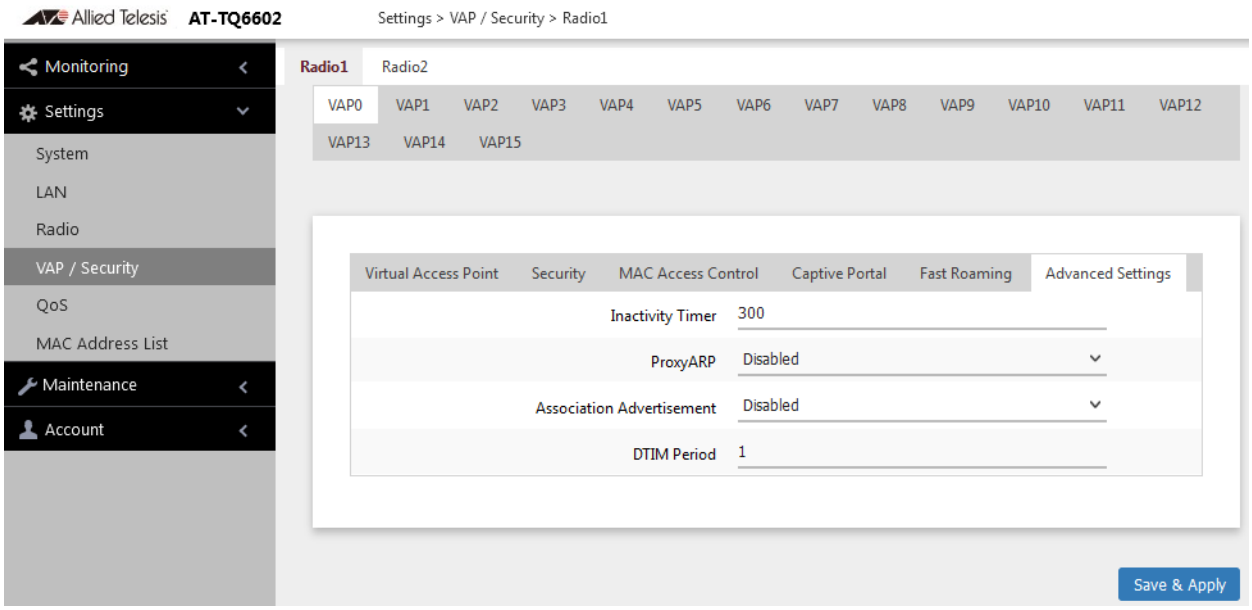


Figure 34. Advanced VAP Settings Window

5. Configure the parameters by referring to Table 18 on page 108.

Table 18. 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 guidelines: - The default is 300 seconds. - The range is from 60 to 65535 seconds.
Proxy ARP	Proxy ARP allows the access point to respond to Address Resolution Protocol (ARP) queries for the target IP address that is not on that network. **Note** Proxy ARP is controlled from Vista Manager EX. The options are: - Enabled: Proxy ARP is enabled. - Disabled: Proxy ARP is disabled. This is the default setting.
Association Advertisement	Specifies 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 other access points to which the clients were previously connected of the change. This advertisement enables access points to update their lists of associated clients more quickly. **Note** Association Advertisement is controlled from Vista Manager EX. The options are: - 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.

Table 18. Advanced Settings Tab (Continued)

Field	Description
DIMP Period	Specifies the Delivery Traffic Indication Maps (DTIMs) period. Access points broadcast a beacon at regular intervals, which includes Delivery Traffic Indication Maps (DTIMs). The DIMP period specifies the number of beacons that an access point transmits before transmitting any buffered broadcast or multicast frames. It allows you to manage power-saving wireless clients to wake up at the appropriate time if they are expecting broadcast or multicast data. Typically, the DTIM value is set to 1. With this setting, the access point transmits broadcast and multicast frames after every beacon. When the DTIM period is 2, the access point transmits broadcast and multicast frames after every other beacon frame. The range is from 1 to 5. The default is 1.

6. Select another VAP to configure from the next sub-menu and repeat Step 4 to Step 5 if necessary.

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

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 69.

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

1. Select **Settings** > **MAC Address List**. Refer to Figure 35.

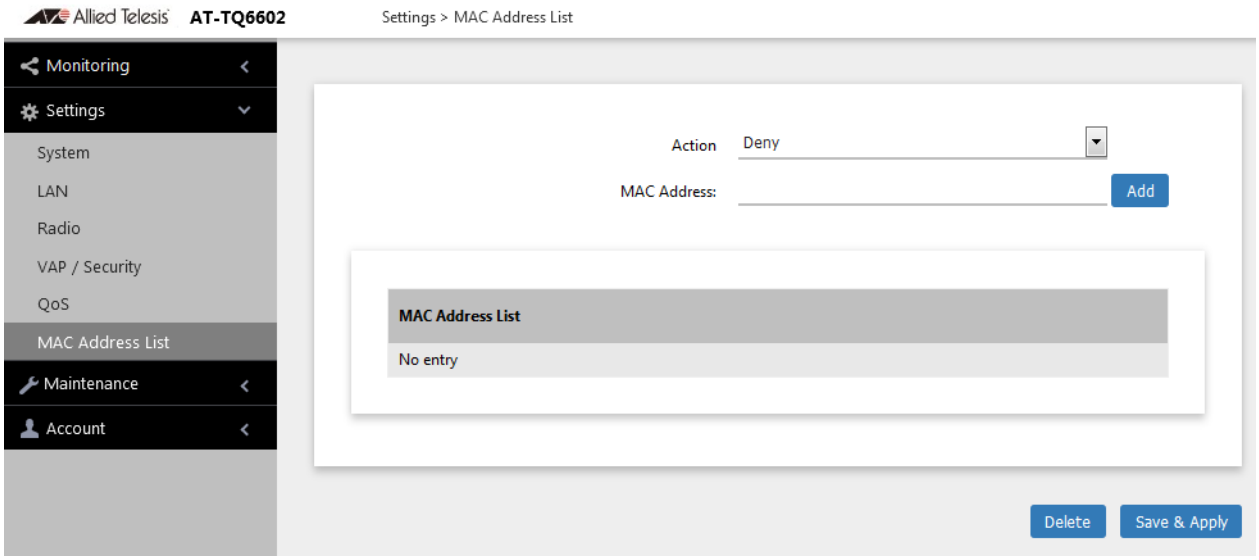


Figure 35. MAC Address List Window

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 Port Statistics

To view VAP and LAN port status and statistics, select **Monitoring** > **Statistics** window. Refer to Figure 36.

