AT-TQ4600-OF13

Enterprise-class AT-TQ4600 Wireless Access Point
with IEEE802.11a/b/g/n/ac Dual Radio
and OpenFlow Protocol

User Guide

613-002584 Rev. A

Contents

Figures

Tables

Preface

This guide explains how to configure the features of the AT-TQ4600-OF13 wireless access point with its web browser management windows. 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 Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

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

For sales or corporate information, go to **www.alliedtelesis.com/purchase**.

Chapter 1
Overview

This chapter describes the AT-TQ4600-OF13 wireless access point and explains how to start a web browser management session. This chapter contains the following sections:

Features of the AT-TQ4600-OF13 Wireless Access Point

The AT-TQ4600-OF13 access point is shown Figure 1.

Figure 1. AT-TQ4600-OF13 Access Point

Features of the unit are listed here:

- Dual 2.4 GHz and 5 GHz radio
- IEEE 802.11a/b/g/n/ac
- 3x3:3ss MIMO with internal omni antennas
- Maximum capacity 2.4 GHz: 450 Mbps
- Maximum capacity 5 GHz: 1300 Mbps
- Internal antennas.
- Rogue access point detection
- Multiple SSIDs
- OpenFlow protocol
- One 10/100/1000Base-T Ethernet port with Auto-Negotiation, auto MDI/MDIX, and IEEE 802.3at Power over Ethernet (PoE+)
- IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), and IEEE 802.3ab (1000Base-T) compliance on the Ethernet port
- Virtual access points for multiple broadcast domains
- DHCP client
- RADIUS accounting with external RADIUS server
- Network Time Protocol (NTP) client
- Domain name server (DNS) client
- IEEE 802.1x authentication
- WPA-Personal and WPA-Enterprise with WPA, WPA2, and CCMP

(AES) authentication and encryption

- ❒ Static WEP encryption
- ❒ HTTP and HTTPS web browser management
- ❒ SNMPv1 and v2c management
- ❒ Event log
- ❒ Syslog client
- ❒ Indoor wall or ceiling installation

Secure Enterprise Software Defined Networking Controller

The AT-TQ4600-OF13 wireless access point is a bundled product of the AT-TQ4600 wireless access point and OpenFlow protocol. It is intended for use with the Secure Enterprise Software Defined Networking (SES) controller. The latter is a management program for Allied Telesis switches and access points. It lets you manage the virtual LAN (VLAN) assignments of hosts, and define where and when hosts can access networks. It can also be used with selected firewalls to automatically implement protective measures, such as blocking or isolating hosts, when viruses, malware. or other network threats are detected.

The SES controller is part of the Software-defined Networking (SDN) solution from Allied Telesis. SDN is a network architecture for controlling network traffic from a central controller instead of managing switches and wireless access points individually. It simplifies network management by removing management tasks and decisions from individual devices, and centralizing them in the controller. This makes it possible for application solutions like the controller to implement network configuration changes from the vantage point of the entire network, rather than from individual devices. Additionally, SDN make it possible to automate network configuration changes that previously had to be handled manually.

Configuration and management instructions from the controller to network devices are transmitted over a network pathway referred to as the control plane. The control plane for the AT-TQ4600-OF13 wireless access point is based on the OpenFlow protocol, which comes pre-installed and activated on the unit. No subscription license is required.

Topology Example

Figure 2 is an example of a network topology of the SDN solution. It consists of an SES controller, OpenFlow switch, and AT-TQ4600-OF13 wireless access point.

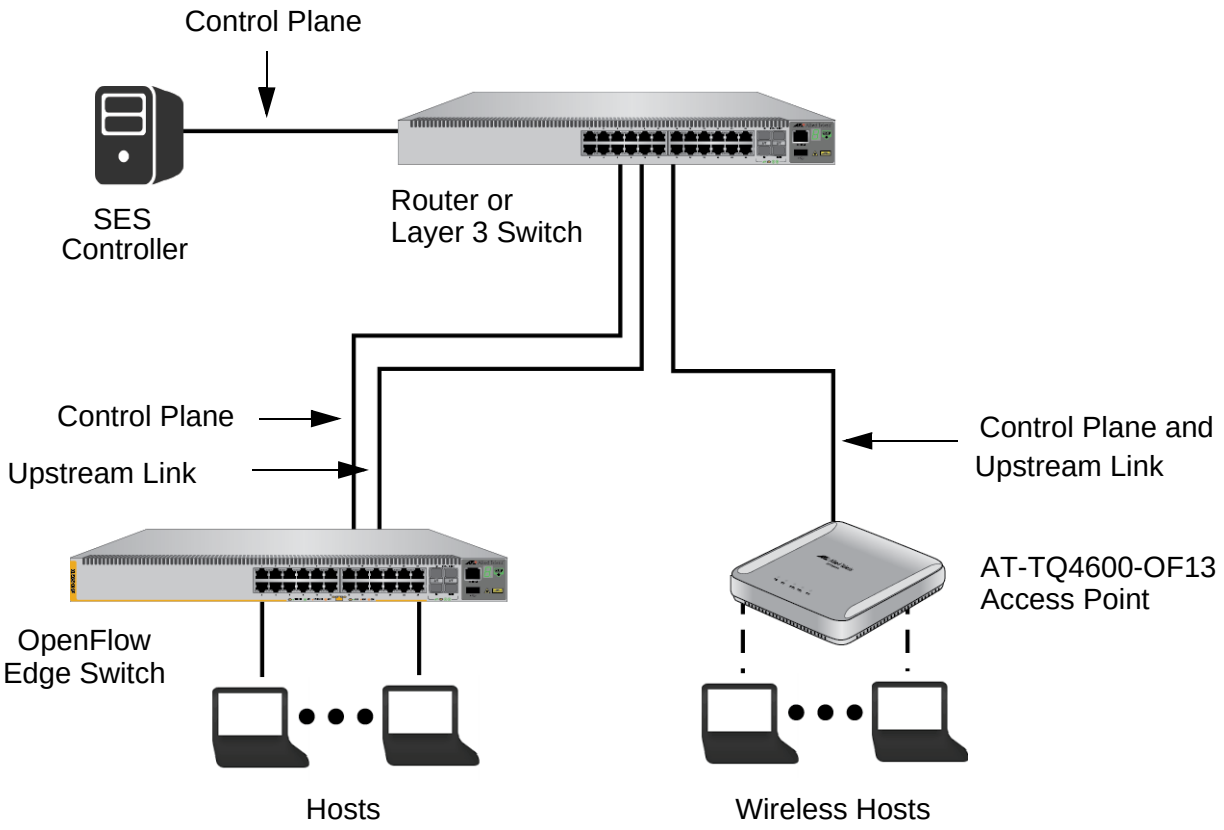


Figure 2. Example Hardware Topology of the SDN Solution with the OpenFlow Protocol

The basic components in the SDN solution are listed in Table 1.

Table 1. SDN Solution with the OpenFlow Protocol

Component	Description
SES controller	Server with the controller software. The controller is used to assign network users to virtual LANs and manage when and where they can access networks. For a list of approved servers, refer to the SES Controller and OpenFlow Protocol Installation Guide.

Table 1. SDN Solution with the OpenFlow Protocol (Continued)

Component	Description
Control plane	Network pathway over which the SES controller communicates with OpenFlow switches and AT-TQ4600-OF13 access points, using the OpenFlow protocol.
Router or Layer 3 switch	Gateway to the higher level network.
Upstream links	Connections from OpenFlow switches and wireless access points to the higher level network.
OpenFlow edge switches	Allied Telesis switches with the OpenFlow protocol. For a list of approved switches, refer to the SES Controller and OpenFlow Protocol Installation Guide.
AT-TQ4600-OF13	AT-TQ4600 wireless access point with the OpenFlow protocol.
Hosts and wireless hosts	Network edge devices, such as laptop computers or smart phones.

Note
The SES controller is designed for managing edge OpenFlow switches and wireless access points. It should not be used to manage devices in a network core.

Management Tools

Here are the management tools for the access point.

- Web browser interface - The access point comes with a web browser interface. You can configure all the device's features and parameters from the interface, except for those functions that require the SES controller. It consists of menus and windows, and is accessed over your network using a web browser at your management workstation. The access point supports both non-secure HTTP and secure HTTPS management sessions. The default setting is HTTP. You can manage only one wireless access point at a time with the interface.
- SES controller and OpenFlow protocol - This management program lets you manage the virtual LAN assignments of wireless hosts and define when and where hosts can access your network. As shown in Figure 2 on page 19, the controller resides on a network server and communicates with access points using the OpenFlow protocol, over a network pathway referred to as control plane. To manage wireless hosts, you add network, location, and schedule policies to the controller. Network policies define the VLAN assignments of wireless hosts, location policies define which OpenFlow switches and wireless access points that hosts can use to access your network, and schedule policies control the days and times when hosts can access networks. For more information, refer to the SES Controller and OpenFlow Protocol User Guide.
- SNMPv1 and v2c - You can also use SNMP to manage the device. The MIB is available from the Allied Telesis web site. You can use SNMP to configure only a limited number of access point parameters. To manage all parameters, you must use the web browser interface and SES controller. For instructions on how to configure the unit for SNMP, refer to the "Configuring SNMPv1 and v2c" on page 100. The default setting for SNMP is disabled. The product does not support SNMPv3.

Note
The AT-TQ4600-OF13 access point does not support the AT-UWC Series Wireless LAN Controller.

SES Controller and AT-TQ4600-OF13 Access Points

You can use the SES controller to manage the following three operating properties of wireless hosts on AT-TQ4600-OF13 access points:

- Specify the access points that hosts are allowed to use to access your network.
- Specify the days and times that wireless hosts can use access points.
- Specify the virtual LAN (VLAN) assignments of wireless hosts.

You manage the properties by adding policies for the wireless hosts to the SES controller. The controller sends the policies as flow rules to the access points as hosts connect to your wireless networks. There are three types of policies, one for each operating property, as listed here:

- Location policies
- Schedule policies
- Network policies

Location Policies

Location policies are used to define the access points that wireless hosts can use to access your network. Wireless hosts with location policies are can access your network only through those access points included in their policies and are denied access to all other access points.

Access points are identified in location policies by their unique datapath IDs, consisting of 16 hexadecimal digits. The default is the access point's MAC address preceded by four zeros (0000). For example, a wireless access point with the MAC address 00:1A:E6:39:65:44, has this default datapath ID:

0000001AE6396544

An access point can have only one datapath ID. To change the value, refer to "Configuring the OpenFlow Protocol" on page 75. To view the MAC address of the unit, select Basic Settings from the main menus.

Schedule Policies

Schedule policies are used to restrict access by wireless hosts to particular days or times. Hosts with schedule policies can attach to access points only during the days and times listed in their policies.

Network Policies

The third operating property manages VLAN assignments of wireless hosts. VLANs are used to segment networks through management software so that nodes with related functions are grouped into separate, logical LAN segments, to improve network performance, increase security, and simplify management. VLANs and their hosts are typically based on similar data needs or security requirements.

VLANs are identified by VLAN identifiers (VIDs), in the range of 0 to 4096. To assign hosts to VLANs, you add network policies with VIDs to the SES controller and then assign the policies to hosts. Once a host has a network policy, its packets are restricted to the designated VLAN in its policy.

SES Controller and Access Point Communications

Here is a overview of the communications between the controller, access point, and wireless hosts:

1. When a wireless host connects to a VAP on the AT-TQ4600-OF13 access point, the device transmits the host's packets to the SES controller over the control plane, using the OpenFlow protocol.
2. The controller examines the packets for the source MAC address to determine the host's address.
3. It searches its database for network, location, or schedule policies assigned to the host.
4. It transmits the policies as flow rules to the access point.
5. The access point applies the rules to the packets from the host, as follows:

   Location policy rules:

   - The access point forwards packets internally and over the upstream link from wireless hosts whose location policies include its datapath ID.
   - The access point blocks all packets from wireless hosts whose location policies do not include its datapath ID.
   - The access point forwards packets internally and over the uplink port from hosts without location policies.

   Schedule policy rules:

   - The access point forwards packets internally and over the uplink port from wireless hosts whose schedule policies include the current date and time.
   - The access point blocks all packets from wireless hosts whose schedule policies do not include the current date and time.
   - The access point forwards packets internally and over the uplink port from wireless hosts that do not have schedule policies.

   Network policy rules:

   - For hosts with network policies, the access point forwards their packets internally and over the upstream link with the VIDs from the policies, as tagged packets.
   - For hosts without network policies or a policy with the VID 0, the access point forwards their packets using the VIDs from the virtual

access points (VAPs).

For instructions on how to configure the wireless access point for the OpenFlow protocol and SES controller, refer to “Configuring the OpenFlow Protocol” on page 75. For more information, refer to the SES Controller and OpenFlow Protocol Installation Guide and SES Controller and OpenFlow Protocol User Guide.

Starting a Management Session on the Access Point

This section explains how to start a management session on the access point from your management workstation. The procedure assumes that the access point has already been assigned an IP address. The address can be a static address that was manually assigned to the unit or it can be a dynamic address from a DHCP server.

> **Note**
> If the access point has not been assigned an IP address and is using its default address 192.168.1.230, refer to “Starting the Initial Management Session on the Access Point” on page 26 for instructions on how to start a management session.

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.

   You should now see the logon window, shown in Figure 3.

Figure 3. Log On Window

3. Enter the username and password for the unit. The default values are “manager” for the username and “friend” for the password. The username and password are case-sensitive.
4. Click the Logon button.

Starting the Initial Management Session on the Access Point

If you just installed the device and are powering it on for the first time, it queries the subnet on the LAN port for a DHCP server. If a DHCP server responds, the unit uses the IP address that the server assigns it. If there is no DHCP server, the access point uses the default IP address 192.168.1.230.

There are a several ways to start the initial management session on the access point. One way is to establish 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. You might perform this procedure if your network does not have a DHCP server and you want to configure the access point before connecting it to your network.

The initial management session may 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 port and your computer to ports on an Ethernet switch that are members of the same VLAN.

If your network has a DHCP server, use the IP address the server assigns it to it to start the management session.

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

- “Starting the Initial Management Session with a DHCP Server” on page 27
- “Starting the Initial Management Session with a Direct Connection” on page 27
- “Starting the Initial Management Session without a DHCP Server” on page 28

Note
The initial management session of the access point has to be conducted through the LAN port because the default setting for the radios is off.

Starting the Initial Management Session with a DHCP Server

This procedure explains how to start the initial management session on the access port when the LAN port is connected to a network that has a DHCP server. This procedure assumes that you have already configured the DHCP server with the appropriate information for the access point (e.g., IP address and default gateway). To start the management session, perform the following procedure:

1. Power on the access point.
2. Start the web browser on your computer.
3. Enter the IP address of the access point in the URL field of the browser and press the Return key. This is the IP address assigned to the access point by the DHCP server. If you do not know the address, refer to the DHCP server.

   You should now see the logon window, shown in Figure 3 on page 25.
4. Enter “manager” for the username and “friend” for the password. The username and password are case-sensitive.
5. Click the **Logon** button.

Starting the Initial Management Session with a Direct Connection

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

> **Note**
> If the access point is using PoE or PoE+, you cannot perform this procedure because it involves a direct connection between your computer and the LAN port on the access point. You may either temporarily attach the power supply to the unit until after you have completed the initial management session or you may perform one of the other procedures for starting the initial management session.

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. (This requires removing the LAN cable you connected earlier in the hardware installation instructions.)
2. Change the IP address on your computer to 192.168.1.*n*, where *n* is a number from 1 to 254, but not 230. Refer to the documentation that accompanies your computer for instructions on how to set the IP address.
3. Set the subnet mask on your computer to 255.255.255.0.
4. Power on the access point.

5. Start the web browser on your computer.
6. Enter the IP address 192.168.1.230 in the URL field of the browser and press the Return key.

   You should now see the logon window, shown in Figure 3 on page 25.
7. Enter “manager” for the username and “friend” for the password. The username and password are case-sensitive.
8. Click the Logon button.

Starting the Initial Management Session without a DHCP Server

This procedure explains how to start the initial management session on the access port 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. If your network has VLANs, check to be sure that your computer and the access port 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 port 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 may connect your computer to any port on the Ethernet switch.
2. Change the IP address on your computer to 192.168.1.*n*, where *n* is a number from 1 to 254, but not 230. Refer to the documentation that accompanies your computer for instructions on how to set the IP address.
3. Set the subnet mask on your computer to 255.255.255.0.
4. Power on the access point.
5. Start the web browser on your computer.
6. Enter the IP address 192.168.1.230 in the URL field of the browser and press the Return key.

   You should now see the logon window, shown in Figure 3 on page 25.
7. Enter “manager” for the username and “friend” for the password. The username and password are case-sensitive.
8. Click the **Logon** button.

Using the Management Menus and Windows

Here is general information about the management menus and windows.

Web Browser Menus

You can control the appearance of the menus with the Navigator pull-down menu in the upper right corner of the web browser windows. The menu options are listed here:

- Horizontal Tabs
- Vertical Tabs
- Dropdown Menus

The Horizontal Tabs selection displays the main menu in a row near the top of the windows. Clicking a menu selection displays the menu options in a row beneath the main menu. Figure 4 shows the Manage menu.

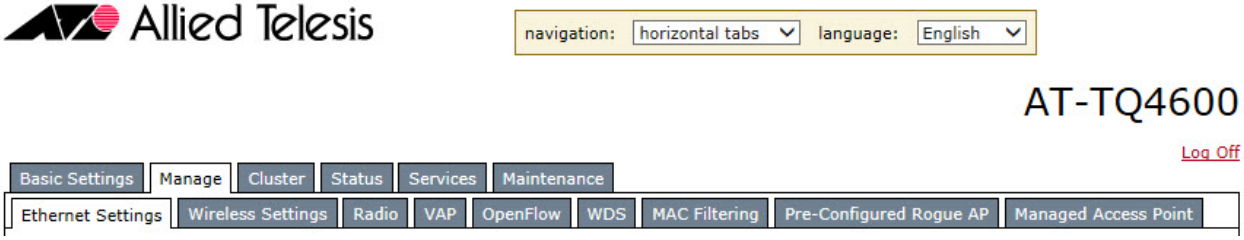


Figure 4. Horizontal Menus

The Vertical Tabs selection displays the menus in a column on the left side of the management windows. Refer to Figure 5 on page 30.