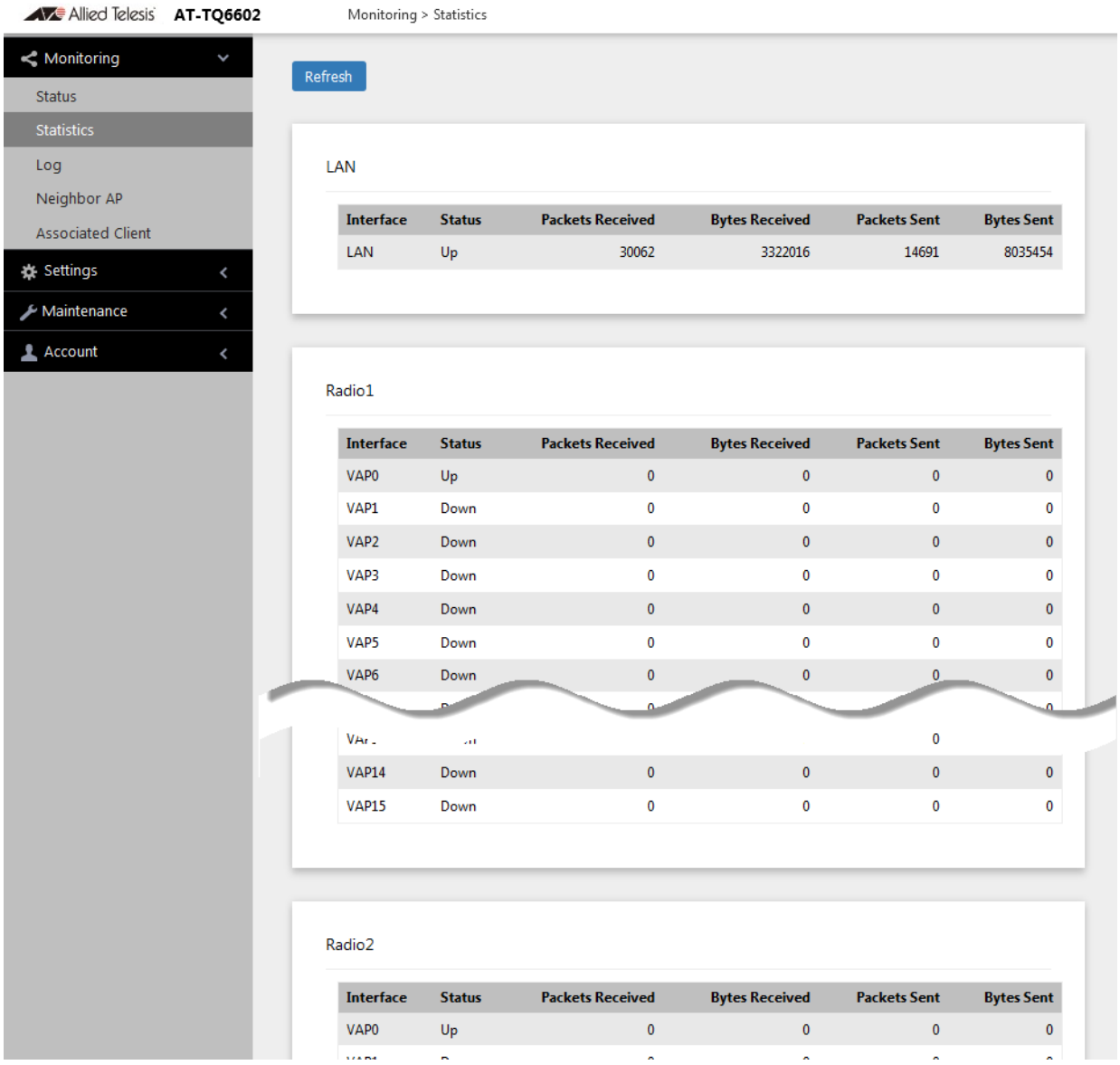


Figure 36. Statistics Window

The columns are defined in Table 19 on page 113.

Table 19. Statistics Window

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

Chapter 5

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 37.

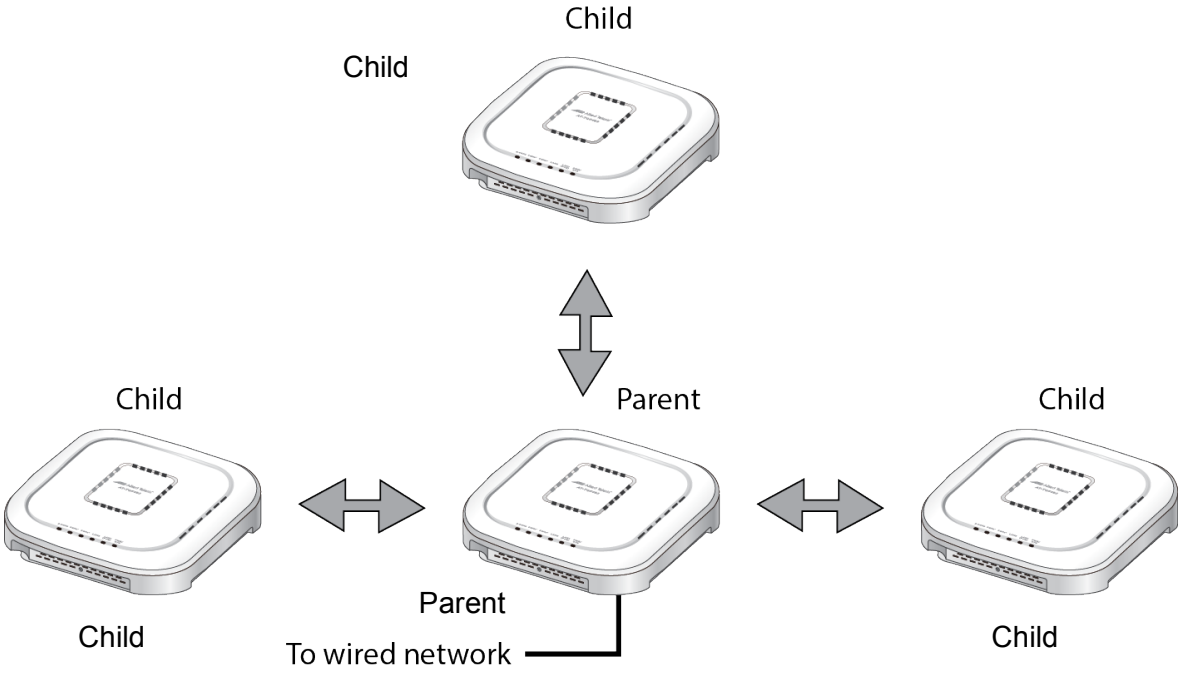


Figure 37. WDS Bridge

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

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

Additionally, because the access points have to use the same channel, you have to select the channel manually, instead of using the default auto channel setting. In the example in Figure 38, the parent and children are using Radio2 and channel 40 for the WDS bridge. Wireless clients can access the network using Radio1.

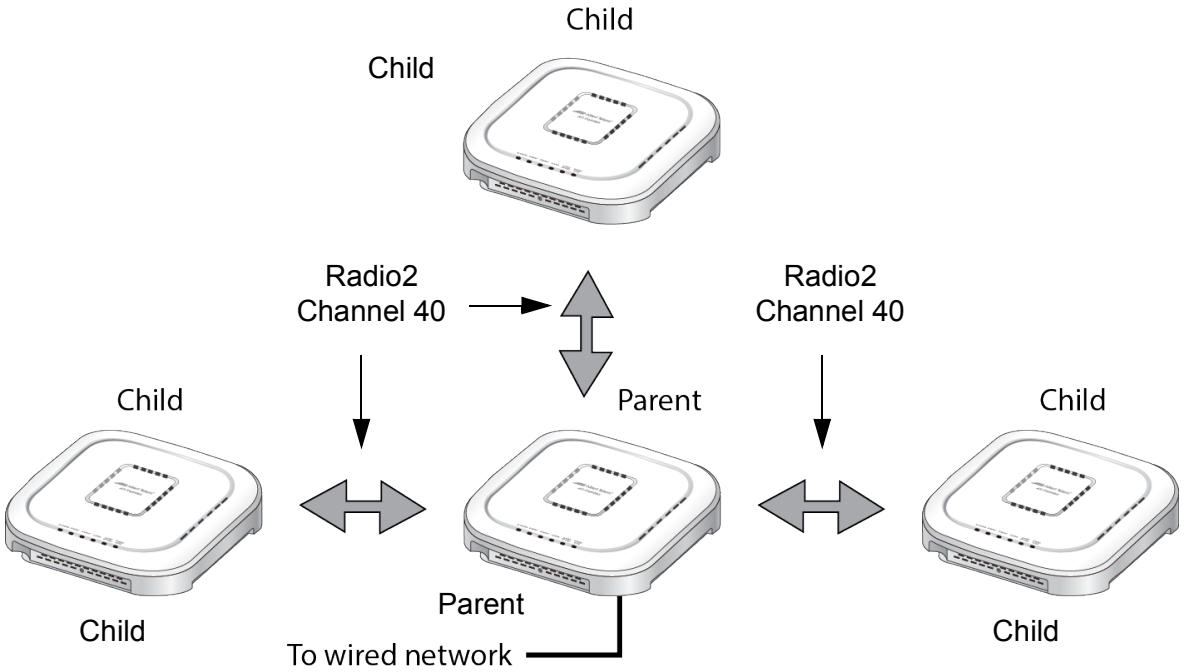


Figure 38. Example of Radio and Channel Assignments in a WDS Bridge

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 39 on page 118 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.

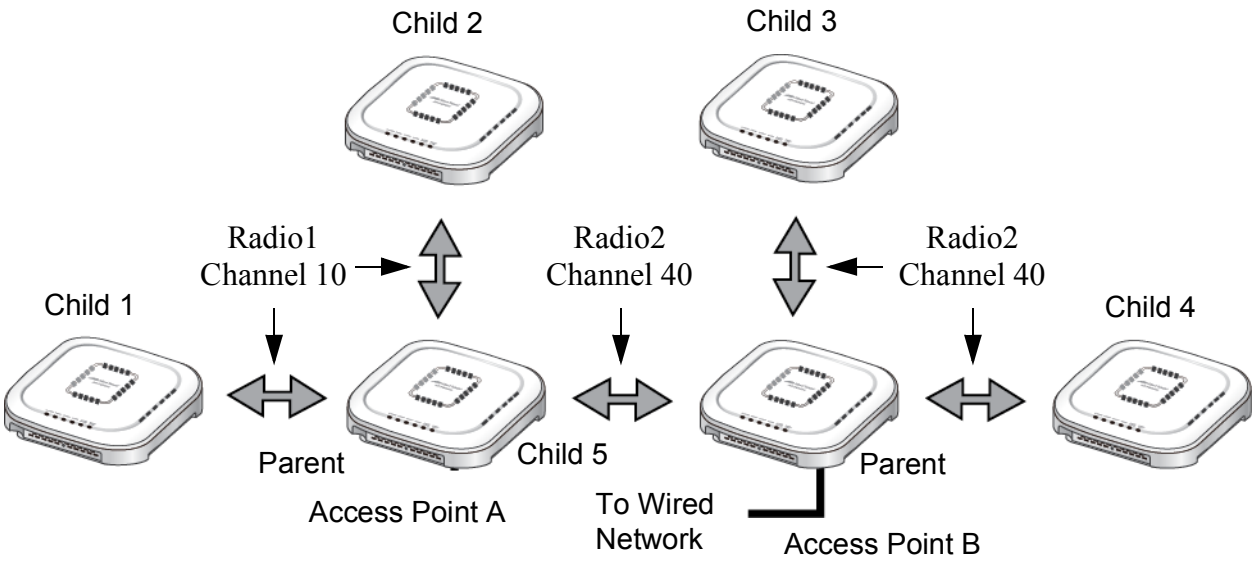


Figure 39. Example of an Access Point as Both Parent and Child

Here are important rules to observe when linking WDS bridges together as shown in Figure 39:

- 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 or Radio2 for a WDS bridge. Here are the guidelines:

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

VAP0

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

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

Radio Channel

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

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

Parents and Children

When configuring an access point for a WDS bridge, you designate it as either parent or child. The parent is usually the unit with its LAN port connected to the wired network. Children are units that access the wired network through the parent. A WDS bridge can have only one parent and no more than three children. An example of a bridge of four units is shown in Figure 37 on page 116.

Security

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

- No encryption
- WPA Personal

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

Dynamic Frequency Selection (DFS)

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 more information, see "Dynamic Frequency Selection (DFS)" on page 65.

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 39 on page 118, you should connect the LAN ports on only one parent to the wired network. Connecting the LAN ports on both access points might form a loop in the network topology.
- The LAN ports on children should not be connected to the wired network.
- You can use Radio1 or Radio2 for the WDS bridge.
- You can use no security (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 only TQ6602 access points.
- The radios of the WDS bridge have to be set to the same mode and channel.
- You must set the channel manually. Do not use the Auto setting.
- If you use Radio2 for the bridge, Allied Telesis recommends selecting a channel that is not part of dynamic frequency selection. 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 or Radio2.
- ❒ You have chosen the radio mode and channel that all the access points will use for the bridges.
- ❒ You have chosen the security level for VAP0 of the selected radio for the bridges. The security level can be none or WPA Personal. Allied Telesis recommends using WPA Personal security.

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

1. Start a management session.
2. On the selected radio for the bridge, set the mode and channel. Refer to "Configuring the Radios" on page 54. 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 74.
4. Select **Settings** > **VAP / Security**.
5. Choose the radio for the WDS bridge by selecting **Radio1** or **Radio2** from the sub-menu.
6. Select **VAP0** from the sub-menu. This is the default VAP.
7. Select the **Virtual Access Point** tab. This is the default tab.
8. From the Mode pull-down menu, select either **WDS Parent** or **WDS Child**. This can only be set on VAP0.
9. Click the **SAVE & APPLY** button to save and update the configuration.

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

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

    When an access point is designated as a child, it automatically begins searching for a parent on the designated radio and channel. If it finds one, it forwards traffic from its wireless clients over the bridge to the parent, as needed, and transmits traffic from the parent to its clients. To view the children of a parent, display the Associated Clients window, as explained in “Displaying Associated Clients” on page 152.

Chapter 6

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 40.

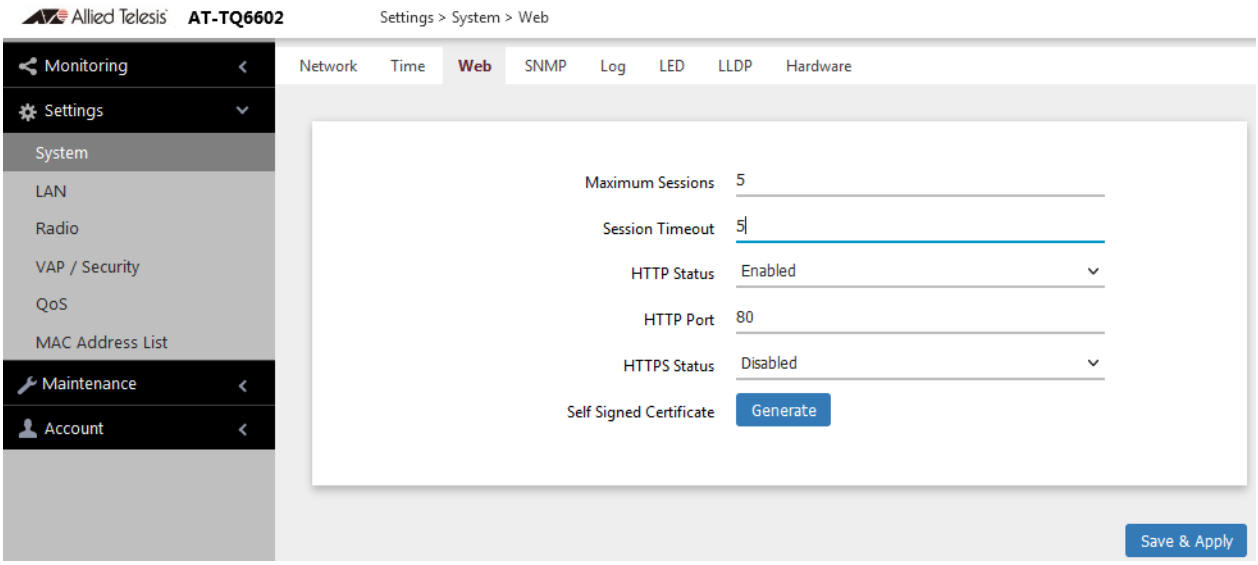


Figure 40. Web Window

3. Configure the fields by referring to Table 20.

Table 20. 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 41.