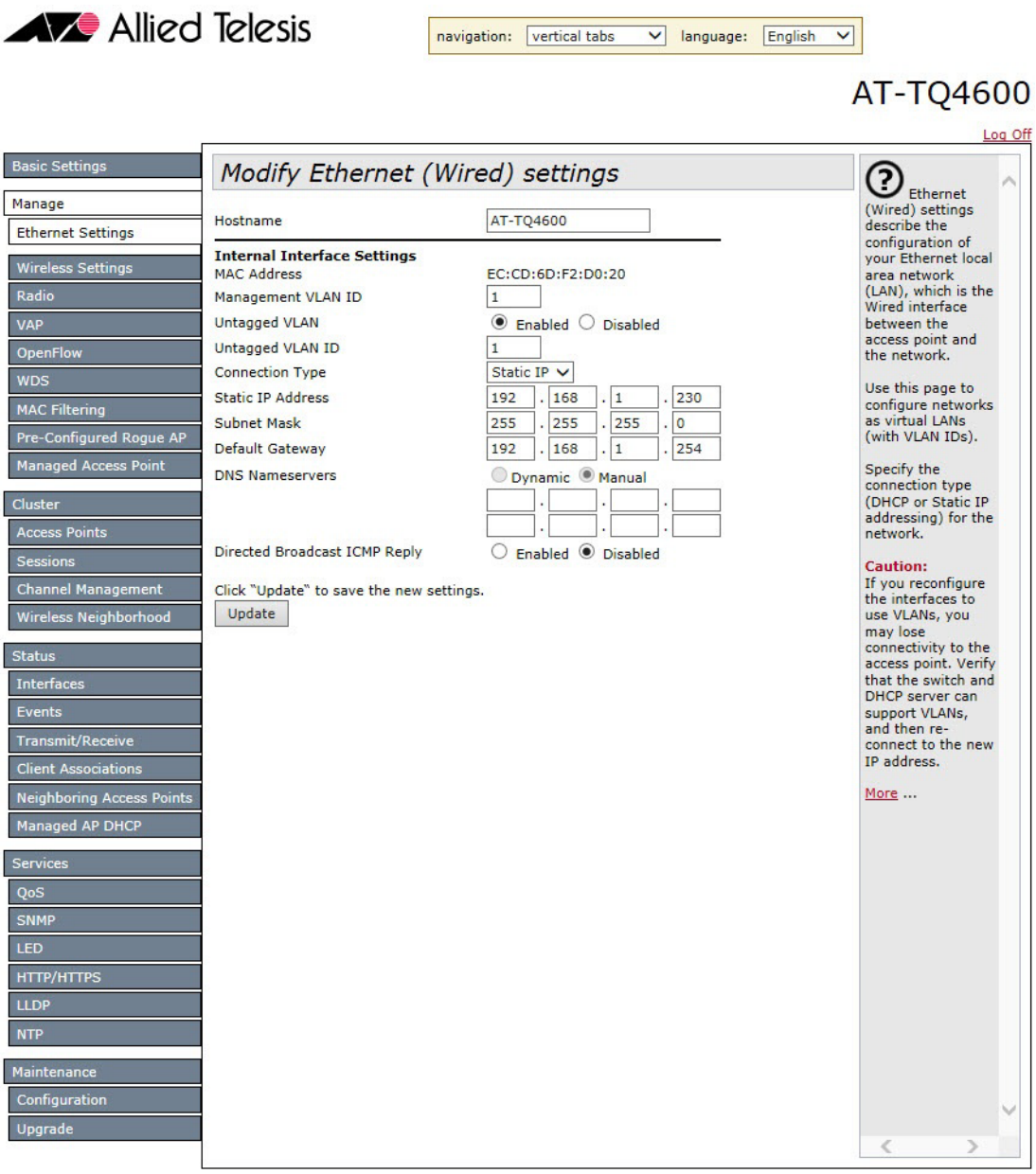


Figure 5. Vertical Menus

The Dropdown Menu option displays the main menu in a horizontal row near the top of the window. Menu options are displayed vertically when you move the mouse over the options in the main menu. Figure 6 on page 31 shows the Manage menu.

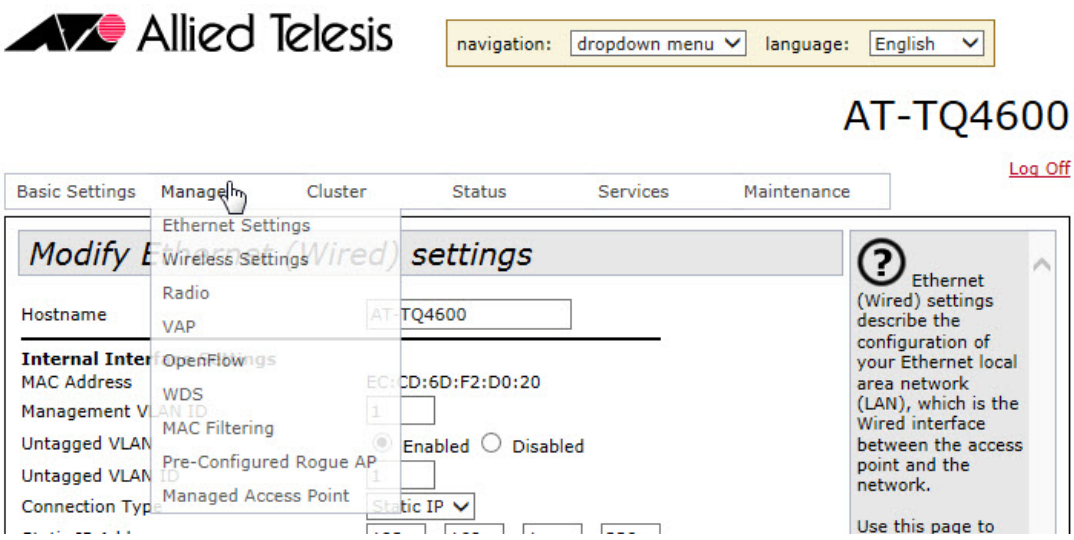


Figure 6. Dropdown Menus

The menus contain the same selections and perform the same functions regardless of the format. You can switch between formats without interrupting your current session or having to stop and start it again.

Saving Your Changes

You need to click the **Update** button 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 activates your changes and saves them in the configuration file. If you modify the settings in a window and then navigate to a different window without clicking the button, your changes are lost and have to be reentered.

Logging Off

You should always log off after managing the unit. To log off, click the **Log Off** option in the upper right corners of the management windows.

Unsupported Features

The management firmware in the AT-TQ4600-OF13 access point has features that are not compatible with the SES controller and OpenFlow protocol. The features are listed in Table 2. They are not documented in this guide and should not be used with the controller. For instructions on the features, refer to the AT-TQ Wireless Access Point Series User Guide.

Table 2. Unsupported Features

Feature	Menu Selection	Window Title
Wireless Distribution System (WDS) bridges	Manage -> WDS	Configure WDS Bridges to Other Access Points
Clusters	Cluster -> Access Points	Manage Access Points in the Cluster
	Cluster -> Sessions	Manage Sessions Associated with the Cluster
	Cluster -> Channel Management	Automatically Manage Channel Assignments
	Cluster -> Wireless Neighborhood	View Neighboring Access Points
MAC Address Filtering	Manage -> MAC Filtering Settings	Configure MAC Filtering of Client Stations
Quality of Service	Services -> QoS	Modify QoS Queue Parameters
AT-UWC Unified Wireless Controller	Manage -> Managed Access Point Settings	Configure Managed Access Point Parameters
	Status -> Managed AP DHCP	View Wireless Controller Information Obtained via DHCP
Link Layer Discovery Protocol	Services - > LLDP	LLDP Configuration
Switching primary and secondary management software images	Maintenance -> Upgrade	Manage Firmware

Documentation

The installation and user guides for the SES controller are listed here:

- SES Controller and OpenFlow Protocol Installation Guide

  This guide explains how to install the SES controller on a network server and configure OpenFlow switches.

- SES Controller and OpenFlow Protocol User Guide

  This guide explains how to use the SES controller to manage network, location, and schedule policies for hosts on OpenFlow switches and AT-TQ4600-OF13 wireless access points.

- AT-TQ4600-OF13 Wireless Access Point Installation Guide

  This guide explains how to install the wireless access point and configure it for the SES controller.

- AT-TQ4600-OF13 Wireless Access Point User Guide

  This guide explains how to use the on-board web interface to manage the radio, virtual access points, and other features in the wireless access point.

- SES Controller and Autonomous Management Framework (AMF) Application Proxy Installation and User Guide

  This guide explains how to install and configure the SES controller for the enhanced firewall protection feature in AMF networks.

Chapter 2

Basic Settings Menu

This chapter describes the management functions of the menu selections in the Basic Settings menu. The chapter contains the following sections:

Displaying Basic Information

This section explains how to display the following information about the access point:

- IP address
- MAC address
- Firmware version number
- Build number
- Operational time

To display the information, select **Basic Settings** from the main menus to display the “Provide basic settings” window. The information is contained in the Review Description of the Access Point section of the window. Refer to Figure 7. The fields are defined in Table 3 on page 37.

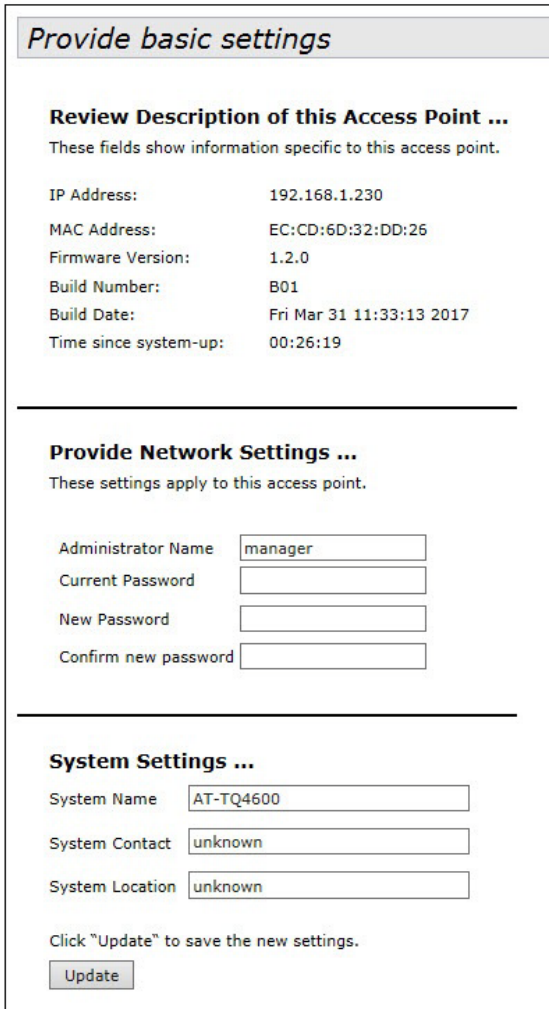


Figure 7. Provide Basic Settings Window

Table 3. Review Description of this Access Point

Field	Description
IP Address	Displays the IPv4 address of the access point. The access point uses the IPv4 address to communicate with the SES controller over the control plane. For instructions on how to set the IPv4 address, refer to “Assigning a Static IPv4 Address to the Access Point” on page 42 or “Assigning a Dynamic IPv4 Address from a DHCP Server to the Access Point” on page 44.
MAC Address	Displays the MAC address of the device and radio 1. Radio 2 has a different MAC address. To view the MAC addresses of both radios, refer to “Configuring Basic Radio Settings” on page 49. You may not change the MAC addresses of the device or radios.
Firmware Version	Displays the version number of the management software on the access point.
Build Number	Displays the build number. This number and the firmware version number identify the management software.
Build Date	Displays the completion date and time of the firmware.
Time since system-up	Displays the amount of time since the unit was last reset or powered on.

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 can have only one manager account.

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

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

1. Select **Basic Settings**.

   The access point displays the "Provide basic settings" window. Refer to Figure 7 on page 36.

2. To change the manager name, select the Administrator Name field in the Provide Network Settings section of the window and enter the new name. Refer to Figure 7 on page 36. The name can be up to 12 alphanumeric characters. The first character must be a letter. It cannot be a number or special character. The name is case-sensitive.

3. To change the password, perform these steps:

   a. Select the **Current Password** field in the Provide Network Settings section of the window and enter the account's current password.

   b. Select the **New Password** field and enter a new password of up to 32 alphanumeric characters. It may not contain spaces or any of these special characters: ", $, :, <, >, ', &, *. The password is case-sensitive. The new password is displayed as a series of asterisks on your screen.

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

4. After editing the fields, click the **Update** button at the bottom of the window to activate and save your changes. You must use the new manager name and password for all future management sessions on the unit.

Changing the System Name, Contact, and Location

This procedure explains how to identify the access point by defining the system name, the person responsible for managing the device, and its location. This information is optional.

To change the system name, contact, and location information, perform the following procedure:

1. Select **Basic Settings**.

   The access point displays the “Provide basic settings” window. Refer to Figure 7 on page 36.

2. To change the system name, select the **System Name** field in the System Settings section of the window and enter a new name. The name can be up to 64 alphanumeric characters. Spaces are allowed. The default name is the model name of the access point.

3. To enter the name of the person responsible for managing the unit, select the **System Contact** field and enter a name. You might also include the phone number and email address of the individual in this field. The name can be up to 64 alphanumeric characters. Spaces are allowed. The default name is “unknown.”

4. To specify the location of the access point, select the **System Location** field and enter the location. The location can be up to 64 alphanumeric characters. Spaces are allowed. The default location is “unknown.”

5. After editing the fields, click the **Update** button at the bottom of the window to activate and save your changes.

Chapter 3

Manage Menu

This chapter describes the management functions of the menu selections in the Manage menu. The chapter contains the following sections:

Assigning a Static IPv4 Address to the Access Point

This section explains how to manually assign an IPv4 address to the access point. The unit uses the address to communicate with the SES controller over the control plane and with your management workstation and web browser.

If you prefer the access point obtain its IPv4 configuration from a DHCP server on your network, refer to “Assigning a Dynamic IPv4 Address from a DHCP Server to the Access Point” on page 44.

Note
Changing the IPv4 address interrupts your management session of the unit. To resume managing the device, start a new management session using the device’s new IPv4 address.

To manually assign an IPv4 address to the control plane on the unit, perform the following procedure:

1. Select **Manage** -> **Ethernet Settings**.

   The access point displays the “Modify Ethernet (Wired) Settings” window in Figure 8.

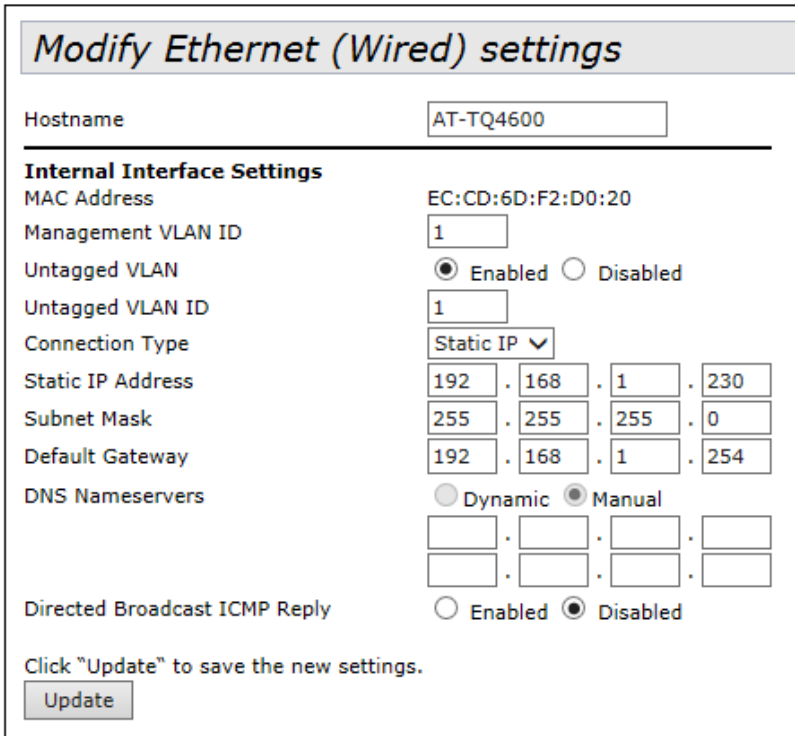


Figure 8. Modify Ethernet (Wired) Settings Window

2. From the Connection Type pull-down menu, select **Static IP**.

   The Static IP Address, Subnet Mask, and Default Gateway fields in the window are activated so that you can change their values.

3. Select the **Static IP Address** field and enter the new IPv4 address for the access point. The default address is 192.168.1.230. You can enter only one IP address.

4. Select the **Subnet Mask** fields and enter the subnet mask for the IP address. The default subnet mask is 255.255.255.0.

5. Select the **Default Gateway** fields and enter the default gateway address for the unit. The default gateway address is 192.168.1.254.

   The default gateway is an IPv4 address of an interface on a router or other Layer 3 routing device. It specifies the first hop to reaching the subnet or network of the SES controller and your management workstation. The access point can have only one default gateway and the network portion of the address must be the same as the IP address entered in step 3.

   You have to assign a default gateway to the access point. If your network does not have a default gateway or you do not want to assign one to the access point at this time, enter an unused IP address of the same network as the IP address entered in step 3.

6. If you want to specify the IPv4 addresses of Domain Name servers, enter up to two IP addresses in the **DNS Nameservers** fields. If you have only one DNS IP address, you must enter it in the top field.

7. Click the **Update** button at the bottom of the window to activate and save your changes.

   Your management session is interrupted.

8. Start a new management session using the new IPv4 address of the device.

Assigning a Dynamic IPv4 Address from a DHCP Server to the Access Point

This section explains how to assign an IPv4 address to the access point from a DHCP server. The unit uses the address to communicate with the SES controller over the control plane and with your management workstation and web browser.

If you network does not have a DHCP server or you prefer to manually assign it an IPv4 address, refer to “Assigning a Static IPv4 Address to the Access Point” on page 42.

Note
Changing the IPv4 address interrupts your management session of the unit. To resume managing the device, start a new management session using the device’s new IPv4 address.

To activate the DHCP client so that the access point obtains its IPv4 configuration from a DHCP server, perform the following procedure:

1. Select **Manage** -> **Ethernet Settings**.

   The access point displays the “Modify Ethernet (Wired) settings” window in Figure 8 on page 42.

2. From the Connection Type menu, select **DHCP**. This is the default setting.

3. If you want to manually specify the IPv4 addresses of Domain Name servers, click **Manual** dialog button for DNS Nameservers and enter up to two IPv4 addresses. If you have only one DNS IPv4 address, you must enter it in the top address field.

4. If you want the access point to use the DNS addresses provided by the DHCP server, click the **Dynamic** circle.

5. Click the **Update** button at the bottom of the window to activate and save your changes.

   Your management session is interrupted. The DHCP client on the unit queries the subnet on the LAN port for a DHCP server. If it receives a response, it uses the IPv4 configuration that the server provides. If there is no response, the unit uses the default IPv4 address 192.168.1.230.

6. To resume your management session on the device, enter the new IPv4 address of the access point in the URL field of your web browser.

Setting the Management VLAN ID for the Control Plane

The Management VLAN ID field in the “Modify Ethernet (Wired) settings” window is used to specify the VID for the control plane on the LAN port of the access point. The access point uses the VID and control plane to communicate with the SES controller to obtain the flow rules for wireless hosts, and with your management workstation when you manage the device with your web browser. You can assign the same VID to the control planes on different OpenFlow devices. The VID, however, must be different from the data plane VIDs for the OpenFlow hosts.

The “Modify Ethernet (Wired) settings” window has two additional fields for setting a VID. They are the Untagged VLAN and Untagged VLAN ID fields. They are non-operational when the unit is functioning as an OpenFlow device. They become operational if the device cannot communicate with the SES controller and is in the Critical Mode Enabled (Accept All) setting, as explained in “Configuring the OpenFlow Protocol” on page 75. For information on the fields, refer to the AT-TQ Series User Guide.

To specify the management VID for the control plane for the access point, perform the following procedure:

1. Select **Manage** -> **Ethernet Settings**.

   The access point displays the “Modify Ethernet (Wired) settings” window in Figure 8 on page 42.

2. Select the **Management VLAN ID** field and enter a value of 1 to 4094.

3. Click the **Update** button to activate and save your changes.

Enabling or Disabling Broadcast Ping Replies

You can configure the access point to either ignore or reply to ICMP echo requests to IP broadcast addresses, also referred to as broadcast pings. To configure broadcast ping replies, perform the following procedure:

1. Select **Manage** -> **Ethernet Settings**.

   The access point displays the “Modify Ethernet (Wired) settings” window in Figure 8 on page 42.

2. In the Directed Broadcast ICMP Reply field, do one of the following:

   - If you want the access point to respond to broadcast pings, click the **Enabled** circle.
   - If you do not want the access point to respond to broadcast pings, click the **Disabled**\ circle.

3. Click the **Update** button to activate and save your changes.

Setting the Country Setting

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

Note
Changing the country setting of the access point disables both radios, causing disruption to network operations if the unit is actively forwarding network traffic.

To set the country setting, perform the following procedure:

1. Select **Manage** -> **Wireless Settings**.

   The access point displays the “Modify wireless settings” window. Refer to Figure 9.

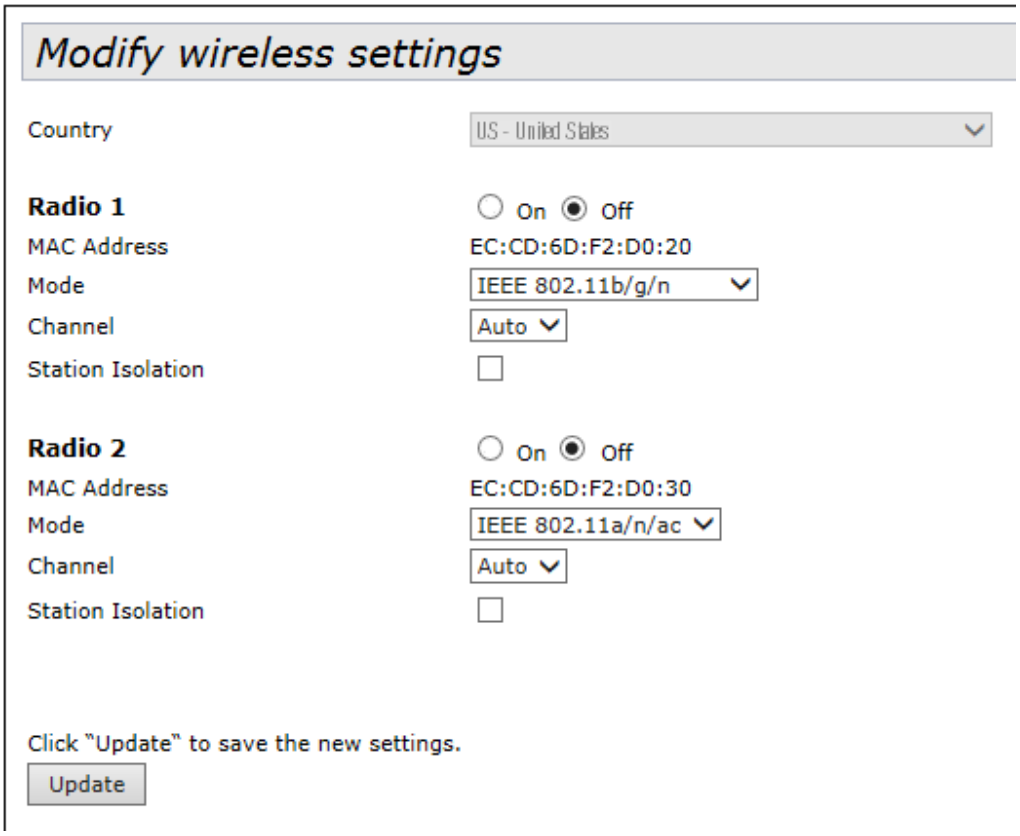


Figure 9. Modify Wireless Settings Window

2. Select the **Country** pull-down menu and select your country or region.

Note
If the Country pull-down menu is deactivated, the country parameter was set by the manufacturer and cannot be changed. Contact your Allied Telesis sales representative for assistance if the setting is not correct for your country or region.

The access point displays a confirmation prompt.

3. Click **OK** to change the country setting or Cancel to cancel the procedure.

   If you click OK, the access point changes the country setting and disables both radios on the access point. For instructions on how to enable the radios and configure their settings, refer to “Configuring Basic Radio Settings” on page 49 and “Configuring the Radio Settings” on page 52.

   This procedure does not require clicking the Update button.

   You must now reboot the access point. The new country setting is not active until the unit is rebooted. To reboot the unit, either power off and on the unit or continue with these steps:

4. Select **Configuration** -> **Maintenance**.

5. Click the **Reboot** button in the To Reboot the Access Point section of the “Manage the Access Point’s Configuration” window.

6. When the access point displays a confirmation prompt, click **OK** to reboot the unit.

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

Configuring Basic Radio Settings

The management software has two windows for configuring the operational settings of the radios in the access point. The “Modify radios settings” window, described in “Configuring the Radio Settings” on page 52, is the main window for adjusting the radio parameters because it has all the parameters, everything from operational mode to broadcast/multicast rate limiting. This is the window to use when you need to fine tune the properties of the radios.

If you are only interested in configuring basic radio parameters, you might find everything you need in the “Modify wireless settings” window, which is the topic of this section. From this window you can perform these basic radio functions:

- Enable or disable a radio
- Select the operational mode
- Select the channel
- Enable or disable the station isolation mode

When you change a radio parameter in the “Modify wireless settings” window, the change is reflected in the “Modify radios settings” window. So you could enable a radio here and perhaps select the channel, and then move to the “Modify radio settings” window to adjust additional parameters.

The “Modify wireless settings” window does contain one parameter, however, that is not in the “Modify radio settings” window, and that is the station isolation mode parameter. The parameter determines whether the clients of a VAP can communicate with each other through the access point. That parameter can only be set from this window.

To configure basic radio settings from the “Modify wireless settings” window, perform the following procedure:

1. Select **Wireless Settings** -> **Manage**.

   The access point displays the “Modify wireless settings” window. An example is shown in Figure 9 on page 47.

2. Configure the settings as needed. The parameters are described in Table 4 on page 50.

3. After configuring the parameters, click the **Update** button to activate and save your changes.

Table 4. Modify Wireless Settings Window

Field	Description
Radio On Off	Enables or disables the radio. The selections are described here: - On: Enables the radio. You have to enable a radio before you can configure its parameter settings. - Off: Disables the radio. This is the default setting.
MAC Address	Displays the MAC address of the radio. This value cannot be changed.
Mode	Specifies the Physical Layer (PHY) standard of the radio. The available modes depend on the radio and country. The modes for the 2.4 GHz radio are listed here: - IEEE 802.11b/g: The access point accepts only 802.11b and 802.11g clients. - IEEE 802.11b/g/n: The access point accepts 802.11b, 802.11g, and 802.11n clients operating at 2.4 GHz. This is the default setting for the 2.4 GHz radio. - 2.4 GHz IEEE 802.11n: The access point accepts 802.11n clients operating at 2.4 GHz. The modes for the 5 GHz radio are listed here: - IEEE 802.11a: The access point accepts 802.11a clients.- IEEE 802.11a/n/ac: The access point accepts 802.11a, 802.11n, and 802.11ac clients operating at 5 GHz. This is the default setting for the 5 GHz radio in the AT-TQ4400e and AT-TQ4600 access points. - 5 GHz IEEE 802.11n/ac: The access point accepts 802.11n and 802.11ac clients operating at 5 GHz.

Table 4. Modify Wireless Settings Window (Continued)

Field	Description
Channel	Specifies the channel for the radio in the access point. The number of available channels varies by radio, mode, and country. Here are the guidelines: - At the Auto setting, the access point sets the channel automatically. The access point listens on the channels and selects the one with the least traffic.This is the default setting. - You can select a channel from the pull-down menu. You may select only one channel.
Station Isolation	Enables or disables station isolation. When station isolation is enabled, the access point does not allow the wireless clients of a VAP to communicate with each other, but does allow them to communicate with clients in other VAPs and with the wired LAN. The feature is disabled when the dialog box is empty and enabled when the dialog box has a check mark. The default setting is disabled. To activate or deactivate the feature, click the dialog box to insert or remove the check mark.

Configuring the Radio Settings

To configure the parameter settings of the 2.4 and 5 GHz radios, perform the following procedure:

1. Select **Manage** -> **Radio**.

   The management software displays the “Modify radio settings window,” shown in Figure 10 on page 53.

2. From the **Radio** pull-down menu, select a radio. Options 1 and 2 are the 2.4 and 5 GHz radios, respectively. The default is radio 1. You can configure only one radio at a time.

3. To activate a radio, click the **On** selection for the Status option. You cannot configure a radio when its status is off. To deactivate a radio, click the **Off** selection.

4. Configure the radio parameters. Refer to Table 5 on page 54.

5. After configuring the parameters, click the **Update** button to activate and save your changes.

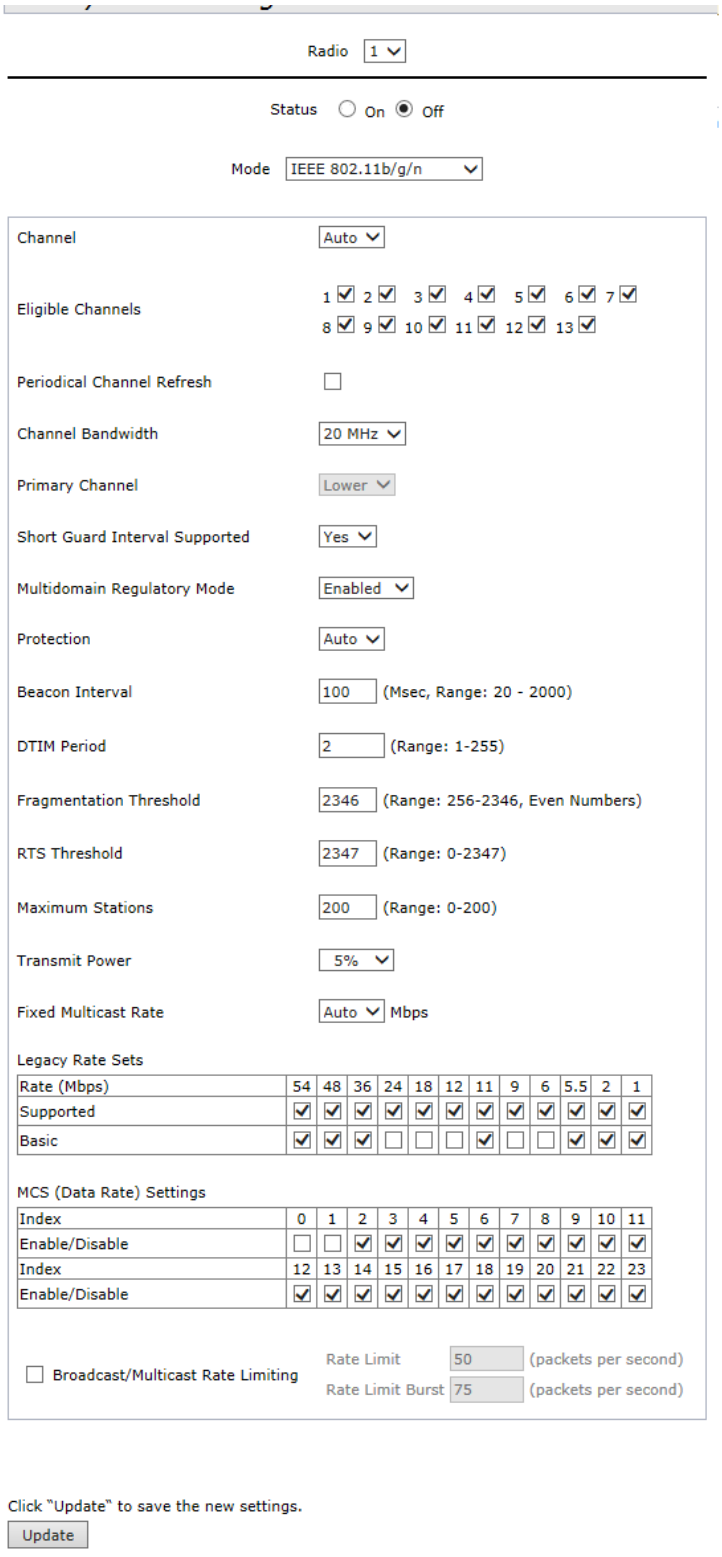


Figure 10. Modify Radio Settings Window

Table 5. Modify Radio Settings Window

Parameter	Description
Mode	Specifies the Physical Layer (PHY) standard of the radio. The available modes depend on the radio and country. The modes for the 2.4 GHz radio are listed here: - IEEE 802.11b/g: The access point accepts only 802.11b and 802.11g clients. - IEEE 802.11b/g/n: The access point accepts 802.11b, 802.11g, and 802.11n clients operating at 2.4 GHz. This is the default setting for the 2.4 GHz radio. - 2.4 GHz IEEE 802.11n: The access point accepts 802.11n clients operating at 2.4 GHz. The modes for the 5 GHz radio are listed here: - IEEE 802.11a: The access point accepts 802.11a clients. - IEEE 802.11a/n/ac: The access point accepts 802.11a, 802.11n, and 802.11ac clients operating at 5 GHz. This is the default setting for the 5 GHz radio. - GHz IEEE 802.11n/ac: The access point accepts 802.11n and 802.11ac clients operating at 5 GHz.
Channel	Specifies the radio channel. The available channels vary by radio, mode, and country. Here are the guidelines: - The Auto setting, the default setting, sets the channel automatically. The access point selects the channel with the least traffic. This is the default setting. - You can set the channel manually using the Channel pull-down menu.

Table 5. Modify Radio Settings Window (Continued)

Parameter	Description
Chanel (continued)	- If you select Auto, you can use the Eligible Channels parameter to restrict the channels from which the access point can choose.
Eligible Channels	Specifies the available channels when the channel is selected automatically. This selection is unavailable when the channel is selected manually. The available channels vary by radio, mode, and country. To deselect a channel, click its dialog box to remove the check mark. The default is all available channels.
Periodical Channel Refresh	Specifies whether the access point periodically reruns the channel selection process. Here are the guidelines: - This selection is only available when the Channel parameter is set to Auto. - Adding a check mark to the dialog box enables the feature. - Removing the check mark from the dialog box disables the feature. This is the default setting. - The access point runs the channel selection process every 24 hours, but only if the radio is not forwarding traffic from wireless clients. If it detects traffic, the access point delays the selection process for thirty minutes.
Channel Bandwidth	Specifies the channel width of a radio. The channel width for the 802.11n modes 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 802.11a/n/ac or 802.11n/ac mode on the 5 GHz radio can have a channel width of 80 or 40 MHz.

Table 5. Modify Radio Settings Window (Continued)

Parameter	Description
Primary Channel	Specifies the location of the Primary and Secondary channels for the 802.11n and 802.11ac modes when operating with channel widths of 40 and 80 MHz, respectively. The bandwidth of the 40 MHz channel for the 802.11n modes is divided into two 20 MHz channels. The bandwidth of the 80 MHz channel for the 802.11ac modes is divided into two 40 MHz channels. The channels are contiguous in the frequency domain. One of the channels is designated as the Primary channel. This channel is used by 802.11n or 802.11ac clients that support only a 20 or 40 MHz channel bandwidth, and for legacy clients. The other half of the channel is designated as the Secondary channel. You may use this parameter to specify the Primary channel of the 40 MHz bandwidth for 802.11n nodes and 80 MHz bandwidth for 802.11ac nodes. - Upper: Designates the upper 20 or 40 MHz of the channel as the Primary channel for the 802.11n or 802.11ac mode, respectively. - Lower: Designates the lower 20 or 40 MHz of the channel as the Primary channel for the 802.11n or 802.11ac mode, respectively. This is the default setting.
Short Guard Interval Supported	Specifies the dead time interval, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode supports a reduction in the interval from 800 nanoseconds, defined in the a and g standards, to 400 nanoseconds. This may provide up to a 10% improvement in data throughput. The selections are described here:

Table 5. Modify Radio Settings Window (Continued)

Parameter	Description
Short Guard Interval Supported (continued)	- Yes: The access point uses a 400 ns guard interval when communicating with clients that also support the feature. This is the default setting. - No: The access point uses an 800 ns guard interval. This parameter is only available in the 802.11n or 802.11n/ac mode.
Multidomain Regulatory Mode	Specifies whether a radio should operate in the Multidomain Regulatory Mode (World Mode) and include the country code in its beacons and probe responses. This allows client stations to operate in any country without reconfiguration. This feature only applies to radio 1 because it operates in the g band (2.4 GHz band). This selection does not apply to radio 2 because it operates in the a band (5 GHz band) and always includes the country code in its beacons, as specified in the 802.11h standard. The settings are described here: - Enabled: Activates the Multidomain Regulatory Mode (World Mode) and includes the country code in the beacons and probe responses. - Disabled: Disables the Multidomain Regulatory Mode (World Mode) and prevents the transmission of the country code in beacons and probe responses.
Protection	Enables or disables rules that guarantee that transmissions do not cause interference with legacy stations or applications. The settings are describe here: - Auto: This setting enables protection when legacy devices are within range of the radio.

Table 5. Modify Radio Settings Window (Continued)

Parameter	Description
Protection (continued)	- Off: This setting disables the protections. Legacy clients and access points within range may be affected by 802.11n transmissions. Here are the guidelines: - The protection applies to 802.11n and 802.11b/g. - Activating protection does not prevent clients from associating with the access point.
Beacon Interval	Specifies the time interval, in milliseconds, for transmissions of beacon frames. The access point transmits beacon frames to announce the existence of the wireless network. The range is 20 to 2000 milliseconds. The default setting is 100 milliseconds (10 beacon frames per second).
DTIM Period	Specifies the Delivery Traffic Information Map (DTIM) period. This value specifies how often clients sleeping in low power mode should check the access point for buffered traffic. The interval is defined in beacon frames. The range is 1 to 255 beacons frames. The default is 2 beacon frames.
Fragmentation Threshold	Specifies packet size for fragmentation. The fragmentation threshold lets you control the maximum size of packets the access point transmits. Packets that exceed the threshold are transmitted as multiple 802.11 packets. The range is 256 to 2346 bytes. Setting the threshold to the maximum value effectively disables the fragmentation threshold.

Table 5. Modify Radio Settings Window (Continued)

Parameter	Description
Fragmentation Threshold (continued)	Fragmentation involves more overhead because of the extra work in dividing up and reassembling frames, which can reduce throughput. But fragmentation can be useful in controlling interference.
RTS Threshold	Specifies the size in octets of MPDUs that initiate a Request to Send (RTS) and Clear to Send (CTS) handshake. The range is 0 to 2347 octets. You may use this parameter to control the use of RTS/CTS handshakes when the access point transmits MPDUs. The access point uses the handshake before transmitting MPDUs that exceed the defined threshold. If you specify a low value, RTS packets are sent more frequently. This may consume more bandwidth and reduce the throughput. But more RTS packets may help a network recover from interference or collisions, which might occur on a busy network.
Maximum Stations	Specifies the maximum number of clients the access point supports. The value is 0 to 200. When this parameter is set to 0, the access point rejects all clients. Allied Telesis recommends setting this parameter to 30 clients. The default is 200 clients.
Transmit Power	Specifies the transmission power of the access point. The power is selected from a list of percentages, in the range of 1% to 100%. The default is 100%. Here are the guidelines: - High transmission power levels are more cost-effective than low settings because the access point has a greater range. This reduces the number of access points required to cover a particular area.

Table 5. Modify Radio Settings Window (Continued)

Parameter	Description
Transmit Power (continued)	- Low transmission power settings can be useful in reducing overlap and interference between access points or increasing security by limiting the wireless signals to a physical location.
Fixed Multicast Rate	Specifies the multicast transmission rate of the access point. At the default Auto setting, the multicast transmission rate is fixed to the minimum rate in the Legacy Rate Sets setting. The value is in Mbps. The OpenFlow protocol on the access point does not support this feature.
Legacy Rate Sets	Specifies the supported and advertised data transmission rates of the access point. Here are the guidelines: - The Supported row specifies the data rates the access point supports. The default setting is all data rates. - The Basic row specifies the data rates the access point advertises to other access points and wireless clients. - The access point is generally more efficient when it advertises a subset of its supported data rates. The OpenFlow protocol on the access point does not support this feature.
MCS (Data Rate) Settings	Specifies the Modulation and Coding Scheme (MCS) index that the radio should advertise to 802.11n clients. The MCS indexes (also known as MCS data rates) are defined in the 802.11n standard. The OpenFlow protocol on the access point does not support this feature.

Table 5. Modify Radio Settings Window (Continued)

Parameter	Description
Broadcast/Multicast Rate Limiting	Controls rate limiting of broadcast and multicast packets. The OpenFlow protocol on the access point does not support this feature. Allied Telesis recommends disabling the feature, the default state.