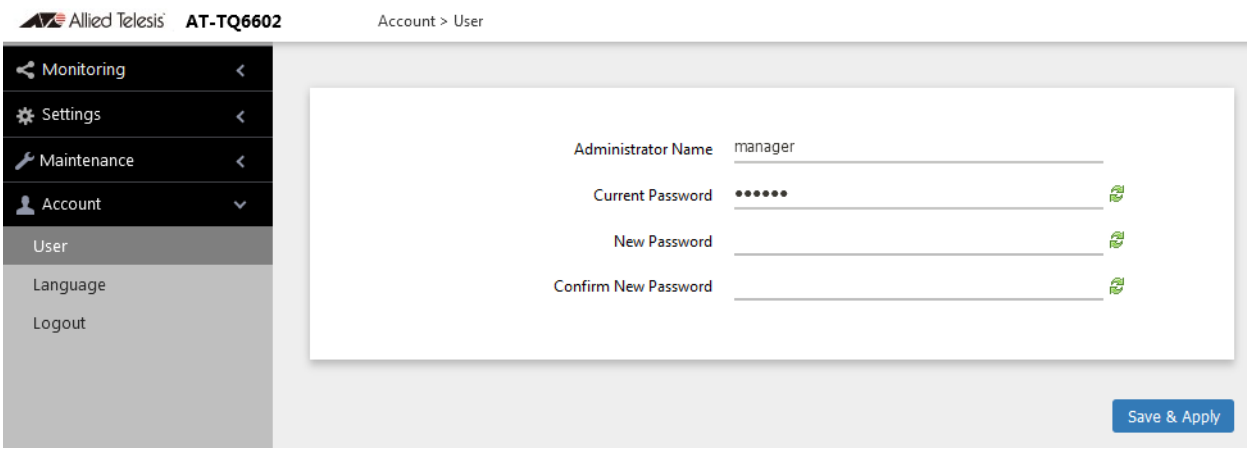


Figure 41. User Window

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

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

   - ❒ The default password: friend

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

4. Select the **New Password** field and enter a new password. 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 42.

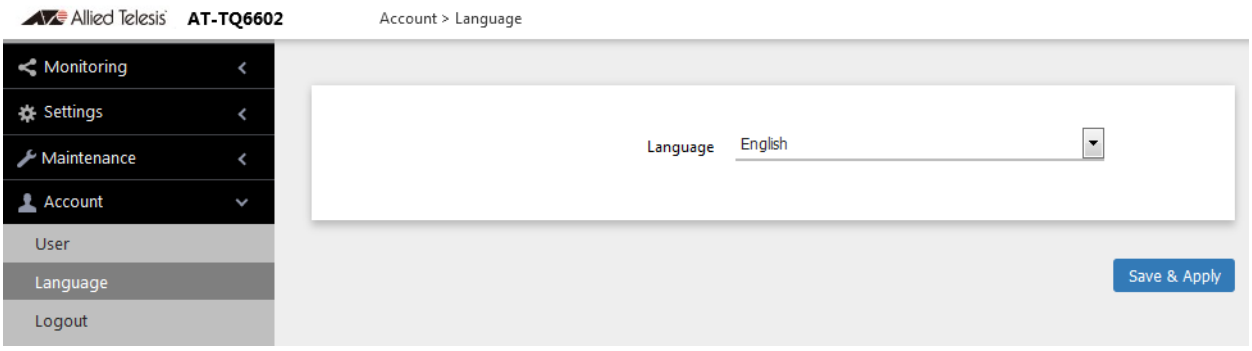


Figure 42. Language Window

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 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 **Radio**1 or **Radio2** from the sub-menu. You can configure only one radio at a time. Refer to Figure 43 on page 133.
3. Configure the QoS parameters by referring to the following sections:
   - "Configuring QoS Basic Settings" on page 134
   - "Configuring AP EDCA Parameters" on page 135
   - "Configuring Station EDCA Parameters" on page 138
4. Click the **SAVE & APPLY** button to save and update your configuration.

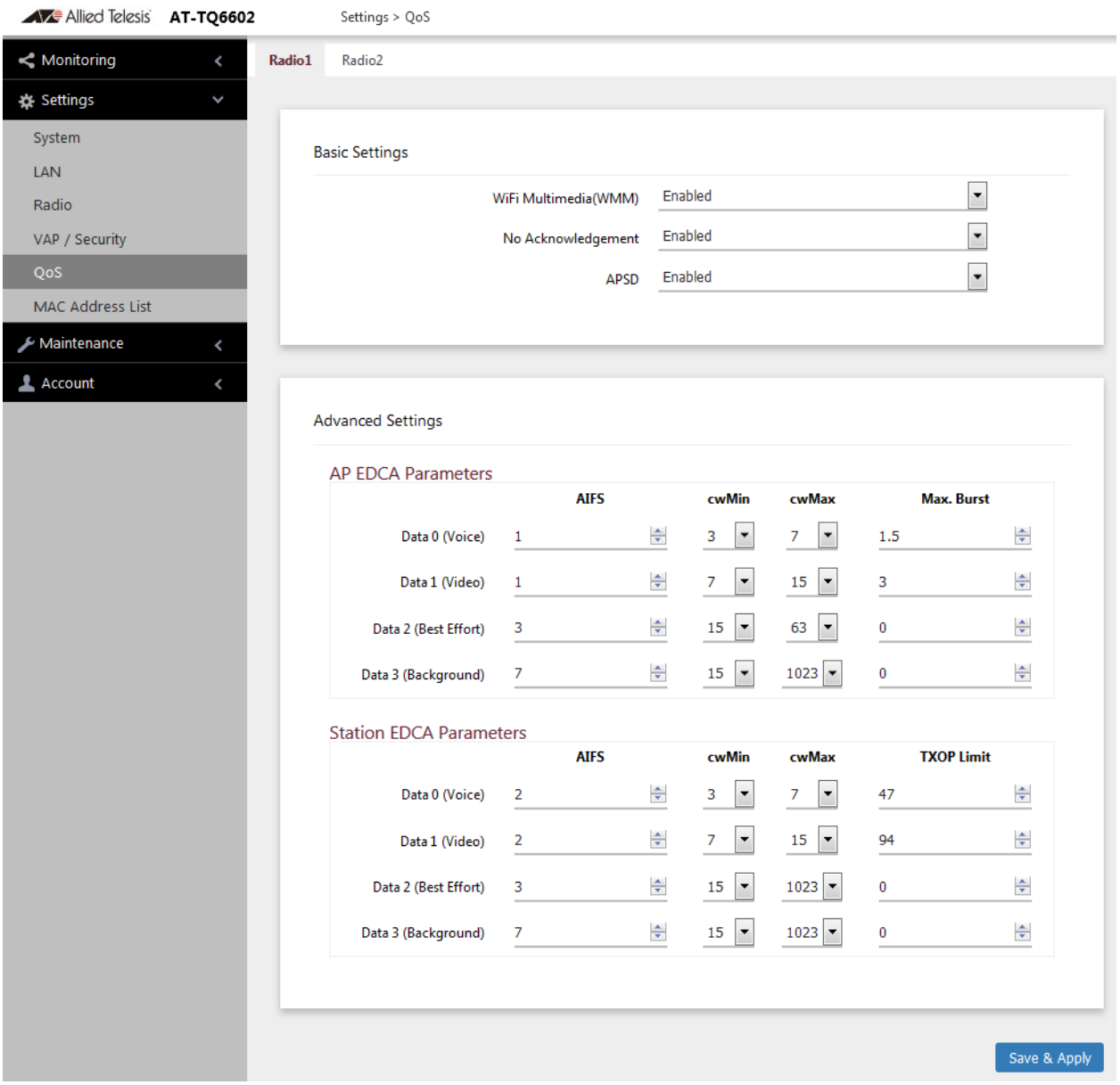


Figure 43. QoS Window

Configuring QoS Basic Settings

The fields for the Basic Settings section are defined in Table 21.

Table 21. 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 802.11ax.
No Acknowledgment	Always enabled.
APSD	Automatic Power Save Delivery (APSD) is a feature that allows mobile devices to conserve battery by letting them enter standby or sleep mode. **Note** APSD is controlled from Vista Manager EX. The options are: - Enabled: APSD allows mobile devices to save battery by providing smooth transition for mobile devices to be in and out of sleep mode with signals from mobile devices. This is the default setting. - Disabled: APSD is disabled.

Configuring AP EDCA Parameters

Table 22 defines the AP EDCA parameters in the QoS window in Figure 43 on page 133.

Table 22. 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 22. 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 22. 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 23 defines the Station EDCA parameters in the QoS window in Figure 43 on page 133.