Configuring Virtual Access Points

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

Here are the guidelines to VAPs:

- Each radio can have up to 16 VAPs. Allied Telesis recommends no more than five VAPs per radio.
- The VAPs are numbered from 0 to 15.
- You can enable and disable the VAPs individually, except for the default VAP, VAP0, which can only be disabled by disabling the radio itself. The access point does not forward traffic on disabled VAPs.
- The security methods for the VAPs are 802.1x, static WEP, Enterprise WPA, and Personal WPA.
- The VAPs of a radio can have different security methods.
- VAPs can have the same or different VLAN IDs (VIDs).
- The access point uses network policies from the SES controller to assign hosts to VLANs. It uses VAP VIDs only for hosts that do not have network policies or if it cannot communicate with the controller. For more information, refer to “Network Policies” on page 22.

To configure VAPs, perform the following procedure:

1. Select **Manage** -> **VAP**.

   The management software displays the “Modify Virtual Access Point settings” window. Refer to Figure 11 on page 63.

2. Use the **Radio** pull-down menu above the list of VAPs to select a radio. Menu options 1 and 2 are the 2.4 and 5 GHz radios, respectively. The default is radio 1. You can configure only one radio at a time.

3. Configure the VAPs. The parameters are described in Table 6 on page 63.

   To display the security settings of a VAP, click its “+” button in the right column.

4. After configuring VAP parameters, click the **Update** button to activate and save your changes.

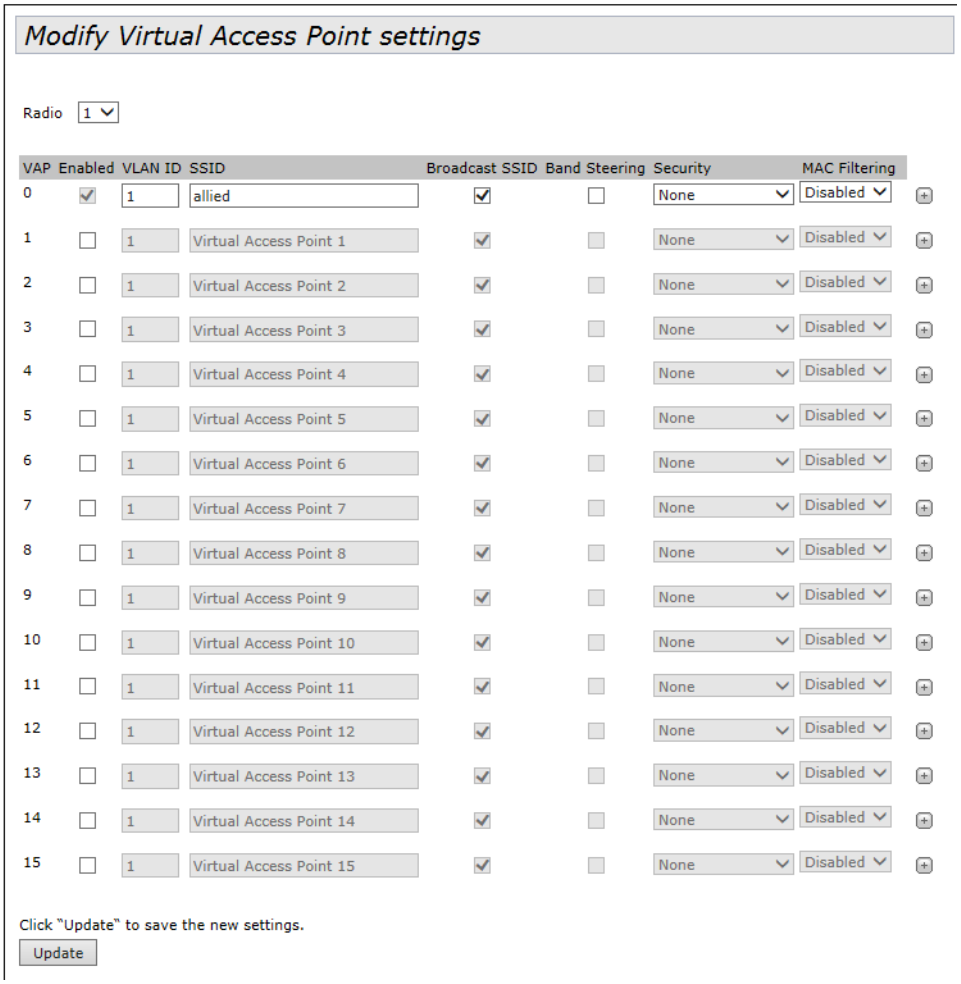


Figure 11. Modify Virtual Access Point Settings Window

Table 6. Modify Virtual Access Point Settings Window

Column	Description
VAP	Displays the ID number of the VAP. The VAPs are number 0 to 15. You cannot change this parameter.
Enabled	Enables or disables the VAP. The VAP is enabled when the check box has a check mark and disabled when it is empty. Here are the guidelines to enabling or disabling the VAP: - You can configure more than one VAP at a time.

Table 6. Modify Virtual Access Point Settings Window (Continued)

Column	Description
Enabled (continued)	- You cannot edit a VAP when it is disabled. -A disabled VAP does not forward network traffic.
VLAN ID	Specifies the 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. - VAP VIDs are ignored for wireless hosts that receive their VID assignments from network policies on the SES controller. VIDs from the SES controller take precedence over VAP VIDs. For more information, refer to “Network Policies” on page 22.
SSID	Specifies a name for the VAP. Here are the guidelines: - A VAP must have a name. - A name can be from 1 to 32 characters. - Spaces are allowed. - You may assign the same name to more than one VAP.
Broadcast SSID	Enables or disables broadcasting the SSID of the VAP by the access point. When the dialog box has a check mark, the default setting, the access point transmits the SSID to advertise the VAP to the clients. When the dialog box is empty, the access point does not advertise the VAP. Clients who want to connect to a VAP that is not advertised have to know its name.

Table 6. Modify Virtual Access Point Settings Window (Continued)

Column	Description
Band Steering	Enables or disables band steering on the VAP. The access point uses band steering to reduce congestion on the VAPs of the 2.4GHz radio by forcing some wireless clients that support both 2.4GHz and 5GHz to associate with the corresponding VAPs on the 5GHz radios. Here are the guidelines: - To implement band steering on a VAP on the 2.4GHz radio, you must enable the same VAP and SSID name on the 5GHz radio. For instance, to use band steering on VAP ID 4 on the 2.4GHz radio, you must enable VAP ID 4 on the 5GHz radio and set both VAPs to the same SSID name. - Ideally, the security settings should be the same on the 2.4GHz and 5GHz VAPs where band steering is enabled. For example, if you enable band steering on VAP ID 5 on the 2.4GHz radio and set the security level to WPA Personal, you should set VAP ID 5 on the 5GHz radio to the same security level and key.
Security	Specifies the security method for the VAP. The security methods are described in the following sections: - “No Security (None)” on page 66 - “IEEE 802.1x Security” on page 66 - “Static WEP” on page 68 - “WPA Enterprise” on page 71 - “WPA Personal” on page 73 The default security level for VAPs is None, which does not provide authentication or packet encryption.

Table 6. Modify Virtual Access Point Settings Window (Continued)

Column	Description
MAC Filtering	Enables or disables MAC address authentication. When the feature is enabled, the access point authenticates wireless clients of the VAP by their MAC addresses. This feature is not compatible with the OpenFlow protocol and should be disabled, the default setting, when the access point is used with the SES controller.

No Security (None)

The None security is intended for VAPs that do not employ encryption or authentication for their wireless clients. This is the default setting.

IEEE 802.1x Security

The guidelines for IEEE 802.1x security are listed here:

- This security method requires an external RADIUS server capable of EAP.
- The authentication server must have Protected EAP (PEAP) and MSCHAP V2 to support Windows clients.
- The clients and VAPs must use the same authentication method.
- This security is only supported in IEEE 802.11b/g and 802.11a modes.

The IEEE 802.1x security parameters are shown in Figure 12 and described in Table 7 on page 67.

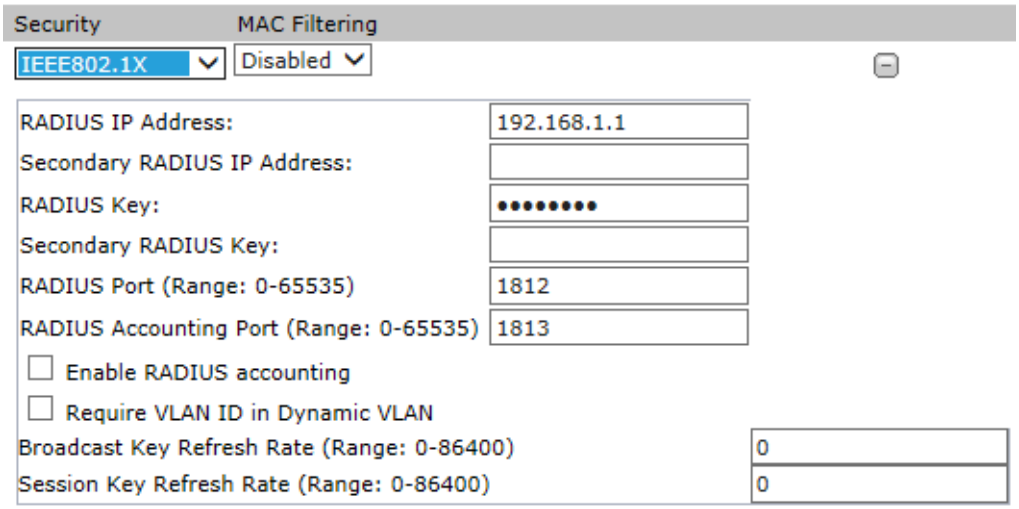


Figure 12. 802.1x Authentication for VAPs

Table 7. IEEE 802.1x

Field	Description
RADIUS IP Address	Enter the IPv4 address of the primary RADIUS server.
Secondary RADIUS IP Address	Enter the IPv4 address of the 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.
RADIUS Key	Enter the shared secret key for the primary RADIUS server. The key can be up to 64 characters and can consist of letters, numbers, and special characters. The key is case-sensitive. This key must be the same as the key on the server.
Secondary RADIUS Key	Enter the shared secret key for the secondary RADIUS server.
RADIUS Port (Range: 0 - 65535)	Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must use the same port number. The default is 1812.
RADIUS Accounting Port (Range: 0 - 65535)	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 default is 1813.
Enable RADIUS Accounting	Enable or disable RADIUS accounting by clicking the dialog box. The feature is enable when the dialog box has a check mark and disabled when the dialog box is empty. The default setting for accounting is disabled.

Table 7. IEEE 802.1x (Continued)

Field	Description
Require VLAN ID in Dynamic VLAN	Enable or disable whether wireless clients receive their VIDs from their accounts on the RADIUS server. When the dialog box has a check mark, the feature is enabled and the wireless clients receive their VIDs from the RADIUS server when they are authenticated. The feature is disabled when the dialog box is empty. The default setting is disabled. The SES controller and OpenFlow protocol do not support this feature. VLAN assignments for wireless hosts should come from the SES controller. Leave the feature disabled, the default setting, with the check mark empty.
Broadcast Key Refresh Rate (Range: 0 - 86400)	Specify the refresh rate for the broadcast (group) key for VAP clients. The range is 0 to 86400 seconds. The default is 0 seconds. The value 0 disables to refresh rate so that the broadcast key is not refreshed.
Session Key Refresh Rate (Range: 0 - 86400)	Specify the refresh rate for the session (unicast) key for VAP clients. The range is 0 to 86400 seconds. The default is 0 seconds. The value 0 disables the refresh rate so that the unicast key is not refreshed.

Static WEP

The parameter settings for static WEP security are shown in Figure 13 on page 69 and defined in Table 8 on page 69. This security level is available in IEEE 802.11b/g and 802.11a modes.

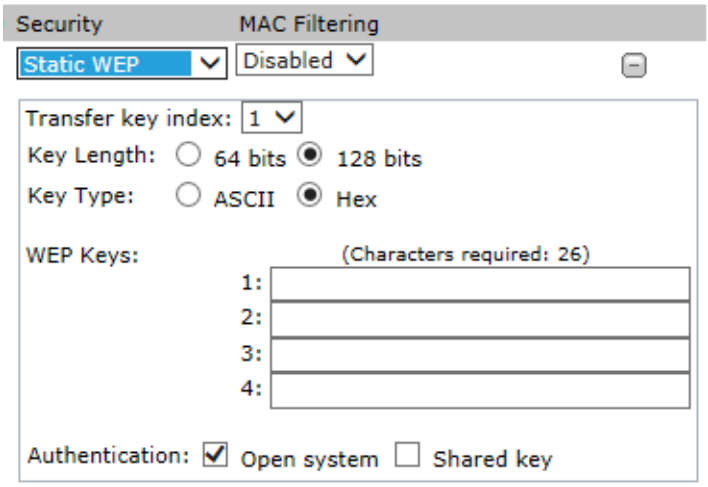


Figure 13. Static WEP Encryption for VAPs

Table 8. Static WEP

Field	Description
Transfer Key Index	Select the key the access point should use to encrypt network traffic.
Key Length	Select the key length of 64 or 128 bits. The default is 128 bits.
Key Type	Select whether the key is ASCII or hexadecimal. The default is hexadecimal.
WEP Keys	Enter up to four WEP keys in the fields numbered 1 to 4. The key lengths and types determine the lengths and formats of the keys. The order of the keys has be the same on the access point and clients. Here are the guidelines for ASCII keys: - An ASCII key may contain upper and lower characters and the numbers 0 to 9. - An ASCII key is case-sensitive. - The key length of 64 bits requires five ASCII characters. - The key length of 128 bits requires 13 ASCII characters.

Table 8. Static WEP (Continued)

Field	Description
WEP Keys (continued)	Here are the guidelines for hexadecimal keys: - A hexadecimal key can contain the letters A to F and numbers 0 to 9. - The key length of 64 bits requires 10 hexadecimal characters. - The key length of 128 bits requires 26 hexadecimal characters.
Authentication	Specify whether or not the access point authenticates VAP clients. The options are described here. - Open System: The access point does not authenticate the VAP clients. All clients, even those without the correct WEP keys, are allowed to connect to the access point. This is the default setting. (Clients in an open system VAP still must have the correct WEP key to encrypt and decrypt the traffic they exchange with the access point.) - Shared Key: Clients must have the correct WEP key to connect with the access point. Clients without the correct WEP key may not associate with the device. Both Open System and Shared Key: Clients configured in WEP shared key mode must have the correct WEP key to connect to the access point. Clients configured in WEP open system mode do not need the correct WEP key to connect to the access point.

WPA Enterprise

The WPA Enterprise security parameters are shown in Figure 14 and defined in Table 9.

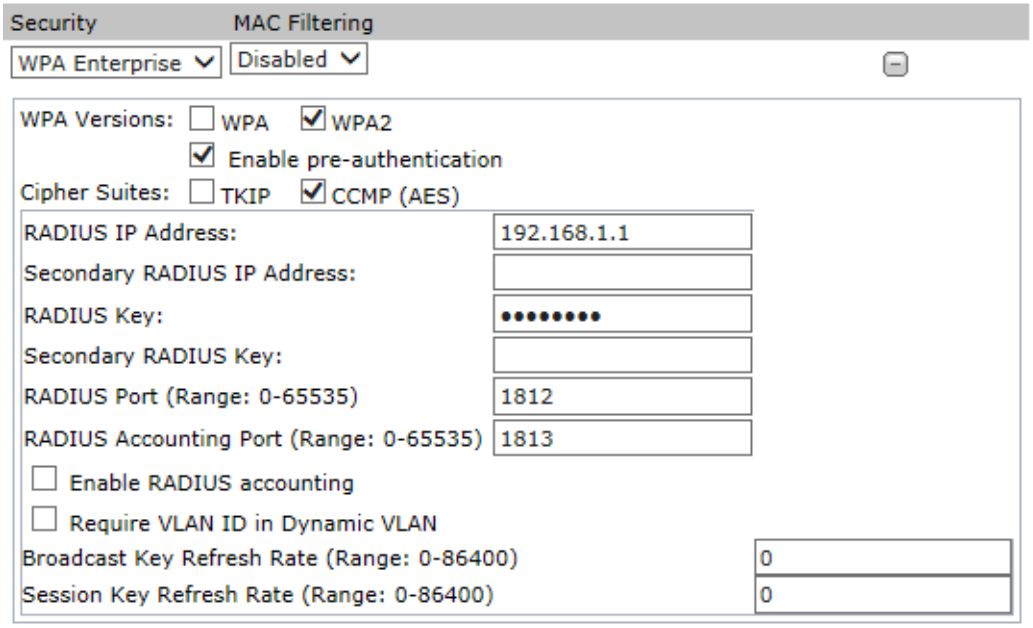


Figure 14. WPA Enterprise for VAPs

Table 9. WPA Enterprise

Field	Description
WPA Versions	Select the WPA version. The options are listed here: - WPA: Select this option if all the wireless clients of the VAP support WPA, but not WPA2. - WPA2: Select this option if all the clients support WPA2, but not WPA. This is the default setting. - Both WPA and WPA2 - Select both options if the VAP has both WPA and WPA2 clients.

Table 9. WPA Enterprise (Continued)

Field	Description
WPA Versions (continued)	- Enable-pre-authentication: Select this option if the VAP has WPA2 clients and you want the access point to share the pre-authentication packets from the clients with other access points. This can speed up authentication for roaming clients who connect to multiple access points. This option does not apply to WPA clients. The SES controller and OpenFlow protocol do not support pre-authentication on the access point. You should disable this option by removing the check mark from the dialog box.
Cipher Suites	Select CCMP (AES) as the cipher suite for the VAP. The SES controller and OpenFlow protocol do not support TKIP or both TKIP and CCMP.
RADIUS IP Address	Enter the IPv4 address of the primary RADIUS server.
Secondary RADIUS IP Address	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.
RADIUS Key	Enter the shared secret key for the primary RADIUS server. The key can be up to 64 characters and can consist of letters, numbers, and special characters. The key is case-sensitive. This key must be same on the access point and server.
Secondary RADIUS Key	Enter the shared secret key for the secondary RADIUS server.
RADIUS Port (Range: 0 - 65535)	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 default is 1812.

Table 9. WPA Enterprise (Continued)

Field	Description
RADIUS Accounting Port (Range: 0 - 65535)	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 default is 1813.
Enable RADIUS Accounting	Enable or disable RADIUS accounting by clicking the dialog box. The feature is enable when the dialog box has a check mark and disabled when the dialog box is empty. The default setting for accounting is disabled.
Require VLAN ID in Dynamic VLAN	Enable this option to require that the wireless clients of the VAP be assigned VLAN IDs from the RADIUS server. When this option is enabled, the VAP does not accept clients that are not assigned VLAN IDs by the RADIUS severs. The option is enabled when it has a check mark. The default setting is disabled. The SES controller and OpenFlow protocol do not support this feature. VLAN assignments for wireless hosts should come from the SES controller. Leave the feature disabled, the default setting, with the check mark empty.
Broadcast Key Refresh Rate (Range: 0 - 86400)	Specify the refresh interval rate for the broadcast (group) key. The range is 0 to 86400 seconds. The value 0 prevents the key from being refreshed.
Session Key Refresh Rate (Range: 0 - 86400)	Specify the refresh interval rate for the session (unicast) keys. The range is 0 to 86400 seconds. The value 0 prevents the keys from being refreshed.

WPA Personal

The options for WPA Personal are shown in Figure 15 on page 74 and defined in Table 10 on page 74.

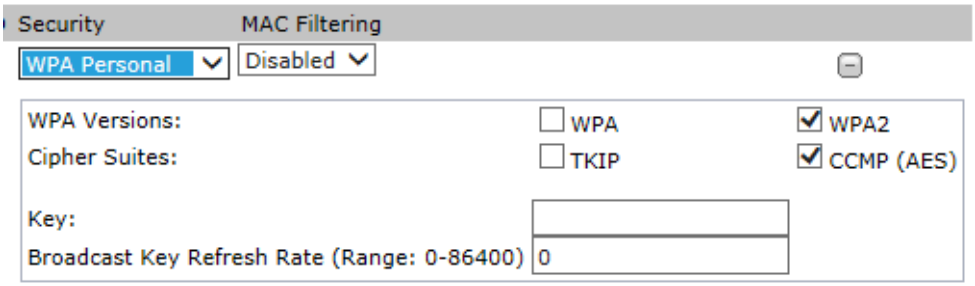


Figure 15. WPA Personal for VAPs

Table 10. WPA Personal

Field	Description
WPA Versions	Select the WPA version. The options are listed here: - WPA: Select this option if the VAP wireless clients support WPA, but not WPA2. - WPA2: Select this option if the clients support WPA2, but not WPA. This is the default setting. - Both WPA and WPA2 - Select both options if the VAP has both WPA and WPA2 clients.
Cipher Suites	Select CCMP (AES) as the cipher suite for the VAP. The SES controller and OpenFlow protocol do not support TKIP or both TKIP and CCMP.
Key	Enter a shared secret key of 8 to 63 alphanumeric characters. The key can include special characters.
Broadcast Key Refresh Rate (Range: 0 - 86400)	Specify the refresh interval rate for the broadcast (group) key. The range is 0 to 86400 seconds. The value 0 prevents the key from being refreshed. The default is 0 seconds.

Configuring the OpenFlow Protocol

To configure the access point for the OpenFlow protocol and SES controller, perform the following procedure:

1. Select **Manage** -> **OpenFlow**.

   The OpenFlow Configuration and Settings window is shown in Figure 16.

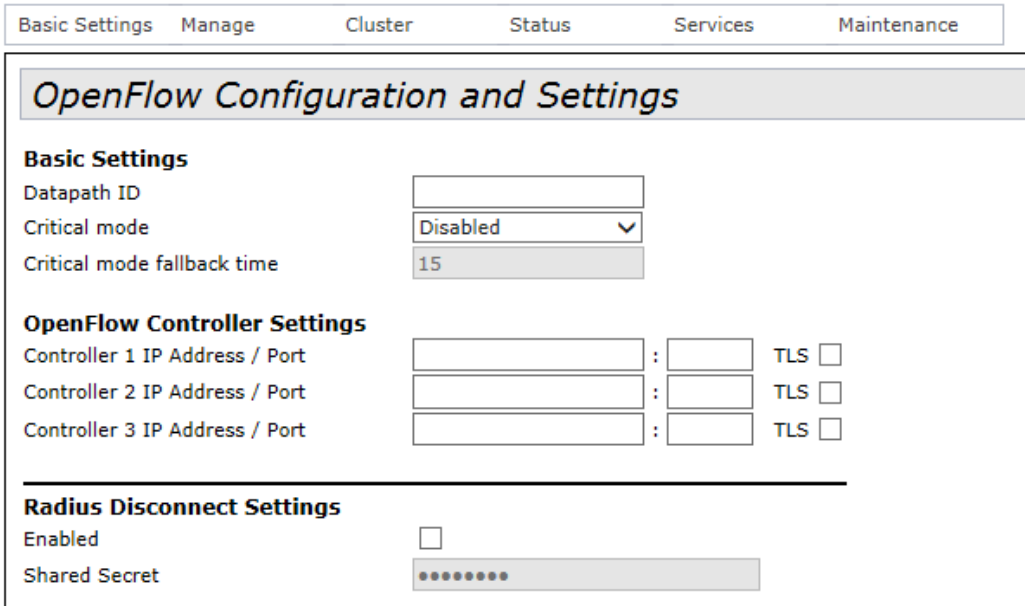


Figure 16. OpenFlow Configuration and Settings Window

2. Configure the OpenFlow protocol settings. The parameters are described in Table 11.

3. After configuring VAP parameters, click the **Update** button to activate and save your changes.

Table 11. OpenFlow Configuration and Settings Window

Parameter	Description
Datapath ID	Enter a unique identifier of 16 hexadecimal digits for the wireless access point. The controller identifies the device by this number. Each OpenFlow switch and access point must have its own unique datapath ID.

Table 11. OpenFlow Configuration and Settings Window (Continued)

Parameter	Description
Datapath ID (continued)	This field does not display the default value. The wireless access point uses its default value when the field is empty. The default is the device's MAC address preceded by four zeros (0000). For example, if the wireless access point has the MAC address 00:1A:E6:39:65:44, its default datapath ID would be: 0000001AE6396544 To view the MAC address of the unit, select Basic Settings from the main menus. Changing the datapath ID of the access point after it has established communications with the SES controller may result in two entries for the device in the controller. One datapath ID will be the new value and the other will be the previous value, which will be obsolete. For this reason it is recommended that if you change this value, you should set it before the access point begins communicating with the controller.
Critical Mode	Select a critical mode option. This controls how the wireless access point responds if it loses communications with the SES controller. You can select only one critical mode: The options are listed here: - Disabled: The wireless access point continues forwarding traffic from known hosts using the OpenFlow flow rules it has already learned from the controller. It blocks all traffic from unknown hosts. Traffic from known hosts become blocked if their flow rules expire before communications with the controller are restored. Once communications with the controller are restored, the access point resumes learning flow rules and forwarding traffic from unknown hosts or hosts whose flow rules had expired. This is the default setting.

Table 11. OpenFlow Configuration and Settings Window (Continued)

Parameter	Description
Critical Mode (continued)	- Enabled (Accept All): The access point deletes all OpenFlow flow rules and functions as a non-OpenFlow access point, forwarding all packets based on the VIDs of the virtual access points (VAPs). Once communications with the controller are restored, the access point begins relearning the flow rules as it receives packets from the wireless hosts, and resumes forwarding packets based on the flow rules. - Enabled (Drop All): The access point deletes all flow rules and blocks all traffic from known and unknown wireless hosts until it reestablishes communications with the controller, after which it begins relearning flow rules.
Critical mode fallback time	Enter the amount of time in seconds that the access point tries to reestablish communications to the controller before activating the critical mode. The default is 15 seconds.
Controller IP Address / Port	Enter the IP address and protocol port number of the SES controller. You can enter up to three addresses.
TLS	Reserved for future development. Leave the check box empty.
Radius Disconnect Settings	Reserved for future development. Do not change the option settings.

Generating Event Messages for Unknown Access Points

The access point can alert you with event messages if it detects unknown access points. It stores the messages in the event log and can also send them to a syslog server on your network. Figure 17 is an example of the message.

```
Apr 22 09:10:45 syslog: Rogue AP found: The MAC address of the Rogue AP is
c0:8a:de:68:32
```

Figure 17. Event Message for Unknown Access Points

At pre-defined time intervals, the access point compares the MAC addresses of neighboring access points against a list of approved addresses that you create, and generates event messages for access points whose MAC addresses are not in the approved list.

Here are the feature guidelines:

- If you want the event messages sent to a syslog server, you must have a syslog server on your network and you need to configure the syslog client on the access point, as explained in “Configuring the Syslog Client” on page 88.
- You need to know the MAC addresses of known neighboring access points. You use the addresses to create a list of approved devices when you configure the feature. The access point does not send event messages for devices in the list. To view the MAC addresses of neighboring access points, refer to “Viewing Neighboring Access Points” on page 90.

Enabling Event Messages for Unknown Access Points

To configure the access point to generate event messages when it detects unknown access points, perform the following procedure:

1. Select **Manage** -> **Pre-Configured Rogue AP**.

   The access point displays the “Configure Pre-Configured Rogue AP” window shown in Figure 18 on page 79.

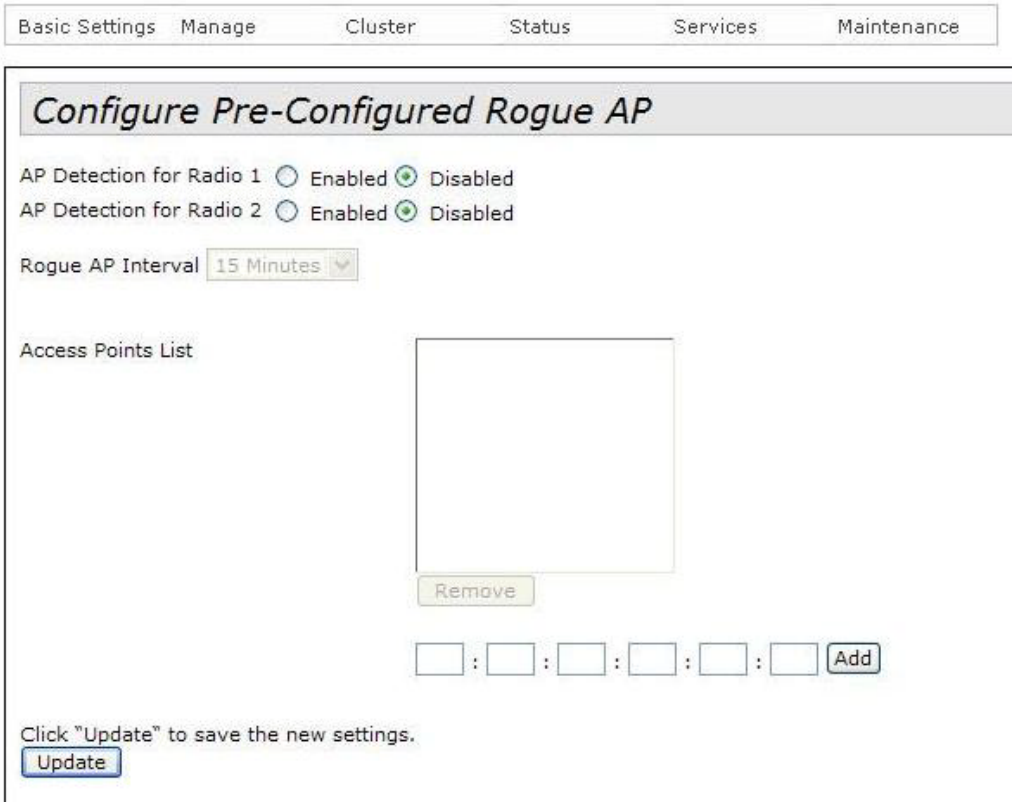


Figure 18. Configure Pre-Configured Rogue AP Window

2. Click the **Enabled** circles for the AP Detection for Radio options. Radios 1 and 2 are the 2.4 and 5 GHz radios, respectively.

   You can activate one or both radio detections. If you are only interested in receiving event messages of unknown access points on one radio, activate that radio detection. If you are interested in receiving event messages for both radios, enable both options.

   Note
   You cannot configure the feature parameters until you enable at least one of the access point detections.

3. Use the **Rogue AP Interval** pull-down menu to select the intervals at which the device tests for unknown access points. The range is 15 minutes to four weeks. The default is 15 minutes.

4. If there are neighboring access points that you want to add to the approved list so that the access points does not generate event messages when it detects them, enter the address of one of them in the fields below the list and click the Add button. You can add only one MAC address at a time.

5. Repeat step 4 to add more access points to the approved list. You may add up to 200 addresses.

6. To remove a MAC address from the list, click the address and then click the **Remove** button. You may delete only one address at a time from the list.

7. Click the **Update** button to activate and save your changes.

   The access point tests for unknown access points when you click the Update button and, if it finds an unknown device, enters an event message in the event log and sends the message to the syslog server. The access point repeats the test at the next time interval.

Disabling Event Messages for Unknown Access Points

To stop the access point from generating event messages when it detects unknown access points, perform the following procedure:

1. Select **Manage** -> **Pre-Configured Rogue AP**.

   The access point displays the “Configure Pre-Configured Rogue AP window” shown in Figure 18 on page 79.

2. Click the **Disabled** circles for the AP Detection for Radio options. Radios 1 and 2 are for the 2.4 and 5 GHz radios, respectively.

3. Click the **Update** button to activate and save your changes.

   The access point stops generating event messages for unknown access points.

Chapter 4

Status Menu

This chapter describes the management functions of the Status menu. The chapter contains the following sections:

Viewing the Associated Clients of an Access Point

To view a list of the associated clients on the access point and the amount of traffic, select **Status** -> **Client Associations Settings**. The access point displays the “View list of currently associate client stations” window. An example is shown in Figure 19.

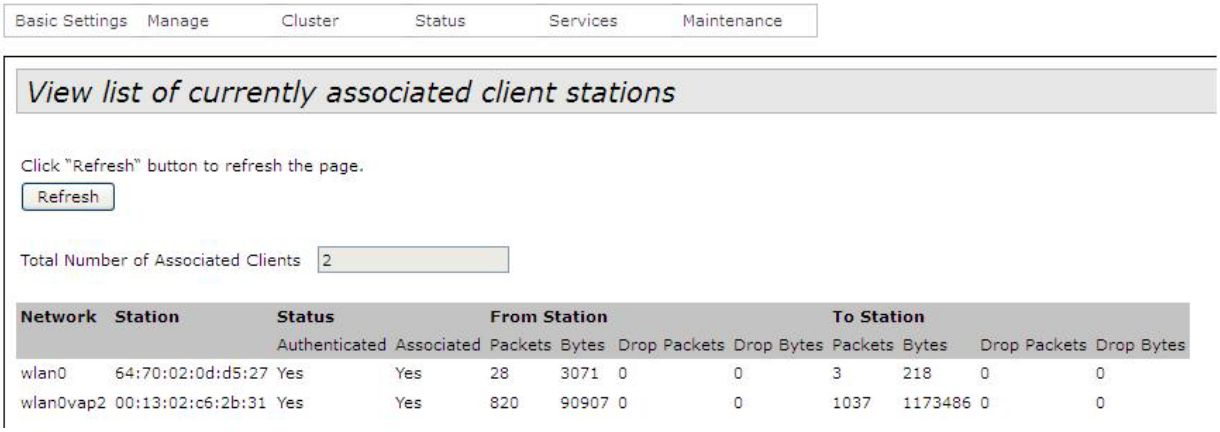


Figure 19. View List of Currently Associated Client Stations

The columns in the window are described in Table 12.

Table 12. View List of Currently Associated Client Stations Window

Column	Description
Network	Displays the radio and VAP where a client is associated. Here is an example of an entry: wlan0vap2 The “wlan#” is the radio where the client is associated. The entry “wlan0” is the 2.4 GHz radio 1 and “wlan1” is the 5 GHz radio 2. The “vap#” is the VAP where the client is associated. The number is the VAP number.
Station	Displays the MAC address of the wireless client.

Table 12. View List of Currently Associated Client Stations Window

Column	Description
Status	
Authenticated	Displays whether a client has been authenticated. (This column does not display IEEE802.1x authentication status, but the underlying status, which is independent of the security level.)
Associated	Displays whether a client is associated with the access point.
From Station	
Packets	Displays the number of packets the access point has received from a client.
Bytes	Displays the number of packet bytes the access point has received from a client.
Drop Packets	Displays the number of packets the access point has dropped after receiving them from a client.
Drop Bytes	Displays the number of packet bytes the access point has received and dropped.
To Station	
Packets	Displays the number of packets the access point has transmitted to a client.
Bytes	Displays the number of packet bytes the access point has transmitted to a client.
Drop Packets	Displays the number of packets the access point has dropped before transmitting them to a wireless client.
Drop Bytes	Displays the number of packet bytes the access point has dropped before transmitting them to a wireless client.

Viewing Event Messages

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 event log. The events and the vital information about system activity that they provide can help in identifying and resolving system problems.

The access point has two types of event messages:

- System messages
- Kernel messages

System messages cover a variety of events, such as authentications of 802.1x wireless users and hardware or software problems. They are divided by severity into the following categories:

- 0 - Emergency
- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warning
- 5 - Notice
- 6 - Informational
- 7 - Debug

System event messages are stored in the event log on the access point and can be viewed from web browser management sessions of the device, as explained in “Viewing System Event Messages” on page 85. The access point can also send the messages to a syslog server on your network for more permanent storage. This is described in “Configuring the Syslog Client” on page 88.

System event messages can be stored in either volatile or non-volatile memory. Messages stored in volatile memory, the default setting, are discarded whenever the unit is reset or powered off.

System event messages stored in non-volatile memory retained even when the unit is powered off or reset. This can be useful if you are troubleshooting a problem with the unit or network. However, using non-

volatile memory for this purpose can prematurely degrade the memory, which can lead to performance problems of the unit. For this reason, you should use non-volatile memory to store event messages only for short periods of time, such as when troubleshooting a network problem.

A better option for permanently storing messages is to have the access point use its syslog client to send its messages to a syslog server on your network. A syslog log server can be located on the wireless or wired part of your network because the access point transmits the messages from both its radios and LAN port.

Kernel event messages are generated by the main component of the management software and generally reflect error conditions, such as dropped frames. Unlike system messages, kernel messages cannot be viewed from web browser management sessions. They can only be viewed on a syslog server. Viewing these messages requires a syslog server to store the messages.

System and kernel messages include the following information:

- Time and date of the event
- Severity of the event
- Feature or management module that generated the event
- Event description

Viewing System Event Messages

To view the system event messages in the event log, select **Status** -> **Events**. The “View events generated by this access point” window is displayed. An example is shown in Figure 20 on page 86.

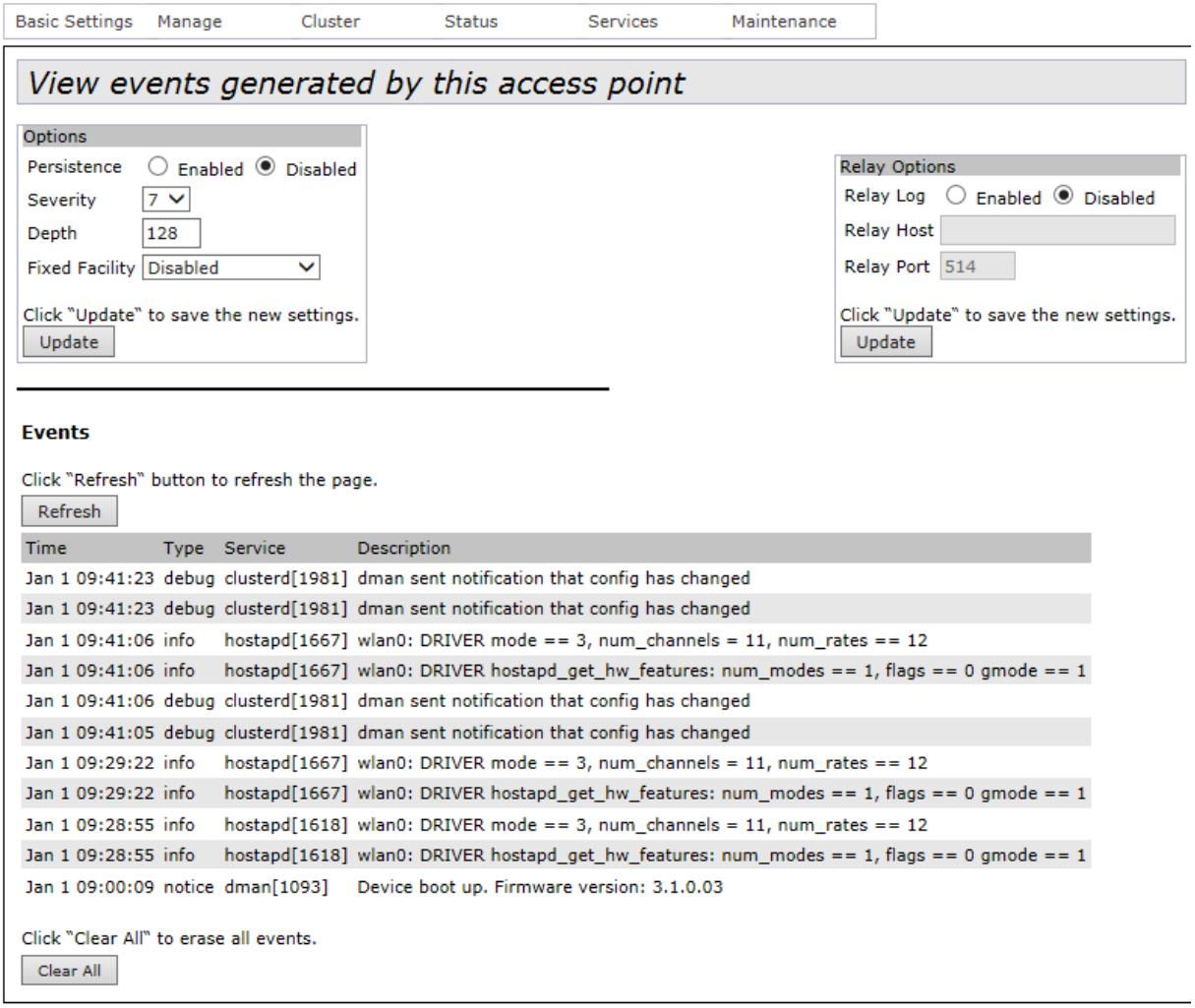


Figure 20. View Events Generated by this Access Point Window

The system messages are displayed from newest to oldest in a table in the Events section of the window. The table columns are described in Table 13.