Table 23. 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 23. 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 23. 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

LAN Port

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 manasession.

To configure the management VLAN, perform the following procedure:

1. Select **Settings** > **LAN** from the main menu. Refer to Figure 44.

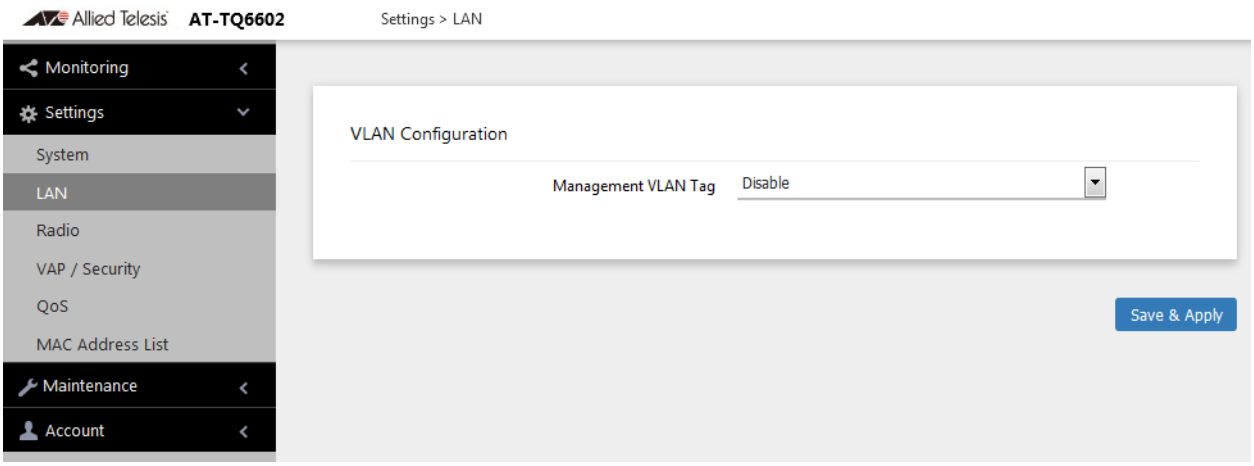


Figure 44. LAN Settings Window

When you select Enable in the Management VLAN Tag field, the window in Table 45 on page 143 appears.

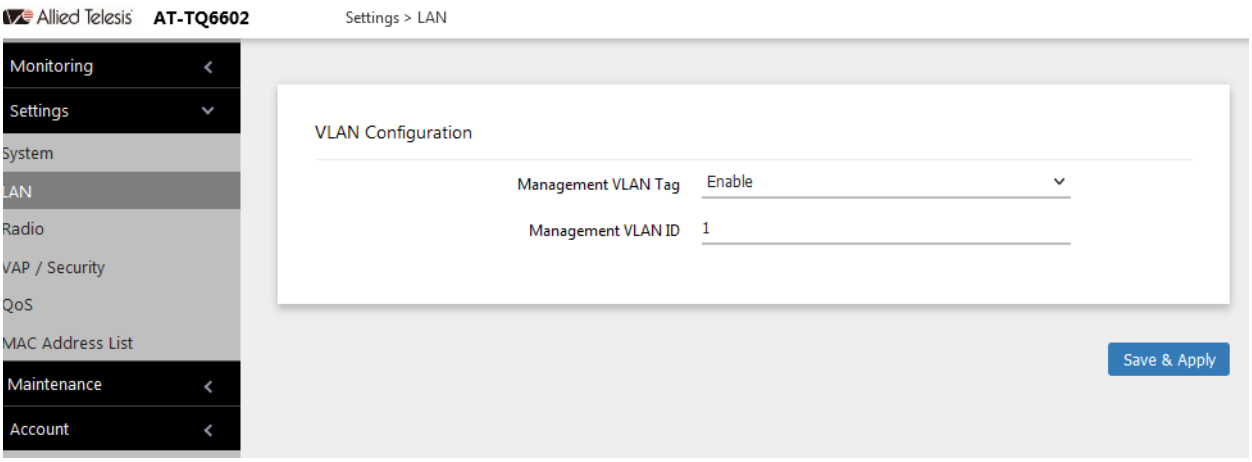


Figure 45. LAN Settings Window - Management VLAN Tag is Eanbled

2. Configure the settings by referring to Table 24.

Table 24. LAN Setting Window

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

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

Displaying the Status of LAN Port

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

1. Select **Monitoring** > **Status** from the main menu.
2. Select **LAN** from the sub-menu. See Figure 46.

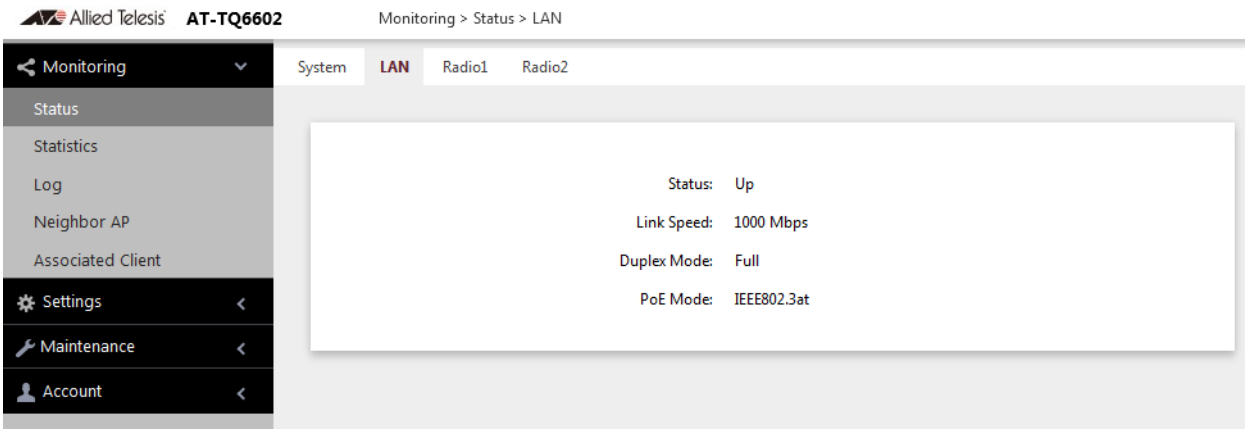


Figure 46. LAN Window

The fields are defined in Table 25.

Table 25. LAN Window

Item Name	Description
Status	Displays the status of the LAN port. The possible states are listed here: - Up: The port has established a link with a network devices, such as an Ethernet switch or router. - Down: The port has not established a link with a network device.
Link Speed	Displays the speed of the link (10Mbps, 100Mbps, 1000Mbps, 2500Mbps, 5000Mbps).
Duplex Mode	Displays the duplex mode of the port, as follows: - Full: Full-duplex. - Half: Half-duplex.

Table 25. LAN Window (Continued)

Item Name	Description
PoE Mode	Displays the PoE mode, as follows. - IEEE802.3at: The access point is powered by PoE. - None: The access point is powered by an external adapter.

Chapter 9

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 47.