Table 13. Event Messages Table

Field	Description
Time	Date and time when a message was generated.
Type	The severity level of the message.
Service	The module in the management software that generated the message.
Description	Description of the message.

The table has two buttons:

- Refresh - Use this button to update the table with the latest messages.
- Clear All - Use this button to delete all the messages in the log.

Configuring the Event Log

You can configure the following event log parameters:

- Whether the event messages are stored in volatile or non-volatile memory. Messages stored in volatile are discarded when the access point is reset or powered off. Messages stored in non-volatile memory are retained when the device is reset or powered off.
- The severity of the displayed messages.
- The number of displayed messages.
- Whether all the messages are assigned the facility level 0, kernel messages, to make them compatible with the AT-TQ2403 Access Point.

To configure the event log, perform the following procedure:

1. Select **Status** -> **Events**.

   The access point displays the “View events generated by this access point” window. Refer to Figure 20 on page 86.

2. To store the messages in non-volatile memory in the access point, click the **Enabled** selection for the **Persistence** parameter. To stop the access point from storing messages in non-volatile memory, click the **Disabled** dialog circle.

   Note
   Event messages should be stored in non-volatile memory only for short periods of time, such as when troubleshooting network problems. Using non-volatile memory to store messages for extended periods can degrade the memory, possibly leading to performance problems for the access point.

3. To limit the messages by severity level, select the **Severity** pull-down menu and select a new value. The range is 0 to 7. The default is 7.

   The access point displays messages of the selected value and all numerically lower (higher severity) levels. For example, selecting severity level 3 displays the messages for levels 0 to 3. The default level 7 displays all messages.

   The Severity parameter applies to messages in volatile and non-volatile memories.

4. To increase or decrease the number of displayed event messages, select the **Depth** field and enter a new value. The range is 1 to 128 messages. The default is 128 messages.

   The Depth parameter applies to messages in volatile and non-volatile memories.

5. To assign a fixed facility code to the messages, select the code from the **Fixed Facility** pull-down menu. You can select only one code. If you want the access point to base the facility codes on the services of the management software, select **Disabled** from the pull-down menu. This is the default setting.

   You cannot view the facility codes of the event messages from the event log. They can only be viewed on a syslog server.

6. Click the **Update** button to activate and save your changes.

Configuring the Syslog Client

This procedure explains how to configure the syslog client. The access point uses the client to send its system and kernel event messages to a syslog server on your network. The messages are sent from the LAN port and radios.

To configure the syslog client, perform the following procedure:

1. Select **Status** -> **Events**.

   The access point displays the “View events generated by this access point” window. Refer to Figure 20 on page 86.

2. Use the **Severity** pull-down menu in the Options section to select the severity of system messages to be transmitted to the syslog server.

   The access point transmits the system messages of the selected level and all numerically lower (higher severity) messages. For example, if you select level 3, error, the device transmits system messages from levels 0 to 3. The default is level 7, debug. This is the highest value, so all messages are sent.

   The severity level setting does not apply to kernel messages.

3. Use the **Fixed Facility** pull-down menu to assign a fixed facility code to the messages. You may select only one code. If you want the access point to base the facility codes on the services of the management software, select Disabled from the pull-down menu. This is the default setting.

   The Facility levels of the messages can only be viewed on a syslog server. They are not displayed in the event log of the access point.

4. Click the **Enabled** selection for the **Relay Log** option in the Relay Options section of the window. You have to enable the feature to configure its parameters.

5. Enter the IP address or DNS name of your syslog server in the **Relay Host** field in the Relay Options section of the window. You can enter only one server.

6. To change the syslog port number, enter a new value in the **Relay Port** field. The default is port 514.

7. Click the **Update** button to activate and save your changes.

   The access point begins to transmit its system and kernel messages to the designated syslog server. Only new messages are sent. The device does not transmit any system messages that are already stored in the event log.

Disabling the Syslog Client

To disable the syslog client to stop the access point from sending its system and kernel messages to a syslog server, perform the following procedure:

1. Select **Status** -> **Events**.

   The access point displays the “View events generated by this access point” window. Refer to Figure 20 on page 86.

2. In the Relay Options section of the window, click the **Disabled** selection for the Relay Log option.

3. Click the **Update** button to activate and save your changes.

Viewing Neighboring Access Points

You can view basic information and statistics about other access points within range of the access point you are managing by selecting the Neighboring Access Points option from the Status menu. The window is shown in Figure 21.

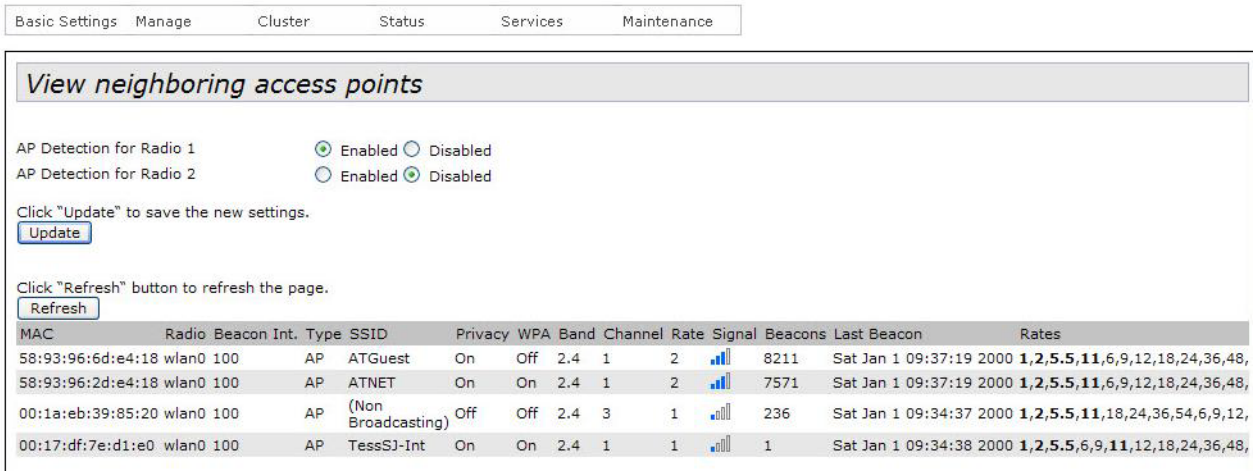


Figure 21. View Neighboring Access Points Window

You can use the AP Detection for Radio options in the window to configure the table to display the neighboring access points discovered on one or both radios. Use the Update button to save your change.

The information in the table is not retain when the access point is reset or powered off. The columns in the table are described in Table 14.

Table 14. Neighboring Access Point Settings Window

Column	Description
Beacon Int.	Displays the beacon interval of the neighboring access point.
Type	Indicates the type of device: AP: Indicates that the neighboring device is an access point that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode.

Table 14. Neighboring Access Point Settings Window (Continued)

Column	Description
Type (continued)	Ad hoc: Indicates that the neighboring device is operating in Ad hoc mode to directly communicate with other Ad hoc devices, without the use of traditional access points. Ad hoc mode is part of the IEEE 802.11 Wireless Networking Framework. It is also referred to as peer-to-peer mode and Independent Basic Service Set (IBSS).
SSID	Displays the Service Set Identifier (SSID) of the neighboring access point.
Privacy	Displays whether the neighboring access point has security: On: The neighboring access point has security. Off: The access point does not have security.
WPA	Displays the status of WPA on the neighboring access point.
Band	Displays the IEEE 802.11 mode of the access point: 2.4: Indicates IEEE 802.11b, 802.11g, 802.11n, or a combination of the modes. 5: Indicates IEEE802.11a, 802.11n, or both modes.
Channel	Displays the channel on which the access point is broadcasting.
Rate	Displays the transmission rate in megabits per second of the access point.
Signal	Displays signal strength. You may view the strength in decibels (dBm) by placing the mouse pointer over the bars.
Beacons	Displays the total number of beacons received from the neighboring access point since it was discovered.

Table 14. Neighboring Access Point Settings Window (Continued)

Column	Description
Last Beacon	Displays the date and time of the most recent beacon from the neighboring access point.
Rates	Displays the supported and basic (advertised) rate sets in megabits per second (Mbps) for the neighboring access point. All supported rates are listed, with basic rates shown in bold.

Displaying Status and Statistics

To display status information and statistics about the LAN port and radios, select **Status** -> **Transmit Receive Settings**. The selection displays the "View transmit and receive statistics for this access point" window, which has these three tables.

- The first table displays basic status information about the LAN port and radios. The radio information is divided by virtual access points (VAPs).
- The second table, labeled Transmit, displays the number of packets and bytes transmitted by the LAN port and radios.
- The third table, labeled Receive, displays the number of packets and bytes received by the LAN port and radios.

For instructions on how to configure VAPs, refer to "Configuring Virtual Access Points" on page 62.

The status table in the window is shown in Figure 22.

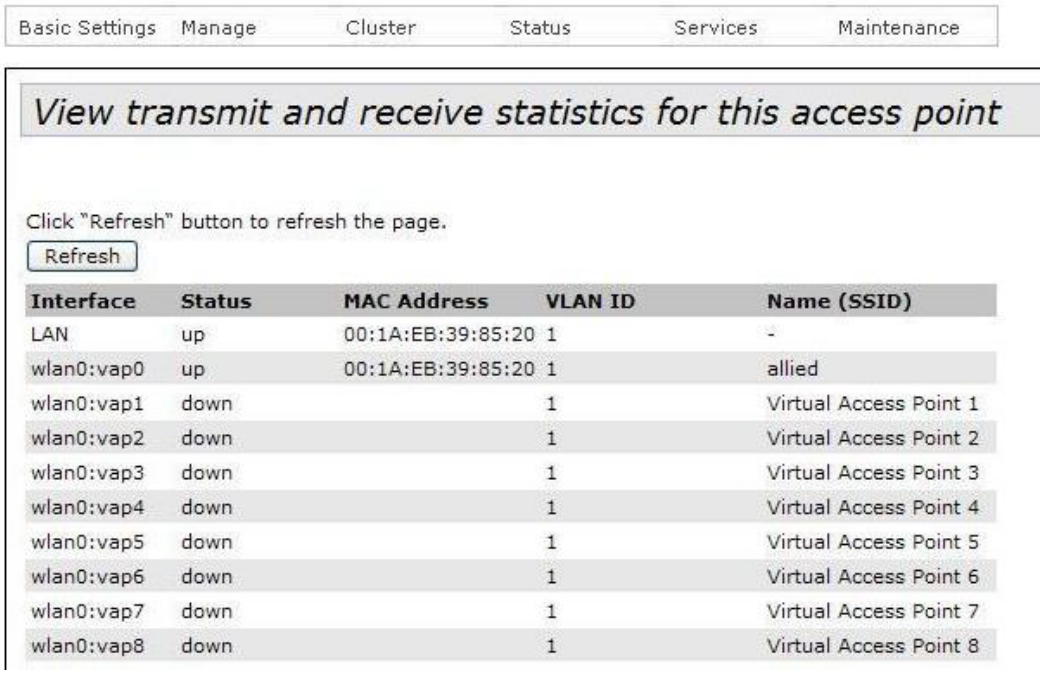


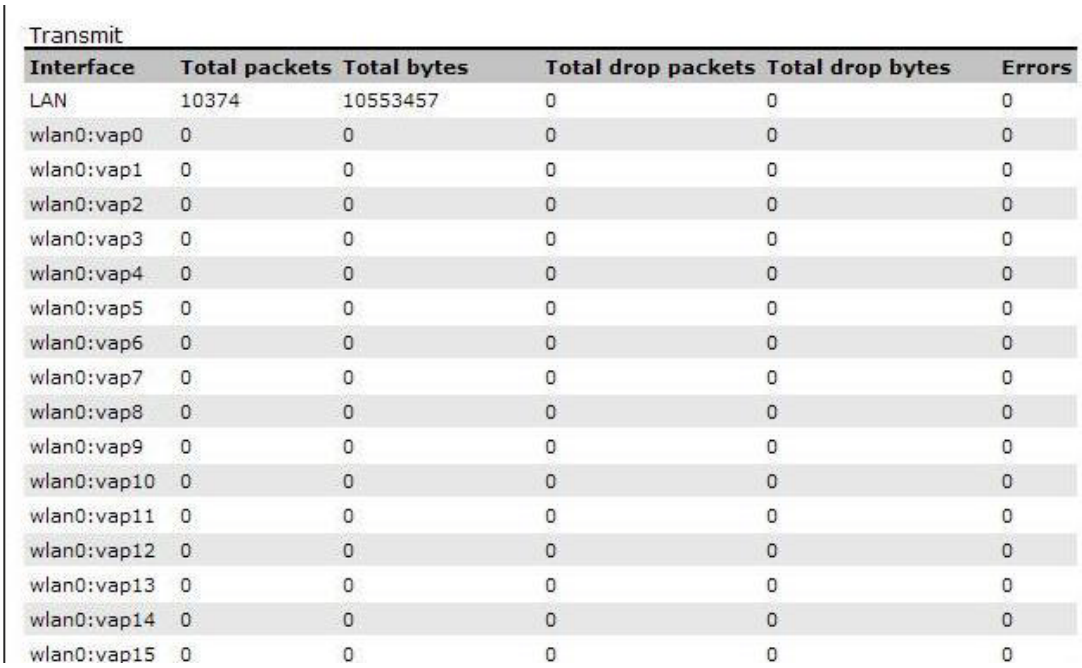
Figure 22. Status Table in the View Transmit and Receive Statistics for this Access Point Window

The columns are described in Table 15.

Table 15. Status Table Information

Column	Description
Interface	Displays the access point interfaces, listed here: - LAN, The LAN port on the rear panel of the access port. - wlan0: 2.4 GHz radio 1 VAPs. - wlan1: 5 GHz radio 2 VAPs. - VAP#: VAP number. Each radio has sixteen VAPs.
Status	Displays the status of the interfaces. The possible states are listed here: - LAN: Up: The LAN port has a valid connection to a port on a network device. - LAN: Down: The LAN port does not have a valid connection to a port on a network device. wlan#:vap#: Up: The VAP is enabled. wlan#:vap#: Down: The VAP is disabled.
MAC Address	Displays the MAC address of the interface. The LAN port and radio 1 (wlan0) share the same MAC address.
VLAN ID	Displays the VID of the VAP. To view the VIDs of wireless hosts, refer to the SES Controller and OpenFlow Protocol User’s Guide.
Name (SSID)	Displays the network name of the interface.

The Transmit statistics table is shown in Figure 23 on page 95.



Transmit

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	10374	10553457	0	0	0
wlan0:vap0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	0	0	0	0	0
wlan0:vap3	0	0	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0

Figure 23. Transmit Statistics Table of the View Transmit and Receive Statistics for this Access Point Window

The columns are described in Table 16.

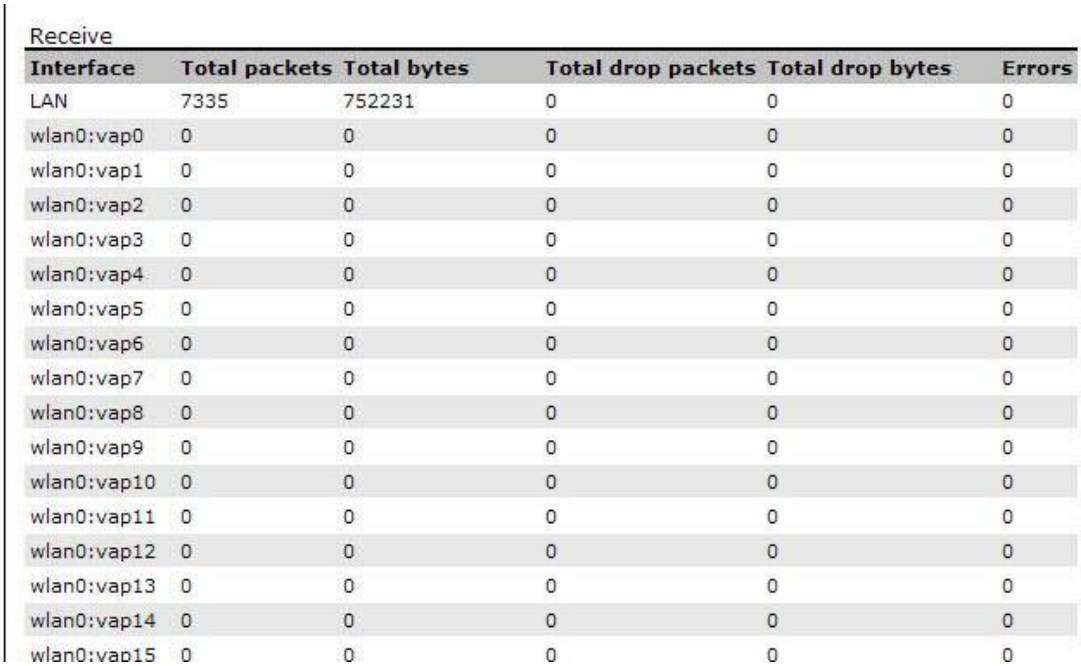
Table 16. Transmit Statistics Table

Column	Description
Interface	Displays the access point interfaces, listed here: - LAN, The LAN port on the rear panel of the access port. - wlan0: 2.4 GHz radio 1 VAPs. - wlan1: 5 GHz radio 2 VAPs. - VAP#: VAP number. Each radio has sixteen VAPs.
Total packets	Displays the total number of packets the interfaces have transmitted.
Total bytes	Displays the total number of bytes the interfaces have transmitted. The values do not include the amount of padding for packets below the minimum size, and for FCS.

Table 16. Transmit Statistics Table (Continued)

Column	Description
Total drop packets	Displays the total number of packets the access point discarded before transmission.
Total drop bytes	Displays the total number of bytes the access point discarded before transmission.
Errors	Displays the total number of packets with errors, such as CRC errors.

The Receive statistics table is shown in Figure 24.



Receive

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	7335	752231	0	0	0
wlan0:vap0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	0	0	0	0	0
wlan0:vap3	0	0	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0

Figure 24. Receive Statistics Table of the View Transmit and Receive Statistics for this Access Point Window

The columns are described in Table 17 on page 97.