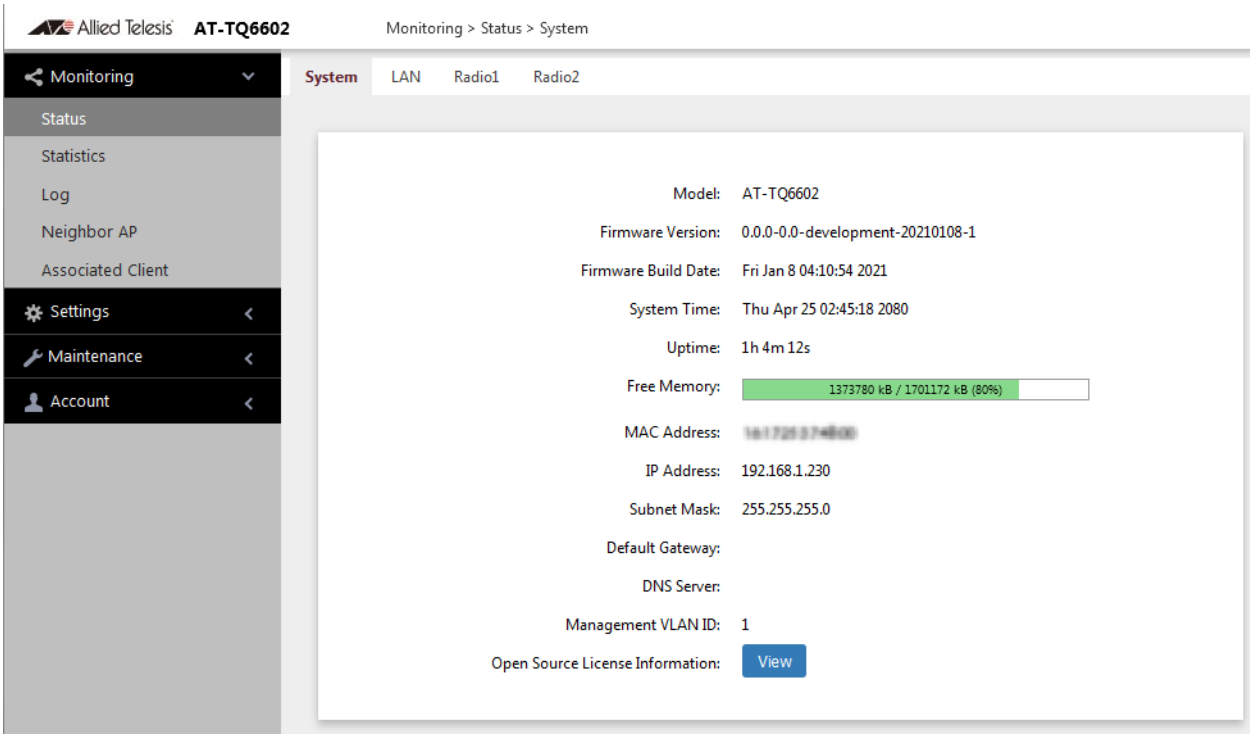


Figure 47. System Window

The fields are defined in Table 26.

Table 26. 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 26. 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 42 or “Setting the Date and Time with the Network Time Protocol (NTP)” on page 39.
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 has a different MAC address. You cannot change the MAC address.
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 26. System Window (Continued)

Item Name	Description
DNS Server	Displays the current DNS server address. Refer to "Assigning a Dynamic IP Address from a DHCP Server" on page 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 142.
Open Source License Information	When you click the **View** button, displays open source license information.

Displaying Neighbor Access Points

To view information about other access points that the access point has detected, select **Monitoring** > **Neighbor AP** from the main menu. Refer to Figure 48.

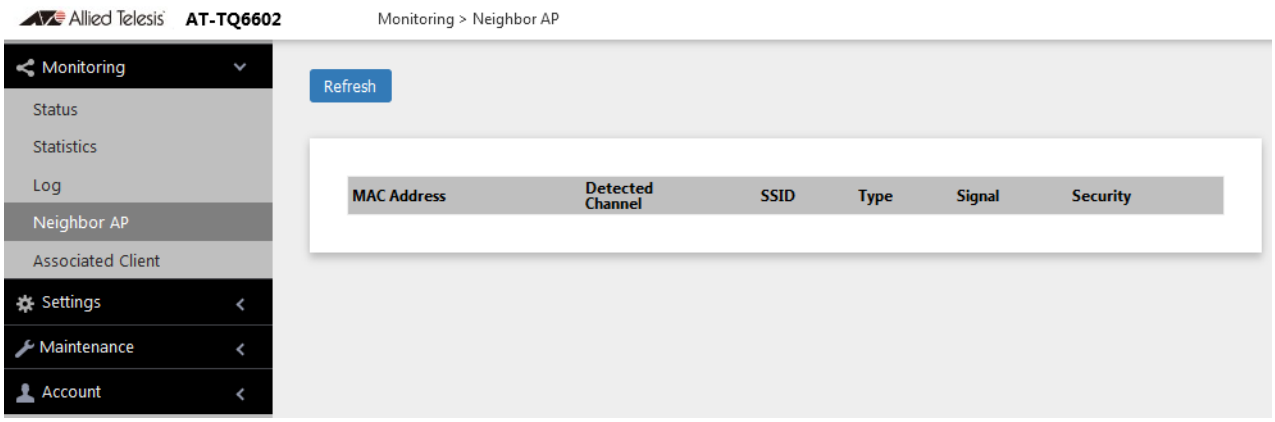


Figure 48. Neighbor AP Window

The columns are defined in Table 27.

Table 27. Neighbor AP Window

Column	Description
MAC Address	Displays the MAC addresses of the detected VAP.
Detected Channel	Displays the detected radio channel.
SSID	Displays the network name (SSIDs) 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 49.

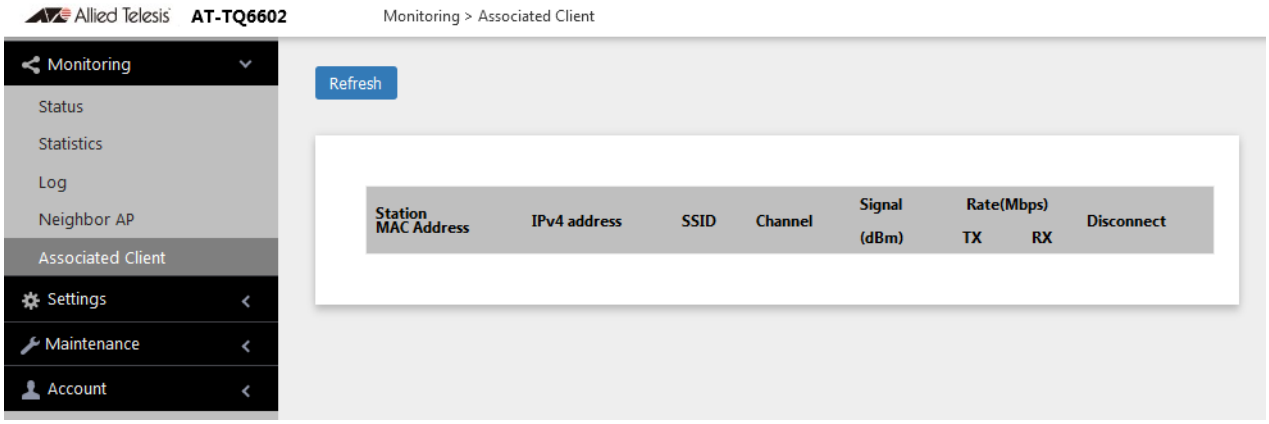


Figure 49. Associated Client Window

The columns are defined in Table 28.

Table 28. Associated Client Window

Column	Description
MAC Address	Displays the MAC addresses of associated clients.
IPv4 Address	Displays the client's IPv4 address.
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.
Disconnect	Displays the Disconnect button. Clicking the button disconnects the client.

Chapter 10

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 29:

Table 29. 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 156.

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 156.

To view the system log, select **Monitoring** > **Log**, Figure 50 on page 155 is an example.