Table 17. Receive Statistics Table

Column	Description
Interface	Displays the access point interfaces, listed here: - LAN, The LAN port on the rear panel of the access port. - wlan0: 2.4 GHz radio 1 VAPs. - wlan1: 5 GHz radio 2 VAPs. - VAP#: VAP number. Each radio has sixteen VAPs.
Total packets	Displays the total number of packets the interfaces have received.
Total bytes	Displays the total number of bytes the interfaces have received.
Total drop packets	Displays the total number of packets the access point dropped after receiving them on the interfaces.
Total drop bytes	Displays the total number of bytes the access point dropped after receiving them on the interfaces.
Errors	Displays the total number of packets with errors, such as CRC errors.

Viewing Basic IP Configuration and Radio Information

To view basic configuration information about the LAN port and radios, select **Status** -> **Interfaces**. This displays the “View settings for network interfaces” window, shown in Figure 25.

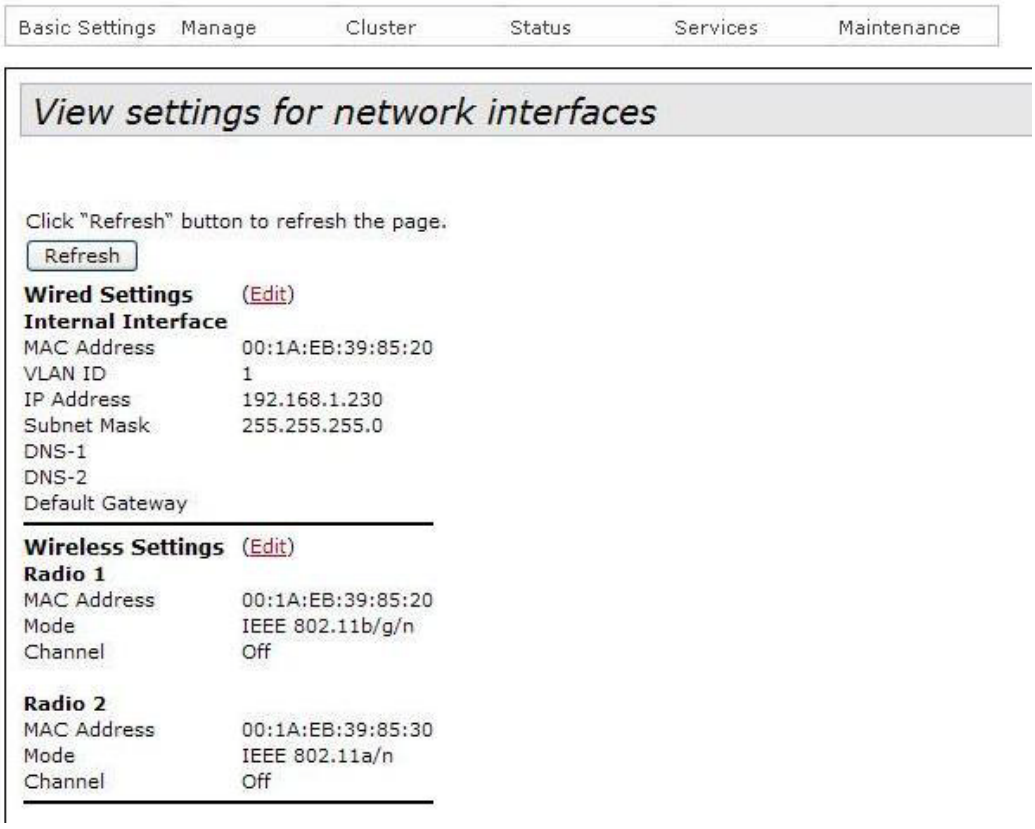


Figure 25. View Settings for Network Interfaces Window

The top section of the window displays the MAC and IP addresses of the access point, along with the subnet mask, default gateway, and domain name servers. To configure the settings, click **Edit** to display the “Modify Ethernet (Wired) settings” window, shown in Figure 8 on page 42. For instructions, refer to “Assigning a Static IPv4 Address to the Access Point” on page 42 and “Assigning a Dynamic IPv4 Address from a DHCP Server to the Access Point” on page 44.

The bottom section of the window displays the basic settings of the radios, including their MAC addresses, operational modes, and channels. To configure the settings, click **Edit** to display the “Modify wireless settings” window, shown in Figure 9 on page 47. For instructions, refer to “Configuring Basic Radio Settings” on page 49. To configure additional radio settings, refer to “Configuring the Radio Settings” on page 52.

Chapter 5

Services Menu

This chapter describes the management functions of the Services menu. The chapter contains the following sections:

Configuring SNMPv1 and v2c

You can use SNMPv1 or v2c to manage the access point and receive traps from the unit. Here are the guidelines to managing the device with SNMP:

- You can use SNMP to manage only a subset of the features of the device. You have to use the web browser interface to manage all the features.
- The access point does not support SNMPv3.
- The access point can have only one read-only community string and one read-write string.
- The MIB for the product is available from the Allied Telesis web site.
- The unit must have an IP address for SNMP management. For instructions, refer to “Assigning a Static IPv4 Address to the Access Point” on page 42 or “Assigning a Dynamic IPv4 Address from a DHCP Server to the Access Point” on page 44.

To enable or disable SNMP, perform the following procedure:

1. Select **Services** -> **SNMP Settings**.

   The access point displays the “SNMP Configuration” window. Refer to Figure 26 on page 101.

2. Click the **Enabled** dialog circle to enable SNMP or the **Disabled** dialog circle to disable it. You must enable SNMP before you can configure the parameter settings.

3. If you enabled SNMP, configure the parameters, as needed. The fields are described in Table 18 on page 102.

4. After configuring the parameters, click the **Update** button to activate and save your changes on the access point.

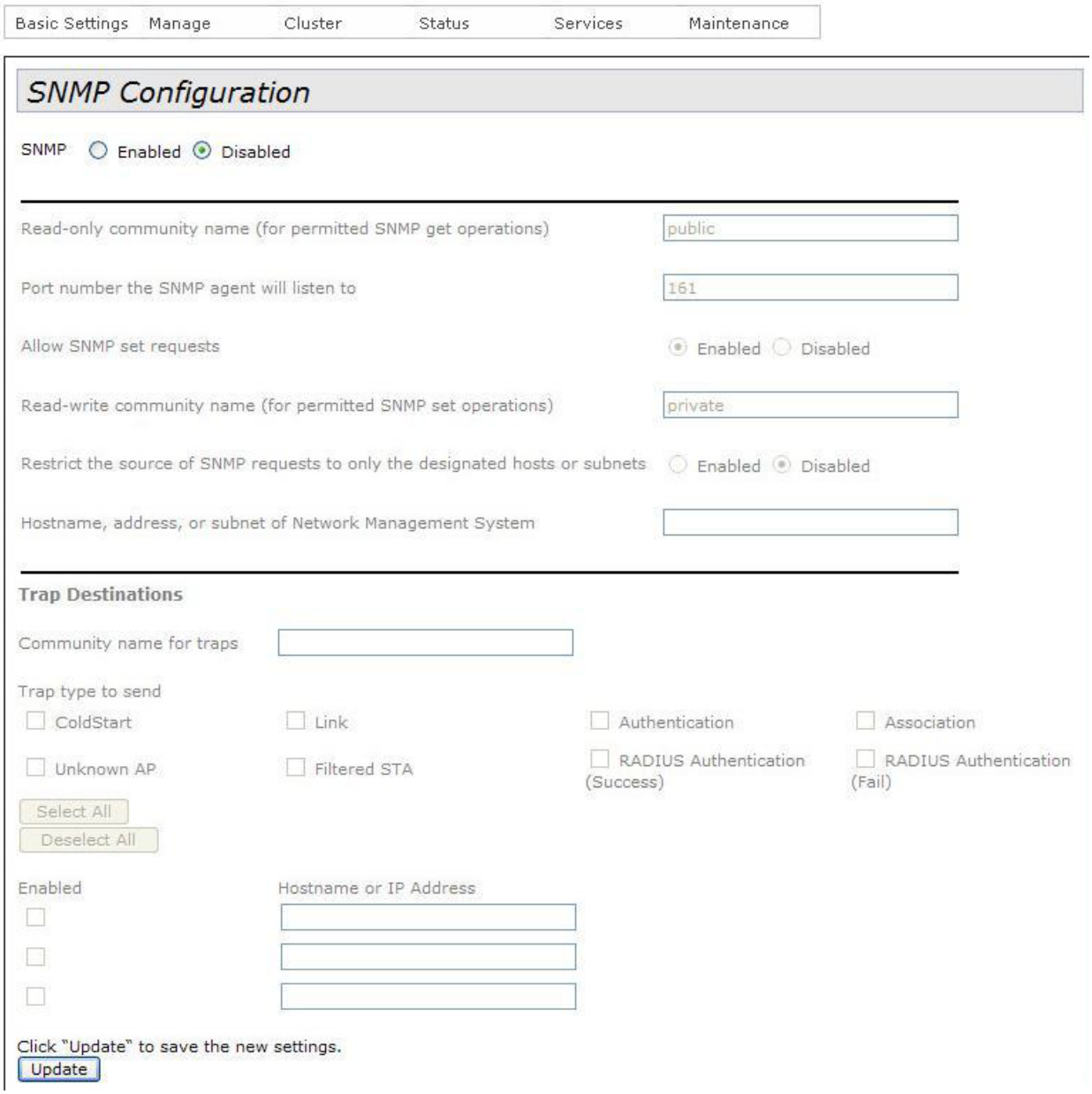


Figure 26. SNMP Configuration Window

Table 18. SNMP Configuration

Field	Description
SNMP Enabled/Disabled	Use this option to activate or deactivate SNMP on the access point. The options are explained here: Enabled: Check this option to activate SNMP and allow managers to use it to view and configure the parameter settings on the access point. When you click the option, the options in the window are activated. Disabled: Check this option to disable SNMP to prevent managers from using it to view and configure the parameter settings on the access point. When you click the option, the options in the window are deactivated and cannot be configured. This is the default setting.
Read-only community name	Use this parameter to specify the read-only community string on the access point. This community string may only be used to view the MIB settings of the device. Here are the guidelines to creating the community string: The community string may be from 1 to 256 characters. The community string may contain both letters and numbers, The community string may not contain any spaces. The community string is case sensitive. You may specify only one read-only community string. You may not leave the field empty. The default read-only community string is “public”.

Table 18. SNMP Configuration (Continued)

Field	Description
Port number the SNMP agent will listen to	Use this parameter to specify the port number for SNMP. The range is 1 to 65535. The default is 161.
Allow SNMP set requests	Use this parameter to either permit or deny managers to use the read-write community string to change the parameter settings of the access point. The choices are described here: Enabled; Check this option to permit managers to use the read-write community string to change the parameter settings of the access point. Disabled: Check this option to prevent managers from using the read-write community string to change the parameter settings. If you click this option, the read-write community string acts as a read-only community string, giving you two read-only strings on the access point.
Read-write community name (for permitted SNMP set operations)	Use this parameter to specify the read-write community string. Here are the guidelines: Managers can use this community string to both view and change the parameter settings on the access point, unless the previous option “Allow SNMP set requests” is disabled. The community string can be from 1 to 256 characters. You may specify only one read-write community string. The community string can contain both letters and numbers, The community string cannot contain spaces.

Table 18. SNMP Configuration (Continued)

Field	Description
Read-write community name (for permitted SNMP set operations) (continued)	The community string is case sensitive. You may not leave the field empty. The default community string is “private.”
Restrict the source of SNMP requests to only the designated hosts or subnets	Use this option to increase the security of the access point by restricting the use of SNMP management to specific subnets or individual workstations. The options are described here: Enabled: Check this option if you want to restrict the use of SNMP on the access point to only those management stations specified in the next field in the window. Restricting SNMP applies to both read-only and read-write community strings. Disabled: Check this option to disable this feature and permit any workstation to manage the unit with SNMP. This is the default setting.
Hostname, address, or subnet of Network Management System	Use this field to specify the management workstations that are allowed to use SNMP to manage the device. This field only applies if you selected the Enabled option in the previous field. You may specify the management workstation by hostname, IP address, or subnet address: Here are the guidelines: You may specify only one value in the field. You may specify an authorized SNMP workstation by its DNS hostname (e.g. smith.abc.com). You may specify an authorized SNMP workstation by its IP address (e.g. 149.23.45.102.)

Table 18. SNMP Configuration (Continued)

Field	Description
Hostname, address, or subnet of Network Management System (continued)	You may specify a subnet to allow all management workstations in the subnet to use SNMP to access the device. The subnet is specified in this format: address/mask You may specify the actual mask or the mask length. Here is an example of a subnet specified by the actual mask: 149.24.42.0/255.255.255.0 Here is the same subnet, specified by mask length: 149.24.42.0/24
Community name for traps	Use this field to specify the community name the access point should use to transmit traps.
Trap type to send	Use these options to specify which traps the access point should transmit. The options are described here: Coldstart: This trap is sent when the SNMP agent is started. Link: This trap is sent when a radio is enabled or disabled. Authentication: This trap is sent when an SNMP authentication fails. Association: This trap is sent when wireless clients connect to or disconnect from the access point. Unknown AP: This trap is sent when the access point detects a rogue access point.

Table 18. SNMP Configuration (Continued)

Field	Description
Trap type to send (continued)	- Filtered STA: This trap is sent when the access point blocks an unauthorized wireless client from accessing the network because the client is not authorized by the MAC address filter. - RADIUS Authentication (Success): This trap is sent when a wireless client successfully logs on the network using RADIUS. - RADIUS Authentication (Fail): This trap is sent when a wireless client fails to log on successfully using RADIUS.
Hostname or IP address	Specify the SNMP trap receivers to receive traps from the access point. Here are the guidelines: You may specify up to three trap receivers. You may specify only one trap receiver per field. You have to click the Enabled dialog box before you can enter or modify a trap receiver. You may specify a trap receiver by its IP address or DNS hostname. You may not specify an IP address range.

Enabling or Disabling the LEDs

You can turn off the LEDs on the front panel of the access point when you are not using them 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 **Services** -> **LED**.

   The unit displays the “Control LEDs” window. Refer to Figure 27.

Figure 27. Control LEDs Window

2. Click the **On** or **Off** selections to turn the LEDs on or off.
3. Click the **Update** button to activate and save your changes on the access point.

Configuring the HTTP Server

The following procedures explain how to enable or disable the HTTP server. You can use the server to manage the access point with your web browser on your workstation. The HTTP server is a non-secure management method. The packets exchanged between your web browser and the access point are sent in clear text, leaving them vulnerable to snooping. For secure remote management, use HTTPS instead, as explained in “Configuring the HTTPS Server” on page 110.

The default setting for the HTTP server is enabled.

Enabling the HTTP Server

To activate the HTTP server, perform the following procedure:

1. Select **Services** -> **HTTP/HTTPS**.

   The access point displays the “Configure Web Server Settings” window. Refer to Figure 28.

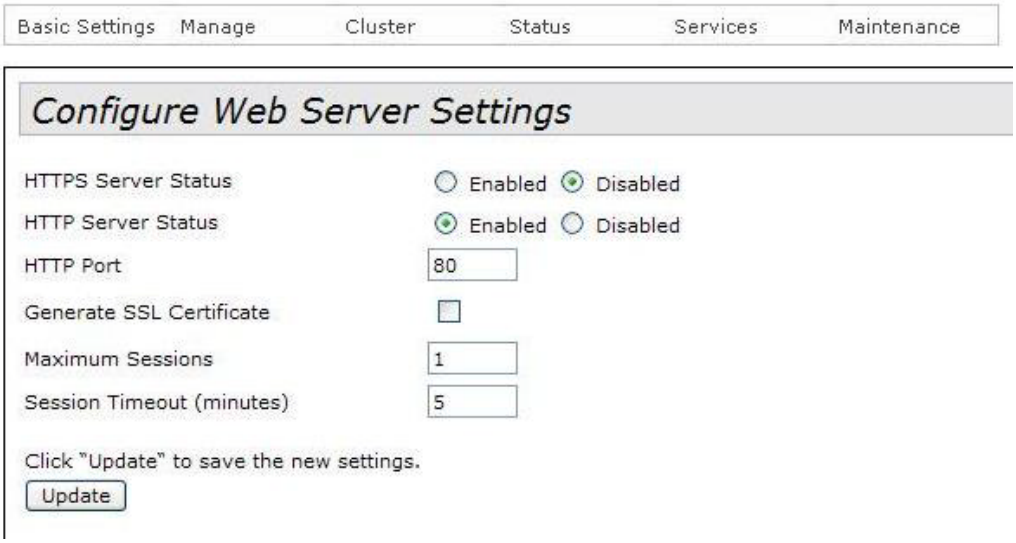


Figure 28. Configure Web Server Settings Window

2. Click the **Enabled** dialog circle for the HTTP Server Status field.
3. To change the HTTP port number, select the HTTP Port field and enter the new value. The default is port 80.
4. Click the **Update** button to activate and save your changes on the access point.

   The HTTP server is now active on the access point. You can now manage the access point with your web browser and HTTP.

Disabling the HTTP Server

The following procedure explains how to disable the HTTP server on the access point. Please review the following guidelines before performing the procedure:

- If you disable the HTTP server while managing the access point with HTTP, your management session is interrupted. To continue managing the unit, you can use either HTTPS or SNMP.
- If the maximum number of active sessions is set to 1, the default value. you might have to wait until the inactive session timer times out before starting an HTTPS session. The default is five minutes. The maximum number of active sessions does not apply to SNMP.
- If you disable HTTP without configuring HTTPS or SNMP, you will not be able to manage the access point. Your only alternative is to return the device to its default settings with the Reset button on the back panel. For instructions, refer to “Restoring the Default Settings to the Access Point” on page 120.

To disable the HTTP server, perform the following procedure:

1. Select **Services** -> **HTTP/HTTPS**.

   The access point displays the “Configure Web Server Settings” window. Refer to Figure 28 on page 108.

2. Click the **Disabled** dialog circle for the HTTP Server Status field.

   The following prompt is displayed.

Figure 29. Disable HTTP Server Prompt

3. Click **OK**.
4. Click the **Update** button to activate and save your changes on the access point.

   The HTTP server is now disabled.

Configuring the HTTPS Server

The following procedures explain how to enable and disable the HTTPS server. You may use the server to manage the access point with your web browser on your computer. Managing the device with HTTPS is more secure that HTTP because your web browser and the access point use encryption to protect the management packets.

The default setting for the server is disabled. The server uses port 443. You may not change that value.

Enabling the HTTPS Server

To activate the HTTPS server, perform the following procedure:

1. Select **Services** -> **HTTP/HTTPS**.

   The access point displays the “Configure Web Server Settings” window. Refer to Figure 28 on page 108.

2. Click the dialog box for the Generate SSL Certificate field.

   The prompt in Figure 30 on page 110 is displayed.

Figure 30. Generate SSL Certificate Prompt

3. Click the **OK** button.
4. Click the **Update** button.
5. Click the **Enabled** circle for the HTTPS Server Status field.
6. Click the **Update** button again.

   You can now manage the access point using HTTPS and encryption from the web browser on your workstation.

   To test the HTTPS server, continue with these steps.

7. Click the **Log Out** button to end your HTTP management session.
8. In the URL field of your web browser, enter the prefix “HTTPS//:” followed by the IP address of the access point. (You must always include the prefix HTTPS://” in the URL field to start secure web browser management sessions on the access point.)

At this point, your web browser might display a security warning message to indicate that it does not consider the access point, which created its own HTTPS certificate, as a trusted certificate authority. If you see a warning message, you should be able to close it and manage the device. To eliminate the message, add the access point as a trusted certificate authority to the web browser. Refer to the web browser documentation for instructions.

9. You should now be able to log on to the access point.

Disabling the HTTPS Server

The following procedure explains how to disable the HTTPS server. Please review the following guidelines before performing the procedure:

- Disabling the HTTPS server while managing the access point with HTTPS interrupts your management session. You can use HTTP or SNMP to continue managing the device.
- If the maximum number of active sessions is set to 1, the default value, you might have to wait until the inactive session timer times out before starting a new session. The default is five minutes. The maximum number of active sessions does not apply to SNMP.
- Do not disable HTTPS without first configuring HTTP or SNMP. Otherwise, you will not be able to manage the device and will have to activate the default settings with the Reset button. For instructions, refer to “Restoring the Default Settings to the Access Point” on page 120.