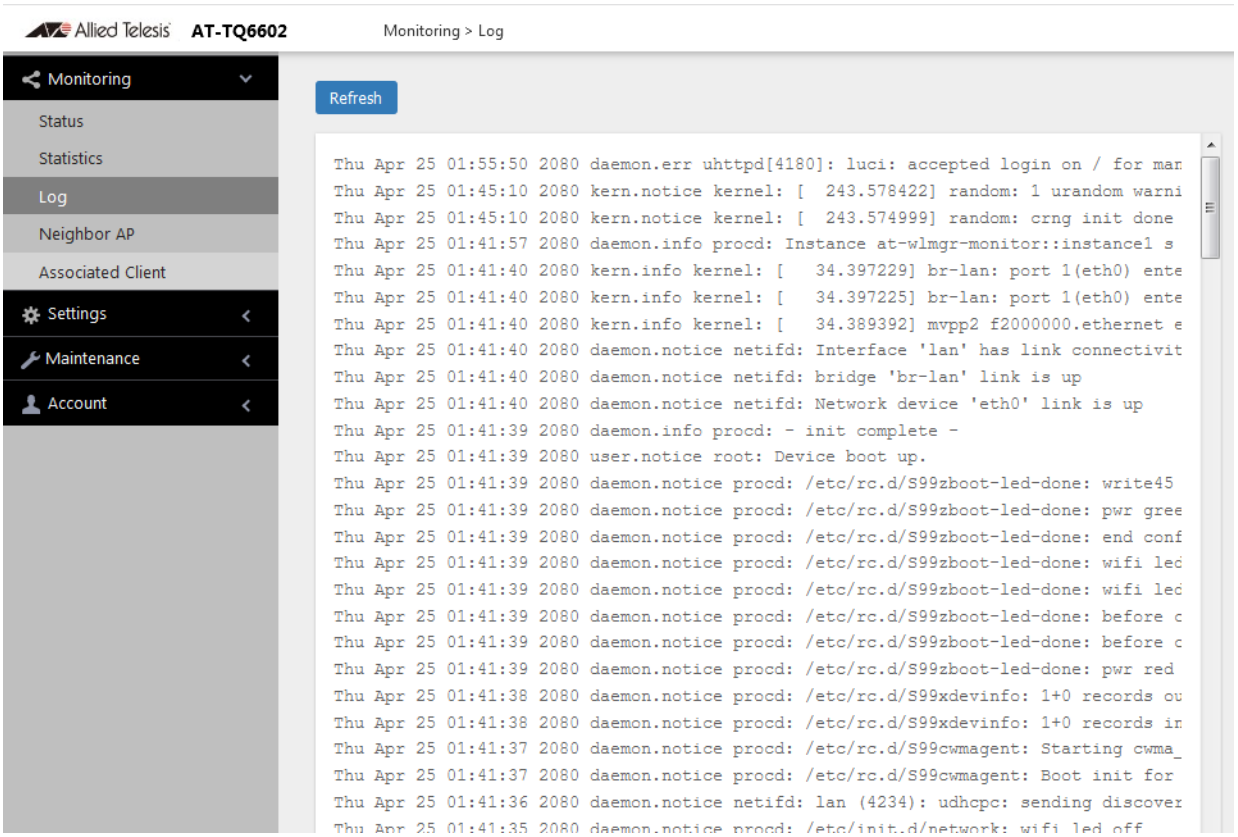


Figure 50. Log Window for Event Messages

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 51.

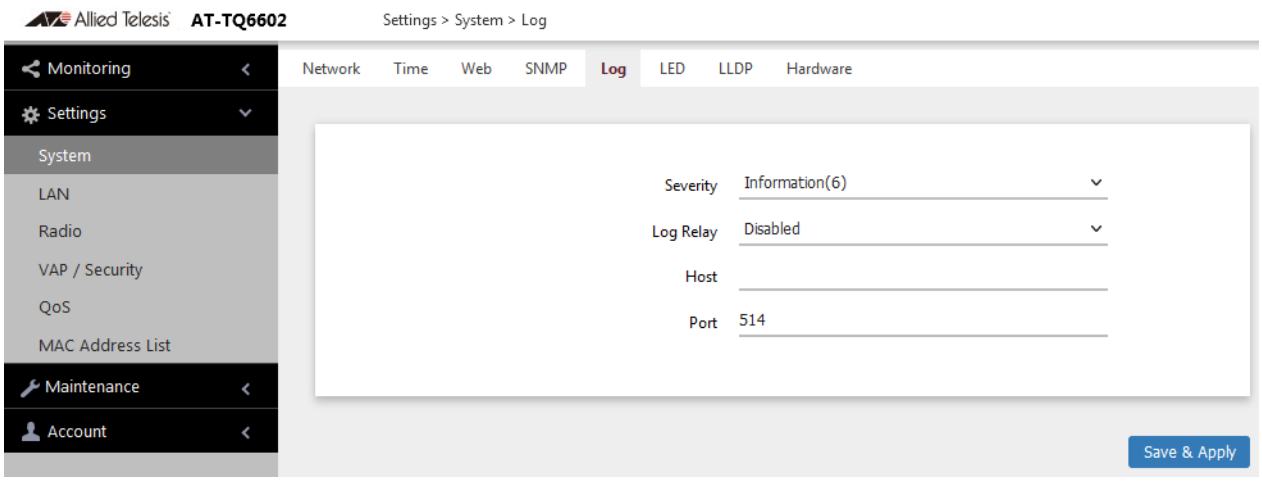


Figure 51. Log Window for Syslog Client

3. Configure the fields by referring to Table 30.

Table 30. 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 29 on page 154. 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 30. 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 11
Maintenance

This chapter has the following procedures:

Downloading the Configuration of the Access Point to Your Computer

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

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

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

1. Select **Maintenance** > **Configuration** from the main menu. Refer to Figure 52.

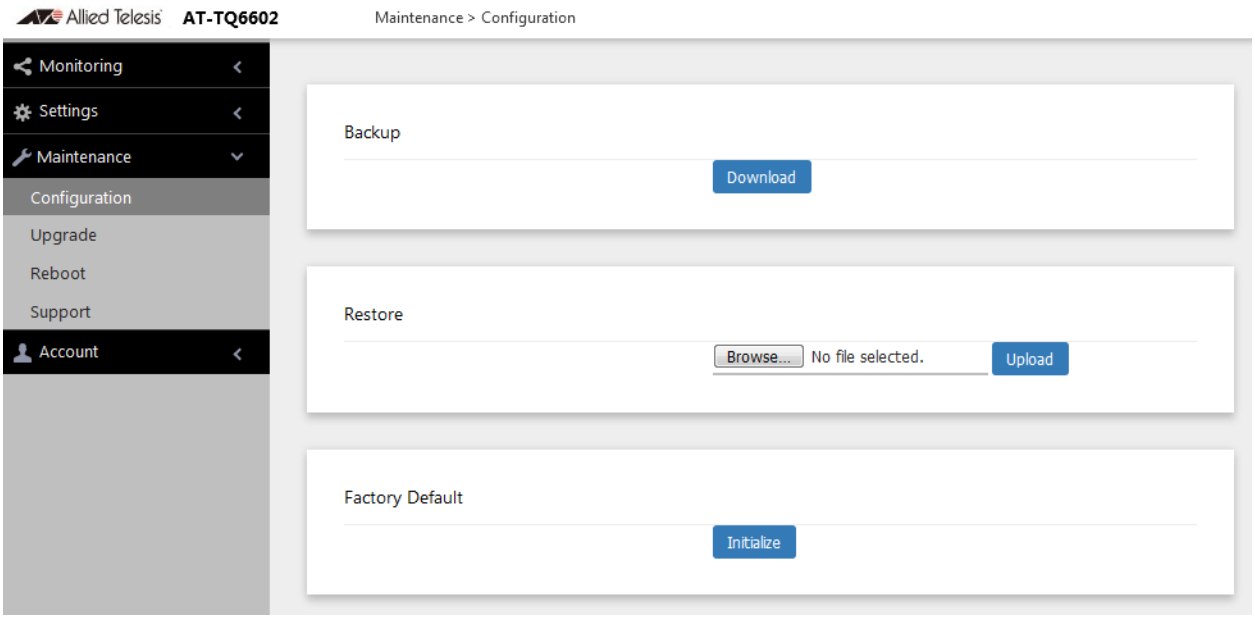


Figure 52. Configuration Window

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 160.
- 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 52 on page 160.
2. Click the **Browse** button in the Restore section of the window and select the configuration file to restore to the access point from your management workstation or network server.
3. Click the **Open** button.
4. Click the **Upload** button.
5. Wait one minute for the access point to upload the file and reboot.
6. To resume managing the unit, establish a new management session.

Restoring the Default Settings to the Access Point

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

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

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

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

1. Select **Maintenance** > **Configuration** from the main menu. Refer to Figure 52 on page 160.
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 23.