To disable the HTTPS server, perform th following procedure:

1. Select **Services** -> **HTTP/HTTPS**.

   The access point displays the “Configure Web Server Settings” window. Refer to Figure 28 on page 108.

2. Click the **Disabled** selection for the HTTPS Server Status field.

   The following prompt is displayed.

Figure 31. Disable HTTPS Server Prompt

3. Click **OK**.

4. Click the **Update** button.

   The HTTPS server is now disabled on the access point.

Configuring the Maximum Number of Active Management Sessions

This procedure explains how to configure the maximum number of active management sessions the access point supports at one time. The range is one to ten sessions. The default is one session. You might want to consider increasing the parameter if the access point will be managed by more than one person.

The maximum number of active management sessions applies to HTTP and HTTPS sessions. It does not apply to SNMP.

To configure the maximum number of active management sessions, perform the following procedure:

1. Select **Services** -> **HTTP/HTTPS**.

   The access point displays the “Configure Web Server Settings” window. Refer to Figure 28 on page 108.

2. Select the dialog box for Maximum sessions and enter the new value. The range is 1 to 10 management sessions.

3. Click the **Update** button to activate and save your change on the access point.

Configuring the Management Session Timer

You should always conclude your management sessions of the access point by logging off so that if you leave your computer unattended, someone cannot use it to make unauthorized changes to the parameter settings of the device.

If you forget to log off, the access point has a timer to detect and log off inactive management sessions for you, automatically. A session is considered inactive if there is no management activity for the duration of the timer.

The default setting for the timer is five minutes.

To configure the management session timer, perform the following procedure:

1. Select **Services** -> **HTTP/HTTPS**.

   The access point displays the “Configure Web Server Settings” window. Refer to Figure 28 on page 108.

2. Select the Session Timeout (minutes) field and enter a new value. The range is 1 to 1440 minutes. (1440 minutes is one day.) The default is 5 minutes.

3. Click the **Update** button to activate and save your change.

Manually Setting the Date and Time

If the access point does not have access to an SNTP server, you can set the date and time manually. The unit adds the date and time to log messages and SNMP traps.

Note
If you configure the date and time manually, you have to reconfigure them whenever the access point is reset or powered off.

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

1. Select **Services** -> **NTP**.

   The access point displays the “Modify How the Access Point Discovers the Time” window.

2. Click the **Manually** circle for the Set System Time parameter. Refer to Figure 32. This is the default setting.

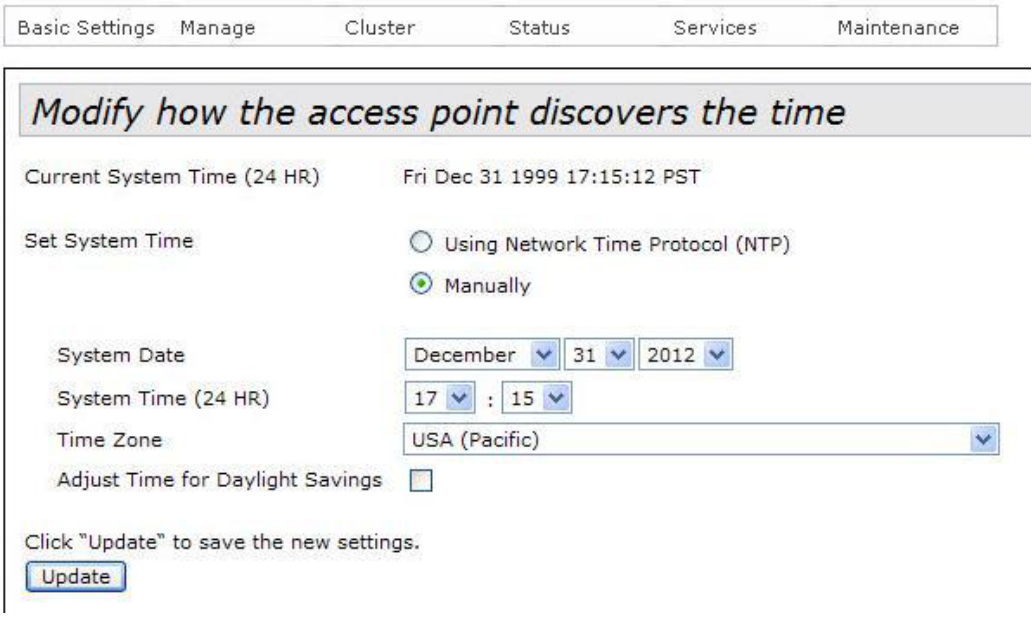


Figure 32. Modify How the Access Point Discovers the Time Window - Manually Setting the Date and Time

3. Use the **System Date** pull-down menus to set the current month, day, and year.

4. Use the **System Time** pull-down menus to set the current hours and minutes. The hours are in 24 hours. For example, 14 represent 2:00 p.m.

5. Use the pull-down menu in Time Zone to set the time zone of the location of the access point.

6. If the location of the access point observes daylight savings time, click the check box for the Adjust Time for Daylight Savings parameter. The window displays the fields in Figure 33.

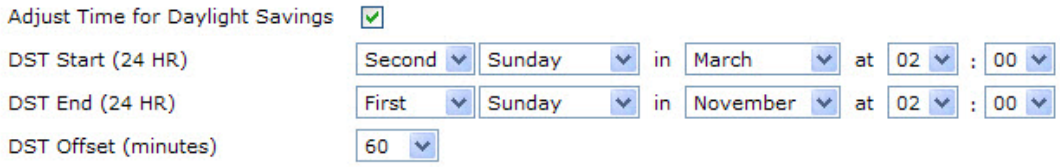


Figure 33. Daylight Savings Time Fields

If the area does not observe Daylight Savings time, leave the check box empty and go to step 10.

7. Use the **DST Start** pull down menus to set the date and time for the start of Daylight Savings time.

8. Use the **DST End** pull down menus to set the date and time for the end of Daylight Savings time.

9. Select the **DST Offset** field and enter the number of minutes to adjust the time at the start and end of Daylight Savings time. The default is 60 minutes.

10. Click the **Update** button to activate and save your changes.

Setting the Date and Time with the Network Time Protocol Client

The access point has a Network Time Protocol (NTP) client. The unit uses the client to obtain the date and time from an SNTP server on your network or the Internet. The access point adds the date and time to log messages and SNMP traps. Here are the guidelines to using the client:

- You need to know the hostname or IP address of an SNTP server on your network or the Internet. You may specify only one server.
- The access point must have an IP address.
- The access point must also have a default gateway address if the SNTP 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 **Services** -> **NTP Settings**.

   The access point displays the “Modify how the access point discovers the time” window, shown in Figure 32 on page 114.

2. Click the **Using Network Time Protocol** circle for the Set System Time parameter. Refer to Figure 34.

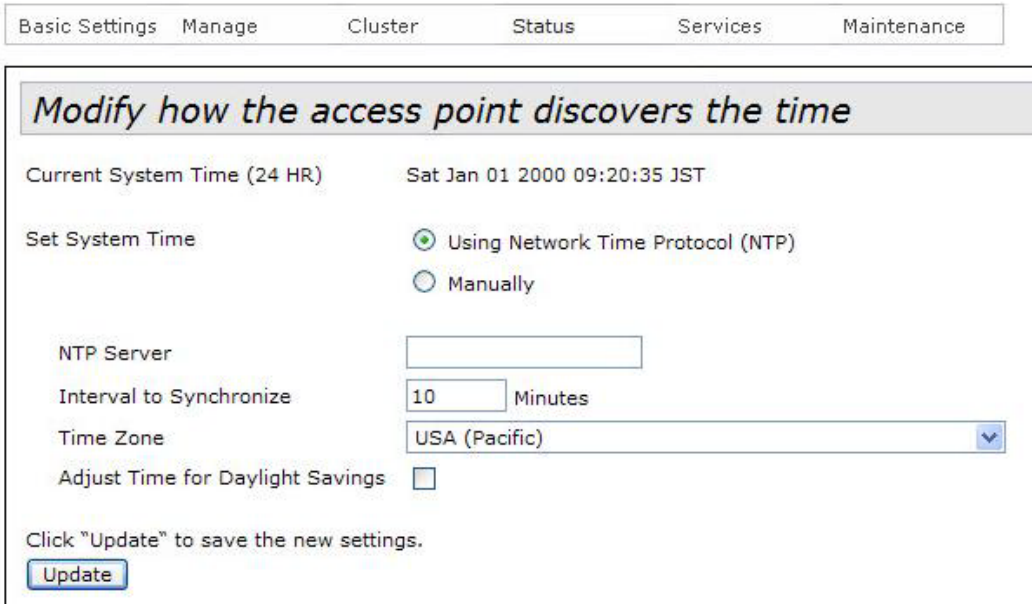


Figure 34. Modify How the Access Point Discovers the Time Window - Configuring the NTP Client

3. Select the **NTP Server** field and enter the IP address or hostname of the SNTP server. You may specify only one server. If you are specifying the server by its hostname, please observe these guidelines:

   - ❒ The first character must be a letter or number. It cannot be a special character.
   - ❒ The last character cannot be a hyphen or period.

4. Select the **Interval to Synchronize** field and specify in minutes how frequently the access point is to synchronize its time with the SNTP server. The range is 1 to 9999 minutes. The default is 10 minutes.

5. Use the **Time Zone** 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.

6. If the location of the access point observes daylight savings time, click the **Adjust Time for Daylight Savings** field. The window displays the fields in Figure 33 on page 115.

   If the area does not observe Daylight Savings time, leave the dialog box empty and go to step 10.

7. Use the **DST Start** pull down menus to set the date and time for the start of Daylight Savings time.

8. Use the **DST End** pull down menus to set the date and time for the end of Daylight Savings time.

9. Select the **DST Offset** field and enter the number of minutes to adjust the time at the start and end of Daylight Savings time. The default is 60 minutes.

10. Click the **Update** button to activate and save your changes.

Chapter 6

Maintenance Menu

This chapter describes the management functions of the menu selections in the Maintenance menu. The chapter contains the following sections:

Restoring the Default Settings to the Access Point

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

- The manager name and password are reset to “manager” and “friend”, respectively.
- If the access point 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.
- Restoring the wireless access point to its default settings does not affect the network, location, or schedule policies on the SES controller.

Note
The access point stops forwarding network traffic from wireless hosts after it is returned to its default settings because the default setting for the radios is off.

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

1. Select **Maintenance** -> **Configuration**.

   The access point displays the “Manage this Access Point’s Configuration” window. Refer to Figure 35 on page 121.

2. Click the **Reset** button in the To Restore the Factory Default Configuration section of the window.

   The device displays a confirmation prompt.

3. Click **OK** to restore the default settings.

4. Wait one minute for the device to reset and then establish a new management session. For instructions, refer to “Starting the Initial Management Session on the Access Point” on page 26.

5. To activate the radios, refer to “Configuring the Radio Settings” on page 52.

6. To restore communications between the wireless access point and SES controller, perform “Configuring the OpenFlow Protocol” on page 75.

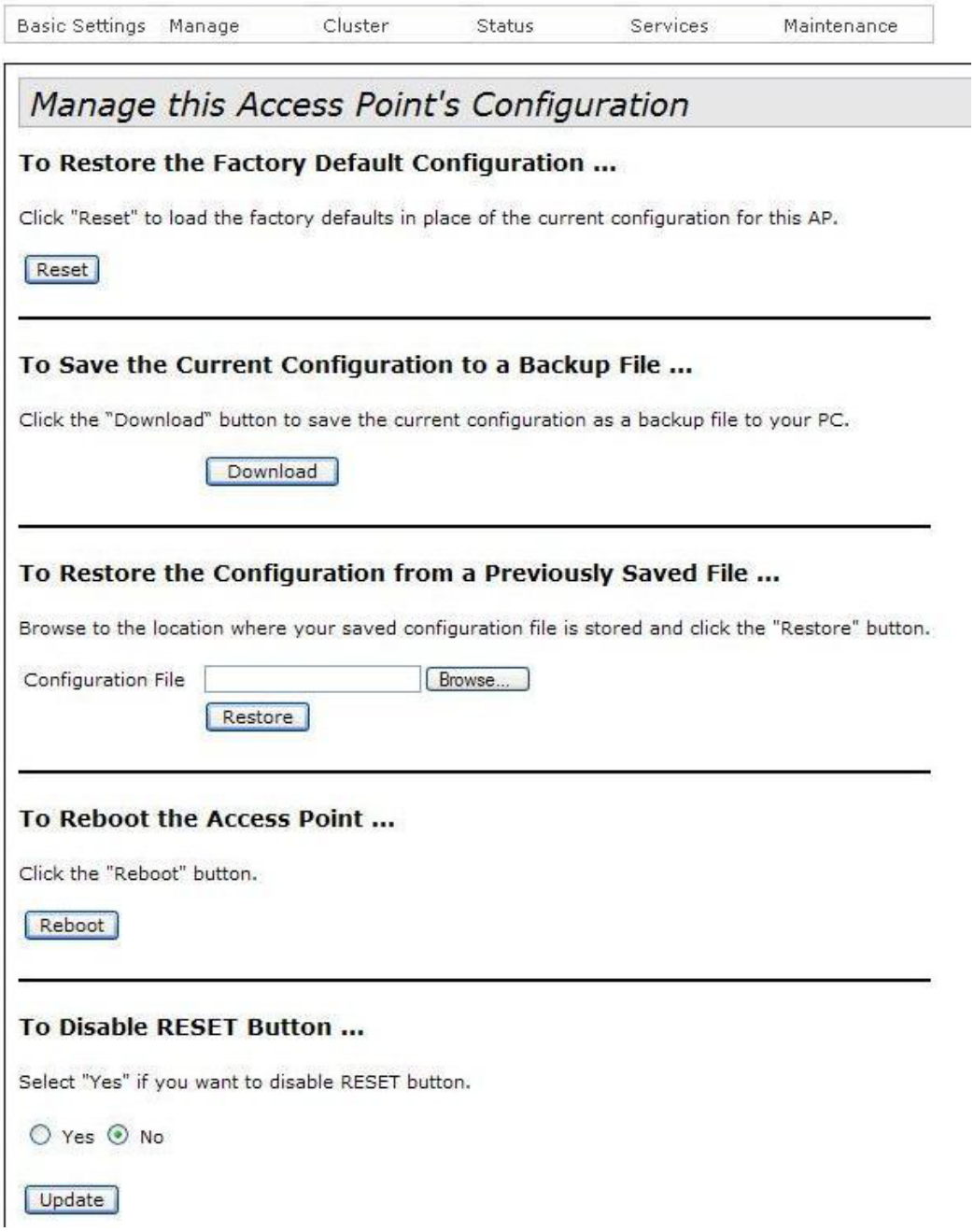


Figure 35. Manage this Access Point's Configuration Window

Downloading the Configuration from the Access Point to Your Computer

This procedure explains how to download the configuration of the access point as a file to your computer or a network server. You might perform this procedure to maintain a history of the configurations of the unit so that you can easily return it to an earlier 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:

- Do not 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 management workstation or network server, perform the following procedure:

1. From the **Maintenance** -> **Configuration**.

   The access point displays the “Manage this Access Point’s Configuration” window. Refer to Figure 35 on page 121.

2. Click the **Download** button in the To Save the Current Configuration to a Backup File section of the window.

3. 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 for the configuration file. The filename suffix must be XML.

5. Click **Save**.

   The access point downloads its configuration to your management workstation and 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 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 from the Access Point to Your Computer” on page 122.
- A configuration file must have the XML 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.
- Do not 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**.

   The access point displays the “Manage this Access Point’s Configuration” window in Figure 35 on page 121.

2. Click the **Browse** button in the To Restore the Configuration from a Previously Saved File section, and select the configuration file to restore to the access point from your management workstation or network server. You can restore only one configuration file.

3. Click the **Open** button.

4. Click the **Restore** button.

5. Wait one minute for the access point to complete initializing its management software.

6. To resume managing the unit, establish a new management session.

Rebooting the Access Point

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

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

Note
Rebooting the access point deletes the flow rules that it learned from the SES controller for the wireless hosts. After rebooting, it immediately begins to relearn the rules as wireless hosts start forwarding traffic.

To reboot the access point, perform the following procedure:

1. Select **Maintenance** -> **Configuration**.

   The access point displays the “Manage this Access Point’s Configuration” window in Figure 35 on page 121.

2. Click the **Reboot** button in the To Reboot the Access Point section of the window.

   The access point displays a confirmation prompt.

3. Click **OK**.

   Your current management session is interrupted.

   The access point deletes the flow rules for the wireless hosts

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

   The access point begins to relearn the flow rules from the SES controller for the wireless hosts as they begin transmitting traffic.

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. The Reset button is used to restore the default settings to the device. The default setting for the button is enabled.

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 and forget the manager account password, 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 **Maintenance** -> **Configuration**.

   The access point displays the “Manage this Access Point’s Configuration” window in Figure 35 on page 121.

2. In the To Disable RESET Button section of the window, click the **Yes** dialog circle to disable the button or the **No** dialog circle to enable it.

3. Click the **Update** button to activate and save your changes on the access point.

Uploading New Versions of the Management Software to the Access Point

Allied Telesis may 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 that 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

The access point does not forward network traffic while it uploads the management software from your computer and writes the file to flash memory. Performing the procedure during periods of low traffic activity, such as during non-business hours, can minimize the disruption to network operations.

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

1. Select **Maintenance** -> **Upgrade**.

   The access point displays the "Manage Firmware" window. Refer to Figure 36 on page 127.

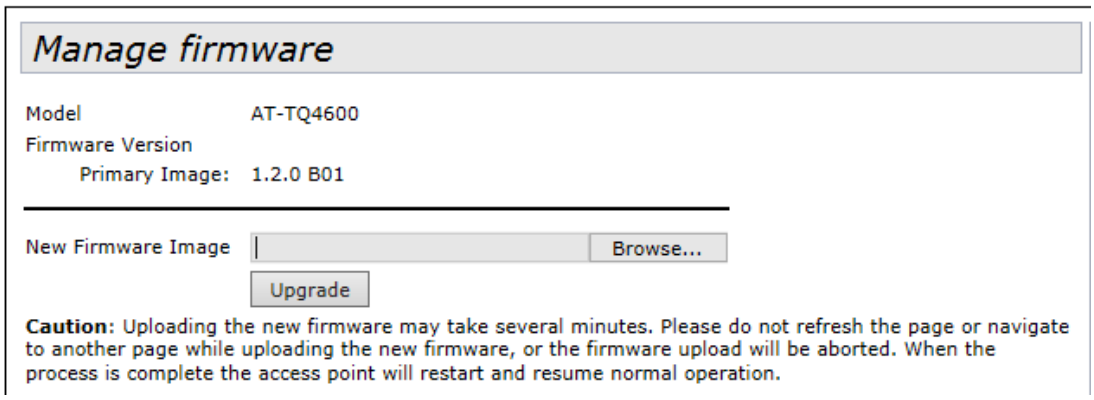


Figure 36. Manage Firmware Window

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

3. Click the **Upgrade** button.

   The access point displays a confirmation prompt.

4. Click the **OK** button to upload the new firmware to the access point or **Cancel** to cancel the procedure.

   The access point performs the following tasks during the upgrade procedure:

   - Uploads the new image to the access point from your workstation or network.
   - Copies the file to flash memory.
   - Resets to initialize the new firmware.

   Note
   The entire process can take up to 10 minutes. Do not close the web browser window or change to a different window until the entire process is finished. Interrupting the transfer may corrupt the file on the access point.

5. To resume managing the unit, start a new management session.