Uploading New Management Software to the Access Point

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

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

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

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

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

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

1. Select **Maintenance** > **Upgrade** from the main menu. Refer to Figure 53 on page 165.

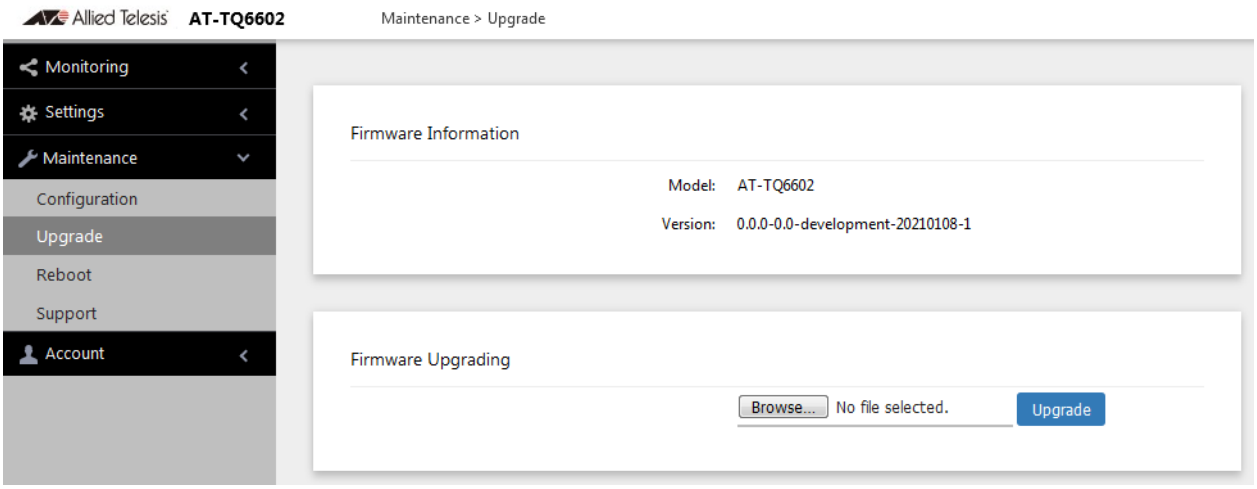


Figure 53. Upgrade Window

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

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

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

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

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

Rebooting the Access Point

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

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

To reboot the access point, perform the following procedure:

1. Select **Maintenance** > **Reboot** from the main menu. Refer to Figure 54.

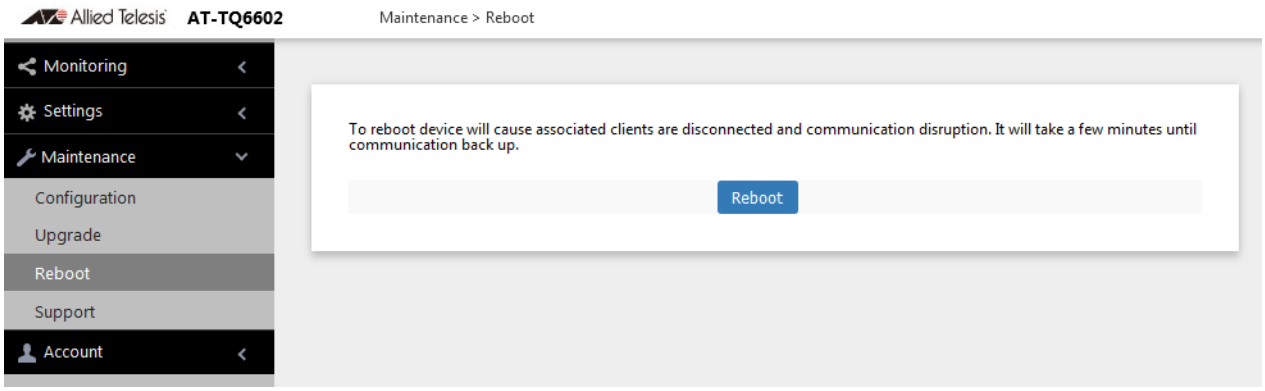


Figure 54. Reboot Window

2. Click the **Reboot** button.

   The access point displays a confirmation prompt.

3. Click **OK**.

   Your current management session is interrupted.

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

Collecting Technical Support Information to a File

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

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

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

1. Select **Maintenance** > **Support** from the main menu. Refer to Figure 55.

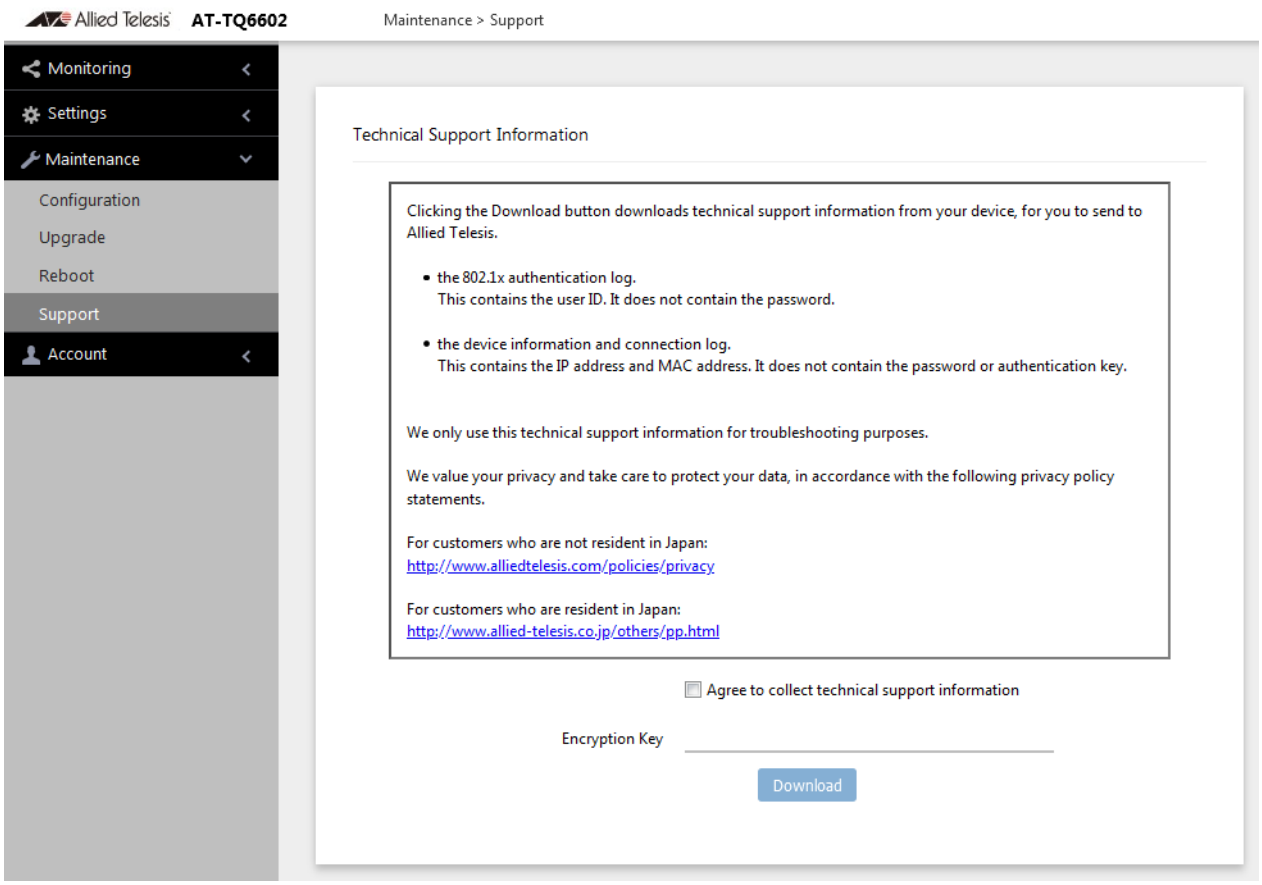


Figure 55. Support Window

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

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

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

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

5. Click the **Download** button.

   Your web browser prompts you to save a zip file.

6. Save the zip file on your system.

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